SKILLCERTPRO

IT CERTIFICATION TRAININGS

0

Microsoft Azure / By SkillCertPro

Practice Set 16

Your results are here!! for" Microsoft Azure AZ-305 Practice Test 16 "

45 of 65 questions answered correctly

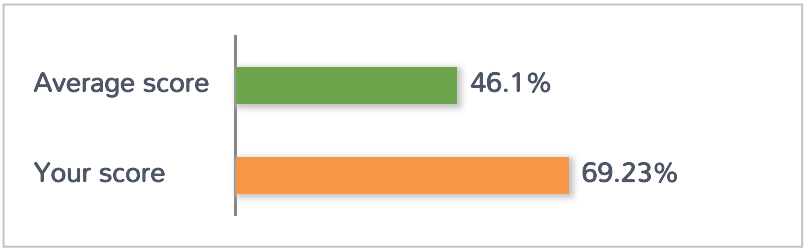
Your time: 02:31:21

Your Final Score is : 45

You have attempted : 65

Number of Correct Questions : 45 and scored 45

Number of Incorrect Questions : 20 and Negative marks 0

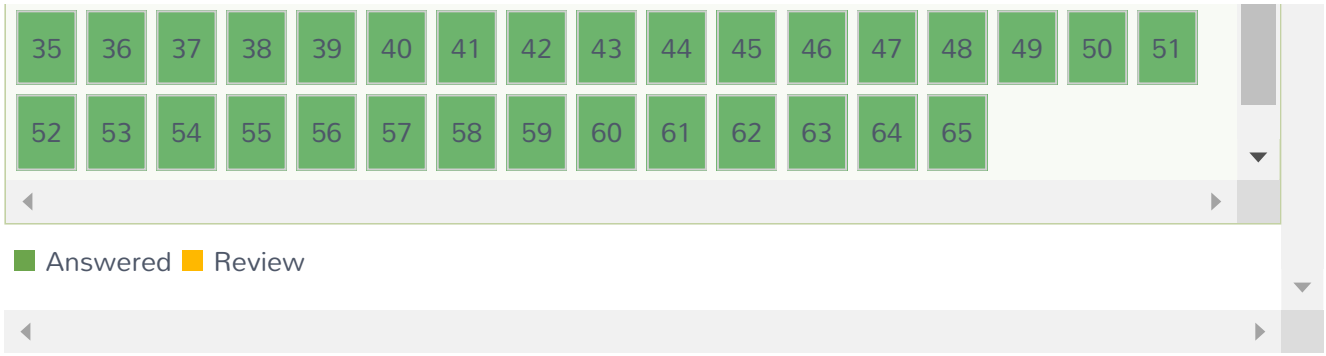


You can review your answers by clicking on “View Answers” option.

Important Note : Open Reference Documentation Links in New Tab (Right Click and Open in New Tab).

Restart Test View Answers

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34



1. Question

You plan to create a storage account and to save the files as shown in the exhibit.

Select the answer choice that completes the following statement based on the information presented in the graphic.

To access the file, you must _____

- A. generate a snapshot
- **B. modify the access tier**
- C. modify the blob type

Correct

The data in the storage account is in archive access tier. To read data in archive storage, you must first change the tier of the blob to hot or cool. This process is known as rehydration and can take hours to complete

Incorrect Answers:

A. generate a snapshot

A snapshot is a read-only version of a blob that's taken at a point in time. You can't take snapshots of a blob in archive storage.

C. modify the blob type

You can access the files that are block blob type without any changes.

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers#archive-access-tier

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-rehydration?tabs=azure-portal#rehydrate-an-archived-blob-to-an-online-tier

Overview of blob rehydration from the archive tier

08/31/2021 • 8 minutes to read •

While a blob is in the archive access tier, it's considered to be offline and can't be read or modified. In order to read or modify data in an archived blob, you must first rehydrate the blob to an online tier, either the hot or cool tier. There are two options for rehydrating a blob that is stored in the archive tier:

- Copy an archived blob to an online tier: You can rehydrate an archived blob by copying it to a new blob in the hot or cool tier with the Copy Blob or Copy Blob from URL operation. Microsoft recommends this option for most scenarios.
- Change a blob's access tier to an online tier: You can rehydrate an archived blob to hot or cool by changing its tier using the Set Blob Tier operation.

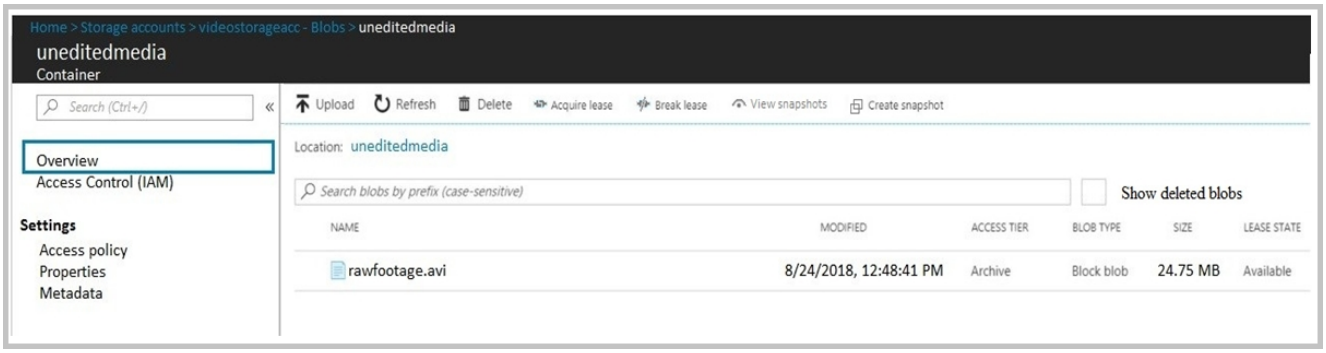
Rehydrating a blob from the archive tier can take several hours to complete. Microsoft recommends rehydrating larger blobs for optimal performance. Rehydrating several small blobs concurrently may require additional time.

You can configure Azure Event Grid to raise an event when you rehydrate a blob from the archive tier to an online tier and to send the event to an event handler. For more information, see Handle an event on blob rehydration.

For more information about access tiers in Azure Storage, see Access tiers for Azure Blob Storage - hot, cool, and archive.

2. Question

You plan to create a storage account and to save the files as shown in the exhibit.



Select the answer choice that completes the following statement based on the information presented in the graphic.

The files will be stored ----------

- A. at the highest storage cost

B. at the lowest data retrieval cost

C. at the lowest storage cost

Correct

The archive tier offers the lowest storage costs but also the highest access costs and latency.

Incorrect Answers:

A. at the highest storage cost

Archive tier offers the lowest storage costs.

B. at the lowest data retrieval cost

Archive tier has highest data retrieval.

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers#archive-access-tier

Archive access tier

The archive access tier has the lowest storage cost but higher data retrieval costs compared to hot and cool tiers. Data must remain in the archive tier for at least 180 days or be subject to an early deletion charge. Data in the archive tier can take several hours to retrieve depending on the specified rehydration priority. For small objects, a high priority rehydrate may retrieve the object from archive in under an hour. See Overview of blob rehydration from the archive tier to learn more.

While a blob is in archive storage, the blob data is offline and can't be read or modified. To read or download a blob in archive, you must first rehydrate it to an online tier. You can't take snapshots of a blob in archive storage. However, the blob metadata remains online and available, allowing you to list the blob, its properties, metadata, and blob index tags. Setting or modifying the blob metadata while in archive isn't allowed. However, you can set and modify the blob index tags. For blobs in archive, the only valid operations are Get Blob Properties, Get Blob Metadata, Set Blob Tags, Get Blob Tags, Find Blobs by Tags, List Blobs, Set Blob Tier, Copy Blob, and Delete Blob.

Example usage scenarios for the archive access tier include:

- Long-term backup, secondary backup, and archival datasets
- Original (raw) data that must be preserved, even after it has been processed into final usable form
- Compliance and archival data that needs to be stored for a long time and is hardly ever accessed

Note

The archive tier is not supported for ZRS, GZRS, or RA-GZRS accounts. Migrating from LRS to GRS is supported as long as no blobs were moved to the archive tier while the account was set to LRS. An account can be moved back to GRS if the update is done less than 30 days from the time the account became LRS, and no blobs were moved to the archive tier while the account was set to LRS.

3. Question

You are designing a storage solution that will use Azure Blob storage. The data will be stored in a cool access tier or an archive access tier based on the access patterns of the data.

You identify the following types of infrequently accessed data:

? Telemetry data: Deleted after two years

? Promotional material: Deleted after 14 days

? Virtual machine audit data: Deleted after 200 days

A colleague recommends using the archive access tier to store the data.

Which statement accurately describes the recommendation?

- A. Storage costs will be based on a minimum of 30 days

B. Access to the data is guaranteed within five minutes

C. Access to the data is guaranteed within 30 minutes

D. Storage costs will be based on a minimum of 180 days

Correct

The archive access tier has the lowest storage cost. But it has higher data retrieval costs compared to the hot and cool tiers. Data must remain in the archive tier for at least 180 days or be subject to an early deletion charge. Data in the archive tier can take several hours to retrieve depending on the priority of the rehydration.

Incorrect Answers:

A. Storage costs will be based on a minimum of 30 days

Storage costs will be based on a minimum of 180 days for archive tier data.

B. Access to the data is guaranteed within five minutes

For the high priority data, the rehydration request will take under one hour to complete. For standard priority, it is up to 15 hours.

C. Access to the data is guaranteed within 30 minutes

For the high priority data, the rehydration request will take under one hour to complete. For standard priority, it is up to 15 hours.

Reference:

https://docs.microsoft.com/en-au/azure/storage/blobs/storage-blob-storage-tiers?tabs=azure-portal#comparing-block-blob-storage-options

Comparing block blob storage options

The following table shows a comparison of premium performance block blob storage, and the hot, cool, and archive access tiers.

	Premium performance	Hot tier	Cool tier	Archive tier
Availability	99.9%	99.9%	99%	Offline
Availability (RA-GRS reads)	N/A	99.99%	99.9%	Offline
Usage charges	Higher storage costs, lower access, and transaction cost	Higher storage costs, lower access, and transaction costs	Lower storage costs, higher access, and transaction costs	Lowest storage costs, highest access, and transaction costs
Minimum storage duration	N/A	N/A	30 days[1]	180 days
Latency (Time to first byte)	Single-digit milliseconds	milliseconds	milliseconds	hours[2]

[1] Objects in the cool tier on GPv2 accounts have a minimum retention duration of 30 days. Blob Storage accounts don't have a minimum retention duration for the cool tier.

[2] Archive Storage currently supports two rehydration priorities, high and standard, offering different retrieval latencies and costs. For more information, see Overview of blob rehydration from the archive tier.

ⓘ Note

Blob Storage accounts support the same performance and scalability targets as general-purpose v2 storage accounts. For more information, see **Scalability and performance targets for Blob Storage.**

4. Question

You are planning to deploy an application named App1 that will run in containers on Azure Kubernetes Service (AKS) clusters. The AKS clusters will be distributed across four Azure regions.

You need to recommend a storage solution for App1. Updated container images must be replicated automatically to all the AKS clusters.

Which storage solution should you recommend?

A. Azure Cache for Redis

B. Azure Content Delivery Network (CDN)

C. Premium SKU Azure Container Registry

D. geo-redundant storage (GRS) accounts

Correct

Store your container images in Azure Container Registry and geo-replicate the registry to each AKS region.

To deploy and run your applications in AKS, you need a way to store and pull the container images. Container Registry integrates with AKS, so it can securely store your container images or Helm charts.

Container Registry supports multi-master geo-replication to automatically replicate your images to Azure regions around the world.

To improve performance and availability, use Container Registry geo-replication to create a registry in each region where you have an AKS cluster. Each AKS cluster then pulls container images from the local container registry in the same region:

Geo-replication is a feature of Premium SKU container registries

Incorrect Answers:

A. Azure Cache for Redis

Azure Cache for Redis provides an in-memory data store based on the Redis software. This is not used as to store container images.

B. Azure Content Delivery Network (CDN)

A content delivery network (CDN) is a distributed network of servers that can efficiently deliver web content to users. CDNs' store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency. This is not used as to store container images.

D. geo-redundant storage (GRS) accounts

GRS Storage accounts are used to store data in secondary region for high durability. The data in the secondary region isn't available for read or write access unless there is a failover to the secondary region.

Reference:

https://docs.microsoft.com/en-us/azure/aks/operator-best-practices-multi-region#enable-geo-replication-for-container-images

Enable geo-replication for container images

> **Best practice**
>
> Store your container images in Azure Container Registry and geo-replicate the registry to each AKS region.

To deploy and run your applications in AKS, you need a way to store and pull the container images. Container Registry integrates with AKS, so it can securely store your container images or Helm charts. Container Registry supports multimaster geo-replication to automatically replicate your images to Azure regions around the world.

To improve performance and availability:

1. Use Container Registry geo-replication to create a registry in each region where you have an AKS cluster.
2. Each AKS cluster then pulls container images from the local container registry in the same region:

When you use Container Registry geo-replication to pull images from the same region, the results are:

- **Faster**: Pull images from high-speed, low-latency network connections within the same Azure region.
- **More reliable**: If a region is unavailable, your AKS cluster pulls the images from an available container registry.
- **Cheaper**: No network egress charge between datacenters.

Geo-replication is a *Premium* SKU container registry feature. For information on how to configure geo-replication, see Container Registry geo-replication.

5. Question

You have an on-premises network and an Azure subscription. The on-premises network has several branch offices.

A branch office in Toronto contains a virtual machine named VM1 that is configured as a file server. Users access the shared files on VM1 from all the offices.

You need to recommend a solution to ensure that the users can access the shared files as quickly as possible if the Toronto branch office is inaccessible.

What should you include in the recommendation?

- A. an Azure file share and Azure File Sync
- B. a Recovery Services vault and Windows Server Backup
- C. a Recovery Services vault and Azure Backup
- D. Azure blob containers and Azure File Sync

Correct

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol. Azure file shares can be mounted concurrently by cloud or on-premises deployments of Windows, Linux, and macOS. Additionally, Azure file shares can be cached on Windows Servers with Azure File Sync for fast access near where the data is being used.

Incorrect Answers:

B. a Recovery Services vault and Windows Server Backup

Recovery services vault is used for BCDR scenarios.

C. a Recovery Services vault and Azure Backup

Recovery services vault is used for BCDR scenarios.

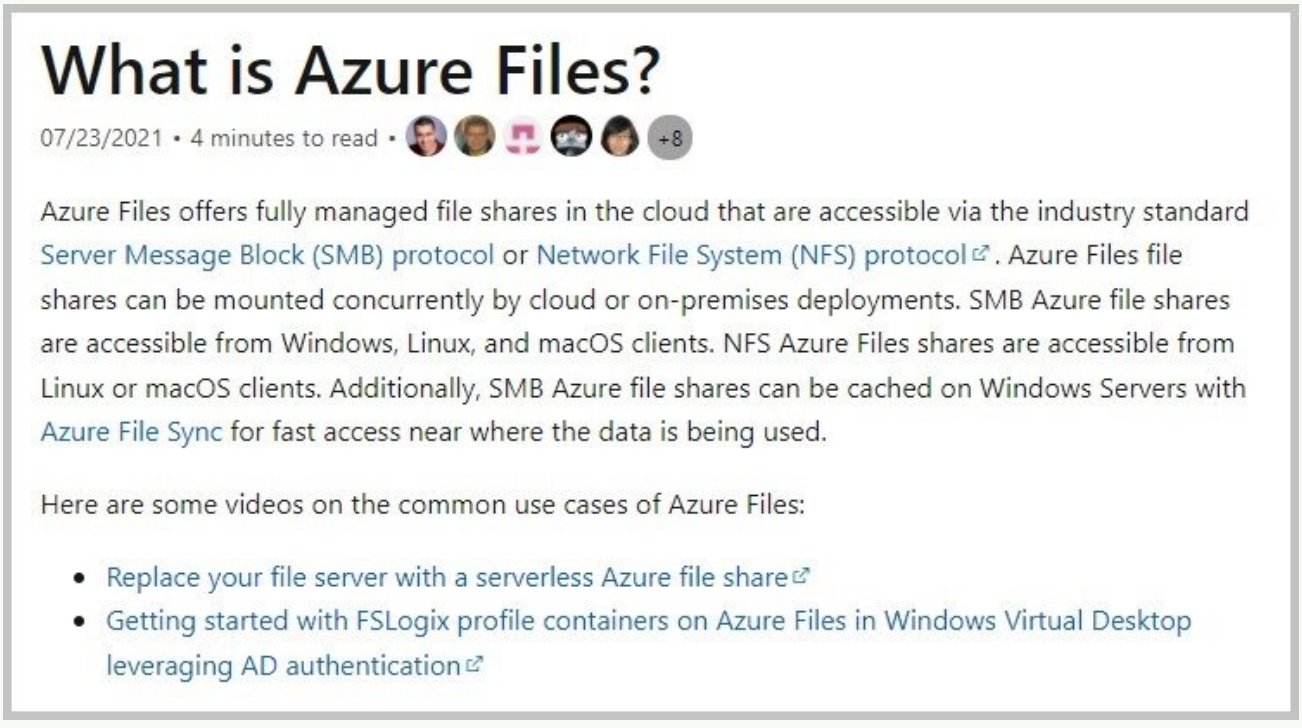
D. Azure blob containers and Azure File Sync

Azure File Sync works with Azure File shares, not with Azure blob containers.

Reference:

https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide

https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction



What is Azure Files?

07/23/2021 • 4 minutes to read • +8

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol or Network File System (NFS) protocol. Azure Files file shares can be mounted concurrently by cloud or on-premises deployments. SMB Azure file shares are accessible from Windows, Linux, and macOS clients. NFS Azure Files shares are accessible from Linux or macOS clients. Additionally, SMB Azure file shares can be cached on Windows Servers with Azure File Sync for fast access near where the data is being used.

Here are some videos on the common use cases of Azure Files:

- Replace your file server with a serverless Azure file share
- Getting started with FSLogix profile containers on Azure Files in Windows Virtual Desktop leveraging AD authentication

6. Question

You plan to deploy 10 applications to Azure. The applications will be deployed to two Azure Kubernetes Service (AKS) clusters. Each cluster will be deployed to a separate Azure region.

The application deployment must meet the following requirements:

? Ensure that the applications remain available if a single AKS cluster fails.

? Ensure that the connection traffic over the internet is encrypted by using SSL without having to configure SSL on each container.

Which Azure service should you include in the recommendation?

- A. AKS ingress controller
- B. Azure Load Balancer
- C. Azure Traffic Manager
- D. Azure Front Door

Correct

Azure Front Door enables you to define, manage, and monitor the global routing for your web traffic by optimizing for best performance and instant global failover for high availability. With Front Door, you can transform your global (multi-region) consumer and enterprise applications into robust, high-performance personalized modern applications, APIs, and content that reaches a global audience with Azure.

Front Door works at Layer 7 or HTTP/HTTPS layer and uses anycast protocol with split TCP and Microsoft's global network for improving global connectivity.

Incorrect Answers:

A. AKS ingress controller

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

B. Azure Load Balancer

Azure Load Balancer operates at layer 4 of the Open Systems Interconnection (OSI) model. It's the single point of contact for clients. Load balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances.

C. Azure Traffic Manager

Azure Traffic Manager uses DNS (layer 3) to shape traffic. SSL works at Layer 6.

Azure Traffic Manager can direct customers to their closest AKS cluster and application instance. For the best performance and redundancy, direct all application traffic through Traffic Manager before it goes to your AKS cluster.

Reference:

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview

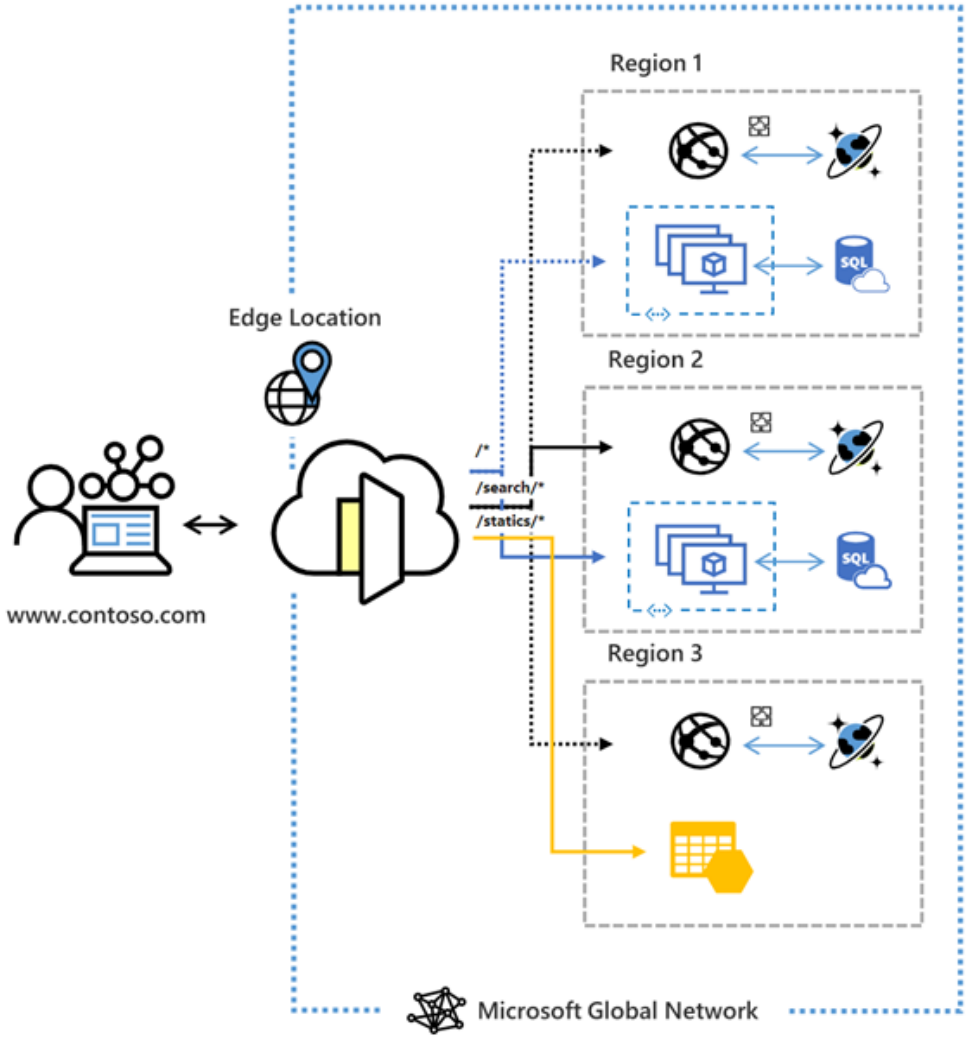
What is Azure Front Door?

03/09/2021 • 2 minutes to read • +6

Important

This documentation is for Azure Front Door. Looking for information on Azure Front Door Standard/Premium (Preview)? View here.

Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. With Front Door, you can transform your global consumer and enterprise applications into robust, high-performing personalized modern applications with contents that reach a global audience through Azure.



7. Question

You have an Azure web app that uses an Azure key vault named KeyVault1 in the West US Azure region.

You are designing a disaster recovery plan for KeyVault1.

You plan to back up the keys in KeyVault1.

You need to identify to where you can restore the backup.

What should you identify?

- A. KeyVault1 only
- B. the same region only
- C. the same geography only
- D. any region worldwide

Correct

When you back up a key vault object, such as a secret, key, or certificate, the backup operation will download the object as an encrypted blob. This blob can't be decrypted outside of Azure. To get usable data from this blob, you must restore the blob into a key vault within the same Azure subscription and Azure geography.

Incorrect Answers:

A. KeyVault1 only

You can restore to other key vaults in same Azure subscription and geography.

B. the same region only

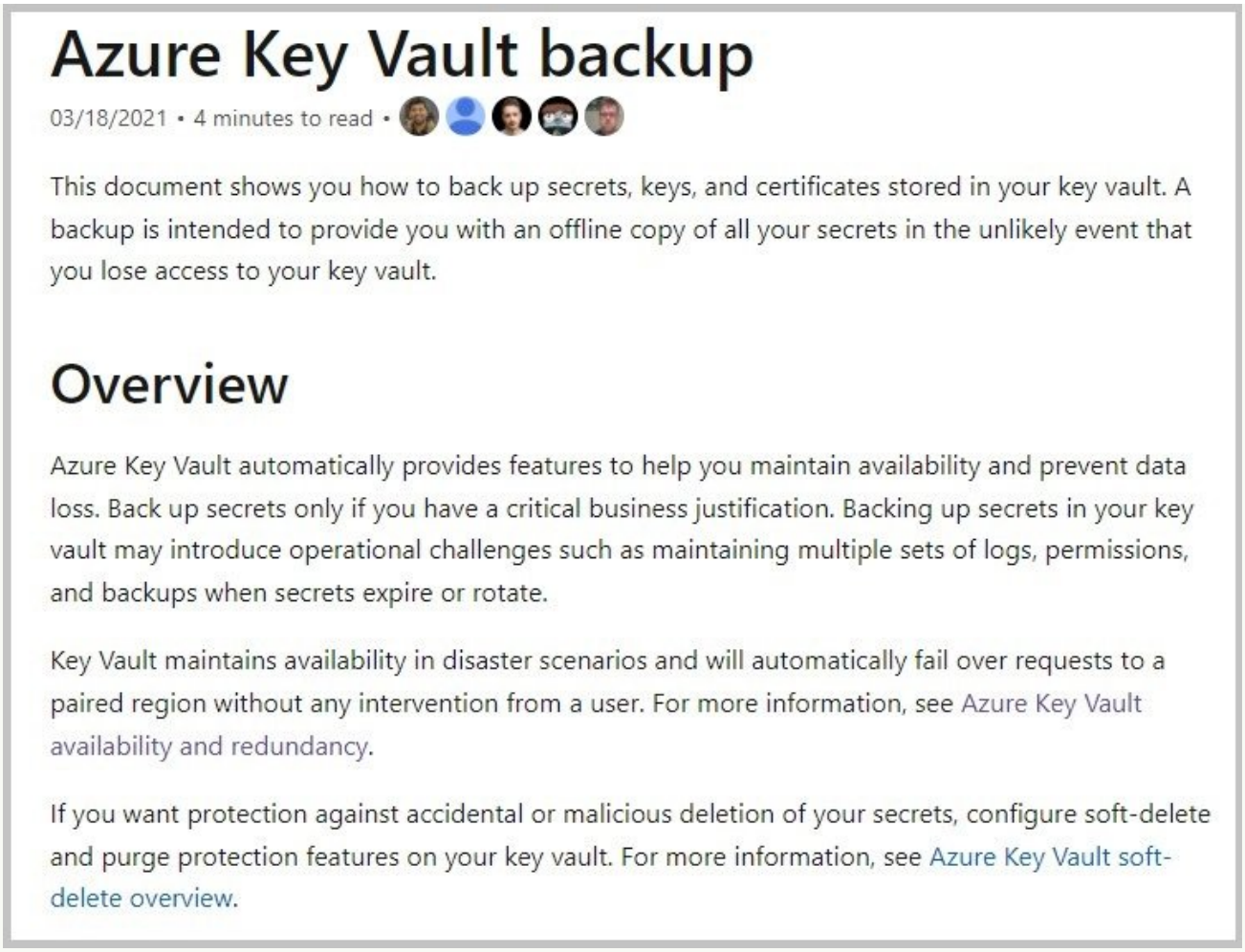
You can restore to any region within same geography.

D. any region worldwide

You must restore within the same geography.

Reference:

https://docs.microsoft.com/en-us/azure/key-vault/general/backup



Azure Key Vault backup

03/18/2021 • 4 minutes to read •

This document shows you how to back up secrets, keys, and certificates stored in your key vault. A backup is intended to provide you with an offline copy of all your secrets in the unlikely event that you lose access to your key vault.

Overview

Azure Key Vault automatically provides features to help you maintain availability and prevent data loss. Back up secrets only if you have a critical business justification. Backing up secrets in your key vault may introduce operational challenges such as maintaining multiple sets of logs, permissions, and backups when secrets expire or rotate.

Key Vault maintains availability in disaster scenarios and will automatically fail over requests to a paired region without any intervention from a user. For more information, see Azure Key Vault availability and redundancy.

If you want protection against accidental or malicious deletion of your secrets, configure soft-delete and purge protection features on your key vault. For more information, see Azure Key Vault soft-delete overview.

8. Question

Your company has the infrastructure shown in the following table.

Location	Resource
Azure	• Azure subscription named Subscription1 • 20 Azure web apps
On-premises Datacenter	• Active Directory domain • Server running Azure AD Connect • Linux computer named Server1

The on-premises Active Directory domain syncs to Azure Active Directory (Azure AD).

Server1 runs an application named App1 that uses LDAP queries to verify user identities in the on-premises Active Directory domain.

You plan to migrate Server1 to a virtual machine in Subscription1.

A company security policy states that the virtual machines and services deployed to Subscription1 must be prevented from accessing the on-premises network.

You need to recommend a solution to ensure that App1 continues to function after the migration. The solution must meet the security policy.

What should you include in the recommendation?

A. Azure AD Application Proxy

B. an Azure VPN gateway

C. Azure AD Domain Services (Azure AD DS)

D. the Active Directory Domain Services role on a virtual machine

Incorrect

Lightweight Directory Access Protocol (LDAP) is an application protocol for working with various directory services. Directory services, such as Active Directory, store user and account information, and security information like passwords. The service then allows the information to be shared with other devices on the network. Azure Active Directory (Azure AD) supports this pattern via Azure AD Domain Services (AD DS). It allows organizations that are adopting a cloud-first strategy to modernize their environment by moving off their on-premises LDAP resources to the cloud.

Incorrect Answers:

A. Azure AD Application Proxy

Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications.

B. an Azure VPN gateway

A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet.

D. the Active Directory Domain Services role on a virtual machine

This is basically setting up Active directory in a VM. The on-premise active directory already syncs with Azure AD.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/auth-ldap#use-when

What is Azure Active Directory Domain Services?

04/28/2021 • 5 minutes to read •

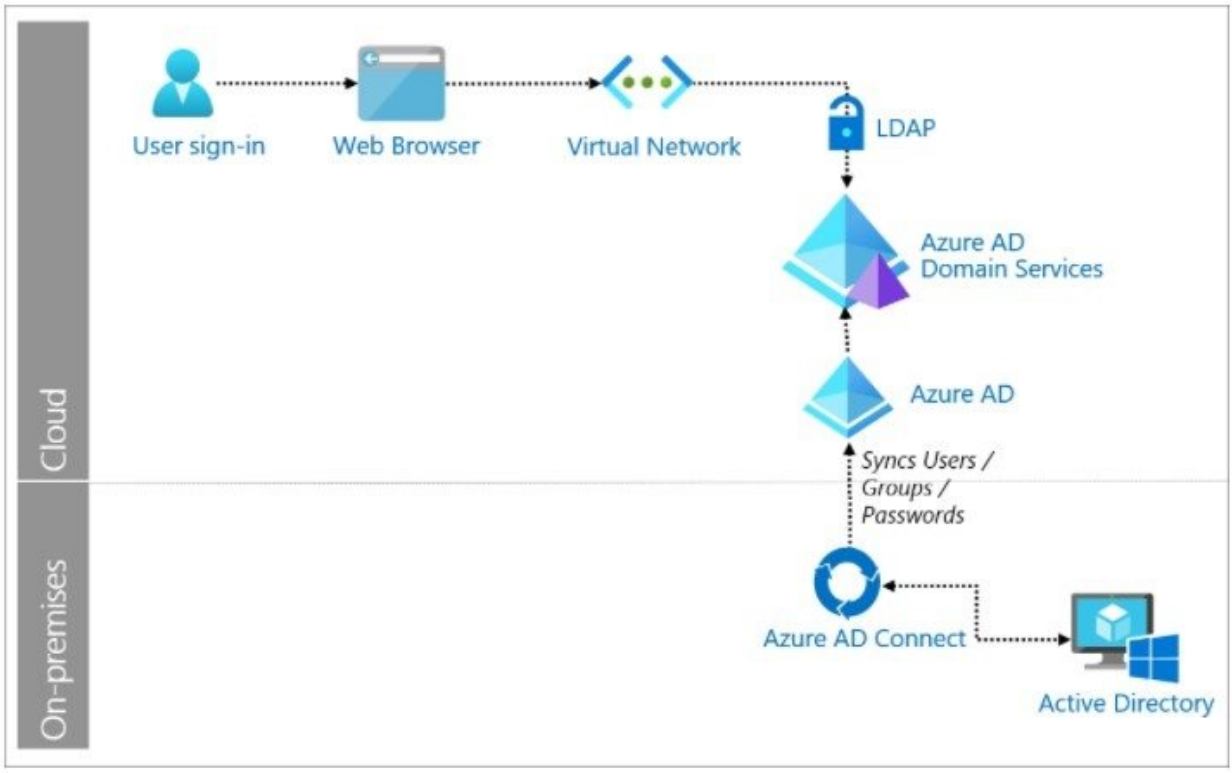
Azure Active Directory Domain Services (Azure AD DS) provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. You use these domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.

An Azure AD DS managed domain lets you run legacy applications in the cloud that can't use modern authentication methods, or where you don't want directory lookups to always go back to an on-premises AD DS environment. You can lift and shift those legacy applications from your on-premises environment into a managed domain, without needing to manage the AD DS environment in the cloud.

Azure AD DS integrates with your existing Azure AD tenant. This integration lets users sign in to services and applications connected to the managed domain using their existing credentials. You can also use existing groups and user accounts to secure access to resources. These features provide a smoother lift-and-shift of on-premises resources to Azure.

Use when

There is a need to for an application or service to use LDAP authentication.



9. Question

You have an application that sends events to an Azure event hub by using HTTP requests over the internet.

You plan to increase the number of application instances.

You need to recommend a solution to reduce the overhead associated with sending events to the hub.

What should you recommend?

- A. Configure the application to send events by using the AMQP protocol
- B. Reduce the retention period of the event hub
- C. Replace the event hub with an Azure Service Bus instance
- D. Configure the application to send events by using the HTTPS protocol

Correct

The Advanced Message Queueing Protocol 1.0 is a standardized framing and transfer protocol for asynchronously, securely, and reliably transferring messages between two parties. It is the primary protocol of Azure Service Bus Messaging and Azure Event Hubs.

Incorrect Answres:

B. Reduce the retention period of the event hub

Changing the retention period would not reduce the overhead.

C. Replace the event hub with an Azure Service Bus instance

Azure event hub has a low latency compared to Azure Service Bus.

D. Configure the application to send events by using the HTTPS protocol

Overhead increases with HTTPS compared to HTTP.

Reference:

https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-amqp-protocol-guide

AMQP 1.0 in Azure Service Bus and Event Hubs protocol guide

04/14/2021 • 28 minutes to read • +7

The Advanced Message Queueing Protocol 1.0 is a standardized framing and transfer protocol for asynchronously, securely, and reliably transferring messages between two parties. It is the primary protocol of Azure Service Bus Messaging and Azure Event Hubs.

AMQP 1.0 is the result of broad industry collaboration that brought together middleware vendors, such as Microsoft and Red Hat, with many messaging middleware users such as JP Morgan Chase representing the financial services industry. The technical standardization forum for the AMQP protocol and extension specifications is OASIS, and it has achieved formal approval as an international standard as ISO/IEC 19494:2014.

Basic AMQP scenarios

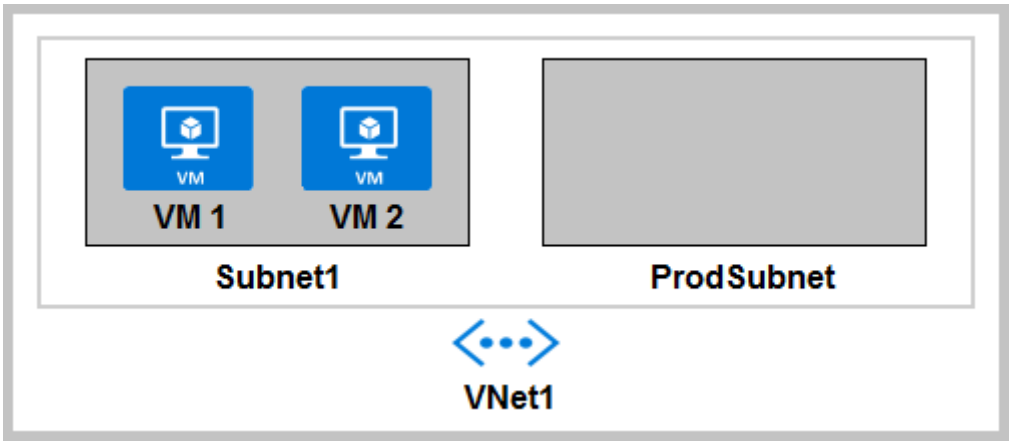
This section explains the basic usage of AMQP 1.0 with Azure Service Bus, which includes creating connections, sessions, and links, and transferring messages to and from Service Bus entities such as queues, topics, and subscriptions.

The most authoritative source to learn about how AMQP works is the AMQP 1.0 specification, but the specification was written to precisely guide implementation and not to teach the protocol. This section focuses on introducing as much terminology as needed for describing how Service Bus uses AMQP 1.0. For a more comprehensive introduction to AMQP, as well as a broader discussion of AMQP 1.0, you can review this video course.

10. Question

Your company develops a web service that is deployed to an Azure virtual machine named VM1. The web service allows an API to access real-time data from VM1.

The current virtual machine deployment is shown in the Deployment exhibit.



The chief technology officer (CTO) sends you the following email message: “Our developers have deployed the web service to a virtual machine named VM1.

Testing has shown that the API is accessible from VM1 and VM2. Our partners must be able to connect to the API over the Internet. Partners will use this data in applications that they develop.“

You deploy an Azure API Management (APIM) service. The relevant API Management configuration is shown in the API exhibit.

For the following statements, select Yes if the statement is true. Otherwise, select No.

The API is available to partners over the Internet

A. Yes

B. No

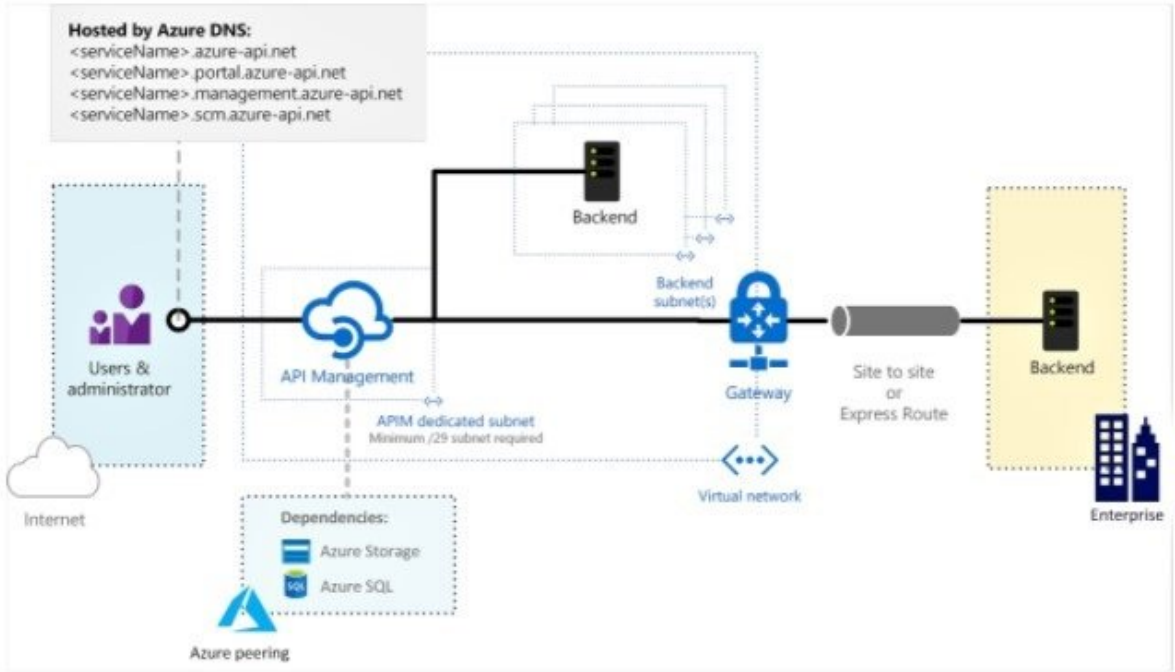
Correct

Yes – Because we are using an APIM, deployed to a VNET but configured to be "External"

Reference:

https://docs.microsoft.com/en-us/azure/api-management/api-management-using-with-vnet

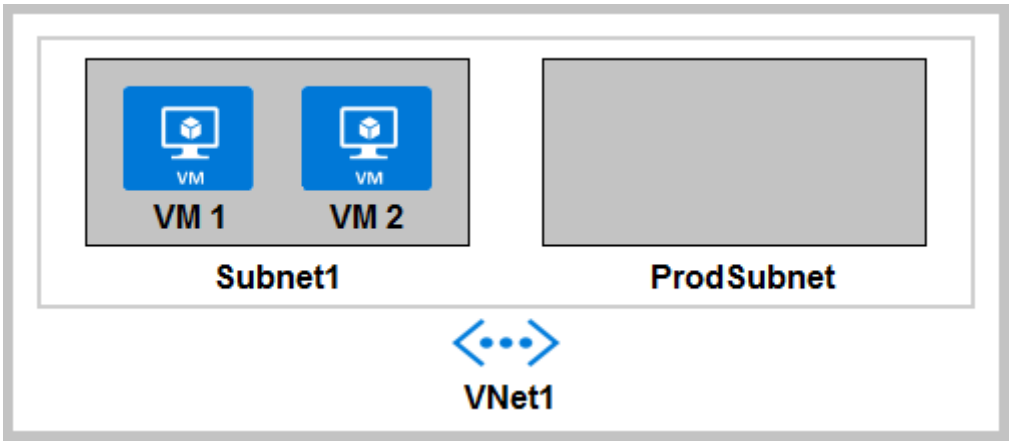
- **External**: The API Management gateway and developer portal are accessible from the public internet via an external load balancer. The gateway can access resources within the VNET.



11. Question

Your company develops a web service that is deployed to an Azure virtual machine named VM1. The web service allows an API to access real-time data from VM1.

The current virtual machine deployment is shown in the Deployment exhibit.



The chief technology officer (CTO) sends you the following email message: “Our developers have deployed the web service to a virtual machine named VM1.

Testing has shown that the API is accessible from VM1 and VM2. Our partners must be able to connect to the API over the Internet. Partners will use this data in applications that they develop.“

You deploy an Azure API Management (APIM) service. The relevant API Management configuration is shown in the API exhibit.

For the following statements, select Yes if the statement is true. Otherwise, select No.

The APIM instance can access real-time data from VM1

- A. Yes
- B. No

Correct

Yes – Because the APIM is deployed in the same vNET as VM1 just in a different subnet.

Communication between subnets are enabled by default and there is no mention of otherwise.

Reference:

https://docs.microsoft.com/en-us/azure/api-management/api-management-using-with-vnet

Connect to a virtual network using Azure API Management

07/23/2021 • 16 minutes to read • +28

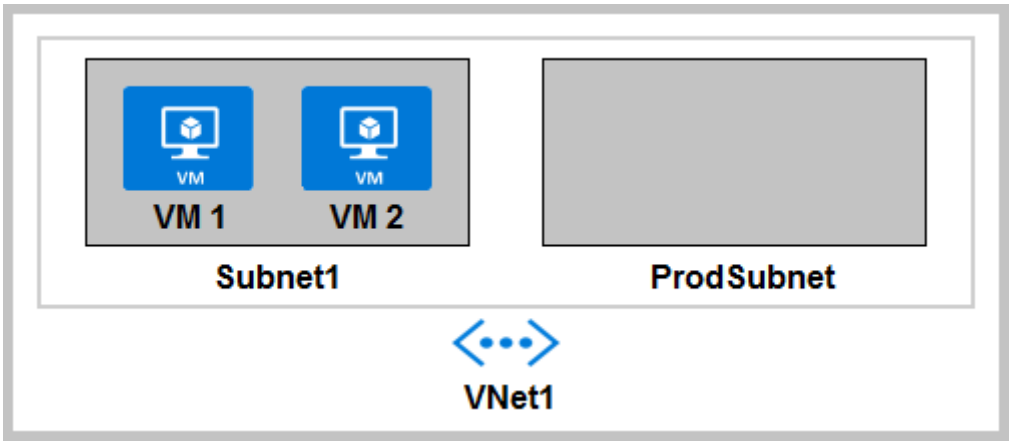
With Azure Virtual Networks (VNETs), you can place any of your Azure resources in a non-internet-routable network to which you control access. You can then connect VNETs to your on-premises networks using various VPN technologies. To learn more about Azure VNETs, start with the information in the Azure Virtual Network Overview.

Azure API Management can be deployed inside the VNET to access backend services within the network. You can configure the developer portal and API gateway to be accessible either from the internet or only within the VNET.

12. Question

Your company develops a web service that is deployed to an Azure virtual machine named VM1. The web service allows an API to access real-time data from VM1.

The current virtual machine deployment is shown in the Deployment exhibit.



The chief technology officer (CTO) sends you the following email message: “Our developers have deployed the web service to a virtual machine named VM1.

Testing has shown that the API is accessible from VM1 and VM2. Our partners must be able to connect to the API over the Internet. Partners will use this data in applications that they develop.“

You deploy an Azure API Management (APIM) service. The relevant API Management configuration is shown in the API exhibit.

For the following statements, select Yes if the statement is true. Otherwise, select No.

A VPN gateway is required for partner access

- A. Yes
- B. No

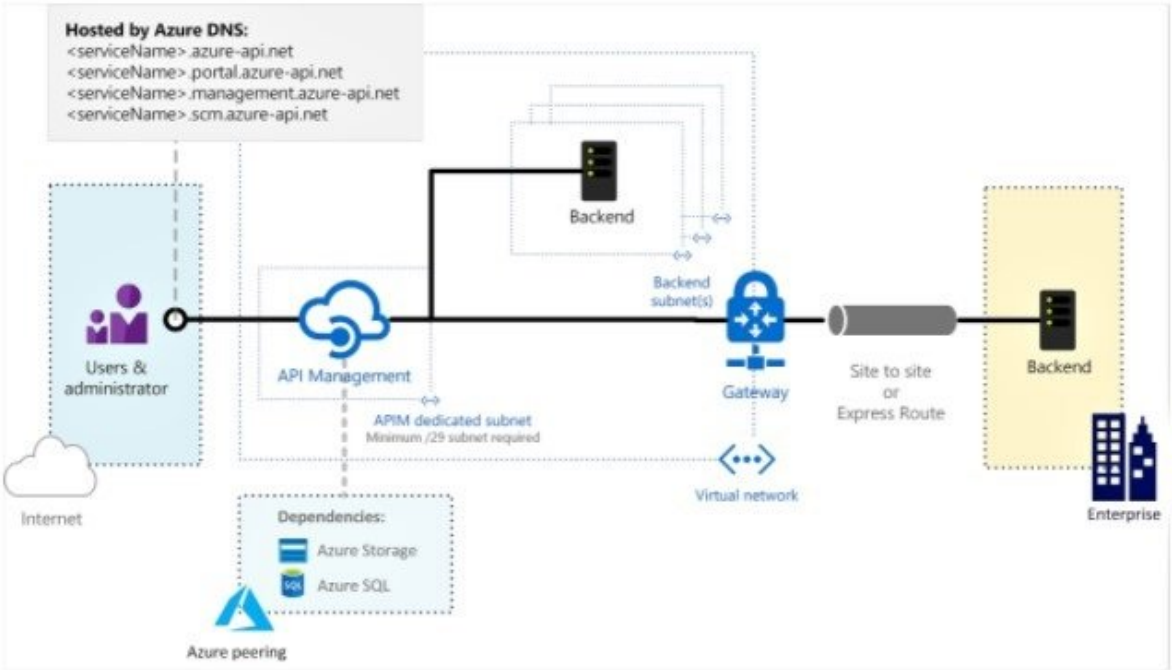
Correct

No VPN required because the APIM is accessible from the internet by virtue of it being configured as "External"

Reference:

https://docs.microsoft.com/en-us/azure/api-management/api-management-using-with-vnet

- **External**: The API Management gateway and developer portal are accessible from the public internet via an external load balancer. The gateway can access resources within the VNET.



13. Question

You have an Azure subscription that contains a storage account.

An application sometimes writes duplicate files to the storage account.

You have a PowerShell script that identifies and deletes duplicate files in the storage account. Currently, the script is run manually after approval from the operations manager.

You need to recommend a serverless solution that performs the following actions:

? Runs the script once an hour to identify whether duplicate files exist

? Sends an email notification to the operations manager requesting approval to delete the duplicate files

? Processes an email response from the operations manager specifying whether the deletion was approved

? Runs the script if the deletion was approved

What should you include in the recommendation?

- A. Azure Logic Apps and Azure Functions
- B. Azure Pipelines and Azure Service Fabric
- C. Azure Logic Apps and Azure Event Grid
- D. Azure Functions and Azure Batch

Correct

Azure Logic Apps and Azure Functions are serverless services. Use Azure Logic Apps to define the workflow and Azure Functions to execute scripts.

When you want to run code that performs a specific job in your logic apps, you can create your own function by using Azure Functions. This service helps you create Node.js, C#, and F# functions so you don‘t have to build a complete app or infrastructure to run code. You can also call logic apps from inside Azure functions. Azure Functions provides serverless computing in the cloud and is useful for performing tasks such as these examples:

? Extend your logic app‘s behavior with functions in Node.js or C#.

? Perform calculations in your logic app workflow.

? Apply advanced formatting or compute fields in your logic app workflows.

Incorrect Answers:

B. Azure Pipelines and Azure Service Fabric

Azure Pipelines are used for CI/CD integration.

C. Azure Logic Apps and Azure Event Grid

We need a service that runs the scripts.

D. Azure Functions and Azure Batch

Use Azure Batch to run large-scale parallel and high-performance computing (HPC) batch jobs efficiently in Azure. The requirement is to run simple scripts.

Reference:

https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-azure-functions

Create and run your own code from workflows in Azure Logic Apps by using Azure Functions

06/14/2021 • 12 minutes to read • +2

When you want to run code that performs a specific job in your logic app workflow, you can create a function by using Azure Functions. This service helps you create Node.js, C#, and F# functions so you don't have to build a complete app or infrastructure to run code. You can also call logic app workflows from inside an Azure function. Azure Functions provides serverless computing in the cloud and is useful for performing certain tasks, for example:

- Extend your logic app's behavior with functions in Node.js or C#.
- Perform calculations in your logic app workflow.
- Apply advanced formatting or compute fields in your logic app workflows.

To run code snippets without using Azure Functions, learn how you can add and run inline code.

Note

Azure Logic Apps doesn't support using Azure Functions with deployment slots enabled. Although this scenario might sometimes work, this behavior is unpredictable and might result in authorization problems when your workflow tries call the Azure function.

14. Question

You have an Azure subscription.

You need to deploy an Azure Kubernetes Service (AKS) solution that will use Windows Server 2019 nodes.

The solution must meet the following requirements:

? Minimize the time it takes to provision compute resources during scale-out operations.

? Support autoscaling of Windows Server containers.

Which scaling option should you recommend?

- A. cluster autoscaler
- B. horizontal pod autoscaler
- C. Kubernetes version 1.20.2 or newer
- D. Virtual nodes with Virtual Kubelet ACI

Incorrect

To keep up with application demands in Azure Kubernetes Service (AKS), you may need to adjust the number of nodes that run your workloads. The cluster autoscaler component can watch for pods in your cluster that can't be scheduled because of resource constraints. When issues are detected, the number of nodes in a node pool is increased to meet the application demand. Nodes are also regularly checked for a lack of running pods, with the number of nodes then decreased as needed. This ability to automatically scale up or down the number of nodes in your AKS cluster lets you run an efficient, cost-effective cluster.

To adjust to changing application demands, such as between the workday and evening or on a weekend, clusters often need a way to automatically scale. AKS clusters can scale in one of two ways:

The cluster autoscaler watches for pods that can't be scheduled on nodes because of resource constraints. The cluster then automatically increases the number of nodes.

The horizontal pod autoscaler uses the Metrics Server in a Kubernetes cluster to monitor the resource demand of pods. If an application needs more resources, the number of pods is automatically increased to meet the demand.

Incorrect Answers:

D. Virtual nodes with Virtual Kubelet ACI

Virtual nodes are only supported with Linux pods and nodes

Reference:

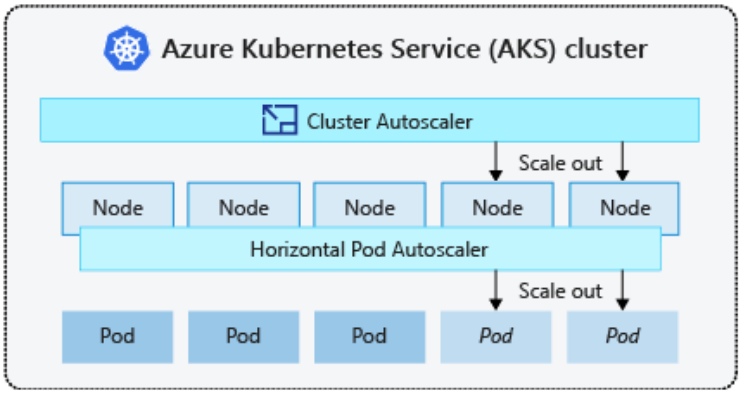
https://docs.microsoft.com/en-us/azure/aks/cluster-autoscaler

https://docs.microsoft.com/en-us/azure/aks/concepts-scale

About the cluster autoscaler

To adjust to changing application demands, such as between the workday and evening or on a weekend, clusters often need a way to automatically scale. AKS clusters can scale in one of two ways:

- The **cluster autoscaler** watches for pods that can't be scheduled on nodes because of resource constraints. The cluster then automatically increases the number of nodes.
- The **horizontal pod autoscaler** uses the Metrics Server in a Kubernetes cluster to monitor the resource demand of pods. If an application needs more resources, the number of pods is automatically increased to meet the demand.



Both the horizontal pod autoscaler and cluster autoscaler can also decrease the number of pods and nodes as needed. The cluster autoscaler decreases the number of nodes when there has been unused capacity for a period of time. Pods on a node to be removed by the cluster autoscaler are safely

scheduled elsewhere in the cluster. The cluster autoscaler may be unable to scale down if pods can't move, such as in the following situations:

- A pod is directly created and isn't backed by a controller object, such as a deployment or replica set.
- A pod disruption budget (PDB) is too restrictive and doesn't allow the number of pods to be fall below a certain threshold.
- A pod uses node selectors or anti-affinity that can't be honored if scheduled on a different node.

For more information about how the cluster autoscaler may be unable to scale down, see What types of pods can prevent the cluster autoscaler from removing a node?

The cluster autoscaler uses startup parameters for things like time intervals between scale events and resource thresholds. For more information on what parameters the cluster autoscaler uses, see Using the autoscaler profile.

The cluster and horizontal pod autoscalers can work together, and are often both deployed in a cluster. When combined, the horizontal pod autoscaler is focused on running the number of pods required to meet application demand. The cluster autoscaler is focused on running the number of nodes required to support the scheduled pods.

Note

Manual scaling is disabled when you use the cluster autoscaler. Let the cluster autoscaler determine the required number of nodes. If you want to manually scale your cluster, **disable the cluster autoscaler**.

15. Question

You have an Azure subscription that contains a Windows Virtual Desktop tenant.

You need to recommend a solution to meet the following requirements:

? Start and stop Windows Virtual Desktop session hosts based on business hours.

? Scale out Windows Virtual Desktop session hosts when required.

? Minimize compute costs.

What should you include in the recommendation?

- A. Microsoft Intune
- B. a Windows Virtual Desktop automation task
- C. Azure Automation
- D. Azure Service Health

Incorrect

You can reduce your total Azure Virtual Desktop deployment cost by scaling your virtual machines (VMs). This means shutting down and deallocating session host VMs during off-peak usage hours, then turning them back on and reallocating them during peak hours. The scaling tool built with the Azure Automation account and Azure Logic App that automatically scales session host VMs in your Azure Virtual Desktop environment.

Incorrect Answers:

A. Microsoft Intune

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM).

B. a Windows Virtual Desktop automation task

Not a valid option, there is no Azure Virtual Desktop automation task.

D. Azure Service Health

Azure Service Health is a suite of experiences that provide personalized guidance and support when issues in Azure services are or may affect you in the future.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-scaling-script

https://www.ciraltos.com/automatically-start-and-stop-wvd-vms-with-azure-automation

16. Question

Your company, named Techzen, Ltd, implements several Azure logic apps that have HTTP triggers. The logic apps provide access to an on-premises web service.

Techzen establishes a partnership with another company named Netizen, Inc.

Netizen does not have an existing Azure Active Directory (Azure AD) tenant and uses third-party OAuth 2.0 identity management to authenticate its users.

Developers at Netizen plan to use a subset of the logic apps to build applications that will integrate with the on-premises web service of Techzen.

You need to design a solution to provide the Netizen developers with access to the logic apps. The solution

must meet the following requirements:

? Requests to the logic apps from the developers must be limited to lower rates than the requests from the users at Techzen.

? The developers must be able to rely on their existing OAuth 2.0 provider to gain access to the logic apps.

? The solution must NOT require changes to the logic apps.

? The solution must NOT use Azure AD guest accounts.

What should you include in the solution?

- A. Azure AD business-to-business (B2B)
- B. Azure Front Door
- C. Azure API Management
- D. Azure AD Application Proxy

Correct

API Management helps organizations publish APIs to external, partner, and internal developers to unlock the potential of their data and services.

API Management provides the core competencies to ensure a successful API program through developer engagement, business insights, analytics, security, and protection.

You can secure API Management using the OAuth 2.0 client credentials flow.

Incorrect Answers:

A. Azure AD business-to-business (B2B)

Azure Active Directory B2B uses guest users.

B. Azure Front Door

Azure Front Door is an Application Delivery Network (ADN) as a service, offering various layer 7 load-balancing capabilities for your applications.

Azure Front Door supports HTTP, HTTPS and HTTP/2.

Applications can be authorized through OAuth 2.0.

D. Azure AD Application Proxy

Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the

Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server.

Application Proxy works with:

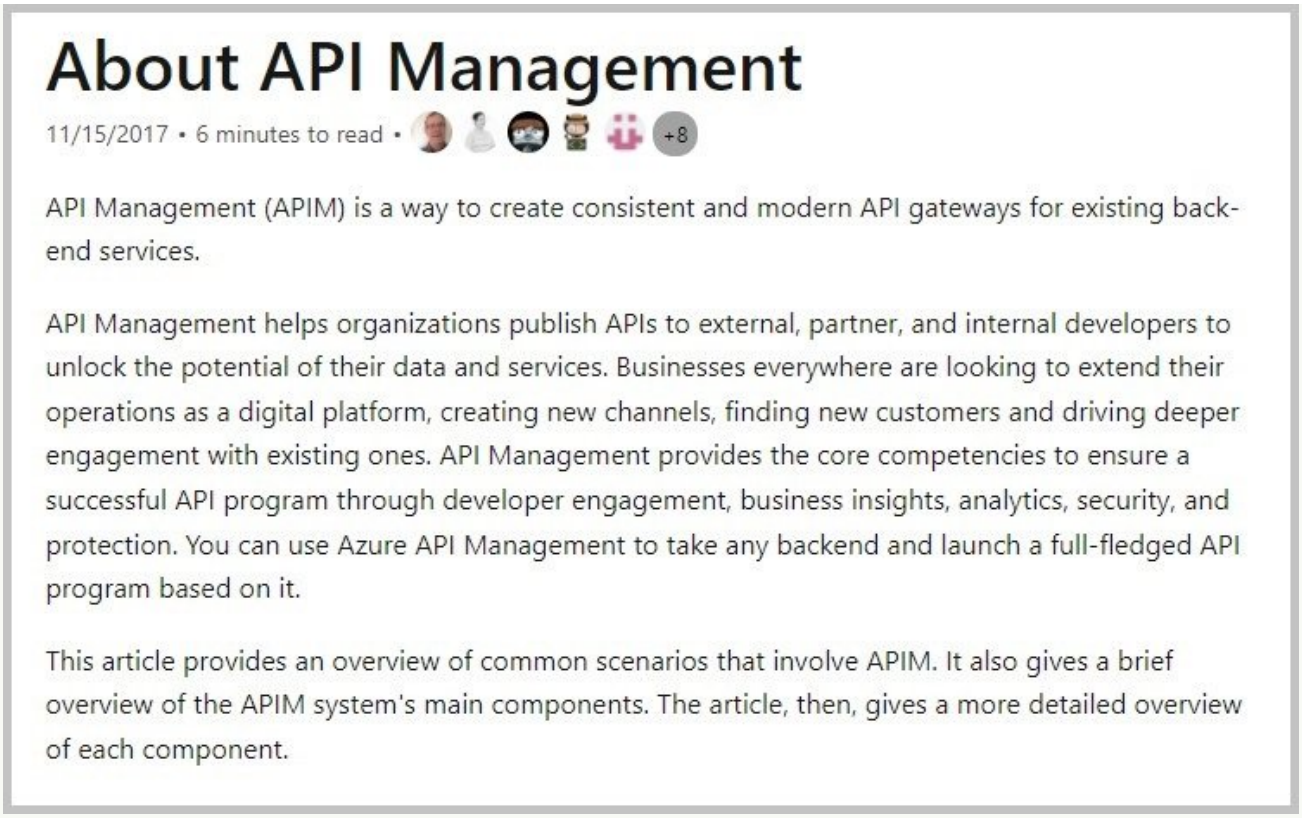
? Web applications that use Integrated Windows Authentication for authentication

? Web applications that use form-based or header-based access

Reference:

https://docs.microsoft.com/en-us/azure/api-management/api-management-key-concepts

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad#enable-oauth-20-user-authorization-in-the-developer-console



About API Management

11/15/2017 • 6 minutes to read • +8

API Management (APIM) is a way to create consistent and modern API gateways for existing back-end services.

API Management helps organizations publish APIs to external, partner, and internal developers to unlock the potential of their data and services. Businesses everywhere are looking to extend their operations as a digital platform, creating new channels, finding new customers and driving deeper engagement with existing ones. API Management provides the core competencies to ensure a successful API program through developer engagement, business insights, analytics, security, and protection. You can use Azure API Management to take any backend and launch a full-fledged API program based on it.

This article provides an overview of common scenarios that involve APIM. It also gives a brief overview of the APIM system's main components. The article, then, gives a more detailed overview of each component.

17. Question

You have an Azure subscription that contains an Azure Blob storage account named store1.

You have an on-premises file server named Server1 that runs Windows Server 2016. Server1 stores 500 GB of company files.

You need to store a copy of the company files from Server 1 in store1.

Which two possible Azure services achieve this goal?

- [x] A. an integration account
- [ ] B. an On-premises data gateway
- [ ] C. an Azure Batch account
- [ ] D. an Azure Import/Export job
- [x] E. Azure Data Factory

Incorrect

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files.

With Data Factory, you can use the Copy Activity in a data pipeline to move data from both on-premises and cloud source data stores to a centralization data store in the cloud for further analysis.

Incorrect Answers:

A. an integration account

Use integration accounts for business-to-business (B2B) solutions and seamless communication between organizations.

B. an On-premises data gateway

The on-premises data gateway acts as a bridge to provide quick and secure data transfer between on-premises data (data that isn't in the cloud) and several Microsoft cloud services. These cloud services include Power BI, PowerApps, Power Automate, Azure Analysis Services, and Azure Logic Apps.

C. an Azure Batch account

Use Azure Batch to run large-scale parallel and high-performance computing (HPC) batch jobs efficiently in Azure. It is not used for data transfer/copy.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service

https://docs.microsoft.com/en-us/azure/data-factory/introduction

What is Azure Import/Export service?

03/04/2021 • 8 minutes to read •

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files.

Supply your own disk drives and transfer data with the Azure Import/Export service. You can also use disk drives supplied by Microsoft.

If you want to transfer data using disk drives supplied by Microsoft, you can use Azure Data Box Disk to import data into Azure. Microsoft ships up to 5 encrypted solid-state disk drives (SSDs) with a 40 TB total capacity per order, to your datacenter through a regional carrier. You can quickly configure disk drives, copy data to disk drives over a USB 3.0 connection, and ship the disk drives back to Azure. For more information, go to Azure Data Box Disk overview.

Connect and collect

Enterprises have data of various types that are located in disparate sources on-premises, in the cloud, structured, unstructured, and semi-structured, all arriving at different intervals and speeds.

The first step in building an information production system is to connect to all the required sources of data and processing, such as software-as-a-service (SaaS) services, databases, file shares, and FTP web services. The next step is to move the data as needed to a centralized location for subsequent processing.

Without Data Factory, enterprises must build custom data movement components or write custom services to integrate these data sources and processing. It's expensive and hard to integrate and maintain such systems. In addition, they often lack the enterprise-grade monitoring, alerting, and the controls that a fully managed service can offer.

With Data Factory, you can use the Copy Activity in a data pipeline to move data from both on-premises and cloud source data stores to a centralization data store in the cloud for further analysis. For example, you can collect data in Azure Data Lake Storage and transform the data later by using an Azure Data Lake Analytics compute service. You can also collect data in Azure Blob storage and transform it later by using an Azure HDInsight Hadoop cluster.

18. Question

You have an on-premises Active Directory forest and an Azure Active Directory (Azure AD) tenant. All Azure AD users are assigned an Azure AD Premium P1 license.

You deploy Azure AD Connect.

Which two features are available in this environment that can reduce operational overhead for your company's help desk?

- [ ] A. Azure AD Privileged Identity Management policies
- [ ] B. access reviews
- [x] C. password writeback
- [x] D. Microsoft Cloud App Security Conditional Access App Control
- [x] E. self-service password reset

Incorrect

P1 lets your hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager (an on-premises identity and access management suite) and cloud write-back capabilities, which allow self-service password reset for your on-premises users.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis#what-are-the-azure-ad-licenses

What are the Azure AD licenses?

Microsoft Online business services, such as Microsoft 365 or Microsoft Azure, require Azure AD for sign-in and to help with identity protection. If you subscribe to any Microsoft Online business service, you automatically get Azure AD with access to all the free features.

To enhance your Azure AD implementation, you can also add paid capabilities by upgrading to Azure Active Directory Premium P1 or Premium P2 licenses. Azure AD paid licenses are built on top of your existing free directory, providing self-service, enhanced monitoring, security reporting, and secure access for your mobile users.

> ⓘ Note
>
> For the pricing options of these licenses, see **Azure Active Directory Pricing**.
>
> Azure Active Directory Premium P1 and Premium P2 are not currently supported in China. For more information about Azure AD pricing, contact the **Azure Active Directory Forum**.

- **Azure Active Directory Free.** Provides user and group management, on-premises directory synchronization, basic reports, self-service password change for cloud users, and single sign-on across Azure, Microsoft 365, and many popular SaaS apps.
- **Azure Active Directory Premium P1.** In addition to the Free features, P1 also lets your hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager (an on-premises identity and access management suite) and cloud write-back capabilities, which allow self-service password reset for your on-premises users.
- **Azure Active Directory Premium P2.** In addition to the Free and P1 features, P2 also offers Azure Active Directory Identity Protection to help provide risk-based Conditional Access to your apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.
- **"Pay as you go" feature licenses.** You can also get additional feature licenses, such as Azure Active Directory Business-to-Customer (B2C). B2C can help you provide identity and access management solutions for your customer-facing apps. For more information, see Azure Active Directory B2C documentation.

For more information about associating an Azure subscription to Azure AD, see Associate or add an Azure subscription to Azure Active Directory and for more information about assigning licenses to your users, see How to: Assign or remove Azure Active Directory licenses.

19. Question

Case Study

This is a case study. In the real exam, case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

Overview

Contoso, Ltd, is a US-based financial services company that has a main office in New York and a branch office in San Francisco.

?? Existing Environment

? Payment Processing System

? Contoso hosts a business-critical payment processing system in its New York data center. The system has three tiers: a front-end web app, a middle-tier web API, and a back-end data store implemented as a Microsoft SQL Server 2014 database. All servers run Windows Server 2012 R2.

? The front-end and middle-tier components are hosted by using Microsoft Internet Information Services (IIS). The application code is written in C# and ASP.NET.

? The middle-tier API uses the Entity Framework to communicate to the SQL Server database. Maintenance of the database is performed by using SQL Server Agent jobs.

? The database is currently 2 TB and is not expected to grow beyond 3 TB.

? The payment processing system has the following compliance-related requirements:

? Encrypt data in transit and at rest. Only the front-end and middle-tier components must be able to access the encryption keys that protect the data store.

? Keep backups of the data in two separate physical locations that are at least 200 miles apart and can be restored for up to seven years.

? Support blocking inbound and outbound traffic based on the source IP address, the destination IP address, and the port number.

? Collect Windows security logs from all the middle-tier servers and retain the logs for a period of seven years.

? Inspect inbound and outbound traffic from the front-end tier by using highly available network appliances.

? Only allow all access to all the tiers from the internal network of Contoso.

? Tape backups are configured by using an on-premises deployment of Microsoft System Center Data Protection Manager (DPM), and then shipped offsite for long term storage.

? Historical Transaction Query System

Contoso recently migrated a business-critical workload to Azure. The workload contains a .NET web service for querying the historical transaction data residing in Azure Table Storage. The .NET web service is accessible from a client app that was developed in-house and runs on the client computers in the New York office.

The data in the table storage is 50 GB and is not expected to increase.

? Current Issues

The Contoso IT team discovers poor performance of the historical transaction query system, as the queries frequently cause table scans.

?? Requirements

? Planned Changes

? Contoso plans to implement the following changes:

? Migrate the payment processing system to Azure.

? Migrate the historical transaction data to Azure Cosmos DB to address the performance issues.

? Migration Requirements

? Contoso identifies the following general migration requirements:

? Infrastructure services must remain available if a region or a data center fails. Failover must occur without any administrative intervention.

? Whenever possible, Azure managed services must be used to minimize management overhead.

? Whenever possible, costs must be minimized.

? Contoso identifies the following requirements for the payment processing system:

? If a data center fails, ensure that the payment processing system remains available without any administrative intervention. The middle-tier and the web front end must continue to operate without any additional configurations.

? Ensure that the number of compute nodes of the front-end and the middle tiers of the payment processing system can increase or decrease automatically based on CPU utilization.

? Ensure that each tier of the payment processing system is subject to a Service Level Agreement (SLA) of 99.99 percent availabilty.

? Minimize the effort required to modify the middle-tier API and the back-end tier of the payment processing system.

? Payment processing system must be able to use grouping and joining tables on encrypted columns.

? Generate alerts when unauthorized login attempts occur on the middle-tier virtual machines.

? Ensure that the payment processing system preserves its current compliance status.

? Host the middle tier of the payment processing system on a virtual machine

? Contoso identifies the following requirements for the historical transaction query system:

? Minimize the use of on-premises infrastructure services.

? Minimize the effort required to modify the .NET web service querying Azure Cosmos DB.

? Minimize the frequency of table scans.

? If a region fails, ensure that the historical transaction query system remains available without any administrative intervention.

? Information Security Requirements

? The IT security team wants to ensure that identity management is performed by using Active Directory. Password hashes must be stored on-premises only.

? Access to all business-critical systems must rely on Active Directory credentials. Any suspicious authentication attempts must trigger a multi-factor authentication prompt automatically.

Question

You need to recommend a compute solution for the middle tier of the payment processing system.

What should you include in the recommendation?

- A. virtual machine scale sets
- B. availability sets
- C. Azure Kubernetes Service (AKS)
- D. Function App

Correct

To protect your virtual machine scale sets from datacenter-level failures, you can create a scale set across Availability Zones. Azure regions that support Availability Zones have a minimum of three separate zones, each with their own independent power source, network, and cooling.

It fits the requirement:

? Ensure that the number of compute nodes of the front-end and the middle tiers of the payment processing system can increase or decrease automatically based on CPU utilization.

? Host the middle tier of the payment processing system on a virtual machine

? Ensure that each tier of the payment processing system is subject to a Service Level Agreement (SLA) of 99.99 percent availabilty

? Infrastructure services must remain available if a region or a data center fails.

? Host the middle tier of the payment processing system on a virtual machine

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-use-availability-zones

20. Question

Case Study

This is a case study. In the real exam, case studies are not timed separately. You can use as much exam

time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

Overview

Contoso, Ltd, is a US-based financial services company that has a main office in New York and a branch office in San Francisco.

?? Existing Environment

? Payment Processing System

? Contoso hosts a business-critical payment processing system in its New York data center. The system has three tiers: a front-end web app, a middle-tier web API, and a back-end data store implemented as a Microsoft SQL Server 2014 database. All servers run Windows Server 2012 R2.

? The front-end and middle-tier components are hosted by using Microsoft Internet Information Services (IIS). The application code is written in C# and ASP.NET.

? The middle-tier API uses the Entity Framework to communicate to the SQL Server database. Maintenance of the database is performed by using SQL Server Agent jobs.

? The database is currently 2 TB and is not expected to grow beyond 3 TB.

? The payment processing system has the following compliance-related requirements:

? Encrypt data in transit and at rest. Only the front-end and middle-tier components must be able to access the encryption keys that protect the data store.

? Keep backups of the data in two separate physical locations that are at least 200 miles apart and can be restored for up to seven years.

? Support blocking inbound and outbound traffic based on the source IP address, the destination IP address, and the port number.

? Collect Windows security logs from all the middle-tier servers and retain the logs for a period of seven years.

? Inspect inbound and outbound traffic from the front-end tier by using highly available network appliances.

? Only allow all access to all the tiers from the internal network of Contoso.

? Tape backups are configured by using an on-premises deployment of Microsoft System Center Data Protection Manager (DPM), and then shipped offsite for long term storage.

? Historical Transaction Query System

Contoso recently migrated a business-critical workload to Azure. The workload contains a .NET web service for querying the historical transaction data residing in Azure Table Storage. The .NET web service is accessible from a client app that was developed in-house and runs on the client computers in the New York office.

The data in the table storage is 50 GB and is not expected to increase.

? Current Issues

The Contoso IT team discovers poor performance of the historical transaction query system, as the queries

frequently cause table scans.

?? Requirements

? Planned Changes

? Contoso plans to implement the following changes:

? Migrate the payment processing system to Azure.

? Migrate the historical transaction data to Azure Cosmos DB to address the performance issues.

? Migration Requirements

? Contoso identifies the following general migration requirements:

? Infrastructure services must remain available if a region or a data center fails. Failover must occur without any administrative intervention.

? Whenever possible, Azure managed services must be used to minimize management overhead.

? Whenever possible, costs must be minimized.

? Contoso identifies the following requirements for the payment processing system:

? If a data center fails, ensure that the payment processing system remains available without any administrative intervention. The middle-tier and the web front end must continue to operate without any additional configurations.

? Ensure that the number of compute nodes of the front-end and the middle tiers of the payment processing system can increase or decrease automatically based on CPU utilization.

? Ensure that each tier of the payment processing system is subject to a Service Level Agreement (SLA) of 99.99 percent availabilty.

? Minimize the effort required to modify the middle-tier API and the back-end tier of the payment processing system.

? Payment processing system must be able to use grouping and joining tables on encrypted columns.

? Generate alerts when unauthorized login attempts occur on the middle-tier virtual machines.

? Ensure that the payment processing system preserves its current compliance status.

? Host the middle tier of the payment processing system on a virtual machine

? Contoso identifies the following requirements for the historical transaction query system:

? Minimize the use of on-premises infrastructure services.

? Minimize the effort required to modify the .NET web service querying Azure Cosmos DB.

? Minimize the frequency of table scans.

? If a region fails, ensure that the historical transaction query system remains available without any administrative intervention.

? Information Security Requirements

? The IT security team wants to ensure that identity management is performed by using Active Directory. Password hashes must be stored on-premises only.

? Access to all business-critical systems must rely on Active Directory credentials. Any suspicious authentication attempts must trigger a multi-factor authentication prompt automatically.

Question

You need to recommend a high-availability solution for the middle tier of the payment processing system. What should you include in the recommendation?

A. the Premium App Service plan

B. an availability set

C. availability zones

D. the Isolated App Service plan

Correct

Availability Zones help provide an SLA of 99.99%. Availability Sets only provide an SLA of 99.95%. The other options are Azure App Service Plans.

Reference:

https://docs.microsoft.com/en-us/azure/availability-zones/az-overview#availability-zones

Availability Zones

An Availability Zone is a high-availability offering that protects your applications and data from datacenter failures. Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there's a minimum of three separate zones in all enabled regions. The physical separation of Availability Zones within a region protects applications and data from datacenter failures. Zone-redundant services replicate your applications and data across Availability Zones to protect from single-points-of-failure. With Availability Zones, Azure offers industry best 99.99% VM uptime SLA. The full Azure SLA explains the guaranteed availability of Azure as a whole.

An Availability Zone in an Azure region is a combination of a fault domain and an update domain. For example, if you create three or more VMs across three zones in an Azure region, your VMs are effectively distributed across three fault domains and three update domains. The Azure platform recognizes this distribution across update domains to make sure that VMs in different zones are not scheduled to be updated at the same time.

Build high-availability into your application architecture by co-locating your compute, storage, networking, and data resources within a zone and replicating in other zones. Azure services that support Availability Zones fall into two categories:

- **Zonal services** – where a resource is pinned to a specific zone (for example, virtual machines, managed disks, Standard IP addresses), or
- **Zone-redundant services** – when the Azure platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).

Note

Both Standard SKU Public IP Addresses and Public IP Address Prefix resource types also have a "no-zone" option. This allows customers to utilize Standard SKU public IPs (and associate them to resources which only allow Standard SKU), but does not give a guarantee of redundancy. (All Public IP addresses that are **upgraded** from Basic to Standard SKU will be of type "no-zone".)

21. Question

Case Study

This is a case study. In the real exam, case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

Overview

Contoso, Ltd, is a US-based financial services company that has a main office in New York and a branch office in San Francisco.

?? Existing Environment

? Payment Processing System

? Contoso hosts a business-critical payment processing system in its New York data center. The system has three tiers: a front-end web app, a middle-tier web API, and a back-end data store implemented as a Microsoft SQL Server 2014 database. All servers run Windows Server 2012 R2.

? The front-end and middle-tier components are hosted by using Microsoft Internet Information Services (IIS). The application code is written in C# and ASP.NET.

? The middle-tier API uses the Entity Framework to communicate to the SQL Server database. Maintenance of the database is performed by using SQL Server Agent jobs.

? The database is currently 2 TB and is not expected to grow beyond 3 TB.

? The payment processing system has the following compliance-related requirements:

? Encrypt data in transit and at rest. Only the front-end and middle-tier components must be able to access the encryption keys that protect the data store.

? Keep backups of the data in two separate physical locations that are at least 200 miles apart and can be restored for up to seven years.

? Support blocking inbound and outbound traffic based on the source IP address, the destination IP address, and the port number.

? Collect Windows security logs from all the middle-tier servers and retain the logs for a period of seven years.

? Inspect inbound and outbound traffic from the front-end tier by using highly available network appliances.

? Only allow all access to all the tiers from the internal network of Contoso.

? Tape backups are configured by using an on-premises deployment of Microsoft System Center Data Protection Manager (DPM), and then shipped offsite for long term storage.

? Historical Transaction Query System

Contoso recently migrated a business-critical workload to Azure. The workload contains a .NET web service for querying the historical transaction data residing in Azure Table Storage. The .NET web service is

accessible from a client app that was developed in-house and runs on the client computers in the New York office.

The data in the table storage is 50 GB and is not expected to increase.

? Current Issues

The Contoso IT team discovers poor performance of the historical transaction query system, as the queries frequently cause table scans.

?? Requirements

? Planned Changes

? Contoso plans to implement the following changes:

? Migrate the payment processing system to Azure.

? Migrate the historical transaction data to Azure Cosmos DB to address the performance issues.

? Migration Requirements

? Contoso identifies the following general migration requirements:

? Infrastructure services must remain available if a region or a data center fails. Failover must occur without any administrative intervention.

? Whenever possible, Azure managed services must be used to minimize management overhead.

? Whenever possible, costs must be minimized.

? Contoso identifies the following requirements for the payment processing system:

? If a data center fails, ensure that the payment processing system remains available without any administrative intervention. The middle-tier and the web front end must continue to operate without any additional configurations.

? Ensure that the number of compute nodes of the front-end and the middle tiers of the payment processing system can increase or decrease automatically based on CPU utilization.

? Ensure that each tier of the payment processing system is subject to a Service Level Agreement (SLA) of 99.99 percent availabilty.

? Minimize the effort required to modify the middle-tier API and the back-end tier of the payment processing system.

? Payment processing system must be able to use grouping and joining tables on encrypted columns.

? Generate alerts when unauthorized login attempts occur on the middle-tier virtual machines.

? Ensure that the payment processing system preserves its current compliance status.

? Host the middle tier of the payment processing system on a virtual machine

? Contoso identifies the following requirements for the historical transaction query system:

? Minimize the use of on-premises infrastructure services.

? Minimize the effort required to modify the .NET web service querying Azure Cosmos DB.

? Minimize the frequency of table scans.

? If a region fails, ensure that the historical transaction query system remains available without any administrative intervention.

? Information Security Requirements

? The IT security team wants to ensure that identity management is performed by using Active Directory. Password hashes must be stored on-premises only.

? Access to all business-critical systems must rely on Active Directory credentials. Any suspicious

authentication attempts must trigger a multi-factor authentication prompt automatically.

Question

You need to recommend a disaster recovery solution for the back-end tier of the payment processing system.

What should you include in the recommendation?

- A. Azure Site Recovery
- B. an auto-failover group
- C. Always On Failover Cluster Instances
- D. geo-redundant database backups

Correct

With Auto-failover groups, you can automate the failover of databases using user policies. Azure Site Recovery is not used for replication of Azure SQL databases. With active geo-replication, you need to perform a manual failover.

Scenario:

? The back-end data store is implemented as a Microsoft SQL Server 2014 database.

? If a data center fails, ensure that the payment processing system remains available without any administrative intervention.

Note: Auto-failover groups is a SQL Database feature that allows you to manage replication and failover of a group of databases on a SQL Database server or all databases in a managed instance to another region. It is a declarative abstraction on top of the existing active geo-replication feature, designed to simplify deployment and management of geo-replicated databases at scale.

Reference:

https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auto-failover-group

Use auto-failover groups to enable transparent and coordinated failover of multiple databases

09/14/2021 • 37 minutes to read • +11

APPLIES TO: Azure SQL Database Azure SQL Managed Instance

The auto-failover groups feature allows you to manage the replication and failover of a group of databases on a server or all databases in a managed instance to another region. It is a declarative abstraction on top of the existing active geo-replication feature, designed to simplify deployment and management of geo-replicated databases at scale. You can initiate failover manually or you can delegate it to the Azure service based on a user-defined policy. The latter option allows you to automatically recover multiple related databases in a secondary region after a catastrophic failure or other unplanned event that results in full or partial loss of the SQL Database or SQL Managed Instance availability in the primary region. A failover group can include one or multiple databases, typically used by the same application. Additionally, you can use the readable secondary databases to offload read-only query workloads. Because auto-failover groups involve multiple databases, these databases must be configured on the primary server. Auto-failover groups support replication of all databases in the group to only one secondary server or instance in a different region.

22. Question

Case Study

This is a case study. In the real exam, case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

Overview

Contoso, Ltd, is a US-based financial services company that has a main office in New York and a branch office in San Francisco.

?? Existing Environment

? Payment Processing System

? Contoso hosts a business-critical payment processing system in its New York data center. The system has three tiers: a front-end web app, a middle-tier web API, and a back-end data store implemented as a Microsoft SQL Server 2014 database. All servers run Windows Server 2012 R2.

? The front-end and middle-tier components are hosted by using Microsoft Internet Information Services (IIS). The application code is written in C# and ASP.NET.

? The middle-tier API uses the Entity Framework to communicate to the SQL Server database. Maintenance of the database is performed by using SQL Server Agent jobs.

? The database is currently 2 TB and is not expected to grow beyond 3 TB.

? The payment processing system has the following compliance-related requirements:

? Encrypt data in transit and at rest. Only the front-end and middle-tier components must be able to access the encryption keys that protect the data store.

? Keep backups of the data in two separate physical locations that are at least 200 miles apart and can be restored for up to seven years.

? Support blocking inbound and outbound traffic based on the source IP address, the destination IP address, and the port number.

? Collect Windows security logs from all the middle-tier servers and retain the logs for a period of seven years.

? Inspect inbound and outbound traffic from the front-end tier by using highly available network appliances.

? Only allow all access to all the tiers from the internal network of Contoso.

? Tape backups are configured by using an on-premises deployment of Microsoft System Center Data Protection Manager (DPM), and then shipped offsite for long term storage.

? Historical Transaction Query System

Contoso recently migrated a business-critical workload to Azure. The workload contains a .NET web service for querying the historical transaction data residing in Azure Table Storage. The .NET web service is accessible from a client app that was developed in-house and runs on the client computers in the New York office.

The data in the table storage is 50 GB and is not expected to increase.

? Current Issues

The Contoso IT team discovers poor performance of the historical transaction query system, as the queries frequently cause table scans.

?? Requirements

? Planned Changes

? Contoso plans to implement the following changes:

? Migrate the payment processing system to Azure.

? Migrate the historical transaction data to Azure Cosmos DB to address the performance issues.

? Migration Requirements

? Contoso identifies the following general migration requirements:

? Infrastructure services must remain available if a region or a data center fails. Failover must occur without any administrative intervention.

? Whenever possible, Azure managed services must be used to minimize management overhead.

? Whenever possible, costs must be minimized.

? Contoso identifies the following requirements for the payment processing system:

? If a data center fails, ensure that the payment processing system remains available without any administrative intervention. The middle-tier and the web front end must continue to operate without any additional configurations.

? Ensure that the number of compute nodes of the front-end and the middle tiers of the payment

processing system can increase or decrease automatically based on CPU utilization.

? Ensure that each tier of the payment processing system is subject to a Service Level Agreement (SLA) of 99.99 percent availabilty.

? Minimize the effort required to modify the middle-tier API and the back-end tier of the payment processing system.

? Payment processing system must be able to use grouping and joining tables on encrypted columns.

? Generate alerts when unauthorized login attempts occur on the middle-tier virtual machines.

? Ensure that the payment processing system preserves its current compliance status.

? Host the middle tier of the payment processing system on a virtual machine

? Contoso identifies the following requirements for the historical transaction query system:

? Minimize the use of on-premises infrastructure services.

? Minimize the effort required to modify the .NET web service querying Azure Cosmos DB.

? Minimize the frequency of table scans.

? If a region fails, ensure that the historical transaction query system remains available without any administrative intervention.

? Information Security Requirements

? The IT security team wants to ensure that identity management is performed by using Active Directory. Password hashes must be stored on-premises only.

? Access to all business-critical systems must rely on Active Directory credentials. Any suspicious authentication attempts must trigger a multi-factor authentication prompt automatically.

Question

You need to recommend a backup solution for the data store of the payment processing system.

What should you include in the recommendation?

- A. Microsoft System Center Data Protection Manager (DPM)
- B. Azure Backup Server
- **C. Azure SQL long-term backup retention**
- D. Azure Managed Disks

Correct

Since the payment processing system DB is still in SQL and in the requirement this payment processing system has been planned to be migrated to Azure where “Infrastructure services must remain available if a region or a data center fails. Failover must occur without any administrative intervention. Whenever possible, Azure managed services must be used to minimize management overhead. Whenever possible, costs must be minimized. If a data center fails, ensure that the payment processing system remains available without any administrative intervention. Keep backups of the data in two separate physical locations that are at least 200 miles apart and can be restored for up to seven years.“

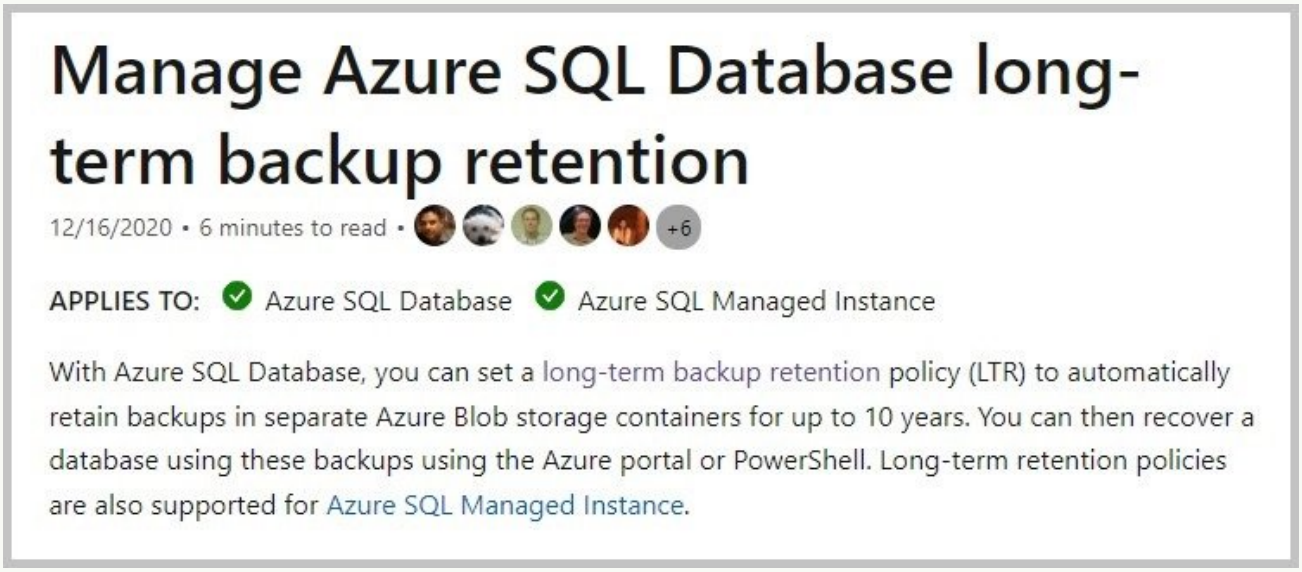
This requirement get satisfied only With Azure SQL Database, you can set a long-term backup retention policy (LTR) to automatically retain backups in separate Azure Blob storage containers for up to 10 years.

You can then recover a database using these backups using the Azure portal or PowerShell. Long-term retention policies are also supported for Azure SQL Managed Instance.

On premise has the requirement: Keep backups of the data in two separate physical locations that are at least 200 miles apart and can be restored for up to seven years

Reference:

https://docs.microsoft.com/en-us/azure/sql-database/sql-database-long-term-backup-retention-configure



Manage Azure SQL Database long-term backup retention

12/16/2020 • 6 minutes to read • +6

APPLIES TO: Azure SQL Database Azure SQL Managed Instance

With Azure SQL Database, you can set a long-term backup retention policy (LTR) to automatically retain backups in separate Azure Blob storage containers for up to 10 years. You can then recover a database using these backups using the Azure portal or PowerShell. Long-term retention policies are also supported for Azure SQL Managed Instance.

23. Question

You are designing an application that will aggregate content for users.

You need to recommend a database solution for the application. The solution must meet the following requirements:

? Support SQL commands.

? Support multi-master writes.

? Guarantee low latency read operations.

What should you include in the recommendation?

- A. Azure Cosmos DB SQL API
- B. Azure SQL Database that uses active geo-replication
- C. Azure SQL Database Hyperscale
- D. Azure Database for PostgreSQL

Correct

With Cosmos DB's novel multi-region (multi-master) writes replication protocol, every region supports both writes and reads. The multi-region writes capability also enables:

? Unlimited elastic write and read scalability.

? 99.999% read and write availability all around the world.

? Guaranteed reads and writes served in less than 10 milliseconds at the 99th percentile.

Reference:

https://docs.microsoft.com/en-us/azure/cosmos-db/distribute-data-globally

https://docs.microsoft.com/en-us/azure/cosmos-db/sql/how-to-multi-master?tabs=api-async

Key benefits of global distribution

Build global active-active apps. With its novel multi-region writes replication protocol, every region supports both writes and reads. The multi-region writes capability also enables:

- Unlimited elastic write and read scalability.
- 99.999% read and write availability all around the world.
- Guaranteed reads and writes served in less than 10 milliseconds at the 99th percentile.

As you add and remove regions to and from your Azure Cosmos account, your application does not need to be redeployed or paused, it continues to be highly available at all times.

Build highly responsive apps. Your application can perform near real-time reads and writes against all the regions you chose for your database. Azure Cosmos DB internally handles the data replication between regions with consistency level guarantees of the level you've selected.

Build highly available apps. Running a database in multiple regions worldwide increases the availability of a database. If one region is unavailable, other regions automatically handle application requests. Azure Cosmos DB offers 99.999% read and write availability for multi-region databases.

Maintain business continuity during regional outages. Azure Cosmos DB supports automatic failover during a regional outage. During a regional outage, Azure Cosmos DB continues to maintain its latency, availability, consistency, and throughput SLAs. To help make sure that your entire application is highly available, Cosmos DB offers a manual failover API to simulate a regional outage. By using this API, you can carry out regular business continuity drills.

Scale read and write throughput globally. You can enable every region to be writable and elastically scale reads and writes all around the world. The throughput that your application configures on an Azure Cosmos database or a container is provisioned across all regions associated with your Azure Cosmos account. The provisioned throughput is guaranteed up by financially backed SLAs.

Choose from several well-defined consistency models. The Azure Cosmos DB replication protocol offers five well-defined, practical, and intuitive consistency models. Each model has a tradeoff between consistency and performance. Use these consistency models to build globally distributed applications with ease.

24. Question

You have SQL Server on an Azure virtual machine. The databases are written to nightly as part of a batch process.

You need to recommend a disaster recovery solution for the data. The solution must meet the following requirements:

? Provide the ability to recover in the event of a regional outage.

? Support a recovery time objective (RTO) of 15 minutes.

? Support a recovery point objective (RPO) of 24 hours.

? Support automated recovery.

? Minimize costs.

What should you include in the recommendation?

- A. Azure virtual machine availability sets
- B. Azure Disk Backup
- C. an Always On availability group
- D. Azure Site Recovery

Incorrect

Your choice of a BCDR technology to recover SQL Server instances should be based on your recovery time objective (RTO) and recovery point objective (RPO) needs as described in the following table.

Combine Site Recovery with the failover operation of your chosen technology to orchestrate recovery of your entire application.

Replication with Azure Site Recover:

? RTO is typically less than 15 minutes.

? RPO: One hour for application consistency and five minutes for crash consistency.

Reference:

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-sql

Combining BCDR technologies with Site Recovery

Your choice of a BCDR technology to recover SQL Server instances should be based on your recovery time objective (RTO) and recovery point objective (RPO) needs as described in the following table. Combine Site Recovery with the failover operation of your chosen technology to orchestrate recovery of your entire application.

Deployment type	BCDR technology	Expected RTO for SQL Server	Expected RPO for SQL Server
SQL Server on an Azure	Always On availability	The time taken to make the secondary	Because replication to the secondary replica is

infrastructure as a service (IaaS) virtual machine (VM) or at on-premises.	group	replica as primary.	asynchronous, there's some data loss.
SQL Server on an Azure IaaS VM or at on-premises.	Failover clustering (Always On FCI)	The time taken to fail over between the nodes.	Because Always On FCI uses shared storage, the same view of the storage instance is available on failover.
SQL Server on an Azure IaaS VM or at on-premises.	Database mirroring (high-performance mode)	The time taken to force the service, which uses the mirror server as a warm standby server.	Replication is asynchronous. The mirror database might lag somewhat behind the principal database. The lag is typically small. But it can become large if the principal or mirror server's system is under a heavy load. Log shipping can be a supplement to database mirroring. It's a favorable alternative to asynchronous database mirroring.
SQL as platform as a service (PaaS) on Azure. This deployment type includes single databases and elastic pools.	Active geo-replication	30 seconds after failover is triggered. When failover is activated for one of the secondary databases, all other secondaries are automatically linked to the new primary.	RPO of five seconds. Active geo-replication uses the Always On technology of SQL Server. It asynchronously replicates committed transactions on the primary database to a secondary database by using snapshot isolation. The secondary data is guaranteed to never have partial transactions.
SQL as PaaS configured with active geo-replication on Azure. This deployment type includes a managed instances, elastic pools, and single	Auto-failover groups	RTO of one hour.	RPO of five seconds. Auto-failover groups provide the group semantics on top of active geo-replication. But the same asynchronous replication mechanism is used.

databases.

SQL Server on an Azure IaaS VM or at on-premises.	Replication with Azure Site Recovery	RTO is typically less than 15 minutes. To learn more, read the RTO SLA provided by Site Recovery.	One hour for application consistency and five minutes for crash consistency. If you are looking for lower RPO, use other BCDR technologies.

25. Question

You plan to move a web app named App1 from an on-premises datacenter to Azure.

App1 depends on a custom COM component that is installed on the host server.

You need to recommend a solution to host App1 in Azure. The solution must meet the following requirements:

? App1 must be available to users if an Azure datacenter becomes unavailable.

? Costs must be minimized.

What should you include in the recommendation?

- A. In two Azure regions, deploy a load balancer and a web app
- B. In two Azure regions, deploy a load balancer and a virtual machine scale set
- C. Deploy a load balancer and a virtual machine scale set across two availability zones
- D. In two Azure regions, deploy an Azure Traffic Manager profile and a web app

Correct

The scaling would allow to reduce cost for situations of lighter traffic. And the use of avail. zones fulfills the requirement of high availability.

Question states data centre unavailable not region and minimise cost. This only leaves option C.

Reference:

https://docs.microsoft.com/en-us/dotnet/azure/migration/app-service

Migrate your .NET web app or service to Azure App Service

Article • 09/15/2021 • 4 minutes to read • 4 contributors

App Service is a fully managed compute platform service that's optimized for hosting scalable websites and web applications. This article provides information on how to lift-and-shift an existing application to Azure App Service, modifications to consider, and additional resources for moving to the cloud. Most ASP.NET websites (Webforms, MVC) and services (Web API, WCF) can move directly to Azure App Service with no changes. Some may need minor changes while others may need some refactoring.

26. Question

You have an Azure SQL database named DB1 that contains multiple tables.

You need to improve the performance of DB1. The solution must minimize administrative effort.

What should you use?

- A. automatic tuning
- B. Azure Advisor
- C. Azure Monitor
- D. Query Performance Insight

Correct

Azure SQL Database and Azure SQL Managed Instance automatic tuning provides peak performance and stable workloads through continuous performance tuning based on AI and machine learning.

Automatic tuning is a fully managed intelligent performance service that uses built-in intelligence to continuously monitor queries executed on a database, and it automatically improves their performance. This is achieved through dynamically adapting database to the changing workloads and applying tuning recommendations. Automatic tuning learns horizontally from all databases on Azure through AI and it dynamically improves its tuning actions. The longer a database runs with automatic tuning on, the better it performs.

Incorrect Answers:

B. Azure Advisor

Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments.

C. Azure Monitor

Azure Monitor helps you maximize the availability and performance of your applications and services. It

delivers a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments.

D. Query Performance Insight

Query Performance Insight helps to identify the top resource consuming and long-running queries in your workload.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/automatic-tuning-overview

Automatic tuning in Azure SQL Database and Azure SQL Managed Instance

03/23/2021 • 5 minutes to read • +1

APPLIES TO: Azure SQL Database Azure SQL Managed Instance

Azure SQL Database and Azure SQL Managed Instance automatic tuning provides peak performance and stable workloads through continuous performance tuning based on AI and machine learning.

Automatic tuning is a fully managed intelligent performance service that uses built-in intelligence to continuously monitor queries executed on a database, and it automatically improves their performance. This is achieved through dynamically adapting a database to changing workloads and applying tuning recommendations. Automatic tuning learns horizontally from all databases on Azure through AI and it dynamically improves its tuning actions. The longer a database runs with automatic tuning on, the better it performs.

Azure SQL Database and Azure SQL Managed Instance automatic tuning might be one of the most important features that you can enable to provide stable and peak performing database workloads.

What can automatic tuning do for you

- Automated performance tuning of databases
- Automated verification of performance gains
- Automated rollback and self-correction
- Tuning history
- Tuning action Transact-SQL (T-SQL) scripts for manual deployments
- Proactive workload performance monitoring
- Scale out capability on hundreds of thousands of databases
- Positive impact to DevOps resources and the total cost of ownership

27. Question

Case Study

This is a case study. In the real exam, case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

Overview

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

? Existing Environment

? Active Directory Environment

The network contains two Active Directory forests named corp.fabrikam.com and rd.fabrikam.com. There are no trust relationships between the forests.

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only.

?Network Infrastructure

Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.

All the offices have a high-speed connection to the Internet.

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

? Problem Statements

The use of WebApp1 is unpredictable. At peak times, users often report delays. At other times, many resources for WebApp1 are underutilized.

? Requirements

? Planned Changes

? Fabrikam plans to move most of its production workloads to Azure during the next few years.

? As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft 365 deployment.

? All R&D operations will remain on-premises.

? Fabrikam plans to migrate the production and test instances of WebApp1 to Azure.

? Technical Requirements

Fabrikam identifies the following technical requirements:

? Web site content must be easily updated from a single point.

? User input must be minimized when provisioning new web app instances.

? Whenever possible, existing on-premises licenses must be used to reduce cost.

? Users must always authenticate by using their corp.fabrikam.com UPN identity.

? Any new deployments to Azure must be redundant in case an Azure region fails.

? Whenever possible, solutions must be deployed to Azure by using the Standard pricing tier of Azure App Service.

? An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.

? Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on- premises network.

? Database Requirements

Fabrikam identifies the following database requirements:

? Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.

? To avoid disrupting customer access, database downtime must be minimized when databases are migrated.

? Database backups must be retained for a minimum of seven years to meet compliance requirements.

? Security Requirements

Fabrikam identifies the following security requirements:

? Company information including policies, templates, and data must be inaccessible to anyone outside the company.

? Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.

? Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.

? All administrative access to the Azure portal must be secured by using multi-factor authentication.

? The testing of WebApp1 updates must not be visible to anyone outside the company.

Question

To meet the authentication requirements of Fabrikam, What is the minimum number of Azure tenants required for the implementation?

- 1
- 2
- 3
- 4

Incorrect

We just need one Azure AD tenant to host the information for corp.cloudportalhub.com

You need “Conditional Access: Block access by location“ to meet this requirement “Company information including policies, templates, and data must be inaccessible to anyone outside the company.“

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-location

Conditional Access: Block access by location

05/26/2020 • 2 minutes to read •

With the location condition in Conditional Access, you can control access to your cloud apps based on the network location of a user. The location condition is commonly used to block access from countries/regions where your organization knows traffic should not come from.

> ⓘ Note
>
> Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

Define locations

1. Sign in to the **Azure portal** as a global administrator, security administrator, or Conditional Access administrator.
2. Browse to **Azure Active Directory** > **Security** > **Conditional Access** > **Named locations**.
3. Choose **New location**.
4. Give your location a name.
5. Choose **IP ranges** if you know the specific externally accessible IPv4 address ranges that make up that location or **Countries/Regions**.
   a. Provide the **IP ranges** or select the **Countries/Regions** for the location you are specifying.
      - If you choose Countries/Regions, you can optionally choose to include unknown areas.
6. Choose **Save**

More information about the location condition in Conditional Access can be found in the article, What is the location condition in Azure Active Directory Conditional Access

28. Question

Case Study

This is a case study. In the real exam, case studies are not timed separately. You can use as much exam

time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

Overview

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

? Existing Environment

? Active Directory Environment

The network contains two Active Directory forests named corp.fabrikam.com and rd.fabrikam.com. There are no trust relationships between the forests.

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only.

?Network Infrastructure

Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.

All the offices have a high-speed connection to the Internet.

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

? Problem Statements

The use of WebApp1 is unpredictable. At peak times, users often report delays. At other times, many resources for WebApp1 are underutilized.

? Requirements

? Planned Changes

? Fabrikam plans to move most of its production workloads to Azure during the next few years.

? As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft 365 deployment.

? All R&D operations will remain on-premises.

? Fabrikam plans to migrate the production and test instances of WebApp1 to Azure.

? Technical Requirements

Fabrikam identifies the following technical requirements:

? Web site content must be easily updated from a single point.

? User input must be minimized when provisioning new web app instances.

? Whenever possible, existing on-premises licenses must be used to reduce cost.

? Users must always authenticate by using their corp.fabrikam.com UPN identity.

? Any new deployments to Azure must be redundant in case an Azure region fails.

? Whenever possible, solutions must be deployed to Azure by using the Standard pricing tier of Azure App Service.

? An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.

? Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on- premises network.

? Database Requirements

Fabrikam identifies the following database requirements:

? Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.

? To avoid disrupting customer access, database downtime must be minimized when databases are migrated.

? Database backups must be retained for a minimum of seven years to meet compliance requirements.

? Security Requirements

Fabrikam identifies the following security requirements:

? Company information including policies, templates, and data must be inaccessible to anyone outside the company.

? Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.

? Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.

? All administrative access to the Azure portal must be secured by using multi-factor authentication.

? The testing of WebApp1 updates must not be visible to anyone outside the company.

Question

To meet the authentication requirements of Fabrikam, What is the minimum number of custom domains required for the implementation?

- 1
- 2
- 3
- 4

Incorrect

We just need one custom domain to be created for corp.fabrikam.com

You need “Conditional Access: Block access by location“ to meet this requirement “Company information

including policies, templates, and data must be inaccessible to anyone outside the company."

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-location

Conditional Access: Block access by location

05/26/2020 • 2 minutes to read •

With the location condition in Conditional Access, you can control access to your cloud apps based on the network location of a user. The location condition is commonly used to block access from countries/regions where your organization knows traffic should not come from.

> ⓘ **Note**
>
> Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

Define locations

1. Sign in to the **Azure portal** as a global administrator, security administrator, or Conditional Access administrator.
2. Browse to **Azure Active Directory** > **Security** > **Conditional Access** > **Named locations**.
3. Choose **New location**.
4. Give your location a name.
5. Choose **IP ranges** if you know the specific externally accessible IPv4 address ranges that make up that location or **Countries/Regions**.
   a. Provide the **IP ranges** or select the **Countries/Regions** for the location you are specifying.
      - If you choose Countries/Regions, you can optionally choose to include unknown areas.
6. Choose **Save**

More information about the location condition in Conditional Access can be found in the article, What is the location condition in Azure Active Directory Conditional Access

29. Question

Case Study

This is a case study. In the real exam, case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included

on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

Overview

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

? Existing Environment

? Active Directory Environment

The network contains two Active Directory forests named corp.fabrikam.com and rd.fabrikam.com. There are no trust relationships between the forests.

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only.

?Network Infrastructure

Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.

All the offices have a high-speed connection to the Internet.

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

? Problem Statements

The use of WebApp1 is unpredictable. At peak times, users often report delays. At other times, many resources for WebApp1 are underutilized.

? Requirements

? Planned Changes

? Fabrikam plans to move most of its production workloads to Azure during the next few years.

? As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft 365 deployment.

? All R&D operations will remain on-premises.

? Fabrikam plans to migrate the production and test instances of WebApp1 to Azure.

? Technical Requirements

Fabrikam identifies the following technical requirements:

? Web site content must be easily updated from a single point.

? User input must be minimized when provisioning new web app instances.

? Whenever possible, existing on-premises licenses must be used to reduce cost.

? Users must always authenticate by using their corp.fabrikam.com UPN identity.

? Any new deployments to Azure must be redundant in case an Azure region fails.

? Whenever possible, solutions must be deployed to Azure by using the Standard pricing tier of Azure App Service.

? An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.

? Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on- premises network.

? Database Requirements

Fabrikam identifies the following database requirements:

? Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.

? To avoid disrupting customer access, database downtime must be minimized when databases are migrated.

? Database backups must be retained for a minimum of seven years to meet compliance requirements.

? Security Requirements

Fabrikam identifies the following security requirements:

? Company information including policies, templates, and data must be inaccessible to anyone outside the company.

? Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.

? Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.

? All administrative access to the Azure portal must be secured by using multi-factor authentication.

? The testing of WebApp1 updates must not be visible to anyone outside the company.

Question

To meet the authentication requirements of Fabrikam, What is the minimum number of conditional access policies required for the implementation?

- 1
- 2
- 3
- 4

Incorrect

Scenario:

? Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.

? Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com

credentials.

? All administrative access to the Azure portal must be secured by using multi-factor authentication.

Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials and all administrative access to the Azure portal must be secured by using multi-factor authentication. As this is the only requirement to create a conditional access policy, so we need only 1.

Note:

Users must always authenticate by using their corp.fabrikam.com UPN identity.

The network contains two Active Directory forests named corp.fabrikam.com and rd.fabrikam.com. There are no trust relationships between the forests.

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only.

Reference:

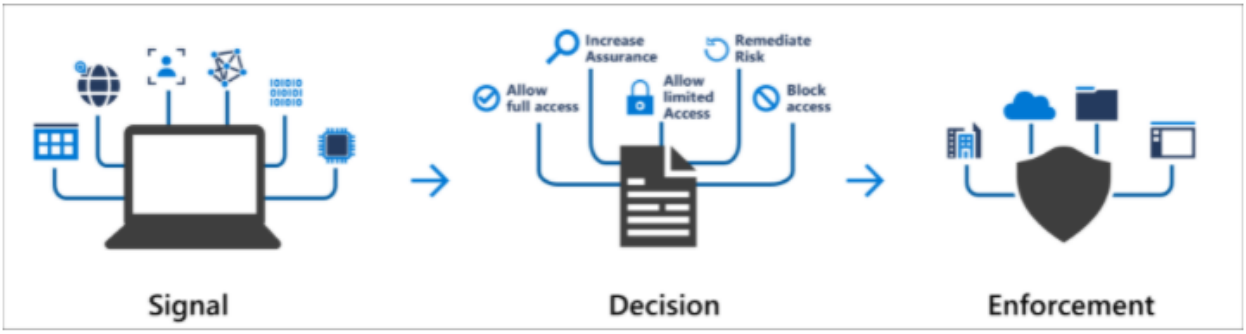
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

What is Conditional Access?

01/27/2021 • 2 minutes to read • +9

The modern security perimeter now extends beyond an organization's network to include user and device identity. Organizations can utilize these identity signals as part of their access control decisions.

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.

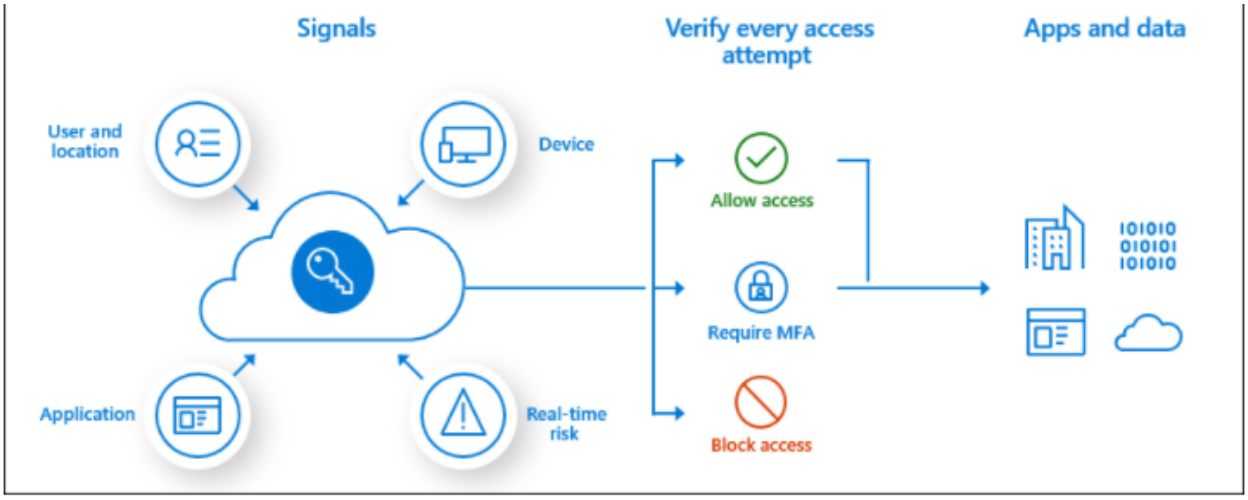


Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it.

Administrators are faced with two primary goals:

- Empower users to be productive wherever and whenever
- Protect the organization's assets

By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.



Important

Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

30. Question

Your company provides customer support for multiple Azure subscriptions and third-party hosting providers.

You are designing a centralized monitoring solution. The solution must provide the following services:

? Collect log and diagnostic data from all the third-party hosting providers into a centralized repository.

? Collect log and diagnostic data from all the subscriptions into a centralized repository.

? Automatically analyze log data and detect threats.

? Provide automatic responses to known events.

Which Azure service should you include in the solution?

- A. Azure Sentinel
- B. Azure Log Analytics
- C. Azure Monitor
- D. Azure Application Insights

Correct

Azure Sentinel is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.

? Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

? Detect previously undetected threats, and minimize false positives using Microsoft's analytics and

unparalleled threat intelligence.

? Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.

? Respond to incidents rapidly with built-in orchestration and automation of common tasks.

Incorrect Answers:

B. Azure Log Analytics

Log Analytics is a tool in the Azure portal to edit and run log queries from data collected by Azure Monitor Logs and interactively analyze their results.

C. Azure Monitor

It delivers a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments.

D. Azure Application Insights

Application Insights is an extensible Application Performance Management (APM) service for developers and DevOps professionals.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/overview

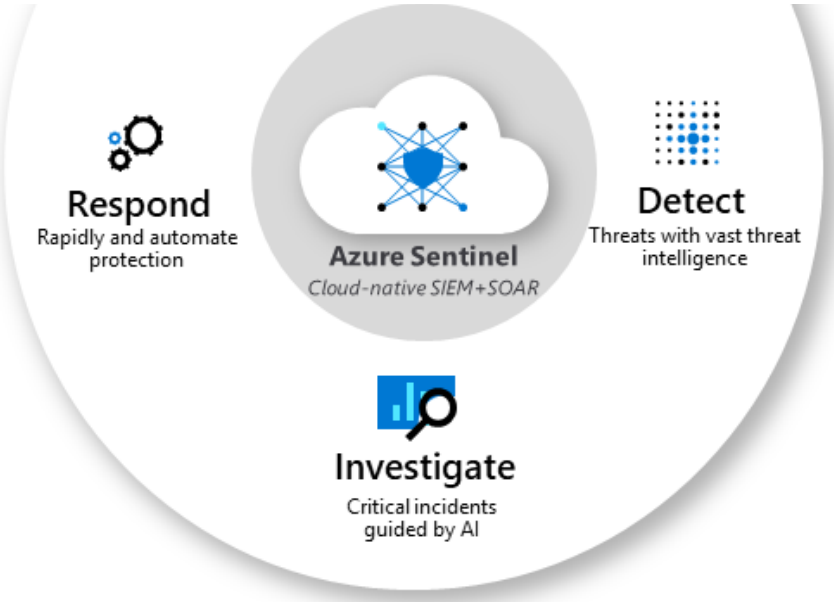
What is Azure Sentinel?

08/23/2021 • 5 minutes to read • +3

Microsoft Azure Sentinel is a scalable, cloud-native, **security information event management (SIEM)** and **security orchestration automated response (SOAR)** solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Azure Sentinel is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.

- **Collect data at cloud scale** across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
- **Detect previously undetected threats**, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.
- **Investigate threats with artificial intelligence**, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.
- **Respond to incidents rapidly** with built-in orchestration and automation of common tasks.



Building on the full range of existing Azure services, Azure Sentinel natively incorporates proven foundations, like Log Analytics, and Logic Apps. Azure Sentinel enriches your investigation and detection with AI, and provides Microsoft's threat intelligence stream and enables you to bring your own threat intelligence.

31. Question

You are designing an access policy for your company.

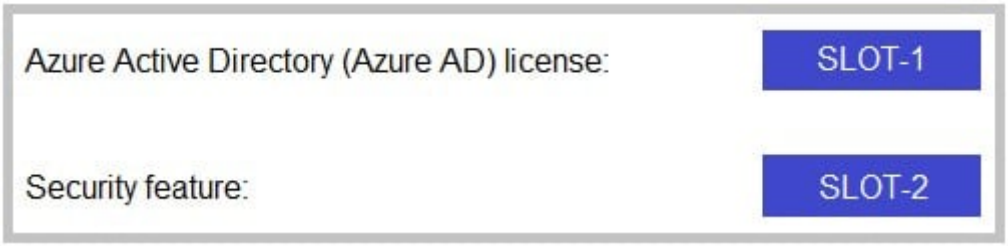
Occasionally, the developers at the company must stop, start, and restart Azure virtual machines. The development team changes often.

You need to recommend a solution to provide the developers with the required access to the virtual machines. The solution must meet the following requirements:

? Provide permissions only when needed.

? Use the principle of least privilege.

? Minimize costs.



Which of the following would go into Slot1?

- A. Free
- B. Premium P1
- C. Premium P2

Correct

To achieve the requirement, you need to implement Azure AD Privileged Identity Management (PIM).

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.

Using PIM feature requires an Azure AD Premium P2 license.

Incorrect Answers:

Free & Premium P1 does not provide PIM feature.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

What is Azure AD Privileged Identity Management?

06/25/2021 • 8 minutes to read •

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune. The following video introduces you to important PIM concepts and features.

Reasons to use

Organizations want to minimize the number of people who have access to secure information or resources, because that reduces the chance of

- a malicious actor getting access
- an authorized user inadvertently impacting a sensitive resource

However, users still need to carry out privileged operations in Azure AD, Azure, Microsoft 365, or SaaS apps. Organizations can give users just-in-time privileged access to Azure and Azure AD resources and can oversee what those users are doing with their privileged access.

License requirements

Using this feature requires an Azure AD Premium P2 license. To find the right license for your requirements, see Comparing generally available features of the Free, Office 365 Apps, and Premium editions.

For information about licenses for users, see License requirements to use Privileged Identity Management.

32. Question

You are designing an access policy for your company.

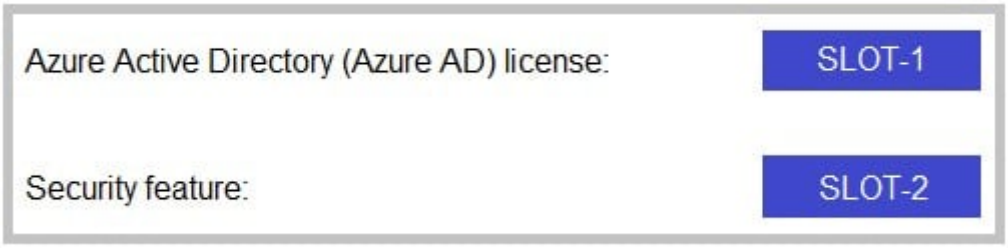
Occasionally, the developers at the company must stop, start, and restart Azure virtual machines. The development team changes often.

You need to recommend a solution to provide the developers with the required access to the virtual machines. The solution must meet the following requirements:

? Provide permissions only when needed.

? Use the principle of least privilege.

? Minimize costs.



Which of the following would go into Slot2?

- A. Just in time VM access
- B. A conditional access policy
- C. Azure AD Privileged Identity Management

Correct

To achieve the requirement, you need to implement Azure AD Privileged Identity Management (PIM).

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.

Incorrect Answers:

A. Just in time VM access

The goal of JIT is to ensure that even though your inbound traffic is locked down, Security Center still provides easy access to connect to VMs when needed. JIT does not provide access to start, stop and restart virtual machines.

B. A conditional access policy

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. This is primarily used to enforce security features like multi factor authentication.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

What is Azure AD Privileged Identity Management?

06/25/2021 • 8 minutes to read •

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune. The following video introduces you to important PIM concepts and features.

Reasons to use

Organizations want to minimize the number of people who have access to secure information or resources, because that reduces the chance of

- a malicious actor getting access
- an authorized user inadvertently impacting a sensitive resource

However, users still need to carry out privileged operations in Azure AD, Azure, Microsoft 365, or SaaS apps. Organizations can give users just-in-time privileged access to Azure and Azure AD resources and can oversee what those users are doing with their privileged access.

License requirements

Using this feature requires an Azure AD Premium P2 license. To find the right license for your requirements, see Comparing generally available features of the Free, Office 365 Apps, and Premium editions.

For information about licenses for users, see License requirements to use Privileged Identity Management.

33. Question

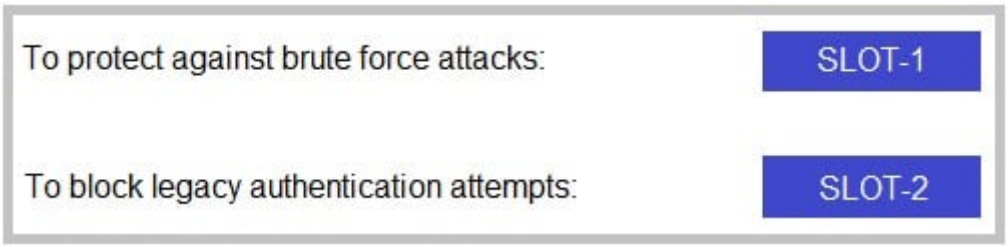
You have the Free edition of a hybrid Azure Active Directory (Azure AD) tenant. The tenant uses password hash synchronization.

You need to recommend a solution to meet the following requirements:

? Prevent Active Directory domain user accounts from being locked out as the result of brute force attacks targeting Azure AD user accounts.

? Block legacy authentication attempts to Azure AD integrated apps.

? Minimize costs.



Which of the following would go into Slot1?

- A. Azure AD Password Protection
- B. Conditional access policies
- C. Pass-through authentication
- D. Smart lockout

Correct

Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in. Smart lockout can recognize sign-ins that come from valid users and treat them differently than ones of attackers and other unknown sources. Attackers get locked out, while your users continue to access their accounts and be productive.

Note: Smart lockout is always on, for all Azure AD customers, with these default settings that offer the right mix of security and usability. Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

34. Question

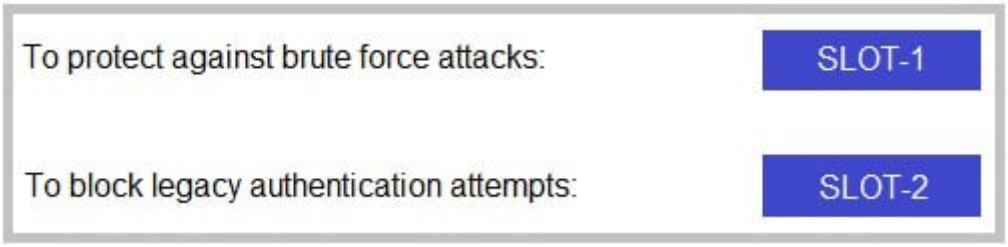
You have the Free edition of a hybrid Azure Active Directory (Azure AD) tenant. The tenant uses password hash synchronization.

You need to recommend a solution to meet the following requirements:

? Prevent Active Directory domain user accounts from being locked out as the result of brute force attacks targeting Azure AD user accounts.

? Block legacy authentication attempts to Azure AD integrated apps.

? Minimize costs.



Which of the following would go into Slot2?

- A. Azure AD Application Proxy
- B. Azure AD Password Protection
- C. Conditional access policies
- D. Enable Security defaults

Incorrect

After security defaults are enabled in your tenant, all authentication requests made by an older protocol will be blocked. Security defaults blocks Exchange Active Sync basic authentication.

Incorrect Answers:

A. Azure AD Application Proxy

Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications.

B. Azure AD Password Protection

Azure AD Password Protection detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization.

C. Conditional access policies

Conditional access policies can be used to block legacy authentication methods. However, this option requires premium license. In this question, free edition of Azure AD is used and costs must be minimized.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults#blocking-legacy-authentication

Blocking legacy authentication

To give your users easy access to your cloud apps, Azure AD supports various authentication protocols, including legacy authentication. *Legacy authentication* is a term that refers to an authentication request made by:

- Clients that don't use modern authentication (for example, an Office 2010 client).
- Any client that uses older mail protocols such as IMAP, SMTP, or POP3.

Today, most compromising sign-in attempts come from legacy authentication. Legacy authentication doesn't support Multi-Factor Authentication. Even if you have a Multi-Factor Authentication policy enabled on your directory, an attacker can authenticate by using an older protocol and bypass Multi-Factor Authentication.

After security defaults are enabled in your tenant, all authentication requests made by an older protocol will be blocked. Security defaults blocks Exchange Active Sync basic authentication.

⚠ **Warning**

Before you enable security defaults, make sure your administrators aren't using older authentication protocols. For more information, see **How to move away from legacy authentication.**

35. Question

A company deploys Azure Active Directory (Azure AD) Connect to synchronize identity information from their on-premises Active Directory Domain Services (AD

DS) directory to their Azure AD tenant. The identity information that is synchronized includes user accounts, credential hashes for authentication (password sync), and group memberships. The company plans to deploy several Windows and Linux virtual machines (VMs) to support their applications.

The VMs have the following requirements:

? Support domain join, LDAP read, LDAP bind, NTLM and Kerberos authentication, and Group Policy.

? Allow users to sign in to the domain using their corporate credentials and connect remotely to the VM by using Remote Desktop.

You need to support the VM deployment.

Which service should you use?

- A. Active Directory Federation Services (AD FS)
- B. Azure AD Privileged Identity Management
- C. Azure Managed Identity
- D. Azure AD Domain Services

Incorrect

Azure Active Directory Domain Services (AD DS) provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. You use these domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.

Incorrect Answers:

A. Active Directory Federation Services (AD FS)

ADFS does not allow authentication protocols, such as LDAP.

B. Azure AD Privileged Identity Management

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization.

C. Azure Managed Identity

Managed identities eliminate the need for developers to manage credentials. Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-overview

What is Azure Active Directory Domain Services?

04/28/2021 • 5 minutes to read • +1

Azure Active Directory Domain Services (Azure AD DS) provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. You use these domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.

An Azure AD DS managed domain lets you run legacy applications in the cloud that can't use modern authentication methods, or where you don't want directory lookups to always go back to an on-premises AD DS environment. You can lift and shift those legacy applications from your on-premises environment into a managed domain, without needing to manage the AD DS environment in the cloud.

Azure AD DS integrates with your existing Azure AD tenant. This integration lets users sign in to services and applications connected to the managed domain using their existing credentials. You can also use existing groups and user accounts to secure access to resources. These features provide a smoother lift-and-shift of on-premises resources to Azure.

36. Question

You have a hybrid deployment of Azure Active Directory (Azure AD).

You need to recommend a solution to ensure that the Azure AD tenant can be managed only from the

computers on your on-premises network.

What should you include in the recommendation?

- A. a conditional access policy
- B. Azure AD roles and administrators
- C. Azure AD Application Proxy
- D. Azure AD Privileged Identity Management

Correct

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Some of the common signals that Conditional Access can take in to account when making a policy decision include the following signals:

IP Location information

Organizations can create trusted IP address ranges that can be used when making policy decisions. Administrators can specify entire countries/regions IP ranges to block or allow traffic from.

Device

Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.

Application

Users attempting to access specific applications can trigger different Conditional Access policies.

Incorrect Answers:

B. Azure AD roles and administrators

This used to configure various roles for users. Configuring the Azure AD roles does not limit the access for an application from specific Device / IP location.

C. Azure AD Application Proxy

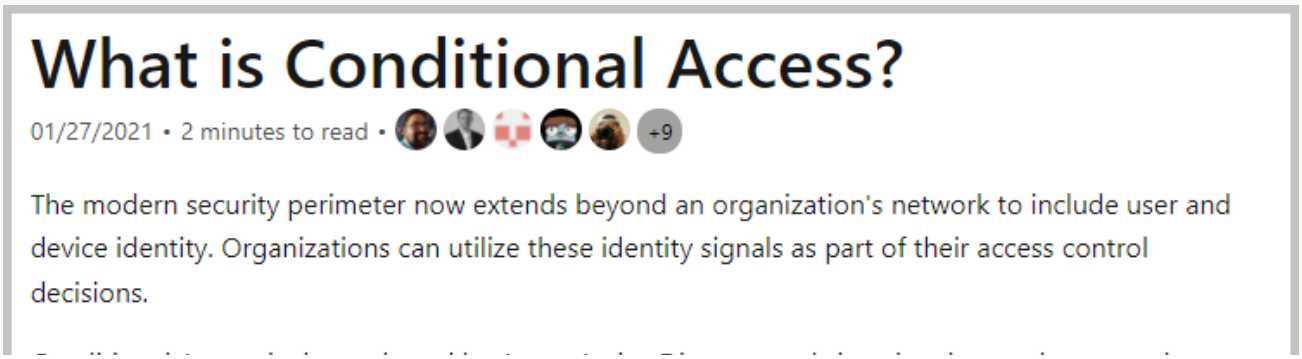
Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications.

D. Azure AD Privileged Identity Management

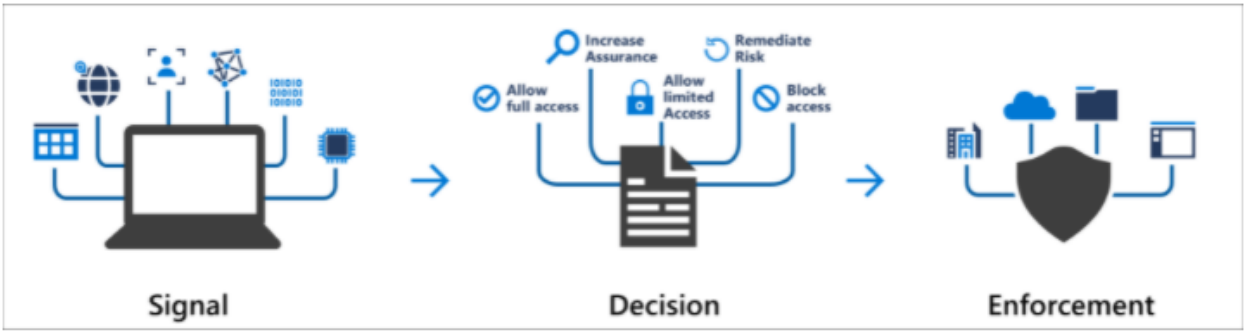
Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview



Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.

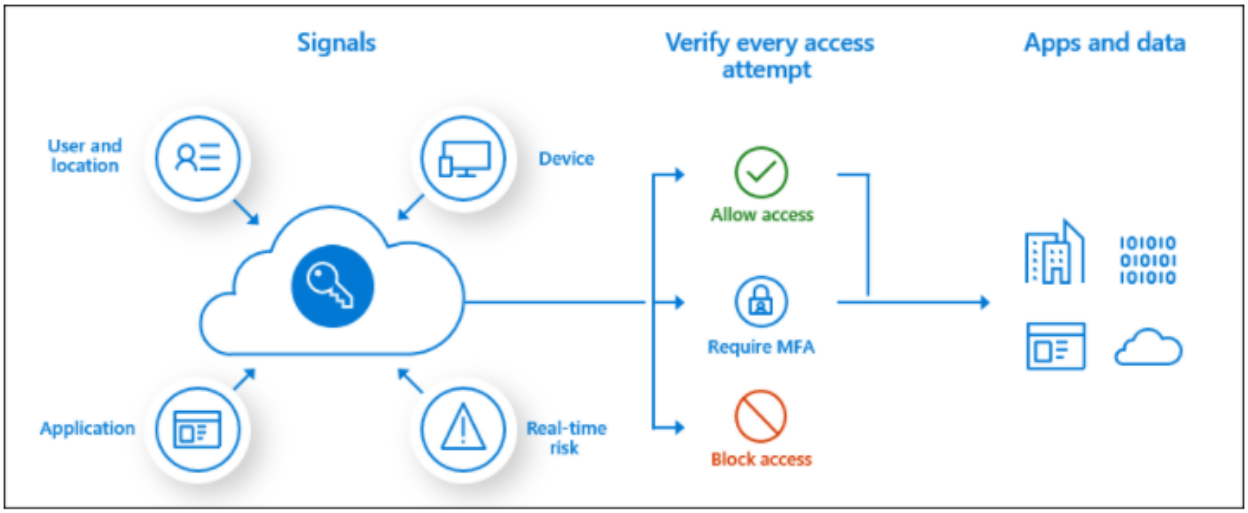


Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it.

Administrators are faced with two primary goals:

- Empower users to be productive wherever and whenever
- Protect the organization's assets

By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.



Important

Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

37. Question

You plan to automate the deployment of resources to Azure subscriptions.

What is a difference between using Azure Blueprints and Azure Resource Manager templates?

A. Azure Resource Manager templates remain connected to the deployed resources

B. Only Azure Resource Manager templates can contain policy definitions

C. Azure Blueprints remain connected to the deployed resources

D. Only Azure Blueprints can contain policy definitions

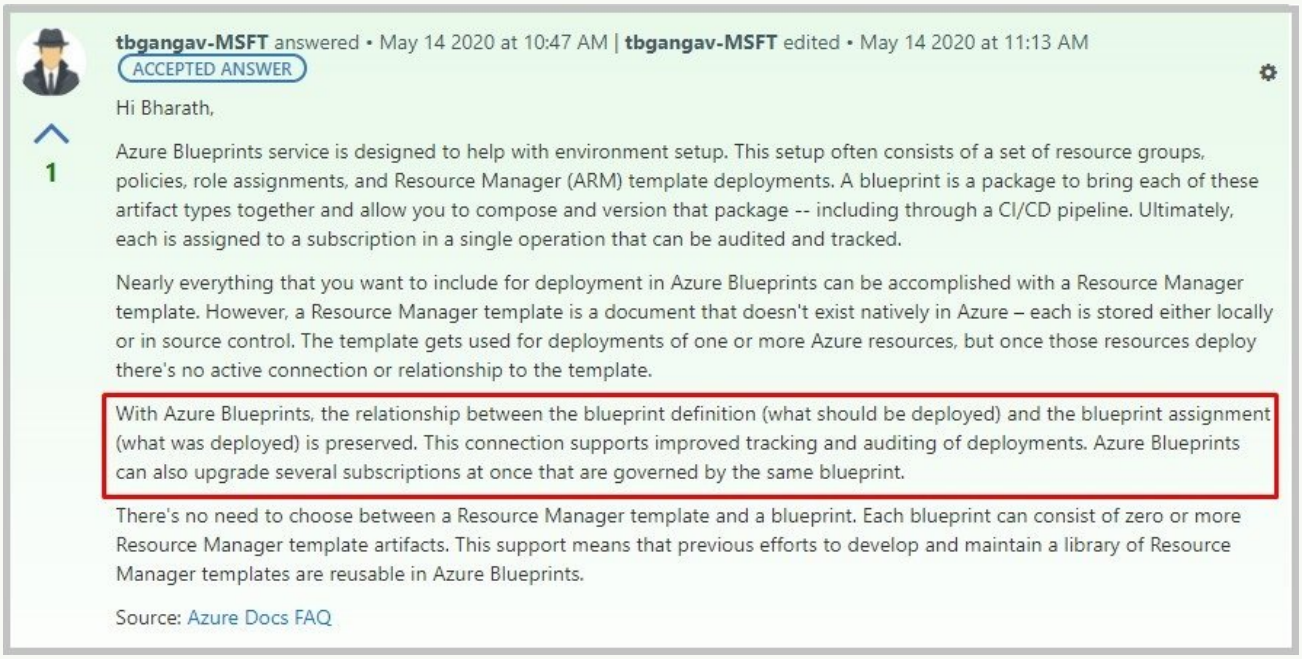
Incorrect

With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved. This connection supports improved tracking and auditing of deployments. Azure Blueprints can also upgrade several subscriptions at once that are governed by the same blueprint.

Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

https://docs.microsoft.com/en-us/answers/questions/26851/how-is-azure-blue-prints-different-from-resource-m.html



tbgangav-MSFT answered • May 14 2020 at 10:47 AM | **tbgangav-MSFT** edited • May 14 2020 at 11:13 AM

ACCEPTED ANSWER

1

Hi Bharath,

Azure Blueprints service is designed to help with environment setup. This setup often consists of a set of resource groups, policies, role assignments, and Resource Manager (ARM) template deployments. A blueprint is a package to bring each of these artifact types together and allow you to compose and version that package -- including through a CI/CD pipeline. Ultimately, each is assigned to a subscription in a single operation that can be audited and tracked.

Nearly everything that you want to include for deployment in Azure Blueprints can be accomplished with a Resource Manager template. However, a Resource Manager template is a document that doesn't exist natively in Azure – each is stored either locally or in source control. The template gets used for deployments of one or more Azure resources, but once those resources deploy there's no active connection or relationship to the template.

With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved. This connection supports improved tracking and auditing of deployments. Azure Blueprints can also upgrade several subscriptions at once that are governed by the same blueprint.

There's no need to choose between a Resource Manager template and a blueprint. Each blueprint can consist of zero or more Resource Manager template artifacts. This support means that previous efforts to develop and maintain a library of Resource Manager templates are reusable in Azure Blueprints.

Source: Azure Docs FAQ

38. Question

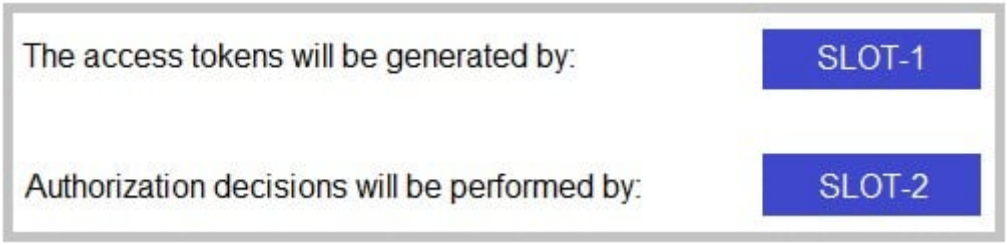
You are designing a software as a service (SaaS) application that will enable Azure Active Directory (Azure AD) users to create and publish online surveys. The

SaaS application will have a front-end web app and a back-end web API. The web app will rely on the web API to handle updates to customer surveys.

You need to design an authorization flow for the SaaS application. The solution must meet the following requirements:

? To access the back-end web API, the web app must authenticate by using OAuth 2 bearer tokens.

? The web app must authenticate by using the identities of individual users.



Which of the following would go into Slot1?

- A. Azure AD
- B. A Web App
- C. A Web API

Incorrect

Azure AD is used to authenticate users and generate access tokens. One of the main features of an identity platform is to verify, or authenticate, credentials when a user signs in to a device, application, or service.

Incorrect Answers:

B. A Web App

Frontends are not used to authenticate users. Usually, authentication is delegated to a different system or backend.

C. A Web API

A web API does not provide built-in mechanism to authenticate users.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/overview-authentication

What is Azure Active Directory authentication?

01/22/2021 • 4 minutes to read •

One of the main features of an identity platform is to verify, or *authenticate*, credentials when a user signs in to a device, application, or service. In Azure Active Directory (Azure AD), authentication involves more than just the verification of a username and password. To improve security and reduce the need for help desk assistance, Azure AD authentication includes the following components:

- Self-service password reset
- Azure AD Multi-Factor Authentication
- Hybrid integration to write password changes back to on-premises environment
- Hybrid integration to enforce password protection policies for an on-premises environment
- Passwordless authentication

39. Question

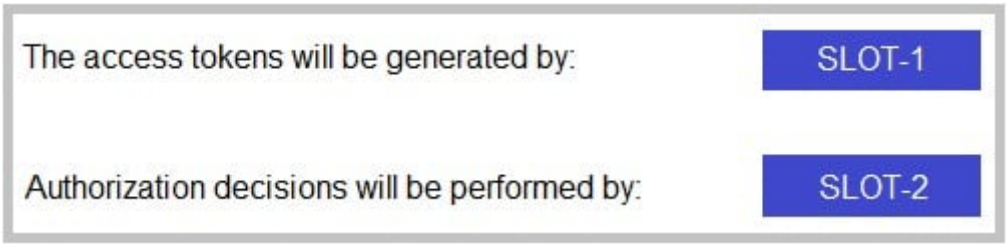
You are designing a software as a service (SaaS) application that will enable Azure Active Directory (Azure AD) users to create and publish online surveys. The

SaaS application will have a front-end web app and a back-end web API. The web app will rely on the web API to handle updates to customer surveys.

You need to design an authorization flow for the SaaS application. The solution must meet the following requirements:

? To access the back-end web API, the web app must authenticate by using OAuth 2 bearer tokens.

? The web app must authenticate by using the identities of individual users.



Which of the following would go into Slot2?

- A. Azure AD
- B. A Web App
- C. A Web API

Incorrect

You can authorize the access based on access token in the Web API

Incorrect Answers:

A. Azure AD

Azure AD is used to authenticate users and generate access tokens.

B. A Web App

Frontends are not used to authenticate or authorize users.

Reference:

https://docs.microsoft.com/lb-lu/azure/architecture/multitenant-identity/web-api

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v2-dotnet-native-aspnet

Quickstart: Call an ASP.NET web API that's protected by Microsoft identity platform

10/05/2020 • 7 minutes to read •

In this quickstart, you download and run a code sample that demonstrates how to protect an ASP.NET web API by restricting access to its resources to authorized accounts only. The sample supports authorization of personal Microsoft accounts and accounts in any Azure Active Directory (Azure AD) organization.

The article also uses a Windows Presentation Foundation (WPF) app to demonstrate how you can request an access token to access a web API.

Prerequisites

- An Azure account with an active subscription. Create an account for free.
- Visual Studio 2017 or 2019. Download Visual Studio for free.

40. Question

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

In the real exam, after you answer a question in this section, you will NOT be able to return to it.

You are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting that displays cost broken down by department.

Solution: Create a resource group for each resource type. Assign tags to each resource group.

Does this meet the goal?

- A. Yes
- B. No

Correct

Instead use tags at resource level

The resource groups in this approach only contain one resource type. So the department deployments are spread across multiple resource groups.

Adding tags to the resource group and grouping by resource group will only show the costs per resource type, not per department

Reference:

https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/group-filter

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies

41. Question

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

In the real exam, after you answer a question in this section, you will NOT be able to return to it.

You are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting that displays cost broken down by department.

Solution: Create a new subscription for each department.

Does this meet the goal?

- A. Yes
- B. No

Correct

Instead use tags at resource level.

Reference:

https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/quick-acm-cost-analysis

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/view-all-accounts

42. Question

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

In the real exam, after you answer a question in this section, you will NOT be able to return to it.

You are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting that displays cost broken down by department.

Solution: Create a separate resource group for each department. Place the resources for each department

in its respective resource group.

Does this meet the goal?

- A. Yes
- B. No

Incorrect

Instead use tags at resource level.

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json#tags-and-billing

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

43. Question

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

In the real exam, after you answer a question in this section, you will NOT be able to return to it.

You are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting that displays cost broken down by department.

Solution: Place all resources in the same resource group. Assign tags to each resource.

Does this meet the goal?

- A. Yes
- B. No

Correct

There are 2 Solutions here : both are correct

1- Place Each department resources in a separate RG . Assign tags to each resource.

2- Place all resources in the same RG. Assign tags to each resource.

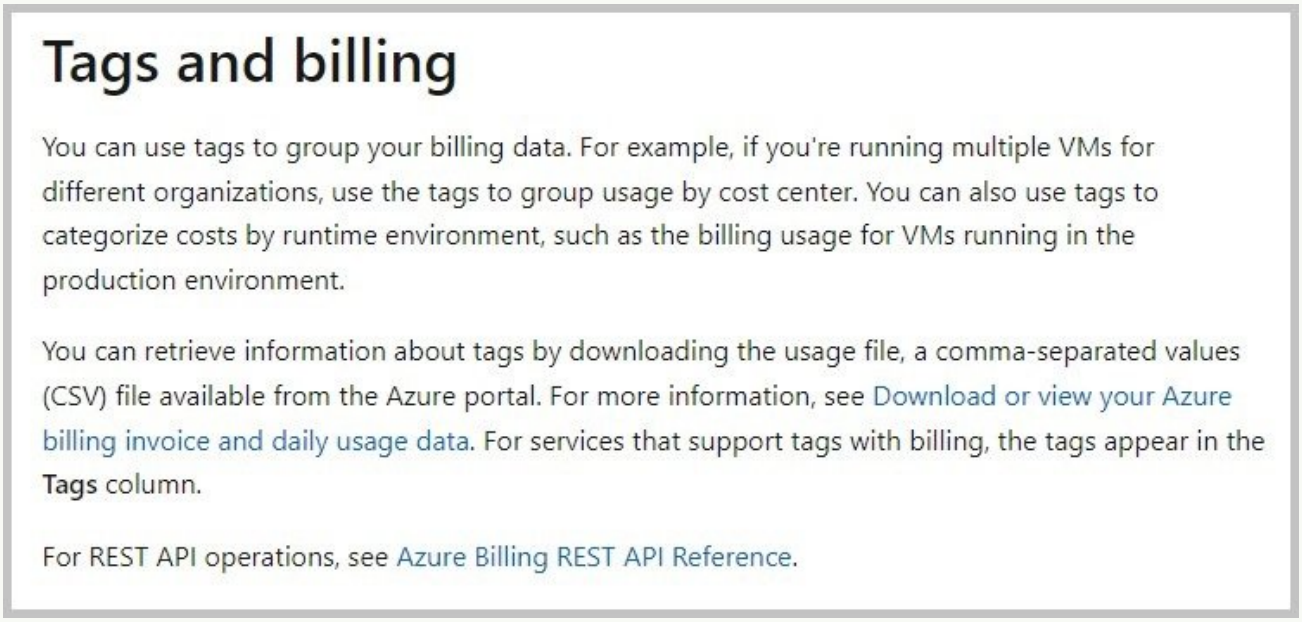
The key point is “Assign tags to each resource“ , as tags are not inherited which means if you assign a tag to a RG >> it will not propagated/inherited to the underneath resources , so you MUST assign tags to each individual resource.

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?

tabs=json#tags-and-billing

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags



Tags and billing

You can use tags to group your billing data. For example, if you're running multiple VMs for different organizations, use the tags to group usage by cost center. You can also use tags to categorize costs by runtime environment, such as the billing usage for VMs running in the production environment.

You can retrieve information about tags by downloading the usage file, a comma-separated values (CSV) file available from the Azure portal. For more information, see Download or view your Azure billing invoice and daily usage data. For services that support tags with billing, the tags appear in the **Tags** column.

For REST API operations, see Azure Billing REST API Reference.

44. Question

You have an Azure SQL database named DB1.

You need to recommend a data security solution for DB1. The solution must meet the following requirements:

? When helpdesk supervisors query DB1, they must see the full number of each credit card.

? When helpdesk operators query DB1, they must see only the last four digits of each credit card number.

? A column named Credit Rating must never appear in plain text within the database system, and only client applications must be able to decrypt the Credit Rating column.

Which of the following would go into Slot1?

- A. Always Encrypted
- B. Azure Advanced Threat Protection (ATP)
- **C. Dynamic data masking**
- D. Transparent Data Encryption (TDE)

Correct

Dynamic data masking (DDM) limits sensitive data exposure by masking it to non-privileged users. It can be used to greatly simplify the design and coding of security in your application.

Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to designate how much of the sensitive data to reveal with minimal impact on the application layer. It's a policy-based security feature that hides the sensitive data in the result set of a query over designated database fields, while the data in the database is not changed.

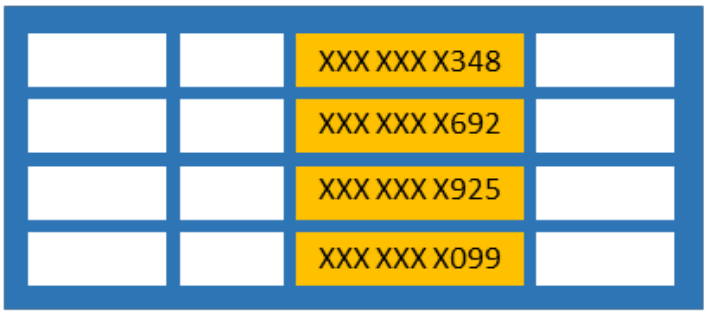
Reference:

https://docs.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking?view=sql-server-ver15

Dynamic Data Masking

03/24/2021 • 9 minutes to read • +16

Applies to: SQL Server 2016 (13.x) and later Azure SQL Database Azure SQL Managed Instance Azure Synapse Analytics



Dynamic data masking (DDM) limits sensitive data exposure by masking it to non-privileged users. It can be used to greatly simplify the design and coding of security in your application.

Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to specify how much sensitive data to reveal with minimal impact on the application layer. DDM can be configured on designated database fields to hide sensitive data in the result sets of queries. With DDM the data in the database is not changed. DDM is easy to use with existing applications, since masking rules are applied in the query results. Many applications can mask sensitive data without modifying existing queries.

- A central data masking policy acts directly on sensitive fields in the database.
- Designate privileged users or roles that do have access to the sensitive data.
- DDM features full masking and partial masking functions, and a random mask for numeric data.
- Simple Transact-SQL commands define and manage masks.

The purpose of dynamic data masking is to limit exposure of sensitive data, preventing users who should not have access to the data from viewing it. Dynamic data masking does not aim to prevent database users from connecting directly to the database and running exhaustive queries that expose pieces of the sensitive data. Dynamic data masking is complementary to other SQL Server security features (auditing, encryption, row level security...) and it is highly recommended to use it in conjunction with them in order to better protect the sensitive data in the database.

Dynamic data masking is available in SQL Server 2016 (13.x) and Azure SQL Database, and is configured by using Transact-SQL commands. For more information about configuring dynamic data masking by using the Azure portal, see Get started with SQL Database Dynamic Data Masking (Azure portal).

45. Question

You have an Azure SQL database named DB1.

You need to recommend a data security solution for DB1. The solution must meet the following requirements:

? When helpdesk supervisors query DB1, they must see the full number of each credit card.

? When helpdesk operators query DB1, they must see only the last four digits of each credit card number.

? A column named Credit Rating must never appear in plain text within the database system, and only client applications must be able to decrypt the Credit Rating column.

Which of the following would go into Slot2?

- A. Always Encrypted
- B. Azure Advanced Threat Protection (ATP)
- C. Dynamic data masking
- D. Transparent Data Encryption (TDE)

Correct

Always Encrypted is a feature designed to protect sensitive data, stored in Azure SQL Database or SQL Server databases from access by database administrators (e.g. the members of the SQL Server sysadmin or db_owner roles), administrators of machines hosting SQL Server instances,), and Azure SQL Database (cloud) administrators. Data stored in the database is protected even if the entire machine is compromised, for example by malware. Always Encrypted leverages client-side encryption: a database driver inside an application transparently encrypts data, before sending the data to the database. Similarly, the driver decrypts encrypted data retrieved in query results.

Reference:

https://azure.microsoft.com/en-us/blog/transparent-data-encryption-or-always-encrypted/

Always Encrypted

Always Encrypted is a feature designed to protect sensitive data, stored in Azure SQL Database or SQL Server databases from access by database administrators (e.g. the members of the SQL Server sysadmin or db_owner roles), administrators of machines hosting SQL Server instances,), and Azure SQL Database (cloud) administrators. Data stored in the database is protected even if the entire machine is compromised, for example by malware. Always Encrypted leverages client-side encryption: a database driver inside an application transparently encrypts data, before sending the data to the database. Similarly, the driver decrypts encrypted data retrieved in query results.

With Always Encrypted, cryptographic operations on the client-side use keys that are never revealed to the Database Engine (SQL Database or SQL Server). There are two types of keys in Always Encrypted:

- Column encryption keys are used to encrypt data in the database. These keys are stored in the database in the encrypted form (never in plaintext).
- Column master keys are used to encrypt column encryption keys. These keys are stored in an external key store, such as Windows Certificate Store, Azure Key Vault or hardware security modules. For keys stored in Azure Key Vault, only the client application has access to the keys, but not the database, unlike TDE.

The unique security benefit of Always Encrypted is the protection of data "in use" – i.e., the data used in computations, in memory of the SQL Server process remains encrypted. As a result, Always Encrypted protects the data from attacks that involve scanning the memory of the SQL Server process or extracting the data from a memory dump file.

By protecting data from high-privilege users who have no "need-to-know," Always Encrypted provides a separation between those who own the data (and can view it) and those who manage the data (but should have no access). This enables customers to confidently store sensitive data in the cloud, delegate on-premises database administration to third parties, or to reduce security clearance requirements for their own DBA staff.

Unlike TDE, this is only partially transparent to applications. Although the client driver transparently encrypts and decrypts data, the application may need to be changed to adhere to requirements/limitations of Always Encrypted. For example, Always Encrypted only supports very limited operations on encrypted database columns. This is one of the reasons why we recommend you use Always Encrypted to protect truly sensitive data in selected database columns.

One thing to call out is the fact that by encrypting data on the client-side, Always Encrypted also protects the data, stored in encrypted columns, at rest and in transit. However, unless your goal is to protect sensitive data in use, TDE is the recommended choice for encryption at rest, and we recommend TLS for protecting data in-transit. In fact, it is often advised to use Always Encrypted, TDE, and TLS together:

- TDE as the first line of defense (and to meet common compliance requirements) to encrypt the entire database at rest.
- TLS to protect all traffic to the database.
- Always Encrypted to protect highly sensitive data from high-privilege users and malware in the database environment.

46. Question

You are designing a data protection strategy for Azure virtual machines. All the virtual machines use managed disks.

You need to recommend a solution that meets the following requirements:

? The use of encryption keys is audited.

? All the data is encrypted at rest always.

? You manage the encryption keys, not Microsoft.

What should you include in the recommendation?

○ A. client-side encryption

B. Azure Storage Service Encryption

C. Azure Disk Encryption

D. Encrypting File System (EFS)

Correct

Azure Disk Encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. It uses the DM-Crypt feature of Linux to provide volume encryption for the OS and data disks of Azure virtual machines (VMs), and is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets.

Reference:

https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview

https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption#customer-managed-keys

https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption#full-control-of-your-keys

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview

Azure Disk Encryption for Linux VMs

08/06/2019 • 9 minutes to read • +3

Applies to: ✔ Linux VMs ✔ Flexible scale sets

Azure Disk Encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. It uses the DM-Crypt feature of Linux to provide volume encryption for the OS and data disks of Azure virtual machines (VMs), and is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets.

Azure Disk Encryption is zone resilient, the same way as Virtual Machines. For details, see Azure Services that support Availability Zones.

If you use Azure Security Center, you're alerted if you have VMs that aren't encrypted. The alerts show as High Severity and the recommendation is to encrypt these VMs.

Customer-managed keys

You can choose to manage encryption at the level of each managed disk, with your own keys. Server-side encryption for managed disks with customer-managed keys offers an integrated experience with Azure Key Vault. You can either import your RSA keys to your Key Vault or generate new RSA keys in Azure Key Vault.

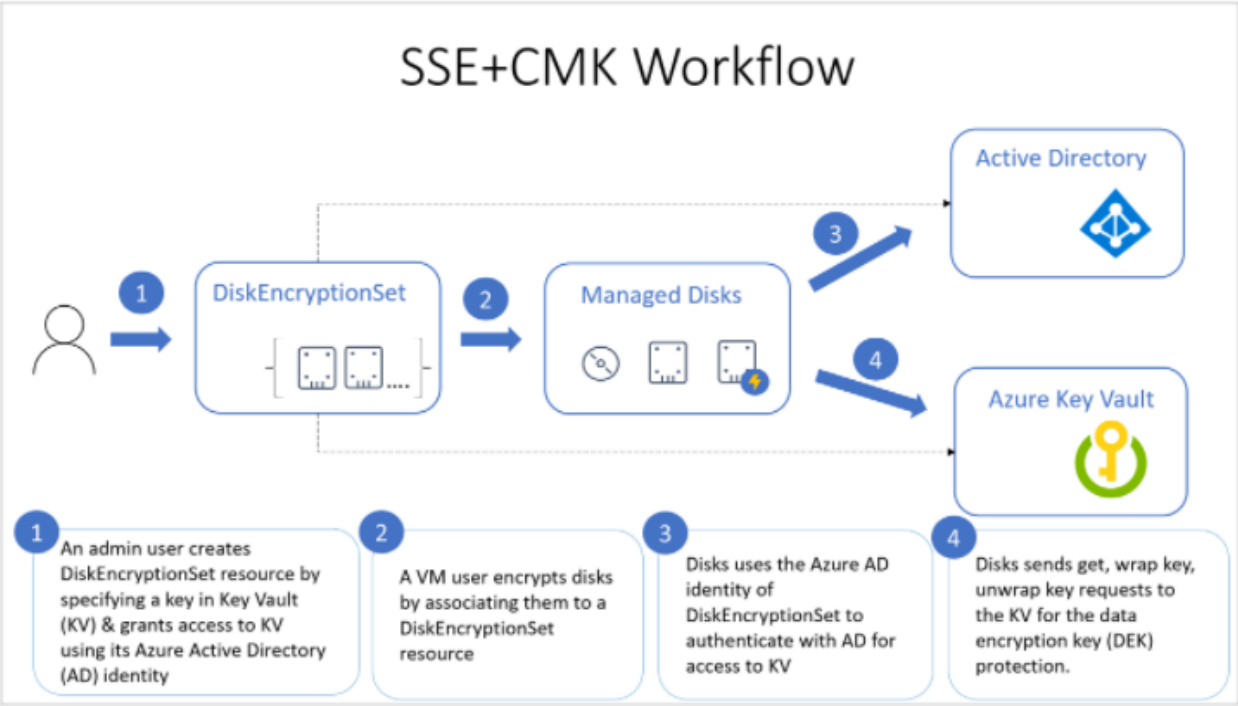
Azure managed disks handles the encryption and decryption in a fully transparent fashion using envelope encryption. It encrypts data using an AES 256 based data encryption key (DEK), which is, in turn, protected using your keys. The Storage service generates data encryption keys and encrypts them with customer-managed keys using RSA encryption. The envelope encryption allows you to rotate (change) your keys periodically as per your compliance policies without impacting your VMs. When you rotate your keys, the Storage service re-encrypts the data encryption keys with the new customer-managed keys.

Full control of your keys

You must grant access to managed disks in your Key Vault to use your keys for encrypting and decrypting the DEK. This allows you full control of your data and keys. You can disable your keys or revoke access to managed disks at any time. You can also audit the encryption key usage with Azure Key Vault monitoring to ensure that only managed disks or other trusted Azure services are accessing your keys.

When you disable or delete your key, any VMs with disks using that key will automatically shut down. After this, the VMs will not be usable unless the key is enabled again or you assign a new key.

The following diagram shows how managed disks use Azure Active Directory and Azure Key Vault to make requests using the customer-managed key:



47. Question

You have an on-premises application named App1 that uses an Oracle database.

You plan to use Azure Databricks to transform and load data from App1 to an Azure Synapse Analytics instance.

You need to ensure that the App1 data is available to Databricks.

Which two Azure services should you include in the solution?

- [ ] A. Azure Data Box Gateway
- [x] B. Azure Data Lake Storage
- [x] C. Azure Import/Export service
- [x] D. Azure Data Factory
- [ ] E. Azure Data Box Edge

Incorrect

Automate data movement using Azure Data Factory, then load data into Azure Data Lake Storage, transform and clean it using Azure Databricks, and make it available for analytics using Azure Synapse Analytics. Modernize your data warehouse in the cloud for unmatched levels of

Note: Integrate data silos with Azure Data Factory, a service built for all data integration needs and skill levels. Easily construct ETL and ELT processes code-free within the intuitive visual environment, or write your own code. Visually integrate data sources using more than 90+ natively built and maintenance-free connectors at no added cost. Focus on your data‘ the serverless integration service does the rest.

Incorrect Answers:

A. Azure Data Box Gateway

Azure Data Box Gateway is a storage solution that enables you to seamlessly send data to Azure.

C. Azure Import/Export service

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter.

E. Azure Data Box Edge

Azure Data Box Edge is a physical network appliance, shipped by Microsoft, that sends data in and out of Azure. Data Box Edge is additionally equipped with AI-enabled edge computing capabilities that help you analyze, process, and transform the on-premises data before uploading it to the cloud.

Reference:

https://azure.microsoft.com/en-us/services/databricks/#capabilities

https://azure.microsoft.com/en-us/services/data-factory/

https://docs.microsoft.com/en-us/azure/data-factory/introduction

48. Question

You have 100 devices that write performance data to Azure Blob storage.

You plan to store and analyze the performance data in an Azure SQL database.

You need to recommend a solution to move the performance data to the SQL database.

What should you include in the recommendation?

- A. Azure Database Migration Service
- B. Azure Data Factory
- C. Azure Data Box
- D. Data Migration Assistant

Incorrect

You can create a Data Factory pipeline that copies data from Azure Blob Storage to Azure SQL Database.

Incorrect Answers:

A. Azure Database Migration Service

Azure Database Migration Service is a fully managed service designed to enable seamless migrations to Azure data platforms with minimal downtime (online migrations).

C. Azure Data Box

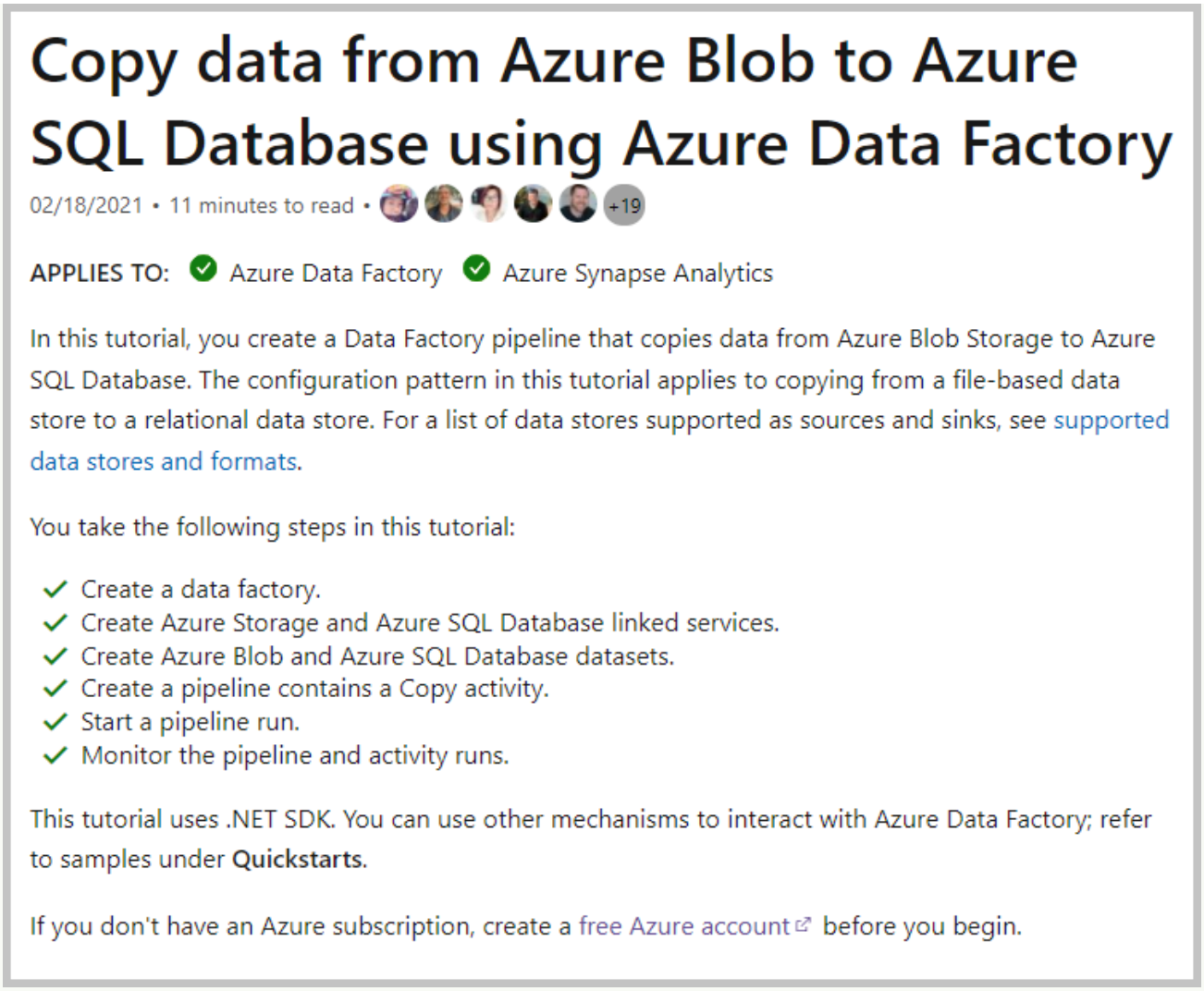
The Microsoft Azure Data Box cloud solution lets you send terabytes of data into and out of Azure in a quick, inexpensive, and reliable way.

D. Data Migration Assistant

The Data Migration Assistant (DMA) helps you upgrade to a modern data platform by detecting compatibility issues that can impact database functionality in your new version of SQL Server or Azure SQL Database.

Reference:

https://docs.microsoft.com/en-us/azure/data-factory/tutorial-copy-data-dot-net



Copy data from Azure Blob to Azure SQL Database using Azure Data Factory

02/18/2021 • 11 minutes to read • +19

APPLIES TO: Azure Data Factory Azure Synapse Analytics

In this tutorial, you create a Data Factory pipeline that copies data from Azure Blob Storage to Azure SQL Database. The configuration pattern in this tutorial applies to copying from a file-based data store to a relational data store. For a list of data stores supported as sources and sinks, see supported data stores and formats.

You take the following steps in this tutorial:

- ✓ Create a data factory.
- ✓ Create Azure Storage and Azure SQL Database linked services.
- ✓ Create Azure Blob and Azure SQL Database datasets.
- ✓ Create a pipeline contains a Copy activity.
- ✓ Start a pipeline run.
- ✓ Monitor the pipeline and activity runs.

This tutorial uses .NET SDK. You can use other mechanisms to interact with Azure Data Factory; refer to samples under **Quickstarts**.

If you don't have an Azure subscription, create a free Azure account before you begin.

49. Question

You have a web application that uses a MongoDB database. You plan to migrate the web application to Azure.

You must migrate to Cosmos DB while minimizing code and configuration changes.

You need to design the Cosmos DB configuration.

Which of the following would go into Slot1?

- A. Database
- B. API
- C. Collection
- D. Account

Incorrect

When you create an Azure Cosmos DB account, you must specify the –kind that enables MongoDB client connections.

az cosmosdb create –name –resource-group myResourceGroup –kind MongoDB

The –kind MongoDB parameter enables MongoDB client connections.

Reference:

https://docs.microsoft.com/en-us/azure/cosmos-db/create-mongodb-nodejs#create-an-azure-cosmos-db-account

Create an Azure Cosmos DB account

Create a Cosmos account with the az cosmosdb create command.

In the following command, please substitute your own unique Cosmos account name where you see the `<cosmosdb-name>` placeholder. This unique name will be used as part of your Cosmos DB endpoint (`https://<cosmosdb-name>.documents.azure.com/`), so the name needs to be unique across all Cosmos accounts in Azure.

Azure CLI Copy Try It

```
az cosmosdb create --name <cosmosdb-name> --resource-group myResourceGroup --kind MongoDB
```

The `--kind MongoDB` parameter enables MongoDB client connections.

When the Azure Cosmos DB account is created, the Azure CLI shows information similar to the following example.

Note

This example uses JSON as the Azure CLI output format, which is the default. To use another output format, see **Output formats for Azure CLI commands.**

JSON Copy

```
{
  "databaseAccountOfferType": "Standard",
  "documentEndpoint": "https://<cosmosdb-name>.documents.azure.com:443/",
  "id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/myResourceGroup
DB/databaseAccounts/<cosmosdb-name>",
  "kind": "MongoDB",
  "location": "West Europe",
  "name": "<cosmosdb-name>",
  "readLocations": [
    {
      "documentEndpoint": "https://<cosmosdb-name>-westeurope.documents.azure.com:443/",
      "failoverPriority": 0,
      "id": "<cosmosdb-name>-westeurope",
      "locationName": "West Europe",
      "provisioningState": "Succeeded"
    }
```

```
    ],
    "resourceGroup": "myResourceGroup",
    "type": "Microsoft.DocumentDB/databaseAccounts",
    "writeLocations": [
      {
        "documentEndpoint": "https://<cosmosdb-name>-westeurope.documents.azure.com:443/",
        "failoverPriority": 0,
        "id": "<cosmosdb-name>-westeurope",
        "locationName": "West Europe",
        "provisioningState": "Succeeded"
      }
    ]
  }
```


50. Question

You have a web application that uses a MongoDB database. You plan to migrate the web application to Azure.

You must migrate to Cosmos DB while minimizing code and configuration changes.

You need to design the Cosmos DB configuration.

Which of the following would go into Slot2?

- A. Cassandra API
- B. DocumentDB API
- C. Graph API
- D. MongoDB API
- E. Table API

Correct

The Azure Cosmos DB API for MongoDB makes it easy to use Cosmos DB as if it were a MongoDB database. You can leverage your MongoDB experience and continue to use your favorite MongoDB drivers, SDKs, and tools by pointing your application to the API for MongoDB account's connection string.

Reference:

https://docs.microsoft.com/en-us/azure/cosmos-db/mongodb-introduction

Azure Cosmos DB API for MongoDB

08/26/2021 • 5 minutes to read •

APPLIES TO: Azure Cosmos DB API for MongoDB

The Azure Cosmos DB API for MongoDB makes it easy to use Cosmos DB as if it were a MongoDB database. You can leverage your MongoDB experience and continue to use your favorite MongoDB drivers, SDKs, and tools by pointing your application to the API for MongoDB account's connection string.

Why choose the API for MongoDB

The API for MongoDB has numerous added benefits of being built on Azure Cosmos DB when compared to service offerings such as MongoDB Atlas:

- **Instantaneous scalability**: By enabling the Autoscale feature, your database can scale up/down with zero warmup period.
- **Automatic and transparent sharding**: The API for MongoDB manages all of the infrastructure for you. This includes sharding and the number of shards, unlike other MongoDB offerings such as MongoDB Atlas, which require your to specify and manage sharding to horizontally scale. This gives you more time to focus on developing applications for your users.
- **Five 9's of availability**: 99.999% availability is easily configurable to ensure your data is always there for you.
- **Cost efficient, granular, unlimited scalability**: Sharded collections can scale to any size, unlike other MongoDB service offerings. API for MongoDB users are running databases with over 600TB of storage today. Scaling is done in a cost-efficient manner, since unlike other MongoDB service offering, the Cosmos DB platform can scale in increments as small as 1/100th of a VM due to economies of scale and resource governance.
- **Serverless deployments**: Unlike MongoDB Atlas, the API for MongoDB is a cloud native database that offers a serverless capacity mode. With Serverless, you are only charged per operation, and don't pay for the database when you don't use it.
- **Free Tier**: With Azure Cosmos DB free tier, you'll get the first 1000 RU/s and 25 GB of storage in your account for free forever, applied at the account level.
- **Upgrades take seconds**: All API versions are contained within one codebase, making version changes as simple as flipping a switch, with zero downtime.
- **Real time analytics (HTAP) at any scale**: The API for MongoDB offers the ability to run complex analytical queries for use cases such as business intelligence against your database data in real time with no impact to your database. This is fast and cheap, due to the cloud native analytical columnar store being utilized, with no ETL pipelines. Learn more about the Azure Synapse Link.

> ⓘ Note
>
> **You can use Azure Cosmos DB API for MongoDB for free with the free Tier!**. With Azure Cosmos DB free tier, you'll get the first 1000 RU/s and 25 GB of storage in your account for free, applied at the account level.

51. Question

You are designing an order processing system in Azure that will contain the Azure resources shown in the following table.

Name	Type	Purpose
App1	Web App	Processes customer orders
Function1	Function	Check product availability at vendor 1
Function2	Function	Check product availability at vendor 2
Storage1	Storage Account	Stores order processing logs

The order processing system will have the following transaction flow:

? A customer will place an order by using App1.

? When the order is received, App1 will generate a message to check for product availability at vendor 1 and vendor 2.

? An integration component will process the message, and then trigger either Function1 or Function2 depending on the type of order.

? Once a vendor confirms the product availability, a status message for App1 will be generated by Function1 or Function2.

? All the steps of the transaction will be logged to storage1.

Which type of resource should you recommend for the integration component?

- A. an Azure Data Factory pipeline
- B. an Azure Service Bus queue
- C. an Azure Event Grid domain
- D. an Azure Event Hubs capture

Incorrect

A data factory can have one or more pipelines. A pipeline is a logical grouping of activities that together perform a task. For example, a pipeline could contain a set of activities that ingest and clean log data, and then kick off a mapping data flow to analyze the log data. The pipeline allows you to manage the activities as a set instead of each one individually. You deploy and schedule the pipeline instead of the activities independently.

The activities in a pipeline define actions to perform on your data. For example, you may use a copy activity to copy data from SQL Server to an Azure Blob Storage. Then, use a data flow activity or a Databricks Notebook activity to process and transform data from the blob storage to an Azure Synapse Analytics pool on top of which business intelligence reporting solutions are built.

Data Factory has three groupings of activities: data movement activities, data transformation activities, and control activities. An activity can take zero or more input datasets and produce one or more output

datasets. The following diagram shows the relationship between pipeline, activity, and dataset in Data Factory:

Relationship between dataset, activity, and pipeline

Look at the question carefully it states:

? An integration component will process the message, and then trigger either Function1 or Function2 depending on the type of order.

The keyword is process the message neither Service Bus nor Event Grid provide those functionalities. There is not mentioned where you would be storing the message but Azure Data Factory can integerate with various platforms and pick messages and based on that could fire either Function1 or Function2 based on order type.

Incorrect Answers:

B. an Azure Service Bus queue

The requirement can be achieved with Service Bus topics/subscriptions by sending the message based on metadata to subscribers listening to a specific topic.

C. an Azure Event Grid domain

An event domain is a management tool for large numbers of Event Grid topics related to the same application. You can think of it as a meta-topic that can have thousands of individual topics.

D. an Azure Event Hubs capture

Azure Event Hubs enables you to automatically capture the streaming data in Event Hubs in an Azure Blob storage

Reference:

https://docs.microsoft.com/en-us/azure/data-factory/concepts-pipelines-activities

Pipelines and activities in Azure Data Factory and Azure Synapse Analytics

09/09/2021 • 16 minutes to read • +19

Select the version of Data Factory service you're using: Current version

APPLIES TO: Azure Data Factory Azure Synapse Analytics

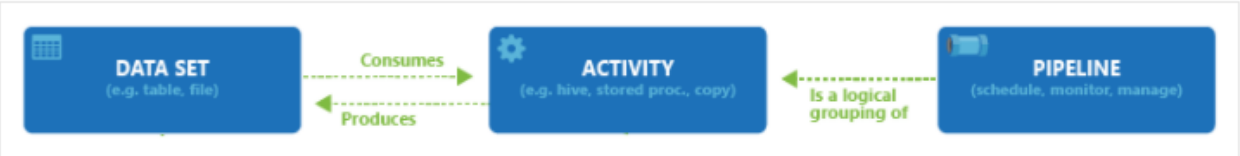
This article helps you understand pipelines and activities in Azure Data Factory and Azure Synapse Analytics and use them to construct end-to-end data-driven workflows for your data movement and data processing scenarios.

Overview

A Data Factory or Synapse Workspace can have one or more pipelines. A pipeline is a logical grouping of activities that together perform a task. For example, a pipeline could contain a set of activities that ingest and clean log data, and then kick off a mapping data flow to analyze the log data. The pipeline allows you to manage the activities as a set instead of each one individually. You deploy and schedule the pipeline instead of the activities independently.

The activities in a pipeline define actions to perform on your data. For example, you may use a copy activity to copy data from SQL Server to an Azure Blob Storage. Then, use a data flow activity or a Databricks Notebook activity to process and transform data from the blob storage to an Azure Synapse Analytics pool on top of which business intelligence reporting solutions are built.

Azure Data Factory and Azure Synapse Analytics have three groupings of activities: data movement activities, data transformation activities, and control activities. An activity can take zero or more input datasets and produce one or more output datasets. The following diagram shows the relationship between pipeline, activity, and dataset:



An input dataset represents the input for an activity in the pipeline, and an output dataset represents the output for the activity. Datasets identify data within different data stores, such as tables, files, folders, and documents. After you create a dataset, you can use it with activities in a pipeline. For example, a dataset can be an input/output dataset of a Copy Activity or an HDInsightHive Activity. For more information about datasets, see Datasets in Azure Data Factory article.

52. Question

You have 70 TB of files on your on-premises file server.

You need to recommend solution for importing data to Azure. The solution must minimize cost.

What Azure service should you recommend?

- A. Azure StorSimple
- B. Azure Batch
- C. Azure Data Box
- D. Azure Stack Hub

Correct

The Microsoft Azure Data Box cloud solution lets you send terabytes of data into and out of Azure in a quick, inexpensive, and reliable way. The secure data transfer is accelerated by shipping you a proprietary Data Box storage device. Each storage device has a maximum usable storage capacity of 80 TB and is transported to your datacenter through a regional carrier. The device has a rugged casing to protect and secure data during the transit.

Incorrect Answers:

A. Azure StorSimple

StoreSimple would not be able to handle 70 TB of data.

B. Azure Batch

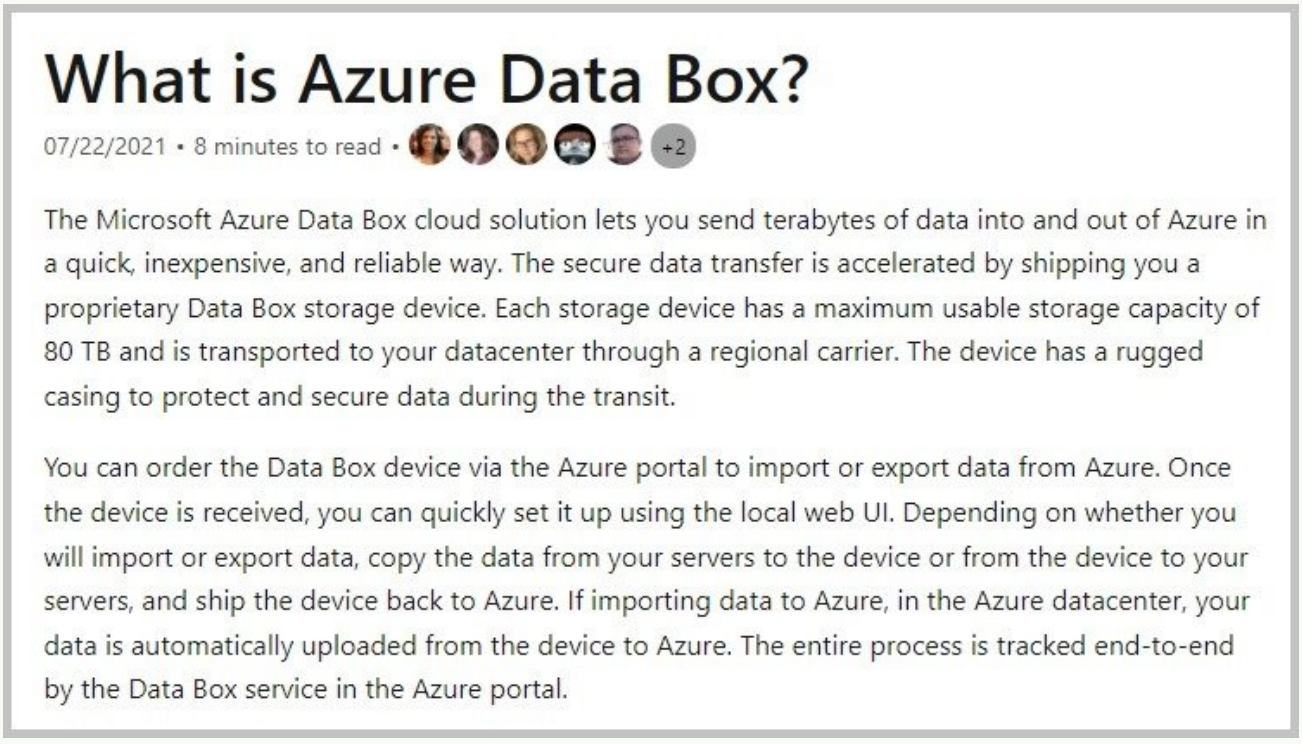
Use Azure Batch to run large-scale parallel and high-performance computing (HPC) batch jobs efficiently in Azure.

D. Azure Stack Hub

Azure Stack Hub is an extension of Azure that provides a way to run apps in an on-premises environment and deliver Azure services in your datacenter.

Reference:

https://docs.microsoft.com/en-us/azure/databox/data-box-overview



What is Azure Data Box?

07/22/2021 • 8 minutes to read • +2

The Microsoft Azure Data Box cloud solution lets you send terabytes of data into and out of Azure in a quick, inexpensive, and reliable way. The secure data transfer is accelerated by shipping you a proprietary Data Box storage device. Each storage device has a maximum usable storage capacity of 80 TB and is transported to your datacenter through a regional carrier. The device has a rugged casing to protect and secure data during the transit.

You can order the Data Box device via the Azure portal to import or export data from Azure. Once the device is received, you can quickly set it up using the local web UI. Depending on whether you will import or export data, copy the data from your servers to the device or from the device to your servers, and ship the device back to Azure. If importing data to Azure, in the Azure datacenter, your data is automatically uploaded from the device to Azure. The entire process is tracked end-to-end by the Data Box service in the Azure portal.

53. Question

You have an Azure subscription that contains 100 virtual machines.

You plan to design a data protection strategy to encrypt the virtual disks.

You need to recommend a solution to encrypt the disks by using Azure Disk Encryption. The solution must provide the ability to encrypt operating system disks and data disks.

What should you include in the recommendation?

- A. a certificate
- B. a key
- C. a passphrase
- D. a secret

Correct

Azure Disk Encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. It uses the Bitlocker feature of Windows to provide volume encryption for the OS and data disks of Azure virtual machines (VMs), and is integrated with Azure Key Vault to help you control and manage the disk encryption keys.

Incorrect Answers:

A. a certificate

Certificate can be used for authentication.

C. a passphrase

Not a valid option.

D. a secret

Secrets are used to store secret data. To encrypt a disk, we need a encryption keys.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-portal-quickstart

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-overview

Azure Disk Encryption for Windows VMs

10/05/2019 • 4 minutes to read • +3

Applies to: ✔ Windows VMs ✔ Flexible scale sets

Azure Disk Encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. It uses the BitLocker feature of Windows to provide volume encryption for the OS and data disks of Azure virtual machines (VMs), and is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets.

Azure Disk Encryption is zone resilient, the same way as Virtual Machines. For details, see Azure Services that support Availability Zones.

If you use Azure Security Center, you're alerted if you have VMs that aren't encrypted. The alerts show as High Severity and the recommendation is to encrypt these VMs.

54. Question

You have data files in Azure Blob storage.

You plan to transform the files and move them to Azure Data Lake Storage.

You need to transform the data by using mapping data flow.

Which Azure service should you use?

- A. Azure Data Box Gateway
- B. Azure Storage Sync
- C. Azure Data Factory
- D. Azure Databricks

Correct

Azure Data Factory can copy data from and to Azure Data Lake Storage Gen2, and use Data Flow to transform data in Azure Data Lake Storage Gen2.

Incorrect Answers:

A. Azure Data Box Gateway

Data Box Gateway can be leveraged for transferring data to the cloud such as cloud archival, disaster recovery, or if there is a need to process your data at cloud scale.

B. Azure Storage Sync

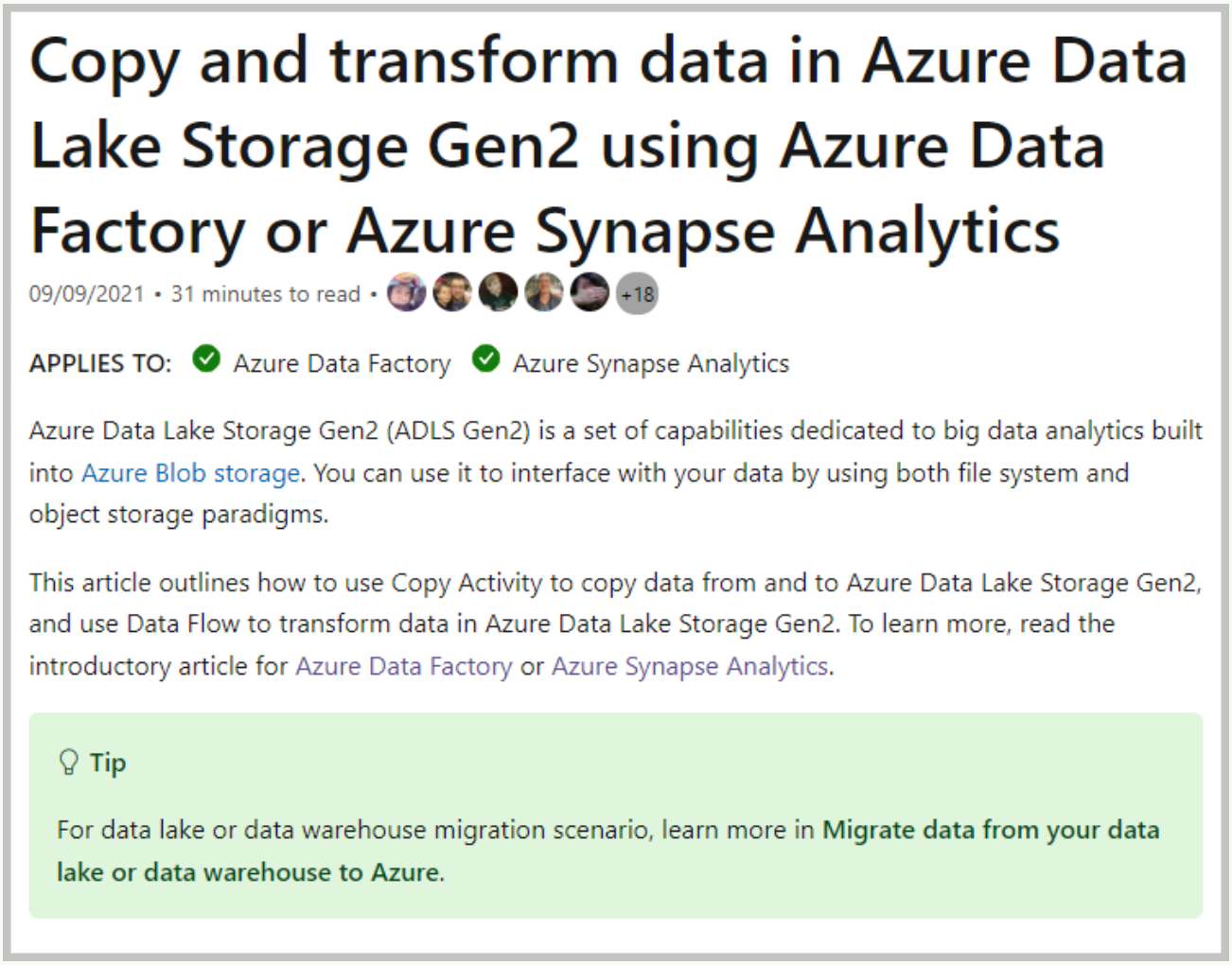
The deployment of Azure File Sync starts with placing a Storage Sync Service resource into a resource group of your selected subscription. We (Microsoft) recommend provisioning as few of these as needed.

D. Azure Databricks

Azure Databricks is a data analytics platform optimized for the Microsoft Azure cloud services platform

Reference:

https://docs.microsoft.com/en-us/azure/data-factory/connector-azure-data-lake-storage



Copy and transform data in Azure Data Lake Storage Gen2 using Azure Data Factory or Azure Synapse Analytics

09/09/2021 • 31 minutes to read • +18

APPLIES TO: Azure Data Factory Azure Synapse Analytics

Azure Data Lake Storage Gen2 (ADLS Gen2) is a set of capabilities dedicated to big data analytics built into Azure Blob storage. You can use it to interface with your data by using both file system and object storage paradigms.

This article outlines how to use Copy Activity to copy data from and to Azure Data Lake Storage Gen2, and use Data Flow to transform data in Azure Data Lake Storage Gen2. To learn more, read the introductory article for Azure Data Factory or Azure Synapse Analytics.

Tip

For data lake or data warehouse migration scenario, learn more in **Migrate data from your data lake or data warehouse to Azure.**

55. Question

You have an application named App1. App1 generates log files that must be archived for five years. The log files must be readable by App1 but must not be modified.

Which storage solution should you recommend for archiving?

- A. Ingest the log files into an Azure Log Analytics workspace
- **B. Use an Azure Blob storage account and a time-based retention policy**
- C. Use an Azure Blob storage account configured to use the Archive access tier
- D. Use an Azure file share that has access control enabled

Correct

Immutable storage for Azure Blob storage enables users to store business-critical data objects in a WORM (Write Once, Read Many) state.

Time-based retention policy support allows Users can set policies to store data for a specified interval.

When a time-based retention policy is set, blobs can be created and read, but not modified or deleted. After the retention period has expired, blobs can be deleted but not overwritten.

Incorrect Answers:

A. Ingest the log files into an Azure Log Analytics workspace

A Log Analytics workspace is a unique environment for Azure Monitor log data.

C. Use an Azure Blob storage account configured to use the Archive access tier

This option is used to archive log file for long term retention. Data in archive tier can be modified by rehydrating the blob.

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage

Store business-critical blob data with immutable storage

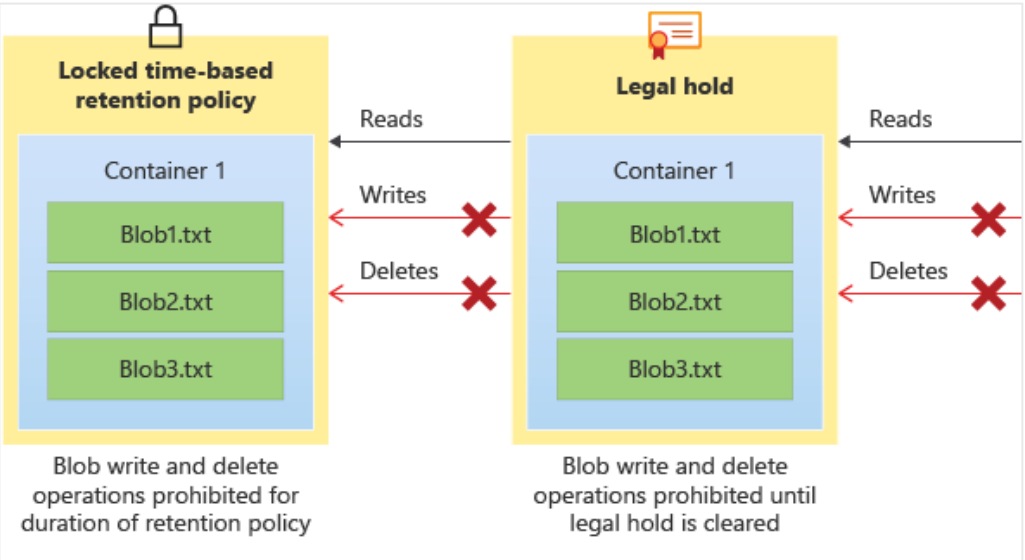
08/31/2021 • 10 minutes to read •

Immutable storage for Azure Blob Storage enables users to store business-critical data in a WORM (Write Once, Read Many) state. While in a WORM state, data cannot be modified or deleted for a user-specified interval. By configuring immutability policies for blob data, you can protect your data from overwrites and deletes.

Immutable storage for Azure Blob storage supports two types of immutability policies:

- **Time-based retention policies**: With a time-based retention policy, users can set policies to store data for a specified interval. When a time-based retention policy is set, objects can be created and read, but not modified or deleted. After the retention period has expired, objects can be deleted but not overwritten. To learn more about time-based retention policies, see Time-based retention policies for immutable blob data.
- **Legal hold policies**: A legal hold stores immutable data until the legal hold is explicitly cleared. When a legal hold is set, objects can be created and read, but not modified or deleted. To learn more about legal hold policies, see Legal holds for immutable blob data.

The following diagram shows how time-based retention policies and legal holds prevent write and delete operations while they are in effect.



56. Question

You have 100 Microsoft SQL Server Integration Services (SSIS) packages that are configured to use 10 on-premises SQL Server databases as their destinations.

You plan to migrate the 10 on-premises databases to Azure SQL Database.

You need to recommend a solution to host the SSIS packages in Azure. The solution must ensure that the

packages can target the SQL Database instances as their destinations.

What should you include in the recommendation?

- A. SQL Server Migration Assistant (SSMA)
- B. Data Migration Assistant
- C. Azure Data Catalog
- **D. Azure Data Factory**

Incorrect

You can now move your SQL Server Integration Services (SSIS) projects, packages, and workloads to the Azure cloud. Deploy, run, and manage SSIS projects and packages in the SSIS Catalog (SSISDB) on Azure SQL Database or SQL Managed Instance with familiar tools such as SQL Server Management Studio (SSMS).

Azure Data Factory hosts the runtime engine for SSIS packages on Azure. The runtime engine is called the Azure-SSIS Integration Runtime (Azure-SSIS IR).

Incorrect Answers:

A. SQL Server Migration Assistant (SSMA)

Microsoft SQL Server Migration Assistant (SSMA) is a tool designed to automate database migration to SQL Server from Microsoft Access, DB2, MySQL, Oracle, and SAP ASE.

B. Data Migration Assistant

The Data Migration Assistant (DMA) helps you upgrade to a modern data platform by detecting compatibility issues that can impact database functionality in your new version of SQL Server or Azure SQL Database.

C. Azure Data Catalog

Data Catalogs are used to discover, understand, and consume data sources.

Reference:

https://docs.microsoft.com/en-us/sql/integration-services/lift-shift/ssis-azure-lift-shift-ssis-packages-overview?view=sql-server-ver15

Lift and shift SQL Server Integration Services workloads to the cloud

09/23/2018 • 7 minutes to read • +4

Applies to: SQL Server (all supported versions) SSIS Integration Runtime in Azure Data Factory

You can now move your SQL Server Integration Services (SSIS) projects, packages, and workloads to the Azure cloud. Deploy, run, and manage SSIS projects and packages in the SSIS Catalog (SSISDB) on Azure SQL Database or SQL Managed Instance with familiar tools such as SQL Server Management Studio (SSMS).

Benefits

Moving your on-premises SSIS workloads to Azure has the following potential benefits:

- **Reduce operational costs** and reduce the burden of managing infrastructure that you have when you run SSIS on-premises or on Azure virtual machines.
- **Increase high availability** with the ability to specify multiple nodes per cluster, as well as the high availability features of Azure and of Azure SQL Database.
- **Increase scalability** with the ability to specify multiple cores per node (scale up) and multiple nodes per cluster (scale out).

Architecture of SSIS on Azure

The following table highlights the differences between SSIS on premises and SSIS on Azure.

The most significant difference is the separation of storage from runtime. Azure Data Factory hosts the runtime engine for SSIS packages on Azure. The runtime engine is called the Azure-SSIS Integration Runtime (Azure-SSIS IR). For more info, see Azure-SSIS Integration Runtime.

Location	Storage	Runtime	Scalability
On premises	SQL Server	SSIS runtime hosted by SQL Server	SSIS Scale Out (in SQL Server 2017 and later) Custom solutions (in prior versions of SQL Server)
On Azure	SQL Database or SQL Managed Instance	Azure-SSIS Integration Runtime, a component of Azure Data Factory	Scaling options for the Azure-SSIS Integration Runtime

57. Question

You need to recommend an Azure Storage account configuration for two applications named Application1 and Application2. The configuration must meet the following requirements:

? Storage for Application1 must provide the highest possible transaction rates and the lowest possible latency.

? Storage for Application2 must provide the lowest possible storage costs per GB.

? Storage for both applications must be optimized for uploads and downloads.

? Storage for both applications must be available in an event of datacenter failure.

What should you recommend for Application1?

- A. Blob Storage with Standard performance, Hot access tier, and Read-access geo-redundant storage (RA-GRS) replication
- **B. BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication**
- C. General purpose v1 with Premium performance and Locally-redundant storage (LRS) replication
- D. General purpose v2 with Standard performance, Hot access tier, and Locally-redundant storage (LRS) replication

Correct

The redundancy requirement for both of the application is data must be available in an event of datacenter failure.

ZRS will suffice the requirement of redundancy for scenarios requiring high availability. Data is copied synchronously across three Azure availability zones in the primary region.

Azure block blob storage offers two different performance tiers:

? Premium: optimized for high transaction rates and single-digit consistent storage latency

? Standard: optimized for high capacity and high throughput

The requirement for application1 is highest possible transaction rates and the lowest possible latency. So, it needs a premium storage.

The requirement for application2 is provide the lowest possible storage costs per GB. Cool tier provides the cost effective storage solution as compared with hot tier.

Reference:

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

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

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-performance-tiers

Performance tiers for block blob storage

05/17/2021 • 3 minutes to read • 

As enterprises deploy performance sensitive cloud-native applications, it's important to have options for cost-effective data storage at different performance levels.

Azure block blob storage offers two different performance tiers:

- **Premium**: optimized for high transaction rates and single-digit consistent storage latency
- **Standard**: optimized for high capacity and high throughput

Zone-redundant storage

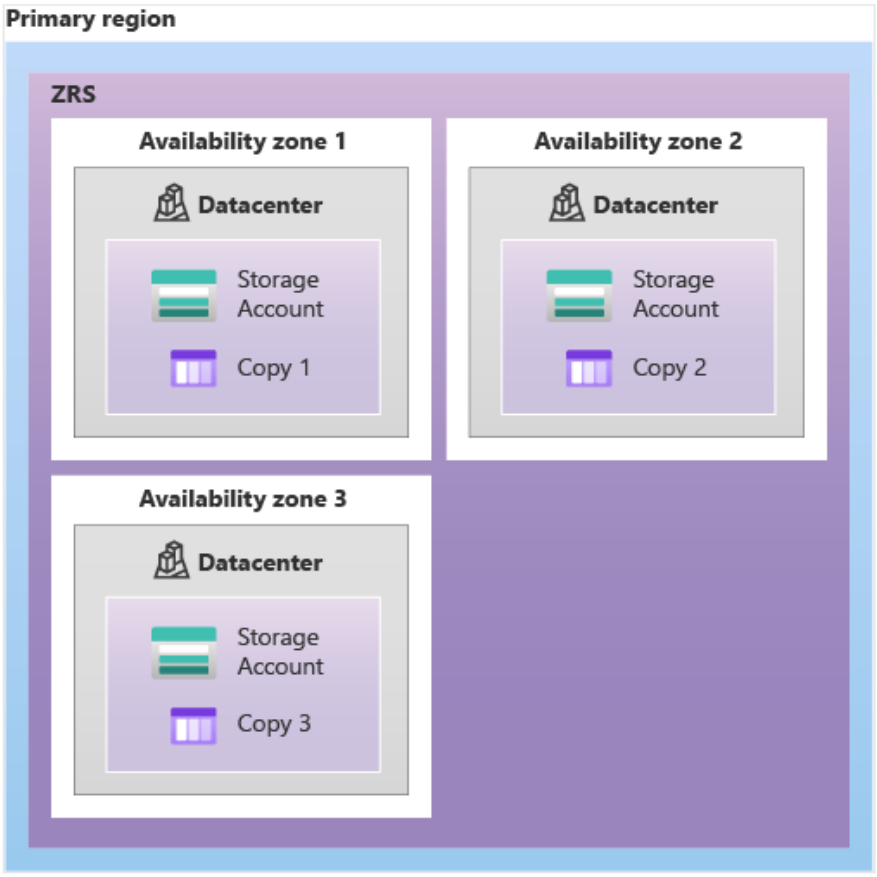
Zone-redundant storage (ZRS) replicates your Azure Storage data synchronously across three Azure availability zones in the primary region. Each availability zone is a separate physical location with independent power, cooling, and networking. ZRS offers durability for Azure Storage data objects of at least 99.9999999999% (12 9's) over a given year.

With ZRS, your data is still accessible for both read and write operations even if a zone becomes unavailable. If a zone becomes unavailable, Azure undertakes networking updates, such as DNS re-pointing. These updates may affect your application if you access data before the updates have completed. When designing applications for ZRS, follow practices for transient fault handling, including implementing retry policies with exponential back-off.

A write request to a storage account that is using ZRS happens synchronously. The write operation returns successfully only after the data is written to all replicas across the three availability zones.

Microsoft recommends using ZRS in the primary region for scenarios that require high availability. ZRS is also recommended for restricting replication of data to within a country or region to meet data governance requirements.

The following diagram shows how your data is replicated across availability zones in the primary region with ZRS:



58. Question

You need to recommend an Azure Storage account configuration for two applications named Application1 and Application2. The configuration must meet the following requirements:

? Storage for Application1 must provide the highest possible transaction rates and the lowest possible latency.

? Storage for Application2 must provide the lowest possible storage costs per GB.

? Storage for both applications must be optimized for uploads and downloads.

? Storage for both applications must be available in an event of datacenter failure.

What should you recommend for Application2?

- A. BlobStorage with Standard performance, Cool access tier, and Geo-redundant storage (GRS) replication
- B. BlockBlob Storage with Premium performance and Zone-redundant storage (ZRS) replication
- C. General purpose v1 with Standard performance and Read-access geo-redundant storage (RA-GRS) replication
- **D. General purpose v2 with Standard performance, Cool access tier, and Read-access geo-redundant storage (RA-GRS) replication**

Correct

General Purpose v2 provides access to the latest Azure storage features, including Cool and Archive storage, with pricing optimized for the lowest GB storage prices. These accounts provide access to Block Blobs, Page Blobs, Files, and Queues. Recommended for most scenarios using Azure Storage.

Reference:

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

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

59. Question

The developers at your company are building a static web app to support users sending text messages.

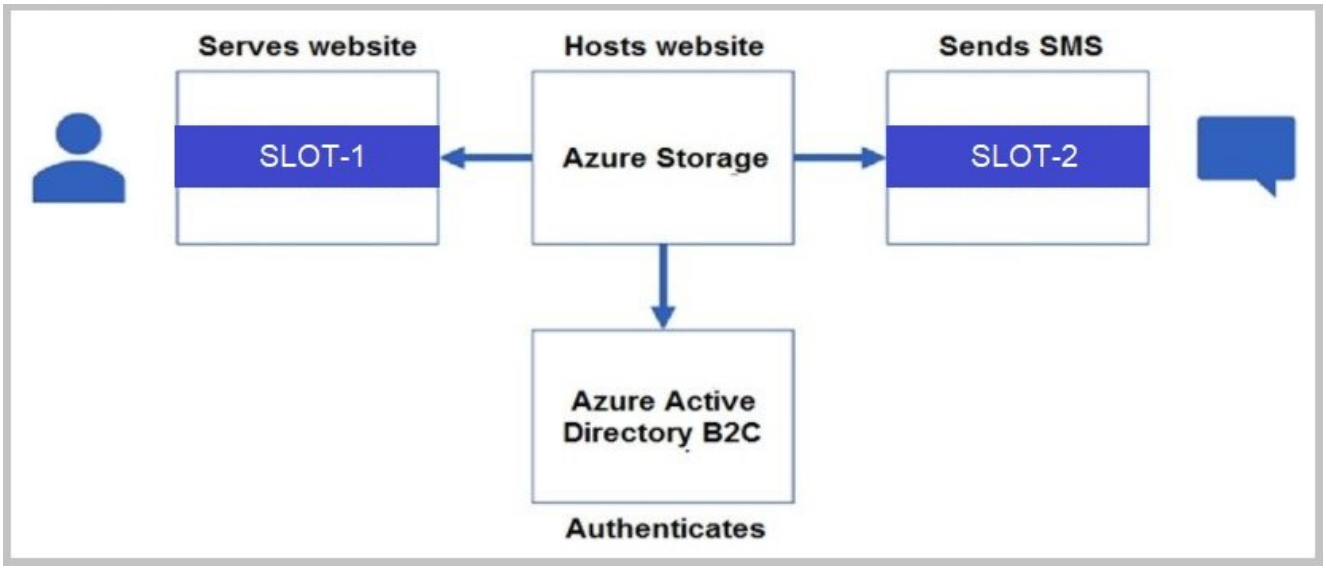
The app must meet the following requirements:

? Website latency must be consistent for users in different geographical regions.

? Users must be able to authenticate by using Twitter and Facebook.

? Code must include only HTML, native JavaScript, and jQuery.

? Costs must be minimized.



Which Azure service would go into Slot1 to complete the architecture?

- A. Azure App Service plan (Basic)
- B. Azure Content Delivery Network (CDN)
- C. Azure Front Door
- D. Azure Functions
- E. Azure Logic Apps

Correct

Since the website latency must be consistent for users in different geographical regions and it is a static app, we can use Azure Content Delivery Network (CDN) that can serve the website.

Incorrect Answers:

A. Azure App Service plan

Serves website: Azure App Service Plan – It provides compute capacity to deploy your application. To improve latency for static content, it is recommended to use CDN.

C. Azure Front Door

This is a load balancing solution.

D. Azure Functions

Azure Functions is a cloud service available on-demand that provides all the continually updated infrastructure and resources needed to run your applications.

E. Azure Logic Apps

Not possible to deploy JavaScript/JQuery code in Logic Apps.

Reference:

https://docs.microsoft.com/en-us/azure/cdn/cdn-overview

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-static-website#multi-region-website-hosting

Multi-region website hosting

If you plan to host a website in multiple geographies, we recommend that you use a Content Delivery Network for regional caching. Use Azure Front Door if you want to serve different content in each region. It also provides failover capabilities. Azure Traffic Manager is not recommended if you plan to use a custom domain. Issues can arise because of how Azure Storage verifies custom domain names.

60. Question

The developers at your company are building a static web app to support users sending text messages.

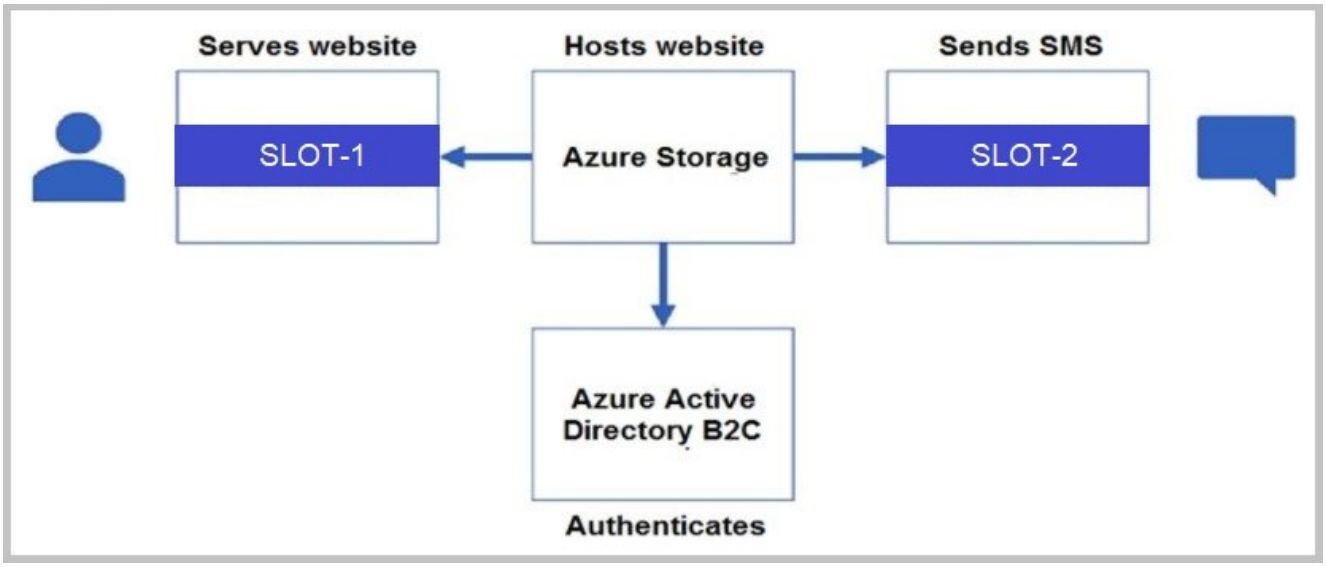
The app must meet the following requirements:

? Website latency must be consistent for users in different geographical regions.

? Users must be able to authenticate by using Twitter and Facebook.

? Code must include only HTML, native JavaScript, and jQuery.

? Costs must be minimized.



Which Azure service would go into Slot2 to complete the architecture?

- A. Azure App Service plan (Basic)
- B. Azure Content Delivery Network (CDN)
- C. Azure Front Door
- D. Azure Functions
- E. Azure Logic Apps

Correct

The functionality of sending SMS can be achieved by using either Logic Apps or Functions. Since code must include only HTML, JavaScript and JQuery, we can use Azure Functions.

Incorrect Answers:

A. Azure App Service plan

Serves website: Azure App Service Plan – It provides compute capacity to deploy your application. To improve latency for static content, it is recommended to use CDN.

B. Azure Content Delivery Network (CDN)

A content delivery network (CDN) is a distributed network of servers that can efficiently deliver web content to users. CDNs' store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.

C. Azure Front Door

This is a load balancing solution.

E. Azure Logic Apps

Not possible to deploy JavaScript/JQuery code in Logic Apps.

Reference:

https://docs.microsoft.com/en-us/azure/azure-functions/functions-overview

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-static-website#multi-region-website-hosting

Multi-region website hosting

If you plan to host a website in multiple geographies, we recommend that you use a Content Delivery Network for regional caching. Use Azure Front Door if you want to serve different content in each region. It also provides failover capabilities. Azure Traffic Manager is not recommended if you plan to use a custom domain. Issues can arise because of how Azure Storage verifies custom domain names.

61. Question

The accounting department at your company migrates to a new financial accounting software. The accounting department must keep file-based database backups for seven years for compliance purposes. It is unlikely that the backups will be used to recover data.

You need to move the backups to Azure. The solution must minimize costs.

Where should you store the backups?

- A. Azure Blob storage that uses the Archive tier
- B. Azure SQL Database
- C. Azure Blob storage that uses the Cool tier

D. a Recovery Services vault

Correct

Archive tier is optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements, on the order of hours. Example usage scenarios for the archive access tier include:

? Long-term backup, secondary backup, and archival datasets

? Original (raw) data that must be preserved, even after it has been processed into final usable form

? Compliance and archival data that needs to be stored for a long time and is hardly ever accessed

Incorrect Answers:

B. Azure SQL Database

We cannot store file based database backups in a SQL database.

C. Azure Blob storage that uses the Cool tier

This is used for infrequently accessed data. Not a cost effective solution for the backups that are unlikely to be used to recover data.

D. a Recovery Services vault

A Recovery Services vault is an entity that stores the backups and recovery points created over time. It is used in BCDR scenarios rather than just a backup solution.

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers

62. Question

Your company has offices in the United States, Europe, Asia, and Australia.

You have an on-premises app named App1 that uses Azure Table storage. Each office hosts a local instance of App1.

You need to upgrade the storage for App1. The solution must meet the following requirements:

? Enable simultaneous write operations in multiple Azure regions.

? Ensure that write latency is less than 10 ms.

? Support indexing on all columns.

? Minimize development effort.

Which data platform should you use?

- A. Azure SQL Database
- B. Azure SQL Managed Instance
- C. Azure Cosmos DB
- D. Table storage that uses geo-zone-redundant storage (GZRS) replication

Correct

Azure Cosmos DB Table API has –

? Single-digit millisecond latency for reads and writes, backed with <10-ms latency reads and <15-ms latency writes at the 99th percentile, at any scale, anywhere in the world.

? Automatic and complete indexing on all properties, no index management.

? Turnkey global distribution from one to 30+ regions. Support for automatic and manual failovers at any time, anywhere in the world.

Reference:

https://docs.microsoft.com/en-us/azure/cosmos-db/table-support

Developing with Azure Cosmos DB Table API and Azure Table storage

08/25/2021 • 2 minutes to read •

APPLIES TO: Table API

Azure Cosmos DB Table API and Azure Table storage share the same table data model and expose the same create, delete, update, and query operations through their SDKs.

Note

The **serverless capacity mode** is now available on Azure Cosmos DB's Table API.

If you currently use Azure Table Storage, you gain the following benefits by moving to the Azure Cosmos DB Table API:

Feature	Azure Table storage	Azure Cosmos DB Table API
Latency	Fast, but no upper bounds on latency.	Single-digit millisecond latency for reads and writes, backed with <10-ms latency reads and <15-ms latency writes at the 99th percentile, at any scale, anywhere in the world.

Throughput	Variable throughput model. Tables have a scalability limit of 20,000 operations/s.	Highly scalable with dedicated reserved throughput per table that's backed by SLAs. Accounts have no upper limit on throughput and support >10 million operations/s per table (in provisioned throughput mode).
Global distribution	Single region with one optional readable secondary read region for high availability which supports automatic and manual account failover.	Turnkey global distribution from one to 30+ regions. Support for automatic and manual failovers at any time, anywhere in the world.
Indexing	Only primary index on PartitionKey and RowKey. No secondary indexes.	Automatic and complete indexing on all properties, no index management.
Query	Query execution uses index for primary key, and scans otherwise.	Queries can take advantage of automatic indexing on properties for fast query times.
Consistency	Strong within primary region. Eventual within secondary region.	Five well-defined consistency levels to trade off availability, latency, throughput, and consistency based on your application needs.
Pricing	Consumption-based.	Available in both consumption-based and provisioned capacity modes.
SLAs	99.99% availability.	99.99% availability SLA for all single region accounts and all multi-region accounts with relaxed consistency, and 99.999% read availability on all multi-region database accounts Industry-leading comprehensive SLAs on general availability.

63. Question

Your company deploys an Azure App Service Web App.

During testing the application fails under load. The application cannot handle more than 100 concurrent user sessions. You enable the Always On feature. You also configure auto-scaling to increase instance counts from two to 10 based on HTTP queue length.

You need to improve the performance of the application.

Which of the following would go into Slot1?

- A. Azure Redis Cache

B. Azure Traffic Manager

C. Azure Content Delivery Network

D. Azure Application Gateway

Correct

A content delivery network (CDN) is a distributed network of servers that can efficiently deliver web content to users. CDNs store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.

Azure Content Delivery Network (CDN) offers developers a global solution for rapidly delivering high-bandwidth content to users by caching their content at strategically placed physical nodes across the world. Azure CDN can also accelerate dynamic content, which cannot be cached, by leveraging various network optimizations using CDN POPs. For example, route optimization to bypass Border Gateway Protocol (BGP).

Incorrect Answers:

A. Azure Redis Cache

Azure Cache for Redis provides an in-memory data store based on the Redis software. Redis improves the performance and scalability of an application that uses backend data stores heavily.

B. Azure Traffic Manager

Azure Traffic Manager is a DNS-based traffic load balancer. It allows you to distribute traffic to your public facing applications across the global Azure regions.

D. Azure Application Gateway

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

Reference:

https://docs.microsoft.com/en-au/azure/cdn/cdn-overview

https://docs.microsoft.com/en-us/azure/cdn/cdn-pop-locations

What is a content delivery network on Azure?

09/05/2018 • 3 minutes to read • +10

A content delivery network (CDN) is a distributed network of servers that can efficiently deliver web content to users. CDNs' store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.

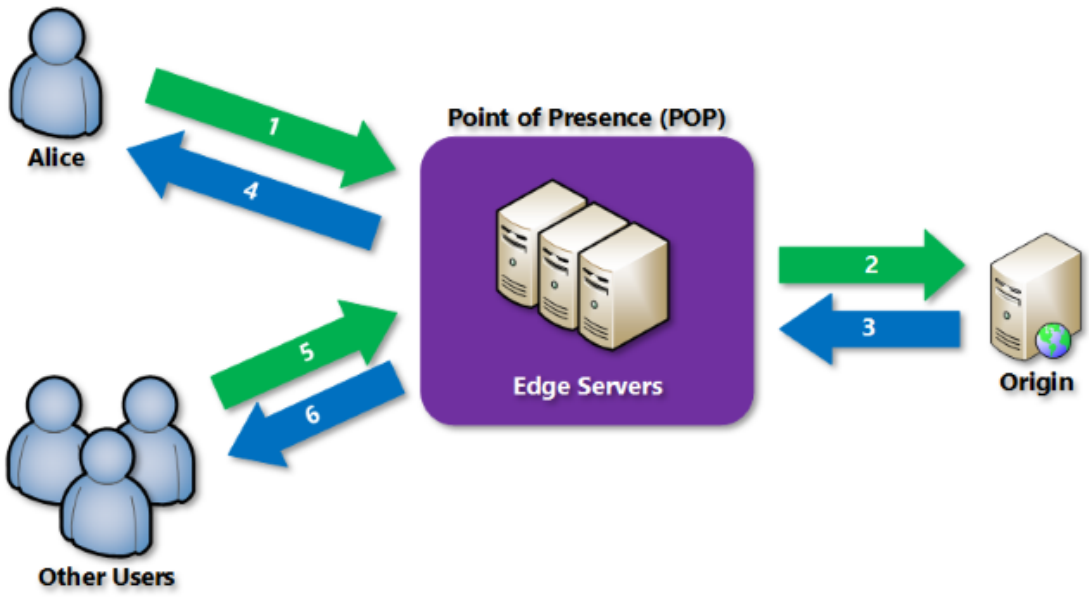
Azure Content Delivery Network (CDN) offers developers a global solution for rapidly delivering high-bandwidth content to users by caching their content at strategically placed physical nodes across the world. Azure CDN can also accelerate dynamic content, which cannot be cached, by leveraging various network optimizations using CDN POPs. For example, route optimization to bypass Border Gateway Protocol (BGP).

The benefits of using Azure CDN to deliver web site assets include:

- Better performance and improved user experience for end users, especially when using applications in which multiple round-trips are required to load content.
- Large scaling to better handle instantaneous high loads, such as the start of a product launch event.
- Distribution of user requests and serving of content directly from edge servers so that less traffic is sent to the origin server.

For a list of current CDN node locations, see Azure CDN POP locations.

How it works



64. Question

Your company deploys an Azure App Service Web App.

During testing the application fails under load. The application cannot handle more than 100 concurrent user sessions. You enable the Always On feature. You also configure auto-scaling to increase instance counts from two to 10 based on HTTP queue length.

You need to improve the performance of the application.

Which of the following would go into Slot2?

- A. Azure Redis Cache
- B. Azure Traffic Manager
- C. Azure Content Delivery Network
- D. Azure Application Gateway

Correct

Azure Cache for Redis is based on the popular software Redis. It is typically used as a cache to improve the performance and scalability of systems that rely heavily on backend data-stores. Performance is improved by temporarily copying frequently accessed data to fast storage located close to the application. With Azure Cache for Redis, this fast storage is located in-memory with Azure Cache for Redis instead of being loaded from disk by a database.

Incorrect Answers:

B. Azure Traffic Manager

Azure Traffic Manager is a DNS-based traffic load balancer. It allows you to distribute traffic to your public facing applications across the global Azure regions.

C. Azure Content Delivery Network

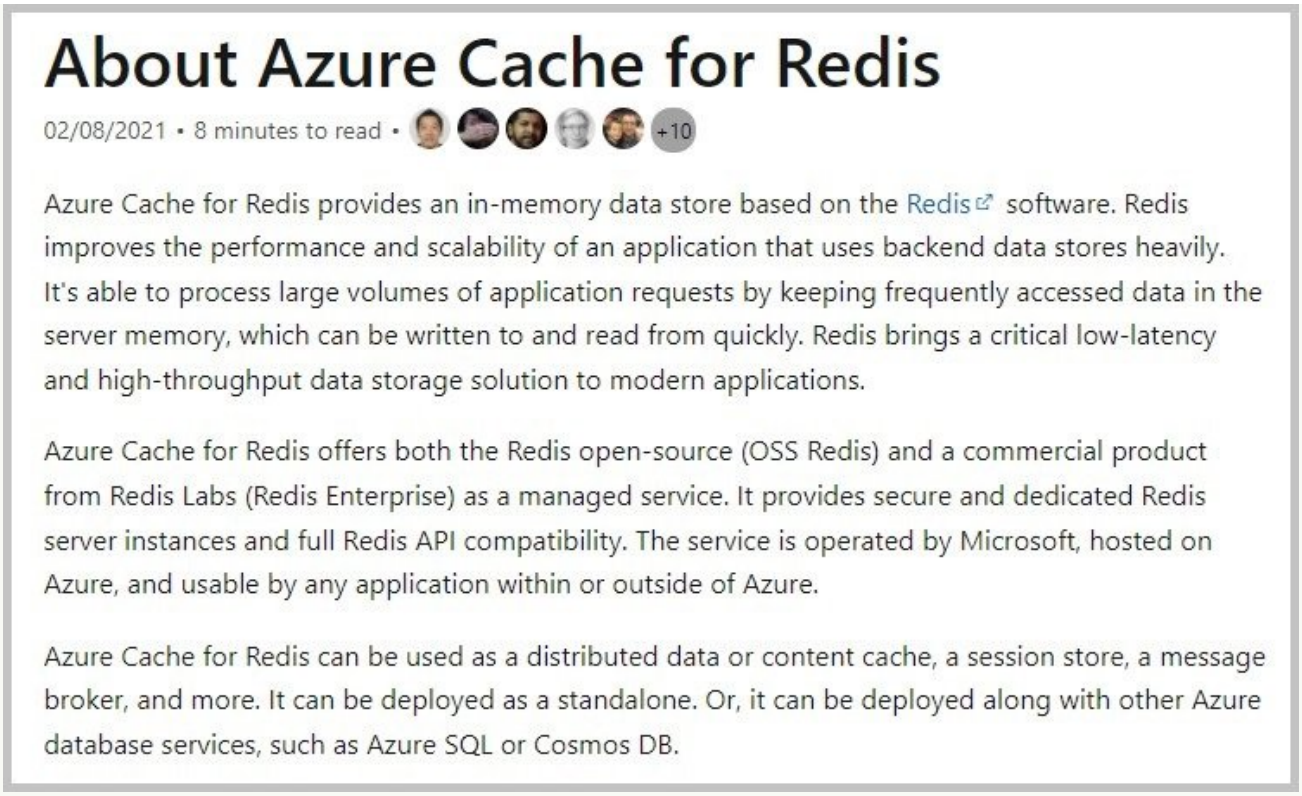
A content delivery network (CDN) is a distributed network of servers that can efficiently deliver web content to users. CDNs' store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.

D. Azure Application Gateway

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

Reference:

https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-overview



About Azure Cache for Redis

02/08/2021 • 8 minutes to read • +10

Azure Cache for Redis provides an in-memory data store based on the Redis software. Redis improves the performance and scalability of an application that uses backend data stores heavily. It's able to process large volumes of application requests by keeping frequently accessed data in the server memory, which can be written to and read from quickly. Redis brings a critical low-latency and high-throughput data storage solution to modern applications.

Azure Cache for Redis offers both the Redis open-source (OSS Redis) and a commercial product from Redis Labs (Redis Enterprise) as a managed service. It provides secure and dedicated Redis server instances and full Redis API compatibility. The service is operated by Microsoft, hosted on Azure, and usable by any application within or outside of Azure.

Azure Cache for Redis can be used as a distributed data or content cache, a session store, a message broker, and more. It can be deployed as a standalone. Or, it can be deployed along with other Azure database services, such as Azure SQL or Cosmos DB.

65. Question

You are planning an Azure solution that will host production databases for a high-performance application.

The solution will include the following components:

? Two virtual machines that will run Microsoft SQL Server 2016, will be deployed to different data centers in the same Azure region, and will be part of an Always On availability group

? SQL Server data that will be backed up by using the Automated Backup feature of the SQL Server IaaS Agent Extension (SQLIaaSExtension)

You identify the storage priorities for various data types as shown in the following table.

Data Type	Storage Priority
Operating System	Speed and availability
Databases and Logs	Speed and availability
Backups	Lowest cost

Which storage type should you recommend for operating system?

- A. A geo-redundant storage (GRS) account
- B. A locally-redundant storage (LRS) account
- C. A premium managed disk
- D. A standard managed disk

Correct

The priority for operating system storage is “Speed and availability“. Premium managed disks provide better performance.

Incorrect Answers:

A. A geo-redundant storage (GRS) account

Storage accounts are not used for operating system disks.

B. A locally-redundant storage (LRS) account

Locally-redundant storage account – Storage accounts are not used for operating system disks.

D. A standard managed disk

Standard disks provide lower IOPS as compared with Premium disks.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/disks-types

What disk types are available in Azure?

06/29/2021 • 14 minutes to read •

Applies to: ✔ Linux VMs ✔ Windows VMs ✔ Flexible scale sets ✔ Uniform scale sets

Azure managed disks currently offers four disk types, each type is aimed towards specific customer scenarios.

Disk comparison

The following table provides a comparison of ultra disks, premium solid-state drives (SSD), standard SSD, and standard hard disk drives (HDD) for managed disks to help you decide what to use.

Detail	Ultra disk	Premium SSD	Standard SSD	Standard HDD
Disk type	SSD	SSD	SSD	HDD
Scenario	IO-intensive workloads such as SAP HANA, top tier databases (for example, SQL, Oracle), and other transaction-heavy workloads.	Production and performance sensitive workloads	Web servers, lightly used enterprise applications and dev/test	Backup, non-critical, infrequent access
Max disk size	65,536 gibibyte (GiB)	32,767 GiB	32,767 GiB	32,767 GiB
Max throughput	2,000 MB/s	900 MB/s	750 MB/s	500 MB/s
Max IOPS	160,000	20,000	6,000	2,000

Use Page numbers below to navigate to other practice tests

Pages: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

← Previous Post

Next Post →