Quick Quiz March 16, 2023

Test ID: 244106237

Question #1 of 50

Question ID: 1371383

You are the administrator of the Nutex Corporation. You manage a blob that must remain in your Azure storage tier for at least 30 days. Currently the same blob is configured to remain in an Azure storage tier for at least 180 days. You want to modify the existing blob.

Which action must you perform?

A) Upload same blob data to storage account

B) **Use blob-level tiering to change to cool tier**

C) Change the tier of the blob with a snapshot

D) Rehydrate the existing blob

Explanation

You should rehydrate the existing blob. You have to first change tier of the blob to hot or cool to read data in archive storage, a process known as rehydration. This process can take up to 15 hours to complete. In this scenario, the blob will remain in archive storage. The archive tier keeps data in the tier for at least 180 days.

You should not use blob-level tiering to change to cool tier. You can use a single operation called Set Blob Tier to change the tier of your data at the object level. You do not have to move data between accounts; instead you can change the access tier of a blob among the hot, cool, or archive tiers as usage patterns change. Tier changes happen immediately. The only exception is when a blob is “rehydrating” from an archive. This process is quite lengthy and can take up to 15 hours. To change to cool tier is not correct here because you want that the blob remains in your Azure storage tier for at least 30 days.

You should not upload same blob data to the storage account because you want to modify the existing blob. If you were to upload the blob data again, it would become a new blob and not the existing blob. In another situation, this solution would save time because the blob rehydration may need up to 15 hours to complete. However, in this scenario, you must use the existing blob.

Azure does not allow you to change the tier of the blob with a snapshot.

Objective:
Implement and manage storage

Sub-Objective:
Configure Azure files and Azure Blob Storage

References:

Microsoft Azure > Storage > Blobs > Azure Blob Storage: hot, cool, and archive storage tiers

---

Question #2 of 50

Question ID: 1480159

The Nutex Corporation has a virtual network named VNET1. A network security group named NutexNSG allows connections from VNET1 to the following virtual machines:

Name	Description	Operating System
NutexVM1	File Server	Windows Server 2022
NutexVM2	File Server	Windows Server 2019
NutexVM3	File Server	Red Hat Enterprise Linux

NutexVM2 and NutexVM3 are configured with Azure Disk encryption.

Azure Backup is used to back up all virtual machines.

Occasionally, users need to recover one or two files from the file servers.

On which of the virtual machines can you perform a file-level restore?

A) NutexVM1

B) **NutexVM3**

C) NutexVM2

Explanation

In this scenario, you can only perform a file-level restore on NutexVM1. You cannot perform a file-level restore on encrypted VMs. Azure Disk encryption can be applied to Windows and Linux virtual machines. It uses BitLocker to encrypt the data disks and the OS disk of the virtual machines. The keys and secrets for disk encryption are integrated with Azure Key Vault.

To restore files from NutexVM2 and NutexVM3, you would have to restore the entire disk.

Objective:
Monitor and maintain Azure resources

Sub-Objective:
Implement backup and recovery

References:

.

Microsoft Docs > Azure > Backup > Support matrix for Azure VM backup

Microsoft Docs > Azure > Virtual Machines > Windows > Azure Disk Encryption for Windows VMs

Microsoft Docs > Azure > Virtual Machines > Linux > Azure Disk Encryption for Linux VMs

---

Question #3 of 50

Question ID: 1477159

You have one virtual machines running Windows Server 2016 that is in availability zone 1. You have another virtual machines running Windows Server 2016 that is in availability zone 2. These virtual machines need to be configured with load balanced connections from the Internet.

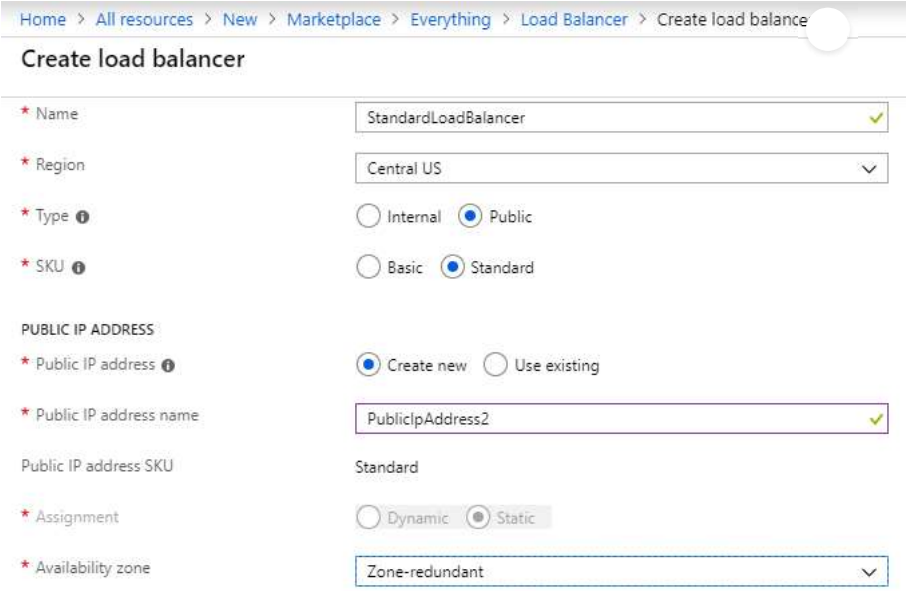
How should you configure the load balancer in the Azure portal?

A) Set the Availability zone to **1**
B) **Set the Availability zone to 1 and 2**
C) Set the Availability zone to **2**
D) Set the SKU to **Standard**
E) Set the Type to **Public**
F) Set the SKU to **Basic**
G) Set the Type to **Internal**
H) **Use a public IP address**
I) Set the Availability zone to **Zone-redundant**

Explanation

You should configure the load balancer as follows:

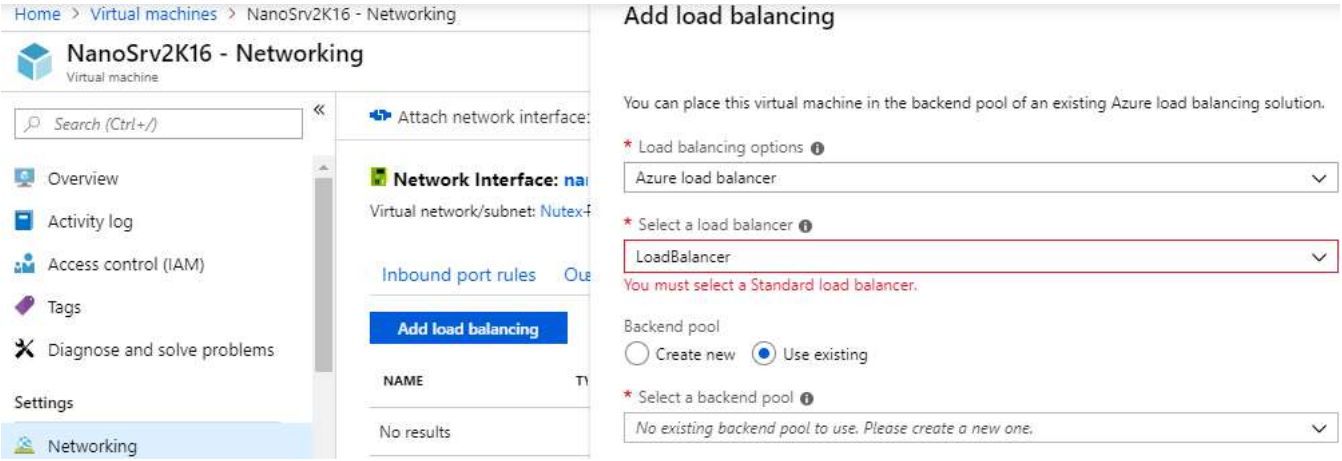
- Set the SKU to **Standard**
- Set the Type to **Public**
- Use a public IP address
- Set the Availability zone to **Zone-redundant**



The Type should be set to **Public** instead of **Internal**. Because the virtual machines need to be configured with load-balanced connections from the Internet, the load balancer will be a public load balancer and will require a public IP address. You can create a new public IP address, or use an existing public IP address.

The Availability zone should be set to **Zone-redundant**. Zone-redundant means all zones, and this configuration can direct traffic across zones as needed (cross-zone load-balancing). You cannot set the Availability zone to both 1 and 2. You can only set the Availability zone to a single zone or Zone-redundant.

The SKU should be set to **Standard** instead of **Basic** because this load balancer will be configured for virtual machines. A virtual machine configuration is not supported with Basic. A Basic load balancer exists within an availability set. A Standard load balancer works the scope of a virtual network. The Standard SKU supports the Availability zone status of **Zone-redundant**.



Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Create and configure VMs

References:

Microsoft Azure > Networking > Standard Load Balancer and Availability Zones

Microsoft Azure > Networking > Load Balancer > Quickstart: Create a Load Balancer to load balance VMs using the Azure portal

Microsoft Azure > Networking > Load Balancer > What is Azure Load Balancer?

Question #4 of 50

Question ID: 1480102

Verigon is a manufacturing company that creates premium golf balls. Verigon works with partner organizations to bring products to market under different names.

Verigon products are manufactured using blueprint files authored and maintained by the company.

Currently, Verigon uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers
- DNS Servers
- Application servers

Your network contains an Active Directory forest named **verigon.com**. All servers and client computers are joined to Active Directory.

You have a public-facing application named **GolfBallApp1**. **GolfBallApp1** is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier contains several virtual machines. Users access the web front end by using HTTPS only.

Production costs have skyrocketed in the past two years. All infrastructure spending must be properly budgeted.

A Recovery Services vault exists for the purpose of testing backups. The Recovery Services vault contains backups of two virtual machines that are file servers for the Marketing department.

Planned Changes

Verigon plans to implement the following changes to the infrastructure:

The Finance department has hired auditors to determine the storage bandwidth consumed so they can budget that amount for future quarters.

The company applications store data, but this data is not easily reconstructed if data loss occurs. The datacenter must be protected from a natural disaster, such as fire or flood. Redundancy must exist. Replicas must not be lost and must be recoverable. A storage account must be configured that replicates synchronously.

The Art department will be consolidated and will now be part of the Marketing department.

The Art department must retrieve files from Marketing that are prototypes. The Art department will build the designs according to specifications from Marketing.

Technical Requirements

Verigon must meet the following technical requirements:

- Move some of the tiers of **GolfBallApp1** to Azure.
- Move all the virtual machines for **GolfBallApp1** to Azure.
- Minimize the number of open ports between the **GolfBallApp1** tiers.
- Ensure that all the virtual machines for **GolfBallApp1** are protected by backups.
- Move the largest product blueprint files to Azure Blob storage.
- Copy the largest product blueprint files to Azure over the Internet to partners.
- Ensure that outdated blueprint files are stored in the archive storage tier.
- Minimize administrative effort whenever possible.

The auditors must upload and download auditing data from Azure blob storage, which is owned by the Finance department.

The Marketing department wants to delete the existing Recovery Services vault. A new Recovery Services vault will be created to keep the backups of both the Marketing department and the Art department.

User Requirements

Verigon identifies the following requirements for users:

- Require users to verify their identity with a mobile phone when they join devices to Azure Active Directory (Azure AD).
- Ensure that only users who have Windows 10 devices that are updated with latest security fixes and are part of a group named **GolfBallManufacturers** can join devices to Azure AD.
- Designate a new user named Jeff1 as the service administrator of the Azure subscription.
- Ensure that a new user named GolfBallUser9 can create network security groups for the Azure subscription.
- Ensure that a user named Wendy from the Art department can map a drive to the Azure file share to retrieve the designs from the Marketing department.

You are designing the infrastructure for the Nutex Corporation's Azure cloud. You create an Azure Storage account named NutexStorage1.

You configure the following lifecycle management rule.

```
{
  "rules": [
    {
      "enabled": true,
```

```
      "name": "sample-rule",
      "type": "Lifecycle",
      "definition": {
        "actions": {
          "version": {
            "delete": {
              "daysAfterCreationGreaterThan": 90
            }
          },
          "baseBlob": {
            "tierToCool": {
              "daysAfterModificationGreaterThan": 5
            },
            "tierToArchive": {
              "daysAfterModificationGreaterThan": 10
            },
            "delete": {
              "daysAfterModificationGreaterThan": 2555
            }
          }
        },
        "filters": {
          "blobTypes": [
            "blockBlob"
          ],
          "prefixMatch": [
            "nutex-container/blob1"
          ]
        }
      }
    }
  ]
}
```

The rule filters the account to run the actions on objects that exist inside `nutex-container` and start with `blob1`. NutexStorage1 uses the Hot access tier.

On March 5, you create a file named TaxReports in `nutex-container`.

On March 17, you rehydrate TaxReports and move the file to the Hot access tier. Several people with read-only access view the file.

When will TaxReports be moved to archive storage?

A) March 22 to March 27

B) March 18 to March 21

C) **March 28 to June 15**

D) Before March 18

Explanation

The file will be moved before March 18. In this scenario, the lifecycle management rule sets limits on when the file is modified, not when it is accessed.

The lifecycle management rule performs the following:

- Tier blob to cool tier 5 days after last modification
- Tier blob to archive tier 10 days after last modification
- Delete blob 2,555 days (seven years) after last modification
- Delete previous versions 90 days after creation

The file's last modification date/time does not change if a blob is moved from one access tier to another. In this scenario, you manually rehydrate an archived blob that contains a file to the Hot tier. Since the file was accessed and not modified, it is moved back to the archive tier by the lifecycle management engine. The file was last modified on March 5. The lifecycle management rule moves it to the archive tier 10 days after modification. Since 10 days have passed, the lifecycle management rule would move it back within 24 hours or before March 18.

```
"tierToArchive": {
   "daysAfterModificationGreaterThan": 10
},
```

If you want to prevent the blob that contains the file from being archived within 24 hours, you should disable the rule. You could also modify the file, which gives you another 10 days before it is moved to the archive tier.

Objective:
Implement and manage storage

Sub-Objective:
Configure Azure files and Azure Blob Storage

References:

Microsoft Docs > Azure > Storage > Blobs > Optimize costs by automatically managing the data lifecycle

---

Question #5 of 50

Question ID: 1285354

You are the administrator of Nutex and are responsible for the website **www.nutex.com**. The website is hosted on Azure in free mode. You have decided to globally scale your website. Your solution must meet the following requirements:

- Up to ten multiple running copies of your website can be automatically generated if needed.
- Azure will automatically handle the load balancing configuration to distribute requests across all instances.
- Costs must be limited.

Which configuration change should you perform?

A) Scale up the instance size to Medium

B) **Switch the mode to basic mode**

C) Switch the mode to premium mode

D) Scale up the instance size to Large

E) Switch the mode to standard mode

F) Scale out to ten instances

Explanation

You would switch the website to standard mode (formerly referred to as reserved mode). Standard mode provides the ability to scale out to up to ten instances and the web site will be load balanced automatically.

With basic mode, you can only scale out to three instances. You have to change to reserved mode first, then you can scale out to up to 10 instances.

You would not switch the website to premium mode. Premium will meet the requirements of having up to 10 instances because premium mode will support 50 instances, but it will not meet the requirement of limiting costs. Premium mode is more expensive than standard mode.

You cannot scale out to ten instances directly from your existing service plan. First you have to switch to standard mode, which will allow you to scale out to ten instances. Then you can use full memory resources available based on the scale up options that you choose.

You should not scale up your instance size to Large or Medium to create up to ten instances. Scaling out creates instances, while scaling up increases CPU size, expands disk and memory allocations, and adds extra features.

Objective:
Configure and manage virtual networking

Sub-Objective:
Configure load balancing

References:

Microsoft Azure > App Service > Azure App Service plan overview

Microsoft Azure > Blog > Scaling Up and Scaling Out in Windows Azure Web Sites

Microsoft Azure > Products > App Service pricing

Microsoft Azure > Video: How Azure Web Sites Scale

Question #6 of 50

Question ID: 1477158

You must configure the Nutex Sales application Azure VM resources for high availability. You decide to implement availability sets to ensure unexpected downtime and planned outages have less of an effect on the availability of your Sales application. There are three load balanced VMs running the Web tier of your application, and two clustered Windows Servers with SQL Server supporting the Data tier.

How should you configure the availability sets to ensure continual service of the Sales application? (Choose all that apply. Each answer is part of the solution.)

A) **Availability Set 1 should contain all of the Web servers**

B) Each VM should be in its own availability set

C) **Availability Set 2 should contain both of the database servers**

D) Availability Set 2 should contain a Web server and a database server

E) Availability Set 3 should contain a Web server

F) Availability Set 1 should contain a Web server and a database server

Explanation

You should configure two availability sets. Availability Set 1 should contain all of the Web servers, and Availability Set 2 should contain both of the database servers. By combining all of the web servers in a single availability set, such as Availability Set 1, you are configuring Azure to provide redundancy. When two or more VMs are in an availability set, at least one VM will be available during planned or unplanned maintenance and will meet the 99.95%Azure SLA.

The database servers should be in the same availability set, such as Availability Set 2. Update and fault domains represent a limited area that a single hardware failure (fault domain) or that planned software update (update domain) might impact.

Azure forces VMs in the same availability set to be placed on separate hardware resources so that faults and updates can only affect one of the VMs at a time.

You should not configure the availability sets with a Web server and a database server together in the same set. There could be a failure that takes out all the Web servers together in this configuration, or all the database servers at the same time.

Placing a VM in an availability set by itself also does not offer any improvement in availability.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Create and configure VMs

References:

Microsoft Azure > Virtual Machines > Windows >- Manage the availability of Windows virtual machines in Azure

Microsoft Azure > Virtual Machines > Windows > Tutorial: Create and deploy highly available virtual machines with Azure PowerShell

---

Question #7 of 50

Question ID: 1477112

You are responsible for managing access to blobs in an Azure container named **vercontainer** in your Azure storage account named **veristacco**. You want to deliver a blob URL to your employee so that she can access the **verfile.txt** file with read and write permissions.

She should only be able to access **verfile.txt** through the Azure Blob Service from October 20 until October 27, 2019, and only if the requesting client comes from the IP range 168.1.1.20 - 168.1.1.50.

You pre-created the Azure shared access signature (SAS):

`Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D`

Which URL you should deliver to the user?

A) `https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&st=2019-10-27T22%3A18%3A26Z&se=2019-10-20T02%3A23%3A26Z&sr=bf&sp=rw&sip=168.1.1.20-168.1.1.50&spr=https&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D`

B) https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&st=2019-10-20T22%3A18%3A26Z&se=2019-10-27T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.1.20-168.1.1.50&spr=https&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D

C) **https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&st=2019-10-20T22%3A18%3A26Z&se=2019-10-27T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.1.20-168.1.1.50&spr=http&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D**

D) https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&st=2019-10-27T22%3A18%3A26Z&se=2019-10-27T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.1.20-168.1.1.50&spr=https&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D

Explanation

You have to use the following URL:

https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&st=2019-10-20T22%3A18%3A26Z&se=2019-10-27T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.1.20-168.1.1.50&spr=https&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D

The URL should begin with the name of the storage account, the container name, and the name of the file, which is **https://veristacco.blob.core.windows.net/vercontainer/verfile.txt**. Then you will have place a question mark (**?**) after verfile.txt to determine what you are searching for.

https://veristacco.blob.core.windows.net/vercontainer/verfile.txt**?**sv=2019-10-5&st=2019-10-20T22%3A18%3A26Z&se=2019-10-27T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.1.20-168.1.1.50&spr=https&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D

You will then add the **sv=** parameter to define the version of the blob file.

https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?**sv=**2019-10-5&st=2019-10-20T22%3A18%3A26Z&se=2019-10-27T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.1.20-168.1.1.50&spr=https&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D

The **st=**parameter defines the start time. The value specified is when the Shared Access Signatures (SAS) becomes valid. The value must be specified in the ISO 8061 format. If you omit the start time value, the SAS will become valid immediately. The following example specifies the start time in the ISO 8061 format as `2019-10-20T22%3A18%3A26Z`:

https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&**st=2019-10-20T22%3A18%3A26Z**&se=2019-10-27T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.1.20-168.1.1.50&spr=https&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D

The **se=** parameters define the expiration time of the SAS and the blob file. The following specifies the end time in the ISO 8061 format as `2019-10-27T02%3A23%3A26Z`:

https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&st=2019-10-20T22%3A18%3A26Z&**se=2019-10-27T02%3A23%3A26Z**&sr=b&sp=rw&sip=168.1.1.20-168.1.1.50&spr=https&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D

The **sr=** parameter defines the resource type. In this case it is **b**, which means it is accessible through the Azure Blob service and not Azure File service. If you type **bf**, it can be used for both.

https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&st=2019-10-20T22%3A18%3A26Z&se=2019-10-27T02%3A23%3A26Z&sr=**b**&sp=rw&sip=168.1.1.20-168.1.1.50&spr=https&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D

The **sip=** parameter defines the IP range from which the client can request access. The following defines the IP address from 168.1.1.20 - 168.1.1.50:

https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&st=2019-10-20T22%3A18%3A26Z&se=2019-10-27T02%3A23%3A26Z&sr=b&sp=rw&**sip=168.1.1.20-168.1.1.50**&spr=https&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D

The **spr=** parameter is for the used to specify the protocol, and this always has to be **https**. HTTP is not allowed for Azure SAS, as shown in the following example:

https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&st=2019-10-20T22%3A18%3A26Z&se=2019-10-27T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.1.20-168.1.1.50&spr=**https**&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D

The **sig=** parameter specifies the signature file that is used to authenticate access to the blob.

https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&st=2019-10-20T22%3A18%3A26Z&se=2019-10-27T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.1.20-168.1.1.50&spr=https&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D

You cannot use the following URL because it uses the wrong start time:

https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&**st=2019-10-27**T22%3A18%3A26Z&se=2019-10-27T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.1.20-168.1.1.50&spr=https&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D

The blob has to be made available from October 20, 2019 until October 27, 2019 and not from October 27, 2019 until October 27, 2019.

You cannot use the following URL because it has the wrong value for the **sr** parameter, **sr=bf**:

https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&st=2019-10-27T22%3A18%3A26Z&se=2019-10-20T02%3A23%3A26Z&**sr=bf**&sp=rw&sip=168.1.1.20-168.1.1.50&spr=https&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D

This URL grants access to both the Azure Blob service and Azure File service. Also, the start time and the end time in this URL should be reversed.

You cannot use the following URL because it has the wrong value for the **spr** parameter:

```
https://veristacco.blob.core.windows.net/vercontainer/verfile.txt?sv=2019-10-5&st=2019-10-20T22%3A18%3A26Z&se=2019-10-27T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.1.20-168.1.1.50&spr=http&sig=Z%2FrHIY5XFg0Mq2rqI3OlWTjFh1tYkboXr1L8ZUXDtkk%3D
```

The HTTP value is not allowed. You can only use HTTPS as the protocol for accessing an Azure blob through an Azure SAS URL.

Objective:
Implement and manage storage

Sub-Objective:
Configure access to storage

References:

Microsoft Azure > Storage > Grant limited access to Azure Storage resources using shared access signatures (SAS)

Question #8 of 50

Question ID: 1487298

You have an Azure virtual machine named **NutexSrv2K16** in the **NutexRG1** resource group. **NutexSrv2K16** was deployed by using a custom Azure Resource Manager (ARM) template.

You need to move **NutexSrv2K16** to a different host in another resource group in a different subscription. What actions should you perform in the Azure Portal?

Choose the appropriate steps and place them in the correct order.

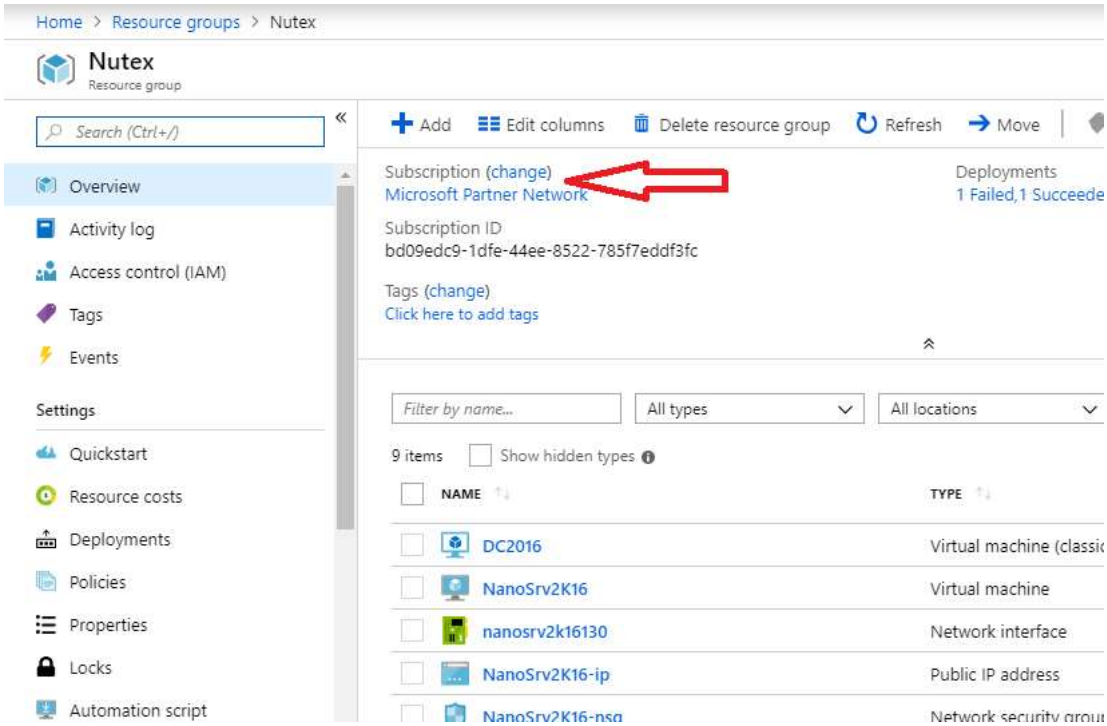
{UCMS id=5761937071669248 type=Activity}

Explanation

You should choose the following:

1. Browse to the **NutexRG1** page
2. Change the subscription to the new subscription
3. Select the new resource group

To move a VM in a resource group to a new resource group in a different subscription, you will first to open the resource group page and click **Move** next to the subscription.



Once you have chosen the appropriate subscription, you can then choose the appropriate resource group or create a new resource group for the VM.

Note: After the VM has been moved, new resource IDs will be created. The new IDs will need to be used with the VM after it has been moved.

You should not choose the **Update Management** blade and click **Enable**. This blade will allow you to manage updates and patches for your machines.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Automate deployment of resources by using templates

References:

Microsoft Azure > Virtual Machines > Windows > Move a Windows VM to another Azure subscription or resource group

---

Question #9 of 50

Question ID: 1477085

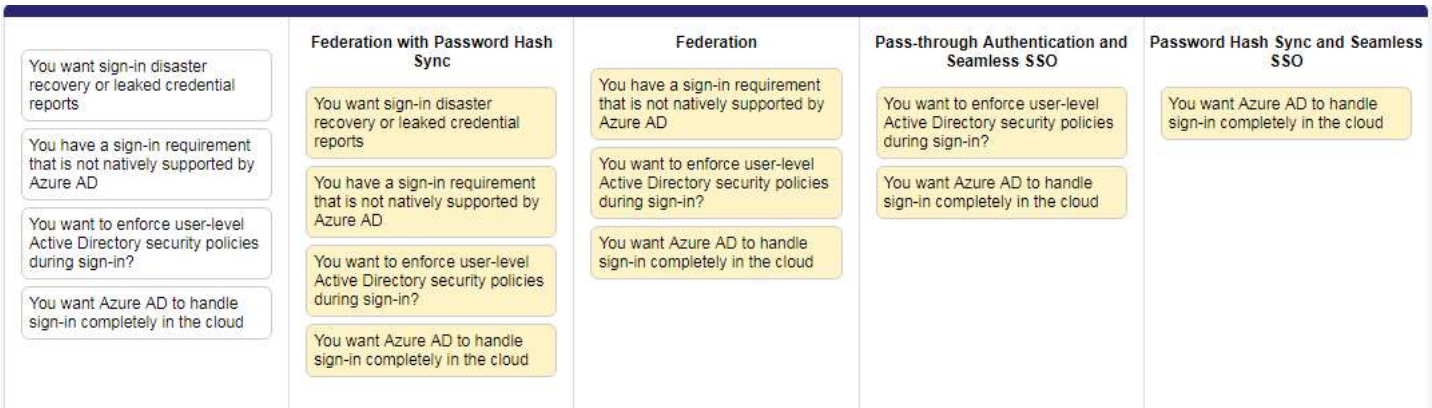
You are planning to implement an Azure AD hybrid identity solution. You need to understand the different authentication methods that can be used with an Azure AD hybrid identity solution that uses Azure AD Connect.

Match the need with the authentication method. (Each need can be used more than once.)

{UCMS id=6616640252805120 type=Activity}

Explanation

You should choose the following:



The Azure AD Password Hash synchronization authentication method allows users to use the same username and password that they use on-premises without another infrastructure. This method allows you provide seamless single sign-on (SSO) which so users can use their cloud apps without providing their user ID or password.

The Azure AD Pass-through Authentication method uses a software agent that runs on one or more on-premises servers to provide password validation for Azure AD authentication services. The on-premises servers validate the users to your on-premises Active Directory. This method allows you provide seamless single sign-on (SSO) which so users can use their cloud apps without providing their user ID or password. This authentication method can allow you to enforce user-level Active Directory security policies during sign-in.

Federation authentication takes care of the authentication process by using a separate trusted authentication system instead of Azure AD. This authentication method can allow you to enforce user-level Active Directory security policies during sign-in. This authentication method can allow you to a sign-in requirement that is not natively supported by Azure AD.

If you use Federation authentication with Password Hash Synchronization, then this authentication method can allow you to have sign-in disaster recovery or leaked credential reports.

Objective:
Manage Azure identities and governance

Sub-Objective:
Manage access control

References:

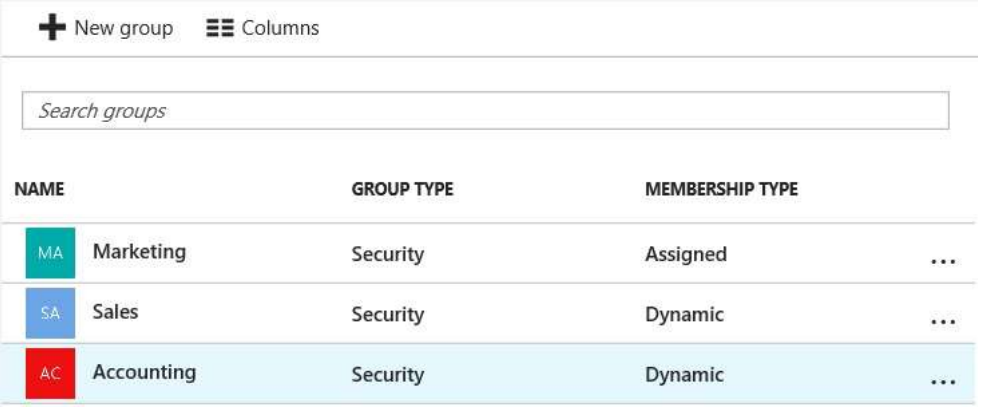
Deployment considerations for Azure AD Multi-Factor Authentication | Microsoft Docs

---

Question #10 of 50

Question ID: 1371332

You are the administrator of the Nutex Corporation. You use Azure AD Basic, and you manage only cloud-based user accounts. You have created the following Azure AD groups in the Azure Portal:



The marketing and sales groups have users as members. The accounting group has devices as members and is based on an advanced dynamic query.

You want to enable self-service password reset for only user accounts that are members of the marketing and sales groups.

Which setting do you have to select within the Password reset properties in the Azure portal?

A) Selected - Select groups: Sales

B) All

C) None

D) **Selected - Select groups: Marketing & Sales**

E) Selected - Select groups: Marketing

Explanation

You should select **All** because you cannot select more than one group when you want to restrict user password reset to only a limited group of users. With the All setting, all user accounts can do self-service password resets, including the users that are members of the marketing and sales groups.

Although it was not given as an alternative, a practical solution could be that you create a new group with all members of the sales and marketing groups and then select this group under **Select groups** in the Password reset properties.

You should not choose **None** because then no user of the marketing or sales group can use the self-service password reset feature.

You should not choose **Selected - Select groups: Marketing** because with that only the users that are members of the marketing group can use the self-service password reset feature.

You should not choose **Selected - Select groups: Sales** because with that only the users that are members of the sales group can use the self-service password reset feature.

You should not choose **Selected - Select groups: Marketing & Sales** because you cannot choose two groups under **Select groups** in the Password reset properties.

Objective:
Manage Azure identities and governance

Sub-Objective:
Manage Azure Active Directory (Azure AD) objects

References:

Microsoft Azure > Active Directory > How it works: Azure AD self-service password reset

---

Question #11 of 50

Question ID: 1477109

You are the Azure administrator for Nutex, Inc. You are concerned with keeping costs down, but the company is even more concerned with storing a large number of customer records on your VHD images. Nutex wants a contingency plan in case a natural disaster disrupts the region that currently holds your Azure VMs, which is the **EastUS** region.

You need to ensure that you can view all of the stored customer data even if a regional disaster happens. Which steps would you take to meet this goal? Select the appropriate steps from the left and drag them to the right. The steps must be in the correct order. Not all steps may be used.

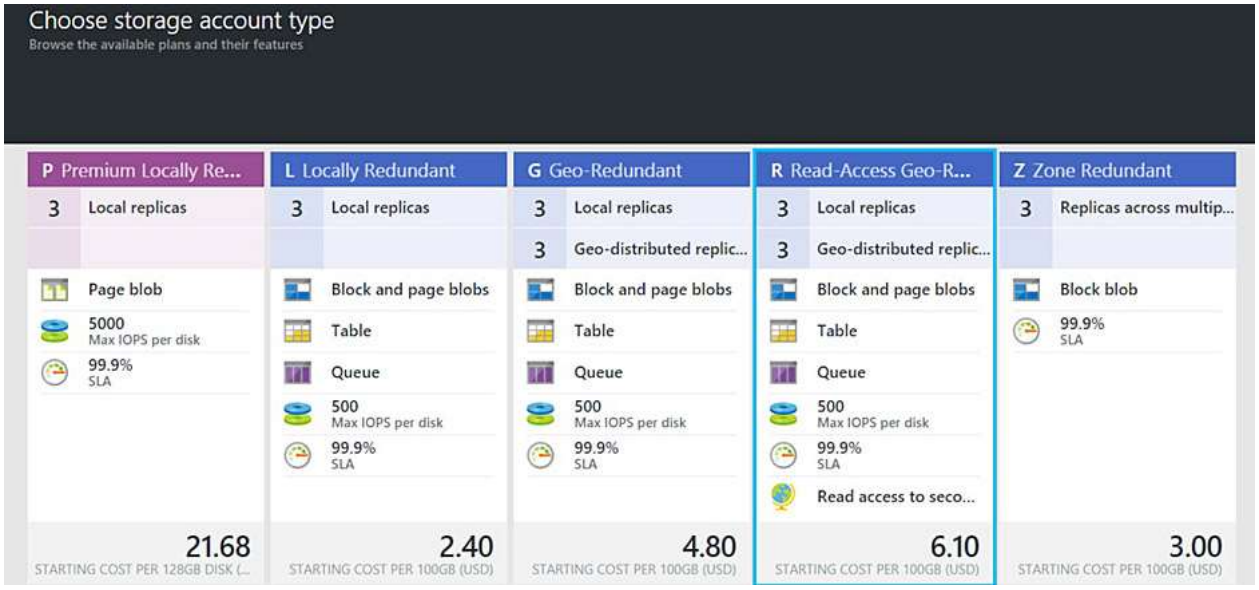
{UCMS id=5185803619663872 type=Activity}

Explanation

You should choose the following:

1. Create an Azure storage account
2. Configure Read-Access Geographically Redundant Storage (RA-GRS)

You would need to create an Azure storage account. The available storage account types are displayed in the following screenshot:



You would need to configure Read-Access Geographically Redundant Storage (RA-GRS) as your data redundancy option. This will provide Nutex with six copies of the data, with three copies stored in each region. This is the most expensive option, but is the only choice that meets the needs of the scenario. You would configure page blob storage to hold the VHDs.

You would not configure Locally Redundant Storage (LRS). This would create three copies, but they may be in the same datacenter, which means a regional disaster may make all copies inaccessible.

You would not configure Geo-Redundant Storage (GRS) and choose **WestUS** as your primary region. While this would achieve the redundancy goal, it would not provide read access to data during an outage, as required by this scenario. An additional reason not to choose **WestUS** as your primary region is that you are charged a "data egress" charge when your data is accessed by an application that is not running in the same region. You get to choose your primary region, but Microsoft chooses the secondary region.

You would not split the Azure VMs into at least two separate availability sets. Creating an availability set may be a good idea in case a single physical rack or switch goes down, but it will not help in a natural disaster that affects the entire facility.

You would not configure Geo-Redundant Storage (GRS) and choose **EastUS** as your primary region. While this would achieve the redundancy goal, it does not provide read access to data during an outage as required by this scenario. (However, if you tried to do so, Microsoft would automatically choose **WestUS** as your secondary region.)

If you are a developer, Microsoft offers an Azure Storage Emulator that emulates Azure storage for testing purposes without the need to create a storage account, or even an Azure subscription.

Objective:
Implement and manage storage

Sub-Objective:
Configure access to storage

References:

Microsoft Azure > Storage > Azure Storage redundancy

Microsoft Azure > Products > Azure Storage Overview pricing

Question #12 of 50

Question ID: 1477130

You are the administrator for the Nutex Corporation. You must replicate block blobs between storage accounts to minimize latency and to enable your clients to consume data from a region that is physically closer to them. You want to use the object replication feature.

Which of the following features or services must be used to implement object replication? (Choose all that apply.)

A) Change feed

B) Blob versioning

C) General-purpose v2 storage account

D) General-purpose v1 storage account

E) Azure Data Lake Storage Gen2 storage account

Explanation

You must have the following to implement object replication:

- Change feed
- Blob versioning
- General-purpose v2 storage account

Change feed must be enabled on the source storage account. The purpose of the change feed is to provide transaction logs of all the changes that occur to the blobs and the blob metadata in your storage account. This is a prerequisite before you can use object replication.

Blob versioning must be enabled on the source account as a prerequisite for object replication. This feature automatically maintains previous versions of a blob when it is modified or deleted.

You would use a general-purpose v2 storage account because the source and target storage accounts must use general-purpose v2 as a prerequisite, not a general-purpose v1 storage account. A general-purpose v1 storage account is a legacy account type for blobs, files, queues, and tables. It is highly recommended to use general-purpose v2 storage accounts instead of general-purpose v1 storage accounts when possible.

You would not use an Azure Data Lake Storage Gen2 storage account because this type of account does not support the object replication feature as of this writing. Azure Data Lake Storage Gen2 has capabilities dedicated to big data analytics, and provides file system semantics, file-level security, and scale.

Objective:
Implement and manage storage

Sub-Objective:
Manage data in Azure storage accounts

References:

Microsoft Docs > Azure > Storage > Blobs > Object replication for block blobs

Microsoft Docs > Azure > Storage > Blobs > Configure object replication for block blobs

Microsoft Docs > Azure > Storage > Blobs > Change feed support in Azure Blob Storage > Enable and disable the change feed

Microsoft Docs > Azure > Storage > Blobs > Enable and manage blob versioning

---

Question #13 of 50

Question ID: 1477141

You are the administrator of the Nutex Corporation. You have developed some Azure ARM templates that need to be deployed from your local machine to the Azure resource group named **Nutex1RG**. **Nutex1RG** includes the following resources:

Virtual Network: **Vnet1**
Storage Account: **Nutex1stac1**
Network Security Group: **NutexNSG1**
Virtual Machines: **NutVM1**, **NutVM2**, **NutVM3**
Network Card: **NutNIC1**, **NutNIC2**, **NutNIC3**

You want to deploy an ARM template based on JSON files saved in your storage account **Nutex1stac1** in the blob container named **Templates** through REST API. All existing resources have to remain in the resource group.

After the ARM template is deployed, existing resources in **Nutex1RG** have to remain in the resource group.

Which PowerShell, Azure CLI, and REST API commands do you have to use? (Choose all that apply.)

A)
```
az group deployment create \
        --name NutexDeployment \
        --mode Complete \
        --resource-group Nutex1RG \
        --template-file c:\MyTemplates\Nutex1.json \
```

B) **New-AzureResourceGroupDeployment -Mode Incremental -Name NutexDeployment -ResourceGroupName Nutex1RG -TemplateFile c:\MyTemplates\Nutex1.json**

C)
```
PUT
https://management.Azure.com/subscriptions/<YourSubscriptionId>/resourcegroups/<YourResourceGroupName>/providers/Microsoft.Resources/deploym
api-version=2015-01-01
   <common headers>
   {
   "properties": {
   "templateLink": {
   "uri": "http://nutexstorageaccount.blob.core.windows.net/templates/template.json",
   "contentVersion": "1.0.0.0"
   },
   "mode": "Complete",
   "parametersLink": {
   "uri": "http://nutexstorageaccount.blob.core.windows.net/templates/parameters.json",
   "contentVersion": "1.0.0.0"
   }
   }
   }
```

D)
```
az group deployment create \
        --name NutexDeployment \
        --mode incremental \
        --resource-group Nutex1RG \
        --template-file c:\MyTemplates\Nutex1.json \
```

E) **PUT https://management.Azure.com/subscriptions/<YourSubscriptionId>/resourcegroups/ Nutex1RG /providers/Microsoft.Resources/deployments/NutexDeployment?api-version=2015-01-01**
```
  <common headers>
   {
   "properties": {
   "templateLink": {
   "uri": "http://nutex1stac1.blob.core.windows.net/templates/Nutex1.json",
   "contentVersion": "1.0.0.0"
   },
   "mode": "Incremental",
   "parametersLink": {
   "uri": "http://nutex1stac1.blob.core.windows.net/templates/Nutex1Parameters.json",
   "contentVersion": "1.0.0.0"
   }
   }
   }
```

F) New-AzureResourceGroupDeployment -Mode Complete -Name NutexDeployment -ResourceGroupName Nutex1RG -TemplateFile c:\MyTemplates\Nutex1.json

Explanation

You should use the following:

```
New-AzureResourceGroupDeployment -Mode Incremental -Name NutexDeployment -ResourceGroupName Nutex1RG -TemplateFile c:\MyTemplates\Nutex1.json
```

```
az group deployment create \
        --name NutexDeployment \
        --mode incremental \
        --resource-group Nutex1RG \
        --template-file c:\MyTemplates\Nutex1.json \
```

```
PUT https://management.Azure.com/subscriptions/<YourSubscriptionId>/resourcegroups/ Nutex1RG
/providers/Microsoft.Resources/deployments/NutexDeployment?api-version=2015-01-01
<common headers>
{
"properties": {
"templateLink": {
"uri": "http://nutex1stac1.blob.core.windows.net/templates/Nutex1.json",
"contentVersion": "1.0.0.0"
},
"mode": "Incremental",
"parametersLink": {
"uri": "http://nutex1stac1.blob.core.windows.net/templates/Nutex1Parameters.json",
"contentVersion": "1.0.0.0"
}
}
}
```

When deploying your resources, you specify that the deployment is either an incremental update or a complete update. The primary difference between these two modes is how Resource Manager handles existing resources in the resource group that are not in the template:

- In complete mode, Resource Manager deletes resources that exist in the resource group but are not specified in the template.
- In incremental mode, Resource Manager leaves unchanged resources that exist in the resource group but are not specified in the template.

By default, Resource Manager uses the incremental mode. You can use the **New-AzureResourceGroupDeployment** cmdlet with the **-Mode** parameter to specify incremental mode:

```
-Mode Incremental -Name NutexDeployment -ResourceGroupName Nutex1RG -TemplateFile c:\MyTemplates\ Nutex1.json
```

You should use the following REST API command:

```
PUT https://management.Azure.com/subscriptions/<YourSubscriptionId>/resourcegroups/ Nutex1RG
/providers/Microsoft.Resources/deployments/NutexDeployment?api-version=2015-01-01
<common headers>
{
"properties": {
"templateLink": {
"uri": "http://nutex1stac1.blob.core.windows.net/templates/Nutex1.json",
"contentVersion": "1.0.0.0"
},
"mode": "Incremental",
  "parametersLink": {
"uri": "http://nutex1stac1.blob.core.windows.net/templates/Nutex1Parameters.json",
"contentVersion": "1.0.0.0"
}
}
}
```

Notice that "mode" is also set to Incremental. To run a complete deployment, you should set the mode to Complete. If you do so, all other resources in the resource group will be deleted. Be careful when using the Complete mode, as you can inadvertently delete resources that are not in your template. In this scenario, the resource has to stay, so the mode should be set to Incremental.

You should not use the following:

```
New-AzureResourceGroupDeployment –Mode Complete -Name NutexDeployment -ResourceGroupName Nutex1RG -TemplateFile c:\MyTemplates\Nutex1.json
```

This PowerShell command has the Mode parameter is set to Complete, which means that all resources that are not defined through the ARM template will be removed from the resource group.

You should not use the following:

```
az group deployment create \
         --name NutexDeployment \
         --mode Complete \
         --resource-group Nutex1RG \
         --template-file c:\MyTemplates\Nutex1.json \
```

This is an Azure CLI command that has the mode set to Complete instead of Incremental.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Automate deployment of resources by using templates

References:

Microsoft Azure > Resource Manager > Templates > Deploy resources with ARM templates and Azure PowerShell

Microsoft Azure > Resource Manager > Templates > Deploy resources with ARM templates and Resource Manager REST API

Microsoft Azure > PowerShell > New-AzResourceGroupDeployment

Question #14 of 50

Question ID: 1481896

You have been asked to add a network interface to one of the Nutex Sales VMs currently running in Azure. What steps in the Azure portal should you take to accomplish this?

{UCMS id=6241870743076864 type=Activity}

Explanation

You should do the following:

1. In the Azure Portal, create a new Network Interface resource.
2. Supply a name that is unique within the resource group.
3. Select the virtual network and subnet for the interface.
4. Select **Dynamic** for the **Private IP Address Assignment** option.
5. Choose the associated subscription, resource group, and location.
6. Click **create** at the bottom of the **Create Network Interface** page.

To create a new network interface within Azure, you could use the Azure Portal, Azure CLI, or PowerShell (either in the cloud or local). Using the Azure Portal imposes some limitations, mostly because the UI omits some specific options.

When scripting your actions in the Azure CLI or Powershell, your abilities within Azure are only limited by your imagination and the depth of your scripting abilities. With Azure CLI, you can use the `az network nic create` command to create a network interface. With PowerShell, you can use the **New-AzNetworkInterface** cmdlet.

You cannot create a new virtual network in the Azure Portal when you are creating a network interface. The virtual network MUST already exist before you create the network interface.

The only two settings for the **Private IP Address** option in the Azure Portal are Dynamic and Static. DHCP is not an option.

You cannot assign a public IP Address from the Azure Portal's **Create Network Interface** page.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Create and configure VMs

References:

Microsoft Azure > Networking > Create, change, or delete a network interface

Microsoft Azure > Networking > Add network interfaces to or remove network interfaces from virtual machines

---

Question #15 of 50

Question ID: 1371380

You have an important application with a lot of online transactions where the application performs many small transactions at a low latency level.

What storage tier will you suggest for this application?

A) Archive

B) Hot

C) **Premium**

D) Cool

Explanation

You would select Premium because it is ideal for sensitive applications with high throughput, such as online transactions, and is suited for workloads where an application performs many small transactions at a low latency level.

The following access tiers are available:

- **Hot –** tier used for data that is frequently accessed. It is more expensive to store data here compared to the Cool and Archive tiers, but cheaper to access.
- **Cool** – tier used for storing less frequently accessed data, such as archived files, backups, and raw or unprocessed data. Cool is designed for data that is likely to be stored for at least 30 days. Cool storage costs less than Hot storage per GB.
- **Archive –**the most cost-effective tier for storing data but is typically more expensive for data retrieval than Hot and Cool tiers. Archive is designed for data that is likely to be stored for at least 180 days, and for systems or scenarios where retrieval latency can be tolerated.

Objective:
Implement and manage storage

Sub-Objective:
Configure Azure files and Azure Blob Storage

References:

Microsoft Azure > Storage > Blobs > Performance tiers for block blob storage

---

Question #16 of 50

Question ID: 1477089

You are the administrator for the Nutex Corporation. You must create a recurring task that automatically exports your cost management data to Azure storage. You want to export a maximum of 90 days of historical costs from a specific date.

Which of the following export types should you choose?

A) Daily export of month-to-date costs

B) **One-time export**

C) Weekly export of costs for the last seven days

D) Monthly export of last month's costs

Explanation

You would choose a one-time export because this allows you to select the historical data's date range to export to Azure Blob storage. The maximum number of days of historical costs you can export is 90 days from a given date. The exported report is stored in the storage account within two hours after it is run.

While other choices allow you to export multiple reports that can cumulatively cover 90 days, only the one-time export report allows you to export a single report with a maximum of 90 days of historical costs.

You would not choose a daily export of month-to-date costs because this export provides your month-to-date costs. The latest data is aggregated from previous daily exports.

You would not choose the weekly export of costs for the last seven days because this creates a weekly export of your costs for the past seven days from the selected start date of your export.

You would not choose the monthly export of last month's costs because this provides you with an export of the previous month's costs compared to the month that you use to create the export. The schedule runs an export on the fifth day of every new month with your previous month’s costs.

Objective:
Manage Azure identities and governance

Sub-Objective:
Manage Azure subscriptions and governance

References:

Microsoft Docs > Azure > Cost Management and Billing > Manage costs and usage > Tutorial: Create and manage exported data

---

Question #17 of 50

Question ID: 1530440

Your organization, the Verigon Corporation, has recently moved to an Azure cloud environment and deployed their applications and solutions to the cloud.

To manage the infrastructure and application code through a unified process, you want to automate deployments and use the practice of Infrastructure as Code (IaC). Which of the following should you use to implement IaC for your Azure solutions?

A) Azure Custom Script Extension

B) Azure Resource Manager (ARM) templates

C) Azure Automation

D) PowerShell Desired State Configuration (DSC)

Explanation

You would use ARM to implement Infrastructure as Code for your Azure solutions. Azure templates are JavaScript Object Notation (JSON)scripts used with your project's configuration and infrastructure details. The infrastructure code becomes part of your project. You can indicate the resources you want to deploy and their properties in the ARM template. You can write template expressions extending the ARM template's JSON capabilities. You can share the ARM template with other users in the organization. Microsoft recommends using Visual Studio code with the ARM Tools extension for creating the ARM templates. You can also use Azure PowerShell or Azure CLI to deploy the templates.

You would not use Azure Automation to implement IaC for your Azure solutions. You can manage existing virtual machines (VMs) using Azure Automation. You can use Azure Automation on Windows and Linux VMs and on-premises virtual and physical machines. It uses runbooks to process the set of tasks on the VMs you target. It also offers the Desired State Configuration (DSC) service that you can use to create definitions of how VMs are configured.

You would not use Azure Custom Script Extension to implement IaC for your Azure solutions. You can download and execute scripts using Azure Custom Script Extension on Linux or Windows Azure VMs. You can use it to write scripts in any language that runs on source VMs.

You would not use PowerShell DSC to implement IaC for your Azure solutions. You can use PowerShell DSC to write configurations of target machines. You can define what you want to install on the machines and how you want to configure the host.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Automate deployment of resources by using templates

References:

Microsoft Learn > Azure > Resource Manager > Templates > What are ARM templates?

Microsoft Learn > Azure > Virtual Machines > Use infrastructure automation tools with virtual machines in Azure

Microsoft Learn > Azure > Resource Manager > Templates > Tutorial: Create and deploy your first ARM template

---

Question #18 of 50

Question ID: 1480108

You have been troubleshooting a Remote Desktop (RDP) connection to Windows-based a Azure virtual machine (VM) named **VM5**. You want to redeploy the VM to help troubleshoot the RDP connection to a new resource group named **NutexRG1**.

You type the following at the PowerShell prompt:

[ ] `-ResourceGroupName "NutexRG1" -Name "VM5"`

What is the missing cmdlet? Type the missing part of the PowerShell command in the textbox provided.

Explanation

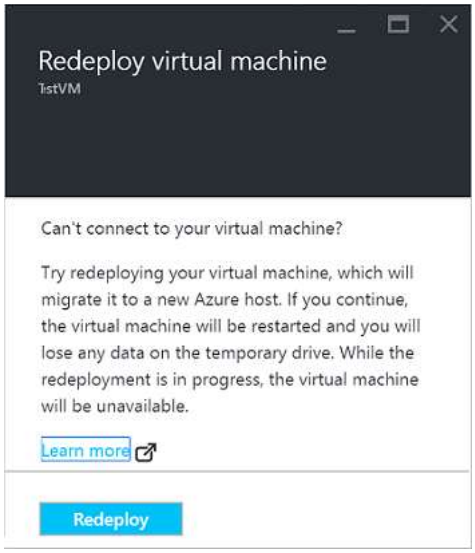
Acceptable answer(s) for field 1:

- Set-AzVM -Redeploy

You can use the **Set-Az-VM** cmdlet with the **-Redeploy** parameter to deploy a VM to another resource group. The following example redeploys **VM5** to help troubleshoot the RDP connection to a new resource group named **NutexRG1**:

```
Set-AzVM -Redeploy -ResourceGroupName "NutexRG1" -Name "VM5"
```

You could also troubleshoot this problem with the Azure Portal by going to the **Support and Troubleshoot** section on the virtual machine page and choosing **Redploy**.



Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Create and configure VMs

References:

Microsoft Azure > Virtual Machines > Redeploy Windows virtual machine to new Azure node

---

Question #19 of 50

Question ID: 1530438

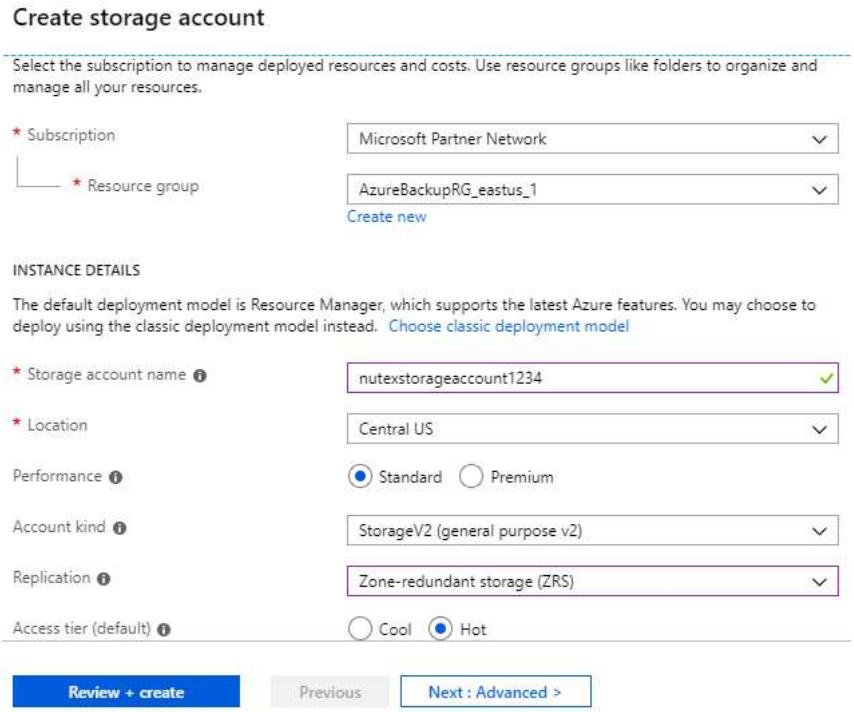
According to Planned Changes, how should you configure the storage account?

{UCMS id=5665388220121088 type=Activity}

Explanation

In this scenario, the datacenter must be protected from a natural disaster such as fire or flood. Redundancy must exist. Replicas must not be lost and must be recoverable. The company applications store data, but this data is not easily reconstructed if data loss occurs. A storage account must be configured that replicates synchronously.

You should use zone-redundant storage (ZRS) as the redundancy option and General-purpose v2 (GPV2) as the storage type.



ZRS syncs data across three storage clusters within a region. ZRS provides great performance as well as low latency. You should consider ZRS if an outage or natural disaster, such as fire or flood, makes an availability zone unavailable.

You should not use Locally redundant storage (LRS). LRS replicates data to a storage scale unit. LRS is lower priced than other redundancy options, but has the least durability. Microsoft recommends using either zone-redundant storage (ZRS) or geo-redundant storage (GRS) to avoid data loss.

ZRS is preferred over Geo-redundant storage (GRS) because ZRS has higher availability with synchronous replication than GRS.

You should not use Read-access geo-redundant storage (RA-GRS) because this redundancy option uses asynchronous replication, not synchronous replication as required by this scenario.

The following chart compares each redundancy option:

Scenario	LRS	GRS	RA-GRS	ZRS
Node unavailability within a data center	Yes	Yes	Yes	Yes
An entire data center (zonal or non-zonal) becomes unavailable	No	Yes	Yes	Yes
A region-wide outage	No	Yes	Yes	No
Read access to your data (in a remote, geo-replicated region) in the event of region-wide unavailability	No	No	Yes	No
Designed to provide __ durability of objects over a given year	<= 99.99% (11 9's)	<= 99.99% (16 9's)	<= 99.99% (16 9's)	<= 99.99% (12 9's)
Supported storage account types	GPv2, GPv1, Blob	GPv2, GPv1, Blob	GPv2, GPv1, Blob	GPv2
Availability SLA for read requests	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.99% (99.9% for Cool Access Tier)	At least 99.9% (99% for cool access tier)
Availability SLA for write requests	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.99% (99.9% for Cool Access Tier)	At least 99.9% (99% for cool access tier)

ZRS supports the General-purpose v2 (GPV2) storage account type.

You should use GPv2 Azure blob hot access tier if the data must be active and is expected to be accessed (read from and written to) frequently. Azure blob hot storage tier has higher storage costs than cool and archive storage, but the lowest access costs. GPv1 storage accounts do not support tiering.

You should use the GPv2 Azure blob cool access tier for data that will reside in the cool tier for at least 30 days.

GPv2 Azure blob archive access tier retrieval costs are much higher when compared to hot and cool storage. This tier should be used for data that does not need to be accessed for several hours and should remain in the archive tier for no less than 180 days. A blob can be in archive storage. The blob can be offline, and the data cannot be read, copied, overwritten, or modified. The metadata of the blob can be read because it is online and available. You cannot make snapshots of a blob while in archive storage. You can change the tier or your blob, you can also delete, list, or get properties/metadata of the blob.

Objective:
Implement and manage storage

Sub-Objective:

Manage data in Azure storage accounts

References:

Azure > Storage > Azure Storage redundancy

Azure > Storage > Zone-redundant storage (ZRS): Highly available Azure Storage applications

---

Question #20 of 50

Question ID: 1477117

Your application uses Azure Storage queues. You need to use Shared Access Signature (SAS) to delegate access to specific storage account resources.

Which set of code correctly creates and uses a SAS token for a queue?

A)
```
CloudQueueClient client = account.CreateCloudQueueClient();
CloudQueue queue = client.GetQueueReference("messagequeue");
SharedAccessQueuePolicy policy = new SharedAccessQueuePolicy();
policy.SharedAccessExpiryTime = DateTime.UtcNow.AddHours(2);
policy.Permissions = SharedAccessQueuePermissions.Read | SharedAccessQueuePermissions.Add |
SharedAccessQueuePermissions.Update | SharedAccessQueuePermissions.ProcessMessages;
policy.SharedAccessStartTime = DateTime.UtcNow.Add(new TimeSpan(0, 5, 0));
CloudQueueClient sasClient = new CloudQueueClient("https://<ACCOUNTNAME>.queue.core.windows.net/",
policy);
CloudQueue sasQueue = sasClient.GetQueueReference("messagequeue");
sasQueue.AddMessage(new CloudQueueMessage("my message"));
```

B)
```
CloudQueueClient client = account.CreateCloudQueueClient();
CloudQueue queue = client.GetQueueReference("messagequeue");
SharedAccessQueuePolicy policy = new SharedAccessQueuePolicy(DateTime.UtcNow.AddHours(2),
DateTime.UtcNow.Add(new TimeSpan(0, 5, 0)));
policy.Permissions = SharedAccessQueuePermissions.Read | SharedAccessQueuePermissions.Add |
SharedAccessQueuePermissions.Update | SharedAccessQueuePermissions.ProcessMessages;
string token = queue.GetSharedAccessSignature(policy);
StorageCredentials credentials = new StorageCredentials(token);
CloudQueueClient sasClient = new CloudQueueClient("https://<ACCOUNTNAME>.queue.core.windows.net/",
credentials);
CloudQueue sasQueue = sasClient.GetQueueReference("messagequeue");
sasQueue.AddMessage(new CloudQueueMessage("my message"));
```

C)
```
CloudQueueClient client = account.CreateCloudQueueClient();
CloudQueue queue = client.GetQueueReference("messagequeue");
SharedAccessQueuePolicy policy = new SharedAccessQueuePolicy();
policy.SharedAccessExpiryTime = DateTime.UtcNow.AddHours(2);
policy.Permissions = SharedAccessQueuePermissions.Read | SharedAccessQueuePermissions.Add |
SharedAccessQueuePermissions.Update | SharedAccessQueuePermissions.ProcessMessages;
policy.SharedAccessStartTime = DateTime.UtcNow.Add(new TimeSpan(0, 5, 0));
string token = queue.GetSharedAccessSignature(policy);
StorageCredentials credentials = new StorageCredentials(token);
CloudQueueClient sasClient = new CloudQueueClient("https://<ACCOUNTNAME>.queue.core.windows.net/",
credentials);
CloudQueue sasQueue = sasClient.GetQueueReference("messagequeue");
sasQueue.AddMessage(new CloudQueueMessage("my message"));
```

D)
```
CloudQueueClient client = account.CreateCloudQueueClient();
CloudQueue queue = client.GetQueueReference("messagequeue");
SharedAccessQueuePolicy policy = new SharedAccessQueuePolicy();
policy.SharedAccessExpiryTime = DateTime.UtcNow.AddHours(2);
policy.Permissions = SharedAccessQueuePermissions.Read | SharedAccessQueuePermissions.Add |
SharedAccessQueuePermissions.Update | SharedAccessQueuePermissions.ProcessMessages;
policy.SharedAccessStartTime = DateTime.UtcNow.Add(new TimeSpan(0, 5, 0));
string token = queue.GetSharedAccessSignature(policy);
StorageCredentials credentials = new StorageCredentials(token);
CloudQueueClient sasClient = new CloudQueueClient("https://azure.
<ACCOUNTNAME>.queue.core.windows.net/");
CloudQueue sasQueue = sasClient.GetQueueReference("messagequeue");
sasQueue.AddMessage(new CloudQueueMessage("my message"), credentials);
```

Explanation

You should use the following code because the policy is set properly, the token is retrieved correctly, and the credentials are created and passed to the `CloudQueueClient` object:

```
CloudQueueClient client = account.CreateCloudQueueClient();
CloudQueue queue = client.GetQueueReference("messagequeue");
SharedAccessQueuePolicy policy = new SharedAccessQueuePolicy();
policy.SharedAccessExpiryTime = DateTime.UtcNow.AddHours(2);
policy.Permissions = SharedAccessQueuePermissions.Read | SharedAccessQueuePermissions.Add |
SharedAccessQueuePermissions.Update | SharedAccessQueuePermissions.ProcessMessages;
policy.SharedAccessStartTime = DateTime.UtcNow.Add(new TimeSpan(0, 5, 0));
string token = queue.GetSharedAccessSignature(policy);
StorageCredentials credentials = new StorageCredentials(token);
CloudQueueClient sasClient = new CloudQueueClient("https://<ACCOUNTNAME>.queue.core.windows.net/", credentials);
CloudQueue sasQueue = sasClient.GetQueueReference("messagequeue");
sasQueue.AddMessage(new CloudQueueMessage("my message"));
```

You can use the following to retrieve storage account from connection string:

```
CloudStorageAccount storageAccount = CloudStorageAccount.Parse(CloudConfigurationManager.GetSetting("StorageConnectionString"));
```

You can use the following to create the queue client:

```
CloudQueueClient queueClient = storageAccount.CreateCloudQueueClient();
```

The following code creates a policy with the proper permissions:

```
policy.Permissions = SharedAccessQueuePermissions.Read | SharedAccessQueuePermissions.Add |
SharedAccessQueuePermissions.Update | SharedAccessQueuePermissions.ProcessMessages;
policy.SharedAccessStartTime = DateTime.UtcNow.Add(new TimeSpan(0, 5, 0));
```

The following code ensures the token is retrieved correctly, and the credentials are created and passed to the `CloudQueueClient` object:

```
string token = queue.GetSharedAccessSignature(policy);
StorageCredentials credentials = new StorageCredentials(token);
CloudQueueClient sasClient = new CloudQueueClient("https://<ACCOUNTNAME>.queue.core.windows.net/", credentials);
CloudQueue sasQueue = sasClient.GetQueueReference("messagequeue");
sasQueue.AddMessage(new CloudQueueMessage("my message"));
```

You should not use the following set of code:

```
CloudQueueClient client = account.CreateCloudQueueClient();
CloudQueue queue = client.GetQueueReference("messagequeue");
SharedAccessQueuePolicy policy = new SharedAccessQueuePolicy();
policy.SharedAccessExpiryTime = DateTime.UtcNow.AddHours(2);
policy.Permissions = SharedAccessQueuePermissions.Read | SharedAccessQueuePermissions.Add |
SharedAccessQueuePermissions.Update | SharedAccessQueuePermissions.ProcessMessages;
policy.SharedAccessStartTime = DateTime.UtcNow.Add(new TimeSpan(0, 5, 0));
CloudQueueClient sasClient = new CloudQueueClient("https://<ACCOUNTNAME>.queue.core.windows.net/", policy);
CloudQueue sasQueue = sasClient.GetQueueReference("messagequeue");
sasQueue.AddMessage(new CloudQueueMessage("my message"));
```

When creating a `CloudQueueClient`, the second parameter must be the storage credentials. You should create a `StorageCredentials` object based on the token you get from the policy, then pass the credentials to the `CloudQueueClient`

You should not use the following set of code:

```
CloudQueueClient client = account.CreateCloudQueueClient();
CloudQueue queue = client.GetQueueReference("messagequeue");
SharedAccessQueuePolicy policy = new SharedAccessQueuePolicy(DateTime.UtcNow.AddHours(2), DateTime.UtcNow.Add(new TimeSpan(0, 5, 0)));
policy.Permissions = SharedAccessQueuePermissions.Read | SharedAccessQueuePermissions.Add |
SharedAccessQueuePermissions.Update | SharedAccessQueuePermissions.ProcessMessages;
string token = queue.GetSharedAccessSignature(policy);
StorageCredentials credentials = new StorageCredentials(token);
CloudQueueClient sasClient = new CloudQueueClient("https://<ACCOUNTNAME>.queue.core.windows.net/", credentials);
CloudQueue sasQueue = sasClient.GetQueueReference("messagequeue");
sasQueue.AddMessage(new CloudQueueMessage("my message"));
```

The `SharedAccessQueuePolicy` class has only a default constructor. You cannot pass the expiry time and start time as parameters. You should set these values separately in the policy.

You should not use the following set of code:

```
CloudQueueClient client = account.CreateCloudQueueClient();
CloudQueue queue = client.GetQueueReference("messagequeue");
SharedAccessQueuePolicy policy = new SharedAccessQueuePolicy();
policy.SharedAccessExpiryTime = DateTime.UtcNow.AddHours(2);
policy.Permissions = SharedAccessQueuePermissions.Read | SharedAccessQueuePermissions.Add |
SharedAccessQueuePermissions.Update | SharedAccessQueuePermissions.ProcessMessages;
policy.SharedAccessStartTime = DateTime.UtcNow.Add(new TimeSpan(0, 5, 0));
string token = queue.GetSharedAccessSignature(policy);
StorageCredentials credentials = new StorageCredentials(token);
CloudQueueClient sasClient = new CloudQueueClient("https://azure.<ACCOUNTNAME>.queue.core.windows.net/");
CloudQueue sasQueue = sasClient.GetQueueReference("messagequeue");
sasQueue.AddMessage(new CloudQueueMessage("my message"), credentials);
```

The URL `Error! Hyperlink reference not valid.` is incorrect. The account name should not be preceded with `azure`. In addition, the call is missing the credentials, which are incorrectly passed to the `AddMesssage` call.

Objective:
Implement and manage storage

Sub-Objective:
Configure access to storage

References:

Microsoft Azure > Storage > Grant limited access to Azure Storage resources using shared access signatures (SAS)

Question #21 of 50

Question ID: 1487297

You are the Azure Administrator of the Nutex Corporation. The administrator of the IT Support department has left the corporation.

You must grant Administrator access for the subscription to two users in the **IT_admins** group. This group will manage Azure resources that were created under that subscription.

In which role will you add the **IT_admins** group?

A) Azure AD App role

B) Azure RBAC role

C) **Azure AD role**

D) Azure AD security group

Explanation

You would choose the Azure RBAC role. Azure RBAC roles are used to manage access to virtual machines, storage, and other Azure resources. The Azure RBAC scope covers management groups, subscriptions, resource groups, and resources.

You would not choose Azure AD roles because these are used to manage access to Azure AD resources, particularly users, groups, and domains.

You would not choose the Azure AD App role because this is used to manage user authorization in a level of an application, and when the application is removed from Azure AD, and Azure AD App role are removed automatically.

You would not choose the Azure AD security group because this is used to assign permissions to users based on membership in a level of application and not Azure resources.

Objective:
Manage Azure identities and governance

Sub-Objective:
Manage Azure subscriptions and governance

References:

Microsoft Azure > Role-based access control > What is role-based access control (RBAC) for Azure resources?

Question #22 of 50

Question ID: 1480121

You plan to create a container instance named **NutexContainerA**. **NutexContainerA** uses a Docker image named NutexImage.

You plan to have an app named NutexApp persist in **NutexContainerA**.

Which of the following should you use to have persistent storage for **NutexContainerA**? (Choose all that apply.)

A) **Azure Files**
B) Scaleout FIle server
C) Storage mounted directly on cluster shared volumes (CSV)
D) **Azure Cosmos DB**
E) DFS share on a Windows Server 2019 server
F) **Azure SQL database**

Explanation

You should use the following:

- Azure Files
- Scaleout File server

A container can have persistent storage using bind mounts or named volumes. You can use the Docker daemon to create the volume and start a container with the mapped volume.

Named volumes are used to create a volume and assign the name of the volume to the container.

You can run a CSV volume on a virtual machine acting as a container host, but it is not possible to bind mounting directly on cluster shared volumes (CSV).

Bind mounts support SMB mounts. SMB mounts include the following:

- Windows servers with volumes accessible with the SMB protocol
- Scaleout File servers
- Azure Files, which is an SMB share in the Azure cloud
- Any third-party implementation of an SMB share

You would not use a DFS, DFSN, or DFSR share on a Windows Server 2019 server. SMB global mapping is not supported on those shares with that version of Windows Server.

A Cosmos database or SQL database cannot be used for persistent storage. A database is not a bind mount, share volume, or named volume.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Create and configure containers

References:

Microsoft Docs > Containers on Windows > Storage > Persistent Storage in Containers

Docker Docs > Guides > Run your app in production > Manage application data > Use volumes

---

Question #23 of 50

Question ID: 1477123

You have been asked to collect log files available inside the Dream Suites Azure subscription. The data from the log files should reside within a single workspace and allow administrators to query the data.

What solution will meet the requirements?

A) Azure Log Analytics

B) Azure Security Center

C) Azure Service Health

D) Azure Network Watcher

Explanation

Azure Log Analytics is a service that is used to collect log data from Azure and on-premises. Insights can be derived from this log repository and stored in a single workspace. A powerful expressive query language is available to transform log data into actionable insight. This option will provide the ability to collect log files in a single workspace.

The Azure Security Center feature is a robust management platform that allows you to monitor threats within on-premises and Azure workloads and to fix discovered vulnerabilities quickly. This security platform provides the visibility to visually manage the security posture of your on-premises and Azure assets. This option will not provide the ability to collect log files in a single workspace.

The Azure Service Health dashboard is the centralized place to track planned maintenance schedules, health advisories, and health alert notifications. This option will not provide the ability to collect log files in a single workspace.

The Azure Network Watcher service provides the ability to monitor network traffic among resources to identify latency, routing topology changes and view logs. For example, you can use the Azure Network Watcher feature to monitor communication between virtual machines to diagnose routing issues or to determine if the endpoint is unreachable. This option will not provide the ability to collect log files in a single workspace.

Objective:
Implement and manage storage

Sub-Objective:
Configure access to storage

References:

Microsoft Azure > Monitor > Overview of log queries in Azure Monitor

---

Question #24 of 50

Question ID: 1477181

You deploy a new VM with default settings to a resource group named RG01. You validate that you can connect to it by using Remote Desktop Connection. When you try to connect to it through PowerShell remoting, it fails.

What should you do to ensure that you can manage the VM by using PowerShell remoting?

A) Create an inbound security rule to allow TCP port 80 and TCP port 443.

B) Create an inbound security rule to allow TCP port 5985 and TCP port 5986.

C) Create an inbound security rule to allow TCP port 20 and TCP port 21.

D) Create an inbound security rule to allow TCP port 3389.

Explanation

You must enable inbound connections to TCP port 5985 for WinRM over HTTP in order for Windows Admin Center to manage the target VM. WinRM access can be enabled at the command prompt on the target VM by typing the following:

```
Winrm quickconfig
```

In order for Windows Admin Center to manage the target VM, an inbound connection to port 5985 for WinRM over HTTP must be enabled. The following will inbound connections to port 5985 on the guest OS:

```
Set-NetFirewallRule -Name WINRM-HTTP-In-TCP-PUBLIC -RemoteAddress Any
```

Inbound TCP ports 80 and 443 are used if you have IIS on your VM which needs to be publicly accessible.

Inbound TCP port 3389 is used for remote desktop connection access to VM.

Inbound TCP ports 20 and 21 are used for FTP access.

Objective:
Configure and manage virtual networking

Sub-Objective:
Configure secure access to virtual networks

References:

Microsoft Docs > Windows Server > Manage Azure IaaS virtual machines with Windows Admin Center

---

Question #25 of 50

Question ID: 1477224

You are the Azure administrator for the Nutex Corporation. You are responsible for your business continuity/disaster recovery (BC/DR) solution and planning. You want to use Azure Site Recovery (ASR) and a Hyper-V Replica for VM workloads running on Hyper-V and VMWare VMs and physical Windows/Linux servers. You have to identify which replication type can be used for which BC/DR solution.

Match the workload replication from the left to its appropriate destination on the right.

{UCMS id=6471289562726400 type=Activity}

Explanation

You can replicate your VM workloads through Azure Site Recovery (ASR) from an on-premises Hyper-V host server in the VMM cloud with SAN storage to a secondary VMWare site with SAN storage. You can replicate your VM workloads through ASR from an on-premises Hyper-V host server in VMM cloud, on-premises Hyper-V site (no VMM), or an on-premises physical server to Azure Storage.

You can replicate your VM workloads through ASR from an on-premises VMWare server and on-premises Hyper-V host sever in the VMM cloud to a secondary VMWare site.

You can replicate your VM workloads through ASR from an on-premises physical server to a secondary datacenter.

You can replicate your VM workloads through ASR from an on-premises VMWare server to a secondary VMWare site.

The following table summarizes the workloads' replication from source to destination:

REPLICATE	REPLICATE FROM	REPLICATE TO
Workloads running on VMware VMs	On-premises VMware server	Azure storage
Workloads running on VMware VMs	On-premises VMware server	Secondary VMware site
Workloads running on Hyper-V VMs	On-premises Hyper-V host server in VMM cloud	Azure storage
Workloads running on Hyper-V VMs	On-premises Hyper-V host server in VMM cloud	Secondary VMM site
Workloads running on Hyper-V VMs	On-premises Hyper-V host server in VMM cloud with SAN storage	Secondary VMM site with SAN storage
Workloads running on Hyper-V VMs	On-premises Hyper-V site (no VMM)	Azure storage
Workloads running on physical Windows/Linux servers	On-premises physical server	Azure storage
Workloads running on physical Windows/Linux servers	On-premises physical server	Secondary datacenter

Objective:
Monitor and maintain Azure resources

Sub-Objective:
Implement backup and recovery

References:

Microsoft Azure > Site Recovery > About Site Recovery

Question #26 of 50

Question ID: 1422637

You are a consultant for a large university in the East Southern Conference. The university's athletic department consists of several autonomous teams (football, basketball, baseball, softball, and so on). Each athletic team has a staff of IT admins who manage users, control access, and set policies for their team.

Since the football team makes millions for the university, the university wants to ensure that athletes on the football team are not subject to the same academic rigors as other students. You are tasked with ensuring that only a person associated with the football team has administrative permissions over only Azure AD users on the football team.

What should you do? (Choose four.)

A) **Create a role with administrative permissions over only Azure AD users in the football team administrative unit**
B) **Create an administrative unit for the football team**
C) Create a role with administrative permissions over only Azure AD users in the football team organizational unit
D) **Add the football IT team to the role, along with its scope**
E) Populate the administrative unit with only the virtual machines of the football players and staff
F) Populate the organizational unit with only the virtual machines of the football players and staff
G) **Populate the administrative unit with the football players and staff**

Explanation

You should choose the following:

1. Create an administrative unit for the football team.
2. Populate the administrative unit with the football players and staff.
3. Create a role with administrative permissions over only Azure AD users in the football team administrative unit.
4. Add the football IT team to the role, along with its scope.

An administrative unit is used as a container for other resources in Azure AD. An administrative unit contains only users and groups, not devices such as virtual machines.

Administrative units can restrict the administrative scope of different divisions in an organization. In this scenario, each team has a staff of IT administrators who can manage users, control access, and set policies for their team.

You should first create an administrative unit for the team. You can create and delete administrative units in the Azure Portal, PowerShell, and Graph. You cannot create or delete administrative units with the Microsoft 365 admin center.

You should then add the appropriate users and group members of the appropriate team to the administrative unit.

You can create a role with administrative permissions over only Azure AD users in the football team administrative unit.

After the role is created, you can assign the IT staff of the appropriate team to the role.

You should not populate the administrative unit with virtual machines. An administrative unit contains only users and groups,

You should not create an organizational unit. An organizational unit (OU) is a container in an Active Directory domain. An OU is not part of Azure Active Directory. An OU can contain Active Directory objects such as users, groups, and devices.

Objective:
Manage Azure identities and governance

Sub-Objective:
Manage Azure Active Directory (Azure AD) objects

References:

Administrative units in Azure Active Directory | Microsoft Docs

Question #27 of 50

Question ID: 1477222

You are the Azure administrator for the Nutex Corporation. You want to use the Azure command line utility **AzCopy** in combination with Azure WebJobs to build your own Azure Storage backup utility. This solution has to back up Azure storage objects asynchronously and continuously from an Azure storage container to another container in another account. You previously have created an Azure website and all necessary WebJobs. You want the backup to be a combination of weekly full backups and incremental daily backups.

Because of the default Azure WebJobs behavior, you have to alter the WebJob. You set the WebJob run mode option of **Run Continuously** so that AzCopy can run multiple times simultaneously.

Which of the following are the relevant configuration steps for the logical model for this solution?

A) Use Azure Websites, Azure Storage, and Azure Site Recovery.
Create three Azure Scheduler tasks and three Azure WebJobs as backup jobs.

Use WebJobs Logs.

B) Use Azure Websites, Azure Storage, and Azure Recovery.
Create two Azure Scheduler tasks and three Azure WebJobs as backup jobs.

Use WebJobs Queues.

C) Use Azure Websites, Azure Storage, and Azure Scheduler.
Create two Azure Scheduler tasks and three Azure WebJobs as backup jobs.

Use WebJobs Queues.

D) Use Azure Websites, Azure Storage, and Azure Recovery.
Create three Azure Scheduler tasks and three Azure WebJobs as backup jobs.

Use WebJobs Queues.

E) Use Azure Websites, Azure Storage, and Azure Site Recovery.
Create two Azure Scheduler tasks and three Azure WebJobs as backup jobs.

Use WebJobs Logs.

F) Use Azure Websites, Azure Storage, and Azure Scheduler.
Create three Azure Scheduler tasks and two Azure WebJobs as backup jobs.

Use WebJobs Logs.

Explanation

You should do the following:

- Use Azure Websites, Azure Storage, and Azure Scheduler.
- Create two Azure Scheduler tasks and three Azure WebJobs as backup jobs.
- Use WebJobs Queues.

You should create three WebJobs for the solution: a full backup job, an incremental backup job, and a BackupExec WebJob with a Queue.BatchSize of 1.

Normally, a continuously running WebJob will read and process up to 16 messages at one time from a queue. AzCopy can run only once per host process, so you have to modify the BackupExec WebJob code to ensure that AzCopy is running once per JobHost process.

You should create two Azure Schedulers: one for a weekly full backup and another for a daily incremental backup.

The WebJobs Storage offers two possibilities: WebJobs Logs and WebJobs Queue. In this case, you use the WebJobs queue for the AzCopy WebJobs to ensure that AzCopy can run multiple times simultaneously. During the backup process, blobs will be copied from the Azure source account to the Azure backup account. This is where the effective backup/copy process will be done.

You should not choose to use Azure Websites, Azure Storage, and Azure Recovery because you have to use Azure Scheduler to schedule the WebJobs to run.

You should not choose to use Azure Websites, Azure Storage, and Azure Site Recovery because you have to use Azure Scheduler to schedule the WebJobs to run.

Objective:
Monitor and maintain Azure resources

Sub-Objective:
Implement backup and recovery

References:

Documentation > Machine Learning > Move Data to and from Azure Blob Storage using AzCopy

Automating backups with Azure WebJobs and AzCopy

Question #28 of 50

Question ID: 1285335

You are trying to ensure that new VMs created to support a sales application will be located in the EastUS region. You plan to edit the Azure Resource Manager template to make this happen in an automated fashion.

Is it necessary for the resource group object, virtual network interface object, the virtual machine object, and the virtual network object to reside in the EastUS region?

A) Yes

B) No

Explanation

No, you can create resource groups in different regions that may store resource objects that are in the local region.

When you are creating resource groups, the `location` parameter defines where the metadata for each object in the resource group is going to be maintained. Therefore, it should be specified in the resource group template. However, the resources in that resource group could be located in different regions.

When creating objects in a resource group, only the metadata is stored in the same location if you put the object being defined into another location.

For instance, you can create a virtual machine in the EastUS location using a resource group that has its location set to WestUS. With this knowledge, when editing the template for the sales application VMs, the virtual machine should set the location to EastUS.

The virtual network interface and virtual network should also be created in EastUS if you want them to be used on the virtual machine and still function properly.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Create and configure VMs

References:

Microsoft Azure > Resource Manager > What is Azure Resource Manager? > Resource Groups

Microsoft Azure > Networking > Create, change, or delete a network interface

Microsoft Azure > Virtual Machines > Windows > Create a Windows virtual machine from a Resource Manager template

---

Question #29 of 50

Question ID: 1477218

You are told that one of the Azure VM web servers supporting the Nutex Sales web application is returning a recently edited home page full of errors. You suspect the edits to the page have managed to make it unusable, and by restoring that page from a recent backup, you might resolve the problem. The backups are being run by policy and maintained in an Azure Recovery Services vault.

What steps must you perform to restore ONLY this file?

Choose the appropriate steps and place them in the correct order.

{UCMS id=5654307875586048 type=Activity}

Explanation

You should choose the following steps:

1. In Azure Cloud Shell identify an appropriate recovery point.
2. Generate and download a script and password necessary to mount the recovery point.
3. Copy the recovery point mount script to the VM in question and run it.
4. Copy the backed up version of the file in the mounted recovery point to its original location.
5. Unmount the recovery point.

In order to restore just a file from an Azure Backup-protected VM, an appropriate recovery point must be identified. This will require some commands to be run in the Azure Cloud Shell. The `az backup recoverypoint list` command lists the most recent recovery points. The following example lists recovery points for the VM named VM1 that is protected in `RecoveryServicesVault1`.:

```
az backup recoverypoint list \
    --resource-group ResourceGroup1 \
    --vault-name RecoveryServicesVault1 \
    --container-name VM1 \
```

```
    --item-name VM1 \
    --query [0].name \
    --output tsv
```

Once the recovery point is identified, a script that mounts the recovery point as a usable volume must be generated and downloaded. This will also return a password meant to be used with the script.

The script must be copied to, and run on, the VM where the file is broken, in order to restore that file from the mounted recovery point. The following example obtains the script for the VM named VM1 that is protected in `RecoveryServicesVault1`, and uses the recovery point named `RecoveryPointName1`:

```
az backup restore files mount-rp \
    --resource-group ResourceGroup1 \
    --vault-name RecoveryServicesVault1 \
    --container-name VM1 \
    --item-name VM1 \
    --rp-name RecoveryPointName1
```

After the file is copied back to its original location (overwriting the broken version), the recovery point should be unmounted on the VM and also in the Azure Cloud Shell.

You should not copy the backed up version of the file in the mounted recovery point to a new location. It should overwrite the file in its original location.

Objective:
Monitor and maintain Azure resources

Sub-Objective:
Implement backup and recovery

References:

Microsoft Azure > Backup > Restore files to a virtual machine in Azure

---

Question #30 of 50

Question ID: 1530437

Your organization, the Verigon Corporation, has an Azure subscription in the West US region. You are creating a Storage account in the same Azure region. There are business applications hosted in Azure in the same region.

You want to implement Azure Storage redundancy. You have the following requirements:

- Lowest cost-redundancy
- Provides at least 99.999999999% durability for business applications
- Replicates your storage account synchronously three times within a single physical location in the primary region
- Restricts replication of data to only the US region to meet regulatory requirements

Which of the following Azure storage redundancy options should you use?

A) Geo-zone-redundant storage

B) Geo-redundant storage

C) Zone-redundant storage

D) **Locally redundant storage**

Explanation

You would use locally redundant storage (LRS) in the primary West US region. Azure Storage accounts replicate data three times in the primary region. It also provides 99.999999999% durability of objects within a given year. LRS is considered a low-cost redundancy option over ZRS, GZRS, and GRS. You would opt for LRS when your applications are restricted to replicating data only within a country due to regulatory requirements. This redundancy option is the least expensive and is not recommended for applications that require high availability or durability.

You would not use the zone-redundant storage (ZRS) option in the primary West US region. ZRS replicates the data synchronously across three Azure availability zones in the primary region. This option is recommended for applications that require high availability. It provides availability for the storage resources of at least 99.9999999999% over a given year and is the recommended option for Azure Files workloads. It is the perfect choice should your data become unavailable since it allows low latency, superior performance, and high resiliency.

You would not use the geo-zone-redundant storage (GZRS) option in the primary West US region. GZRS is one of the redundancy options Azure Storage provides for replicating your data to a secondary region. Using this option, data is replicated synchronously across three Azure availability zones in the primary region and then replicated to a secondary

region for protection from regional disasters. This redundancy option is recommended for applications requiring top-notch performance, durability, high availability, and resiliency. GZRS provides 99.99999999999999% durability of objects over a given year.

You would not use the geo-redundant storage (GRS) option in the primary West US region. GRS is one of the redundancy options Azure Storage provides for replicating your data to a secondary region. Using this redundancy option, data is synchronously replicated three times within the primary location. Data is then asynchronously replicated to a datacenter in a secondary region far away from the primary region. GRS provides at least 99.99999999999999% durability of objects over a given year.

Objective:
Implement and manage storage

Sub-Objective:
Manage data in Azure storage accounts

References:

Microsoft Learn > Azure > Storage > Azure Storage redundancy

Question #31 of 50

Question ID: 1477129

You are the administrator for the Nutex Corporation. You have some on-premises file servers, and you use Azure File Sync to synchronize files to Azure File Storage. You do not use an LDAP-based directory solution in Azure. You want to force AD permissions on your file share directly in the cloud.

Which of the following prerequisites is needed?

A) Join a premium file shares storage account to Azure AD

B) Synchronize through ADSync

C) Join storage account to on-premises Active Directory (AD)

D) **Join a standard general purpose v2 storage account to Azure AD**

Explanation

You would join a storage account to the on-premises AD. Integrating Active Directory Domain Services (AD DS) with Azure Files is a method for storing directory data that is then available to users and administrators. Security is integrated with AD DS through logon authentication and access control to objects in the directory. Windows-style discretionary access control lists (ACLs) are used by Azure File Sync and enforced on server endpoints by Windows Server.

When directly mounting the Azure file share, ACLs can also be enforced with additional configuration. When changes are made directly to the Azure file share, they take longer to sync to the server endpoints in the sync group. You should enforce your AD permissions on your file share directly in the cloud as well. This can be accomplished by domain joining your storage account to your on-premises AD, similar to joining a Windows file server to a domain.

You would not synchronize through ADSync because, with the ADSync service, you synchronize identities between on-premises AD and AAD, and you do not force AD permissions on your file share directly with that.

You would not join a storage account whether it is a general purpose v2 storage account or a premium file shares storage account to Azure AD because this will not force AD permissions on your file share directly in the cloud. Also interesting here, Azure AD-joined Windows virtual machines (VMs) cannot access Azure file shares with your Azure AD credentials.

Objective:
Implement and manage storage

Sub-Objective:
Configure access to storage

References:

Microsoft Docs > Azure > Storage > File Sync > Planning for an Azure File Sync deployment > Identity

Microsoft Docs Azure > Storage > Files > Overview of Azure Files identity-based authentication options for SMB access

Microsoft Docs > Windows Server > Windows Commands > Commands by Server Role > robocopy

Microsoft Docs > Azure > Active Directory > Hybrid Identity > Azure AD Connect sync service features

---

Question #32 of 50

Question ID: 1530443

Your organization, the Nutex Corporation, has an Azure Active Directory (Azure AD) environment. You have virtual machines that are hosted in Azure. Details for the resources are as follows:

Resource	Resource Name
Key Vault Resource Group	KVResGrp1
VMs	VM1, VM2, VM3
Virtual Machine Resource Group	VMResGrp1
Key Vault	KeyVault1

You are enabling encryption on VM1, VM2, and VM3. Below is the PowerShell script you will use to do this:

```
$KVRGname = 'KVResGrp1';
$VMRGName = 'VMResGrp1';
$vmName = 'VM1', 'VM2', 'VM3';
$KeyVaultName = 'KeyVault1';
$KeyVault = A
-VaultName $KeyVaultName -ResourceGroupName $KVRGname;
$diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;
$KeyVaultResourceId = $KeyVault.ResourceId;
B
-ResourceGroupName $VMRGname -VMName $vmName -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -DiskEncryptionKeyVaultId
$KeyVaultResourceId;
```

Drag the missing cmdlets, parameters, or values to the appropriate letter.

{UCMS id=5196368780984320 type=Activity}

Explanation

You would choose the following:

Cmdlets, parameters, or values	A	B
Get-AzKeyVaultKey	Get-AzKeyVault	Set-AzVMDiskEncryptionExtension
Get-AzKeyVault		
Set-AzVMDiskEncryptionExtension		
Get-AzVmDiskEncryptionStatus		
az vm encryption enable		
az vm encryption show		

Below is the complete script with the correct values.

```
$KVRGname = 'KVResGrp1';
$VMRGName = 'VMResGrp1';
$vmName = 'VM1', 'VM2', 'VM3';
$KeyVaultName = 'KeyVault1';
$KeyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $KVRGname;
$diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;
$KeyVaultResourceId = $KeyVault.ResourceId;

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGname -VMName $vmName -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -
DiskEncryptionKeyVaultId $KeyVaultResourceId;
```

The **Get-AzKeyVault** cmdlet displays the key vault information, such as the vault name, resource group name, location, and resource ID, of the key vaults in a subscription. This cmdlet will display all of the key vault instances in a subscription.

The above script initializes the variables and runs the **Set-AzVMDiskEncryptionExtension** cmdlet to enable encryption on running VMs in the Azure cloud.

The **Get-AzKeyVaultKey** cmdlet is not the correct cmdlet to use in the given script. This cmdlet is used to get key vault keys, not the name of the key vault.

The **Get-AzVMDiskEncryptionStatus** cmdlet is not the correct cmdlet to use in the given script. This cmdlet displays the encryption status of the VMs running in the Azure cloud.

The `az vm encryption enable` command would not be used in the given script. It is an Azure CLI command that enables encryption when using Azure CLI scripts, not PowerShell.

The `az vm encryption show` command would not be used in the given script. It is an Azure CLI command that displays the encryption status of the VMs running on the Azure cloud.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Create and configure VMs

References:

Microsoft Learn > Azure > Virtual Machines > Windows > Azure Disk Encryption scenarios on Windows VMs

Microsoft Learn > Azure > Azure PowerShell > Reference > Key Vault > Get-AzKeyVault

---

Question #33 of 50

Question ID: 1481902

You are the Azure administrator for the Nutex Corporation. Nutex needs to limit threats, such as port scanning and malware, that target its VMs in Azure. The company should maintain seamless RDP and SSH access to the VMs.

You have a virtual network named VNET1 that consists of the following:

- SubnetA, which has an address space of 10.10.0.0/24
- SubnetB, which has an address space of 10.10.1.0/24

You have two VMs named Srv10 and Srv11 deployed in SubnetB. All of the VMs have Remote Desktop enabled.

You must configure an Azure Bastion to protect the VMs. Which steps should you perform? Place the appropriate steps in the correct order.

{UCMS id=5762314306322432 type=Activity}

Explanation

You should perform these steps:

1. Create a subnet named AzureBastionSubnet with a /26 mask.
2. Add AzureBastionSubnet to VNET1.
3. Add a public IP address to the Azure Bastion.

Azure Bastion allows RDP and SSH connectivity to your VMs in a provisioned virtual network. The bastion host is deployed in a subnet that MUST be called **AzureBastionSubnet**. All other names are incorrect.

The **AzureBastionSubnet** subnet must support at least 30 hosts. The subnet mask must be at least /26 or larger (/26, /25, /24, etc.). The following example creates the **AzureBastionSubnet** subnet with a network address of 10.0.0.0/26 in the virtual network VNET1 within a resource group named NutexResourceGroup in the East US:

```
$subnetName = "AzureBastionSubnet"
$subnet = New-AzVirtualNetworkSubnetConfig -Name $subnetName -AddressPrefix 10.0.0.0/26
$vnet = New-AzVirtualNetwork -Name "VNET1" -ResourceGroupName "NutexResourceGroup" -Location "eastus" -AddressPrefix 10.10.0.0/16 -Subnet
$subnet
```

You must use the **New-AzPublicIpAddress** cmdlet to create a public IP address for the Azure Bastion. This public IP address MUST be in the same region as the Azure Bastion resource. The following creates a public IP address in the East US:

```
$IpAddress = New-AzPublicIpAddress -ResourceGroupName "NutexResourceGroup" -name "myPublicIP" -location "eastus" -AllocationMethod Static -Sku
Standard
```

It would be best if you used the **New-AzBastion** cmdlet to create the Azure Bastion resource in the AzureBastionSubnet of your virtual network. It can take several minutes for the Bastion resource to deploy.

```
$bastion = New-AzBastion -ResourceGroupName "NutexResourceGroup" -Name "myBastion" -PublicIpAddress $IpAddress -VirtualNetwork $vnet
```

You do not need to create a new virtual network. You have to create a new subnet named **AzureBastionSubnet**, but it can be part of the same virtual network.

The VMs named Srv10 and Srv11 deployed in SubnetB do not need public IP addresses. The bastion host will have a public IP address. The public IP address of the bastion host resource must reside in the same region as the bastion host resource. The deployment of the bastion host will allow you to connect to the Srv10 and Srv11 using their private IP addresses.

Objective:
Configure and manage virtual networking

Sub-Objective:
Configure secure access to virtual networks

References:

Microsoft Docs > Azure > Networking > Bastion > Deploy Bastion using Azure PowerShell

---

Question #34 of 50

Question ID: 1477198

You are the administrator of the Nutex Corporation. You want to monitor and troubleshoot your external networking through Azure Network Watcher's VPN troubleshooting.

Which gateways and connections are supported with Network Watcher troubleshooting?

Move each gateway, VPN, or connection type to the column that indicates whether or not it is supported by Network Watcher.

{UCMS id=5707680058441728 type=Activity}

Explanation

You should choose the following:

Gateway, VPN, or Connection Type	Supported	Not Supported
Gateway type: VPN	Gateway type: VPN	Gateway type: ExpressRoute
Gateway type: ExpressRoute	Route based VPN type	Policy based VPN type
Route based VPN type	Connection type: IPSec	Connection type: ExpressRoute
Policy based VPN type	Connection type: VNet2Vnet	Connection type: VPNClient
Connection type: IPSec		
Connection type: VNet2Vnet		
Connection type: ExpressRoute		
Connection type: VPNClient		

Network Watcher supports VPN gateways, route-based VPNs, and IPSec and VNet2VNet connection types.

ExpressRoute gateways are not supported.

You cannot troubleshoot policy-based VPNs with Network Watcher.

You cannot monitor or troubleshoot ExpressRoute connections with Azure Network Watcher's VPN troubleshooting tool. However, you can use the Network Watcher Network Performance Monitor (NPM) to monitor ExpressRoute connections.

Objective:
Configure and manage virtual networking

Sub-Objective:
Monitor virtual networking

References:

Microsoft Azure > Networking > Network Watcher > Introduction to resource troubleshooting in Azure Network Watcher

Microsoft Azure > Networking > ExpressRoute > Configure Network Performance Monitor for ExpressRoute

---

Question #35 of 50

Question ID: 1477092

As the Azure Architect, you are required to design a strategy for Azure roles to be used in your new tenant.

System administrators who are new to Azure are not sure what the difference is between Azure RBAC roles and Azure AD administrator roles.

Which statements are true for Azure RBAC roles? (Choose three.)

A) Scope is at the tenant level.

B) Role information can be accessed in Microsoft Graph.

C) Role information can be accessed in Azure CLI.

D) Manage access to Azure Active Directory resources.

E) Scope can be specified at multiple levels (subscription, resource group, resource).

F) Manage access to Azure resources.

Explanation

In Azure RBAC roles, information can be accessed in Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, and REST API. Scope in Azure RBAC can be specified at multiple levels (management group, subscription, resource group, resource). RBAC roles can manage access to Azure resources.

Role information cannot be accessed in Microsoft Graph because that is available only for Azure AD administrator roles.

The scope of a role is not at the tenant level for most roles. Only Azure AD administrator roles have a scope at the tenant level.

You cannot manage access to Azure Active Directory resources for most roles. You can control access to Azure Active Directory resources only for Azure AD administrator roles.

Objective:
Manage Azure identities and governance

Sub-Objective:
Manage Azure subscriptions and governance

References:

Microsoft Azure > Role-based access control > Classic subscription administrator roles, Azure RBAC roles, and Azure AD administrator roles > Differences between Azure RBAC roles and Azure AD administrator roles

---

Question #36 of 50

Question ID: 1477143

Viruart, Inc. has a variety of on-premises servers, websites, and Hyper-V machines that they want to migrate to Azure. VirtuArt also wants to add some new computing tasks. Azure offers many options for creating virtual machines and websites. You need to choose the appropriate cmdlet or method to perform the following tasks:

Task A - Upload an existing on-premises VHD in Azure
Task B - Create a single VM based on an image
Task C - Add a VM using an existing OS disk and VM configuration file
Task D - See a list of available images to use for building VMs

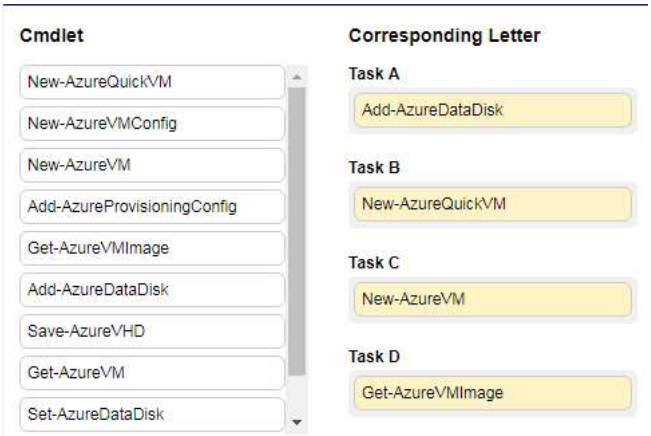
To answer, drag the appropriate cmdlet or method to the correct task. Each cmdlet may be used only ONCE. Not all cmdlets will be used.

{UCMS id=6268009482027008 type=Activity}

Explanation

You should choose the following:

Task A - **Add-AzureVHD**
Task B - **New-AzureQuickVM**
Task C - **New-AzureVM**
Task D - **Get-AzureVmImage**



You would run the **Add-AzureVHD** cmdlet to use an existing on-premises VHD with Azure. This cmdlet uploads an on-premises VHD to Azure. If you have a VHD that you are already using on-premises, this is an easy way to make it available for use with your Azure virtual machines. You will need to **sysprep** it before uploading to Azure. This cmdlet currently only works with VHD format virtual disks, not VHDX.

You would use **New-AzureQuickVM** to create a single VM based on an image. This is best for a one-off creation with a simple configuration. This cmdlet only works with an image; you cannot use this to create a VM from a disk. This cmdlet does not accept the configuration cmdlets (**New-AzureVMconfig**) for input.

You would use **New-AzureVM** to add a VM to Azure using an existing OS disk and VM configuration file. The configuration file can be created with the **New-AzureVMconfig** cmdlet. The configuration can include options not available with the **New-AzureQuickVM** cmdlet, such as setting the time zone, or including AD domain join information.

You would use **Get-AzureVMImage** to see a list of available images to use for building VMs. The **Get-AzureVM** cmdlet would allow you to see information on a single VM or multiple VMs on a cloud service, but would not list available images.

You should not choose **New-AzureWebsite**. This cmdlet allows you to create a website in Azure. If you wanted to use the Azure Portal to create a website, you would choose **App Services**, then **Add**. Websites created in Azure are now referred to as web apps.

You would not use the **New-AzureVMconfig** cmdlet to perform any of the listed tasks directly. This cmdlet would be used to create a configuration file for use with **New-AzureVM**.

You would not use the **Save-AzureVHD** cmdlet to perform any of the tasks listed. It is the reverse of the **Add-AzureVHD** cmdlet, and can be used to download VHDs from Azure blob storage to a local file.

You would not use the **Add-AzureDataDisk** cmdlet to perform any of the tasks listed. This cmdlet add a new data disk to a virtual machine object.

You would not use the **Set-AzureDataDisk** cmdlet to perform any of the tasks listed. This cmdlet sets the host-cache mode on an existing data disk object.

You should not use the **Add-AzureProvisioningConfig** cmdlet to perform any of the tasks listed. This cmdlet adds the provisioning configuration to an Azure virtual machine.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Automate deployment of resources by using templates

References:

Microsoft Azure > PowerShell > New-AzureVM

Microsoft Azure > PowerShell > New-AzureQuickVM

Microsoft Azure > PowerShell > Add-AzureVhd

Microsoft Azure > PowerShell > Get-AzureVMImage

Microsoft Azure > Virtual Machines > Windows > Upload a generalized VHD and use it to create new VMs in Azure

---

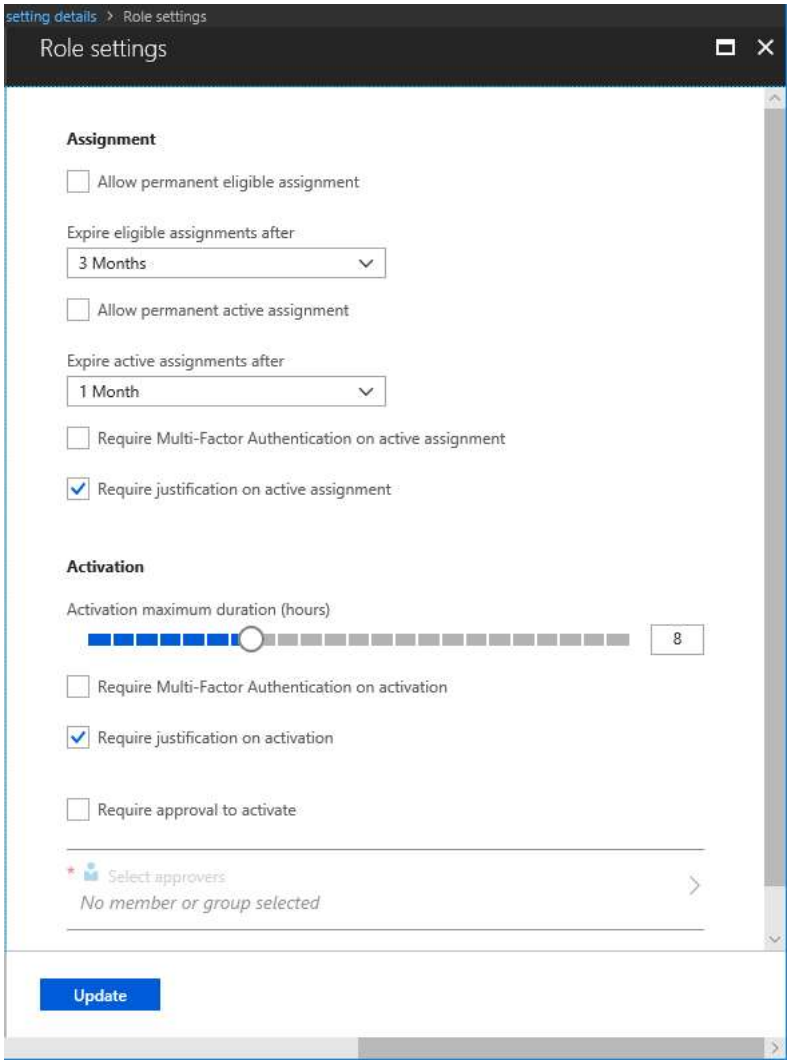
Question #37 of 50

Question ID: 1477082

You are a cloud administrator of the Nutex Corporation. You are responsible for RBAC, multi-factor authentication (MFA), and Privileged Identity Management. You want to configure the following Azure resource configuration for the BizTalk Contributor role:

- Resource administrators can assign permanent eligible membership.
- Eligible members are required to run MFA before they can activate.

Select the appropriate setting in the following configuration window (choose all that apply):



A) **35,118,286,152**

B) **39,495,419,528**

C) 37,314,410,344

D) 37,587,425,625

E) 38,212,292,248

Explanation

You would select the following:

- Allow permanent eligible assignment
- Require Multi-Factor Authentication on activation.

The “Allow permanent eligible assignment” setting allows resource administrators to assign permanent eligible membership for the role.

The “Require Multi-Factor Authentication on activation” setting verifies that the user who is requesting activation.

You want to enforce MFA when the user activates as well as when they use their role assignments. This is why you would choose “Require Multi-Factor Authentication on activation” instead of “Require Multi-Factor Authentication on active assignment”, which is only for a short duration. This is so that role members use MFA before they activate.

You do not have to set the “Require approval to activate” setting. Nothing in the scenario suggests that this is needed.

Objective:
Manage Azure identities and governance

Sub-Objective:
Manage access control

References:

Microsoft Azure > Active Directory > Configure Azure resource role settings in Privileged Identity Management

Question #38 of 50

Question ID: 1480117

Your Azure subscription has an Azure container registry.

You create an Azure Kubernetes Service cluster that uses Kubernetes version 1.2.2.

You want to integrate the AKS cluster with your Azure container registry.

What should you configure?

A) Upgrade Kubernetes to version 1.2.3 or later.

B) Configure the authentication method to use an Azure Active Directory managed identity.

C) Configure the authentication method to use a shared access signature (SAS).

D) Specify `winscontainer` as the container runtime for the node pool within the AKS cluster.

E) Specify `containerd` as the container runtime for the node pool within the AKS cluster.

Explanation

To integrate Azure Container Registry (ACR) with Azure Kubernetes Service (AKS), you must use an authentication mechanism for ACR and AKS to interact. An Azure Active Directory **managed identity** is used to allow an AKS cluster to interact with ACR.

A managed identity for Azure resources can authenticate seamlessly to an Azure container registry from another resource in Azure. The managed identity does not need to provide or manage registry credentials. A managed identity on a Linux VM can read container images in your Azure Container Registry. You could also configure your AKS cluster to pull container images from ACR by using a managed identity.

The version of Kubernetes would not matter in this scenario. Kubernetes version 1.2.2 can allow an AKS cluster to integrate with ACR.

You would not configure the authentication method to use a shared access signature (SAS). An SAS is a URI that grants restricted access rights to your storage account without compromising the security of your data. SAS is a way to grant clients limited access to objects in your storage account. In addition, you do not have to expose your account key. This is important with untrusted clients. By distributing an SAS URI to these users, you can grant them access to a resource for a specified period of time with a specified set of permissions. An SAS will not act as an authentication method between ACR and AKS.

You would not specify either `winscontainer` or `containerd` as the container runtime for the node pool within the AKS cluster. `containerd` is the name of the container runtime for Windows Server node pools. You will need this if you are adding Windows servers to a container. `winscontainer` is not the name of the container runtime for Windows Server node pools in a container. Configuring the name of the container runtime for Windows Server node pools will not act as an authentication method between ACR and AKS.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Create and configure containers

References:

Microsoft Docs > Azure > Container Registry > Use an Azure managed identity to authenticate to an Azure container registry

Microsoft Docs > Azure > AKS > Authenticate with Azure Container Registry from Azure Kubernetes Service

Question #39 of 50

Question ID: 1477187

You are the administrator of the Nutex Corporation. You have created the following Azure NSG Firewall rule with the **New-AzNetworkSecurityRuleConfig** PowerShell cmdlet to allow TCP traffic on port 80:

```
$httprule = New-AzNetworkSecurityRuleConfig
-Name "NutexNetworkSecurityGroupRule"
-Description "Allow HTTP"
-Access "Allow"
-Protocol "Tcp"
-Direction "Inbound"
-Priority "100"
-SourceAddressPrefix "Internet"
-SourcePortRange *
```

```
-DestinationAddressPrefix *
-DestinationPortRange 80
```

You want to assign this rule to a subnet named **NutexSubnet**. What are the next steps? Choose the appropriate cmdlets and place them in the correct order.

{UCMS id=4513059521429504 type=Activity}

Explanation

The correct sequence of cmdlets is:

```
New-AzNetworkSecurityGroup
Get-AzVirtualNetwork
Set-AzVirtualNetworkSubnetConfig
Set-AzVirtualNetwork
```

You would first use the **New-AzNetworkSecurityGroup** cmdlet to create your network security group and assign the HTTP rule you just created as follows:

```
$nsg = New-AzNetworkSecurityGroup -ResourceGroup Name "NutexResourceGroup" -Location "WestUS" -Name "NutexNetworkSecurityGroup" -SecurityRules
$httprule
```

You would then use the **Get-AzVirtualNetwork** cmdlet to assign your network security group to a subnet. For example, the following assigns the network security group `myResouceGroup` to the subnet named `myVnet`:

```
Get-AzVirtualNetwork -ResourceGroupName "NutexResourceGroup" -Name "NutexVnet"
```

You would then use the **Set-AzVirtualNetworkSubnetConfig** cmdlet to associate your network security group with your subnet. The following example associates the subnet named `NutexSubnet` with the network security group stored in the `$nsg` variable:

```
$subnetPrefix = $vnet.Subnets|?{$_.Name -eq 'NutexSubnet'};
Set-AzVirtual NetworkSubnetConfig -VirtualNetwork $vnet -Name "NutexSubnet" -AddressPrefix $subnetPrefix. AddressPrefix -NetworkSecurityGroup
$nsg
```

At the end, you would use the **Set-AzVirtualNetwork** cmdlet to update your virtual network with the changes.

Objective:
Configure and manage virtual networking

Sub-Objective:
Configure secure access to virtual networks

References:

Microsoft Azure > Virtual Machines > Windows > How to open ports and endpoints to a VM in Azure using PowerShell

---

Question #40 of 50

Question ID: 1477204

The Verigon company website has been successfully migrated to Azure. Verigon wants to keep a tight budget on Azure spending when possible. Auto-scaling up to seven instances has been sufficient to meet the company needs so far. However, careful analysis of the usage statistics, SQL performance, and a few other metrics has not been satisfactory. You have decided that switching to four cores for each instance will alleviate the bottleneck.

What change should you make using the Azure portal?

- **A)** On the **Settings** blade, choose to **Scale Up**, and make a **Premium** pricing tier selection.
- **B)** On the **Settings** blade, choose to **Scale Up**, and choose any selection marked with a star.
- **C)** **On the Settings blade, choose to Scale Up, and choose S2 Standard.**
- **D)** On the **Settings** blade, choose to **Scale Up**, and choose **S3 Standard**.
- **E)** On the **Settings** blade, choose to **Scale Up**, and choose **B3 Standard**.

Explanation

You should go to the **Settings** blade, choose to **Scale Up**, and choose **S3 Standard** for your pricing tier. The scenario indicates that Verigon is taking advantage of auto-scaling, so you are already on the Standard pricing tier. You need to move to the S3 instance size to meet the requirement for four cores, which will also increase RAM from 3.5 to 7 GB.

The instance sizes are now numbered. In previous versions of the plans, they were labelled Small, Medium, and Large.

You would not choose to **Scale Up** and choose S2 Standard. The S2 size only supports two cores.

You would not choose to **Scale Up** and make a Premium pricing tier selection. You need to change the instance size, not the other environmental options. The Standard pricing tier already meets your feature needs; you just need a larger size.

You would not choose to **Scale Up** and choose any selection marked with a star. The settings with a star are the recommended instance sizes within each pricing tier, but a recommended selection would not necessarily offer four cores.

You would not choose to **Scale Up** and choose **B3 Standard**. While the "3" size meets the four-core requirement, the Basic pricing tier does not include the needed number of instances, or the auto-scaling referenced in the scenario.

You can easily switch between instance sizes or pricing tiers at any time. However, you may need to adjust any spending caps that you have placed on your account.

Note that auto-scaling only affects the number of instances. You cannot auto-scale the size of the instances.

Objective:
Monitor and maintain Azure resources

Sub-Objective:
Monitor resources by using Azure Monitor

References:

Microsoft Azure > App Service > Azure App Service plan overview

Microsoft Azure > Products > Azure pricing

Question #41 of 50

Question ID: 1285351

You are working on a new version of a custom application. The last revision of this application was plagued by common web-based attacks such as SQL injections, cross-site scripting attacks, and session hijacks.

You need to provide Layer 7 load balancing for a custom application that only uses the HTTPS protocol. Round robin distribution of incoming traffic must be provided. You also want to ensure that a user session is on the same back-end.

What solution should you recommend?

A) Azure Traffic Manager

B) Azure User Defined Routing (UDR)

C) **Azure Application Gateway**

D) Azure Load Balancer

Explanation

You should use Azure Application Gateway to provide Layer 7 load balancing for a custom application that only uses the HTTPS protocol. Azure Application Gateway provides round robin load balancing as well as the following features:

- Web application firewall
- Cookie-based session affinity, which saves the session state on the back-end server for a user session
- Secure Sockets Layer (SSL) offload.

You would not use Azure Traffic Manager. The Traffic Manager uses global DNS load balancing and endpoint monitoring. Azure Traffic Manager uses the round robin method. To avoid overwhelming the endpoints and a chain of failures in the next closest datacenter, the Traffic Manager will distribute traffic to endpoints in other datacenters. The round robin method distributes load across a set of endpoints in the same datacenter or across different datacenters. Azure Traffic Manager does not provide Layer 7 load balancing.

You would not use an Azure Load Balancer. This service can load balance incoming Internet traffic. This service does not offer SSL offloading or provide Layer 7 load balancing. You should use Azure Application Gateway if you need to have SSL offload or HTTPS request Application layer (Layer 7) processing.

You would not choose Azure User Defined Routing (UDR). UDR allows you to create network routes so that your third party devices can handle the traffic both between your subnets and to the Internet. UDR does not provide load balancing.

Objective:
Configure and manage virtual networking

Sub-Objective:
Configure load balancing

References:

Microsoft Azure > Networking > What is Azure Application Gateway?

Question #42 of 50

Question ID: 1480125

You plan to deploy an Azure web app with the following settings:

Name	NutexWebApp1035
Publish	Docker Container
Operating System	Windows
Region	Central US
App Service Plan	Windows Plan Asp-nutexresourcegroup-87d1
Zone Redundancy	Disabled
Application Insights	Disabled

Which setting should you modify to use the Java 17 runtime stack?

A) App Service Plan

B) Publish

C) Application Insights

D) Operating System

E) Zone Redundancy

Explanation

You should change the instance detail of Publish from **Docker Container** to **Code**.

Home > App Services >

Create Web App ...

Subscription * (Disabled) Microsoft Partner Network

Resource Group * nutex-resource-group

Create new

Instance Details

Need a database? Try the new Web + Database experience.

Name * NutexWebApp1035 .azurewebsites.net

Publish * Code Docker Container Static Web App

Runtime stack * Java 17

Java web server stack * Java SE (Embedded Web Server)

Operating System * Linux Windows

Region * Central US

Not finding your App Service Plan? Try a different region or select your App Service Environment.

App Service Plan

Review + create < Previous Next : Deployment >

Once you select **Code**, you have the option to choose a runtime stack, such as Java, ASP, PHP, or Ruby.

Home > App Services >

Create Web App ...

Subscription *

Resource Group *

Instance Details

Need a database? Try the new Web + Datab

Name *

Publish *

.NET

.NET 6 (LTS)

.NET Core 3.1 (LTS)

ASP.NET V4.8

ASP.NET V3.5

Java

Java 17

Java 11

Java 8

If you choose **Docker Container** as the setting for Publish, you cannot choose a runtime stack. However, you can use either the Windows or Linux operating system.

Home > App Services >

Create Web App ...

Basics Docker Networking (preview) Monitoring Tags Review + create

App Service Web Apps lets you quickly build, deploy, and scale enterprise-grade web, mobile, and API apps running on any platform. Meet rigorous performance, scalability, security and compliance requirements while using a fully managed platform to perform infrastructure maintenance. Learn more

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * (Disabled) Microsoft Partner Network

Resource Group * nutex-resource-group

Create new

Instance Details

Need a database? Try the new Web + Database experience.

Name * NutexWebApp1035 .azurewebsites.net

Publish * Code Docker Container Static Web App

Operating System * Linux Windows

Region * Central US

Not finding your App Service Plan? Try a different region or select your App Service Environment.

The App Service Plan is determined by the operating system that you choose. If you choose Windows then the App Service Plan will be a Windows plan.

Create Web App ...

Instance Details

Need a database? Try the new Web + Database experience.

Name * NutexWebApp1036 .azurewebsites.net

Publish * (•) Code ( ) Docker Container ( ) Static Web App

Runtime stack * .NET 6 (LTS)

Operating System * ( ) Linux (•) Windows

Region * Central US

Not finding your App Service Plan? Try a different region or select your App Service Environment.

App Service Plan

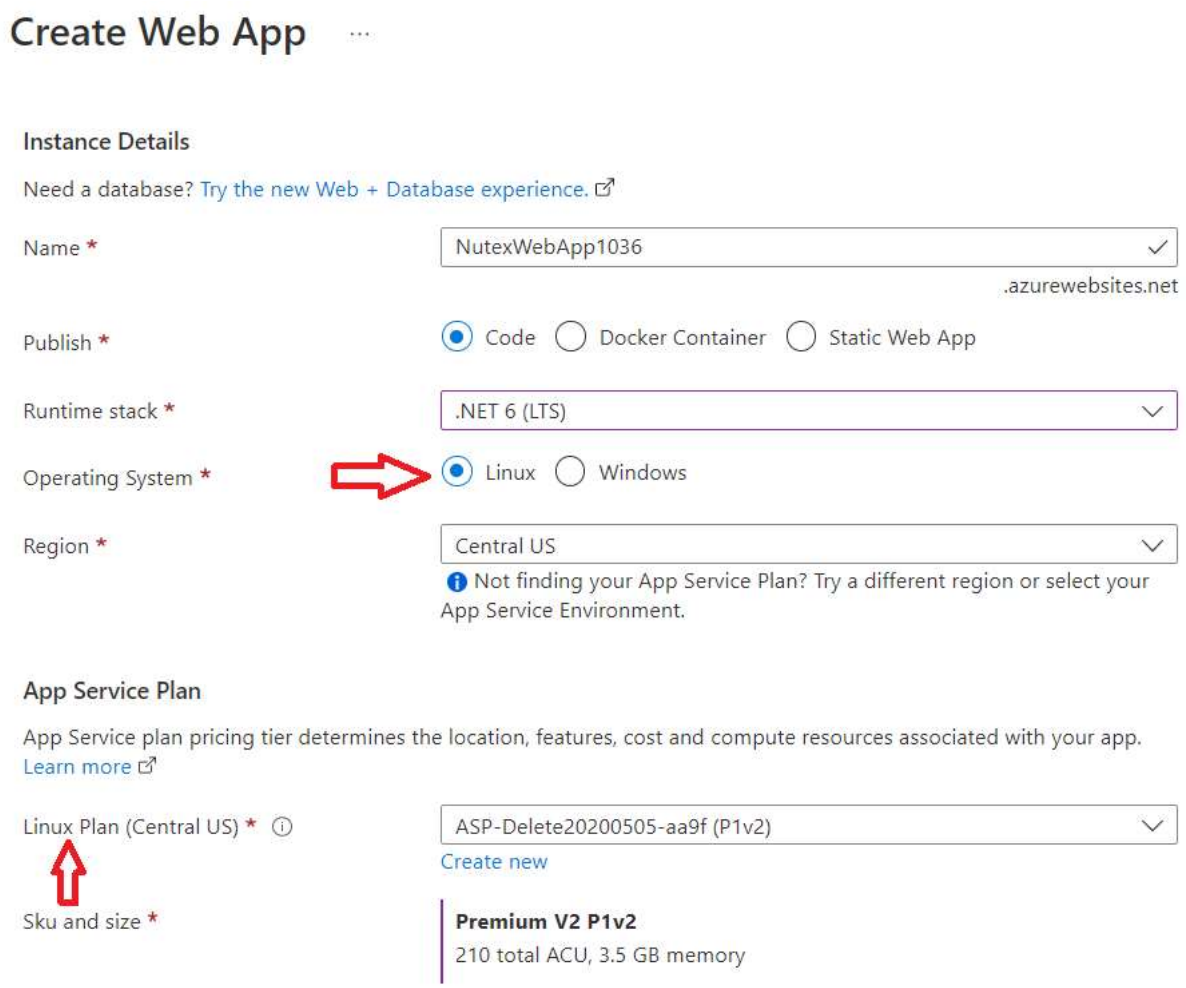
App Service plan pricing tier determines the location, features, cost and compute resources associated with your app. Learn more

Windows Plan (Central US) * ASP-Delete20200505-b480 (S1)

Create new

Sku and size * **Standard S1**
100 total ACU, 1.75 GB memory

If you choose Linux, then the App Service Plan will be a Linux plan.



The App Service Plan determines the SKU and size of the hardware that will run the operating system. If the app is in the same App Service plan as your other apps, you can improve its performance by moving it into a separate App Service plan. Doing so allows you to improve the performance by using a separate CPU and memory from another SKU.

The App Service Plan matches the operating system in this scenario. There is no need to change it.

Zone redundancy allows the App Service plan as a redundant service. You can choose to enable or disable this feature unless you choose Code as the Publish setting, in which case it cannot be enabled. When this setting is enabled, the App Service plan instance count will be three. When this setting is disabled, the instance count will be one. You cannot make an App Service plan redundant after you disabled zone redundancy and deployed the plan. In this scenario, zone redundancy is not a requirement.

Application Insights is an Application Performance Management (APM) service that automatically monitors your application and detects performance anomalies. It also contains analytics tools to investigate issues and to understand what users are doing with your app. Enabling or disabling Application Insights does not depend on whether you choose Code or Docker Container as the Publish setting.

The region does not matter in this scenario. All available regions support either **Code** or **Docker Container** as the Publish setting.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Create and configure an Azure App Service

References:

Microsoft Docs > Learn > Browse > Host a web application with Azure App Service > Create a web app in the Azure portal

---

Question #43 of 50

Question ID: 1477177

You successfully created a website at **nutex1.azurewebsites.net** and uploaded all the content. You created a custom domain pointing to **nutex.com**. The following steps were used to configure the custom domain:

- You created a CNAME record named **awverify.nutex.com** that points to **awverify.nutex1.azurewebsites.net**.

- You created an A record with the host value of **@** in the **nutex.com** zone that points to 127.0.0.1.
- You created a CNAME record with a host value of **www** that points to **nutex1.azurewebsites.net**.
- In the Azure websites configuration page, you clicked **Manage custom domains** and added **www.verigon.com** as a domain name.
- **www.verigon.com** was successfully configured to the custom domain.

Users that work for the Nutex complain that when they type **nutex.com** in the address bar without the **www** suffix, the website will not open.

Which of the following actions you should perform to resolve the issue?

A) In the DNS records for **nutex.com**, change the A record that currently points to 127.0.0.1 to **nutex1.azurewebsites.net**.

B) Restart the website using the **restart** button on the tab.

C) Call the domain names provider and notify them that DNS records are not being updated properly.

D) Add **nutex.com** to the Azure websites configuration page and save the page by clicking **ok**.

Explanation

To resolve the issue, you need to add **nutex.com** on the Azure websites configuration page and save the page by clicking **ok**. From the Azure website configuration page, choose **Domain names** and click **Manage custom domains**. You should ensure you have added both **www.nutex.com** and **nutex.com** to allow users to access the website with or without the **www** prefix, as shown in the exhibit:

|~CustomDomain.jpg~|

Calling the domain names provider and telling them that DNS records are not being updated properly will not solve the issue. If DNS records were not updated, then users would not be able to open the website using **www.nutex.com**.

You should not open the DNS records of **nutex.com** and change the A record pointed to 127.0.0.1 to point to **nutex1.azurewebsites.net** because there is no need to change DNS records in the **Domain** control panel. After updating CNAME and A records in DNS in the **Domain** control panel, **www.nutex.com** should work. As www.nutex.com is working, there is no need to update any DNS records in the **Domain** control panel.

Restarting the website will not make it access **nutex.com** without the HTTP prefix.

Objective:
Configure and manage virtual networking

Sub-Objective:
Configure virtual networks

References:

Microsoft Azure > App Service > Configure a custom domain name in Azure App Service with Traffic Manager integration

Microsoft Azure > App Service > Tutorial: Map an existing custom DNS name to Azure App Service

---

Question #44 of 50

Question ID: 1477176

You are an administrator for the Nutex Corporation. You must configure private endpoints to connect privately and securely to a service powered by Azure Private Link.

Which of the following statements about private endpoints is NOT true?

A) Multiple private endpoints can be created using the same private link resource.
B) Multiple private endpoints can be created only on the same subnet within the same virtual network.
C) The private endpoint must be deployed in the same region as the virtual network.
D) The private link resource can be deployed in a different region than the virtual network and private endpoint.

Explanation

You would choose multiple private endpoints can be created only on the same subnet within the same virtual network because multiple private endpoints can be created on the same or different subnets within the same virtual network.

The other options are all true statements about private endpoints.

The private endpoint must be deployed in the same region as the virtual network.

The private link resource can be deployed in a different region than the virtual network and private endpoint.

Multiple private endpoints can be created using the same private link resource. For a single network using a common DNS server configuration, the recommended practice is to use a single private endpoint for a given private link resource to avoid duplicate entries or conflicts in DNS resolution.

Objective:
Configure and manage virtual networking

Sub-Objective:
Configure virtual networks

References:

Microsoft Docs > Azure > Networking > Private Link > What is Azure Private Endpoint?

Question #45 of 50

Question ID: 1371385

You are designing a storage solution to support on-premises resources and Azure-hosted resources. You need to provide on-premises storage that has built-in replication to Azure and does not require extended recovery time. If there is minimal disruption, normal operations should be able to continue.

What should you include in your storage solution?

A) Azure Blob storage
B) Azure StorSimple
C) Azure Table storage
D) Azure Queue storage

Explanation

You should include Azure StorSimple. Azure StorSimple is a storage area network (SAN) solution that is an efficient and cost-effective which manages storage tasks between on-premises devices and Microsoft Azure cloud storage.

StorSimple allows you create scheduled backups and on-demand backups, which can be stored locally or in the cloud. StorSimple file shares enable complete replication and recovery.

You should not use Azure Blob storage. The Blob storage is optimized for storing data. While this storage solution can be used to store a backup, it does not provide built-in replication.

You should not use Azure Queue storage. This storage solution is used to store large number of messages from authenticated calls using HTTP or HTTPS. This solution is not designed to store files.

You should not use Azure Table storage. This storage solution is used for non-relational, key-value-pair, storage system which is optimized for querying data. This solution does not have built-in replication.

Objective:
Implement and manage storage

Sub-Objective:
Configure Azure files and Azure Blob Storage

References:

Microsoft Azure > StorSimple > Automated Disaster Recovery solution using Azure Site Recovery for file shares hosted on StorSimple

Microsoft Azure > StorSimple > Introduction to the StorSimple Virtual Array

---

Question #46 of 50

Question ID: 1371417

You are an administrator for the Nutex Corporation. You configure network connections for AKS and deployed your AKS cluster. You have the following requirements:

- You want to avoid multiple hops in your datapath before requests reach the AKS cluster.
- You do not want to use NodePort or KubeProxy services to improve the network performance of the application hosted on your AKS cluster.
- You must use an existing service.
- Your AKS cluster and your solution must include automatic updates to the latest version.

Which of the following components should you use? (Choose two.)

A) Helm Greenfield Deployment

B) HTTP application routing add-on

C) AKS Add-on Brownfield Deployment

D) Application Gateway Ingress Controller

Explanation

You would use the Application Gateway Ingress Controller (AGIC). With AGIC, you do not have to have another load balancer/public IP in front of an AKS cluster. AGIC helps avoid multiple hops in your datapath before accessing to the AKS cluster. Application Gateway uses a private IP address to talk to pods. It does not need NodePort or KubeProxy services, so providing better performance to your deployments. AGIC is supported by Standard_v2 and WAF_v2 SKUs, which provide autoscaling benefits. These benefits include reacting to an increase or decrease in traffic load and scaling accordingly without consuming any resources from your AKS cluster.

You would also use the AKS Add-on Brownfield Deployment. This allows you to install the AGIC add-on on an AKS cluster with an existing application gateway.

You would not use the Helm Greenfield Deployment. This allows you to install the AGIC for a new AKS cluster and for a new application gateway on blank-slate infrastructure.

You would not use an HTTP application routing add-on because, in AKS, you can create an Ingress resource using something similar to NGINX, or use the AKS HTTP application routing feature. When you enable HTTP application routing for an AKS cluster, the Azure platform creates the Ingress Controller and an external DNS controller. As new Ingress resources are created in Kubernetes, the required DNS A records are created in a cluster-specific DNS zone.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Create and configure containers

References:

Microsoft Docs > Azure > AKS > Network concepts for applications in Azure Kubernetes Service (AKS)

Microsoft Docs > Azure > Networking > Application Gateway > What is Application Gateway Ingress Controller?

Question #47 of 50

Question ID: 1477137

You have designed a specific infrastructure in Azure with many virtual machines and virtual networks. You need to create the same configuration for the remaining three environments in the company. You have to be sure that your deployments are consistent.

What will you choose to accomplish this?

A) Azure Resource Manager (ARM) templates

B) Chef

C) Custom scripts

D) Desired State Configuration

Explanation

You would choose Azure Resource Manager (ARM) templates. With ARM templates and their JSON templates, you can make sure that your deployments are consistent.

You would not choose the Desired State Configuration because it helps you define a state for your machines instead of writing detailed manual instructions on how to achieve that state for each machine.

You would not choose custom scripts because those are used for post-deployment configuration, software installation, or any other configuration or management task.

You would not choose Chef because it is a tool for delivering automation and desired state configurations.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Automate deployment of resources by using templates

References:

Microsoft Azure > Resource Manager > Templates > What are ARM templates?

Question #48 of 50

Question ID: 1480162

The Nutex Corporation has an Azure subscription with a Recovery Services vault named NutexVault1. You back up the following resources to NutexVault1 by using a backup policy named NutexPolicy1.

Resource	Description
SQL1	VM with SQL Server
Linux1	VM running Linux
SRV5	VM running Windows 2022
SRV4	VM running Windows 2019
Share1	Azure File Share

You need to view reports on the cloud storage consumed for each VM and File Share that is being backed up.

What should you configure? Place the appropriate three steps in the correct order.

{UCMS id=5649116148269056 type=Activity}

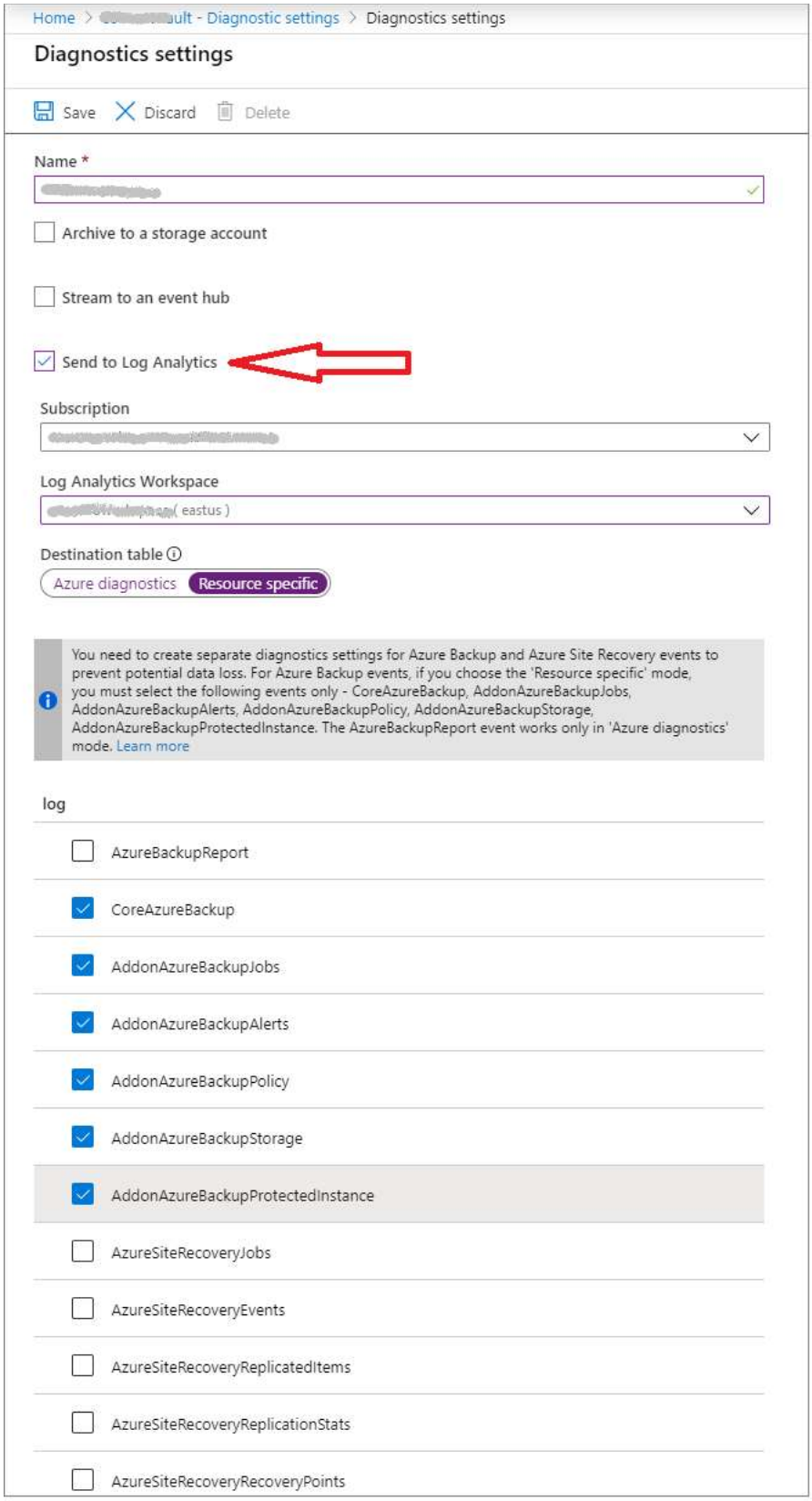
Explanation

You should perform the following steps:

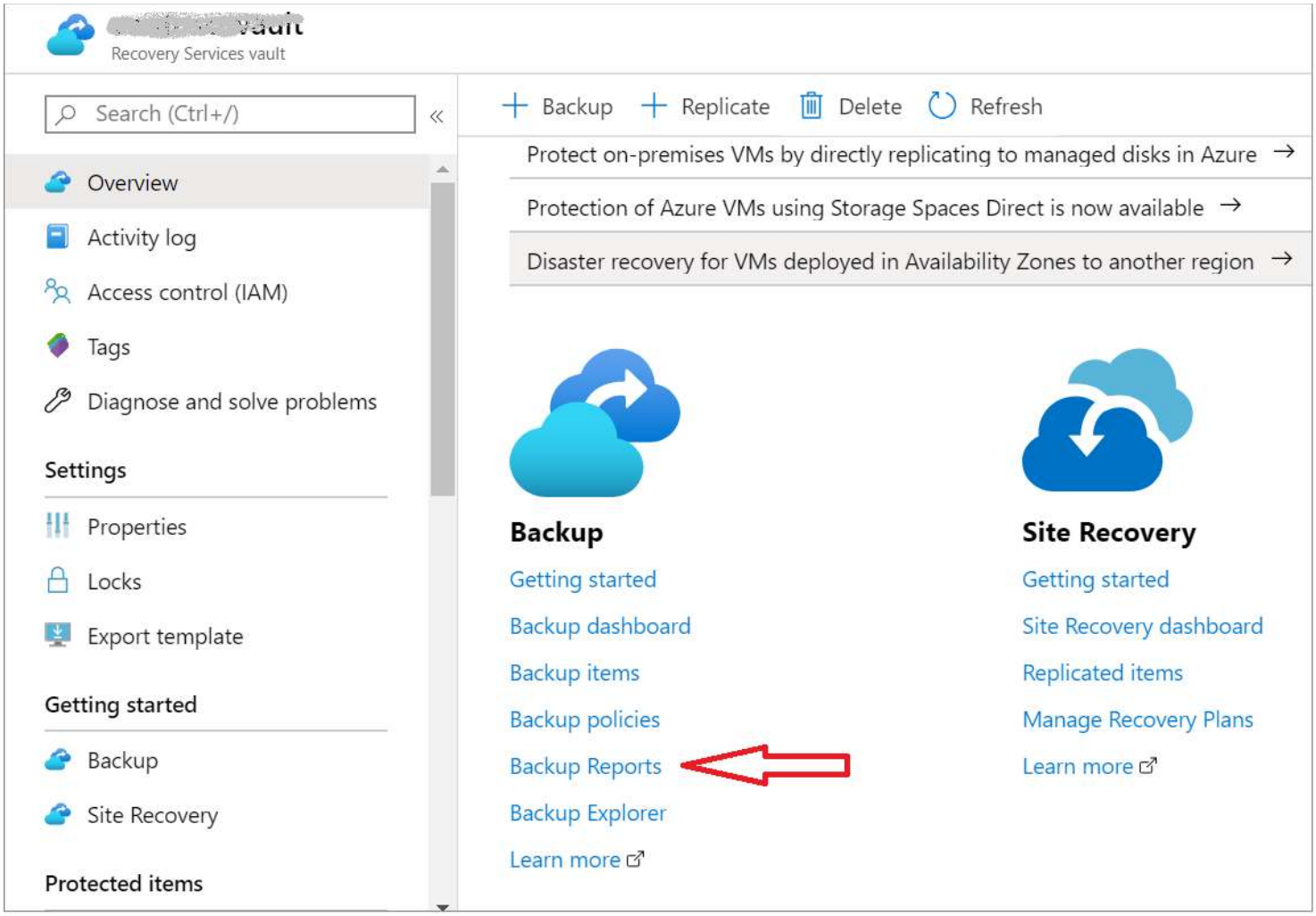
1. Create a Log Analytics workspace
2. Configure diagnostics settings for NutexVault1
3. Select Backup Reports in the properties of NutexVault1

Backup Reports allows you to view reports on the cloud storage consumed for each VM and File Share that is being backed up. To configure Backup Reports, you will need a Log Analytics workspace to store Backup reporting data. You can create a new Log Analytics workspace or use an existing one. The Log Analytics workspace does not have to be in the same location nor be in the same subscription where the vault is located. Data in a Log Analytics workspace exists for 30 days by default. You can change the retention period to keep data for a longer time.

You should then configure the diagnostics settings for your Recovery Services vault. You will need to specify the target for the diagnostic data of the Recovery Services vault. You should check the **Send to Log Analytics** option, and specify the subscription that contains the Log Analytics Workspace and the name of the Log Analytics Workspace.



You should open your Recovery Services vault. Under **Overview**, you should select **Backup Reports** to view the Backup Reports.



You would not choose Backup Explorer. This is an Azure Monitor workbook that is a central location to monitor operational activities, which gives you an aggregated view of the backup items, jobs, alerts, policies, and resources.

You would not change the options of the Azure Backup policy. You can configure many options in an Azure Backup policy, such as whether Azure Backup should back up virtual machines, whether Recovery Services vaults use private endpoints for backups, and whether Azure Recovery Services vaults should use customer-managed keys for encrypting backup data. You cannot specify the target for the diagnostic data of the Recovery Services vault in an Azure Backup policy.

Objective:
Monitor and maintain Azure resources

Sub-Objective:
Implement backup and recovery

References:

Microsoft Docs > Azure > Backup > Configure Azure Backup reports

---

Question #49 of 50

Question ID: 1480167

You are the administrator of the Nutex Corporation. You have to design your high availability and disaster recovery solution including geo-replication capabilities for your Azure SQL Database solution. Your solution has to include the regions WestEurope and EastUS.

You have the following characteristic sets.

Characteristic set 1:

- The end users from different geographies access the application.
- The application includes read-only workloads that do not depend on full synchronization with the latest updates.
- Write access to data should be supported in the same geography for the majority of the users.

- Read latency is critical to the end user experience.

Characteristic set 2:

- Any data loss is a high business risk.
- If an outage is caused by a catastrophic failure, database failover can only be used.
- The application supports both read-only and read-write modes of operations.
- The application can operate in "read-only mode" for a period of time.

Characteristic set 3:

- The application is active in only one of the Azure regions.
- All database sessions require read and write access (RW) to data.
- Web tier and data tier must be collocated to reduce latency and traffic cost.

You have the following HA/DR scenarios:

- Scenario 1: Using two Azure regions for business continuity with minimal downtime.
- Scenario 2: Using Azure regions for business continuity with maximum data preservation.
- Scenario 3: Application relocation to a different geography without data loss and near zero downtime.

Which application characteristic set matches each HA/DR scenario? In the work area, drag the scenario to the matching set of application characteristics.

{UCMS id=5407527900545024 type=Activity}

Explanation

You should choose the following:

Scenarios	Character Sets
Scenario 1	Character Set 3
Scenario 2	Character Set 2
Scenario 3	Character Set 1

You should use Scenario1 for the following application characteristics:

- The application is active in only one of the Azure regions
- All database sessions require read and write access (RW) to data
- Web tier and data tier must be collocated to reduce latency and traffic cost

When you use two Azure regions for business continuity with minimal downtime, the application deployment topology is optimized for handling regional disasters when all application components need to fail over together. For geographic redundancy, the application's resources are deployed to WestEurope and EastUS. However, the resources in EastUS are not utilized until WestEurope fails. To manage database connectivity, replication, and failover, a failover group has to be configured between the two regions. The web service in both regions is configured to access the database via the read-write listener. The priority routing method is used by the Traffic Manager.

You should use Scenario2 for the following application characteristics:

- Any data loss is a high business risk.
- If an outage is caused by a catastrophic failure, database failover can only be used.
- The application supports both read-only and read-write modes of operations.
- The application can operate in "read-only mode" for a period of time.

In this scenario, the application switches to read-only mode if the read-write connections begin to time out. The Web Application is deployed to multiple regions, and has different connection to the read-only listener endpoint including a connection to the read-write listener endpoint. The priority routing method is used by the traffic manager. The application endpoint in each region should have end-point monitoring enabled.

You should use Scenario3 for the following application characteristics:

- The end users from different geographies access the application.
- The application includes read-only workloads that do not depend on full synchronization with the latest updates.
- Write access to data should be supported in the same geography for the majority of the users.
- Read latency is critical to the end user experience.

With this scenario, you assume that the user device is constantly connected to the application in the geographic region for browsing or other read-only operations. OLTP operations are processed in the same geographic region; however, they could be processed in a different geographic region during off hours. Optimal performance is guaranteed if the end user activity happens during the working hours for most of the users most of the time. The priority routing method is used by the traffic manager. It ensures that the end user's device is connected to the web service in the closest region. Traffic manager should be set up with end point monitoring enabled for each web service end point.

Objective:
Monitor and maintain Azure resources

Sub-Objective:
Implement backup and recovery

References:

Microsoft Azure > SQL Database > Designing globally available services using Azure SQL Database

---

Question #50 of 50

Question ID: 1481900

You have a Windows 11 tablet. You need to upload a container image into an Azure container registry. You need to log in to the registry to work with the container images.

What must you have installed on the Windows 11 tablet?

A) NGINX image 1.21.6 or later
B) Docker Desktop 4.9.00 or later
C) Azure CLI version 2.0.55 or later
D) Azure PowerShell 7.0 or later

Explanation

You must have Docker Desktop installed locally on the client. The client can be a Windows, Linux, or MacOS client. Docker Desktop allows you to run the docker daemon and all of its associated commands. Azure Container Registry is used as a private repository for containers, and then you have to deploy those containers in ACI or in Azure App Service.

You can use the Azure portal, PowerShell, an ARM template, the Bicep language, or Azure CLI to create an Azure container registry. The following creates an Azure container registry using the `az acr create` command in Azure CLI:

```
az acr create --resource-group NutexResourceGroup \
  --name NutexContainerRegistry001 --sku Basic
```

Prior to managing the images from the client by using the `docker push` and `docker pull` commands, you must log in to the registry. The following command logs in to `NutexContainerRegistry001`:

```
az acr login --name NutexContainerRegistry001
```

The following command is run from the client to pull an image named `image1` from the Microsoft container registry:

```
docker pull mcr.microsoft.com/image1
```

Before you can upload or push the image to your Azure container registry, you need to tag it with the fully qualified name of your registry login server:

```
docker tag mcr.microsoft.com/image1 nutexcontainerregistry.azurecr.io/image1:v1
```

Once you have tagged the image, you can push the image to your registry instance. The following `docker push` command creates the `image1` repository that contains the `image1:v1` image:

```
docker push nutexcontainerregistry.azurecr.io/image1:v1
```

The Azure portal, Azure CLI, and Azure PowerShell do not contain Docker commands and will not allow you to tag, push, or pull an image.

You do not need the NGINX image. This is a Docker image that is an open-source proxy server and web server.

Objective:
Deploy and manage Azure compute resources

Sub-Objective:
Create and configure containers

References:

Microsoft Docs > Azure > Container Registry > Quickstart: Create a private container registry using the Azure CLI

Microsoft Docs > Azure > Container Registry > Introduction to Container registries in Azure