SKILLCERTPRO

IT CERTIFICATION TRAININGS

0

Microsoft Azure / By SkillCertPro

Practice Set 17

Your results are here!! for" Microsoft Azure AZ-305 Practice Test 17 "

38 of 63 questions answered correctly

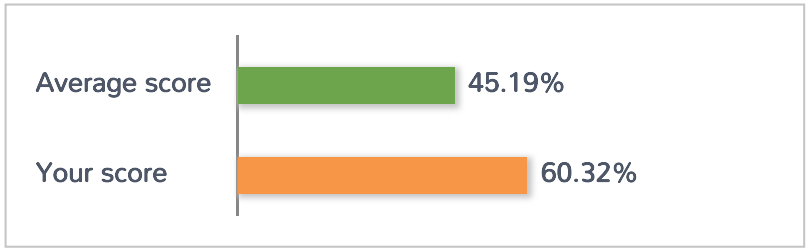
Your time: 01:28:51

Your Final Score is : 38

You have attempted : 63

Number of Correct Questions : 38 and scored 38

Number of Incorrect Questions : 25 and Negative marks 0

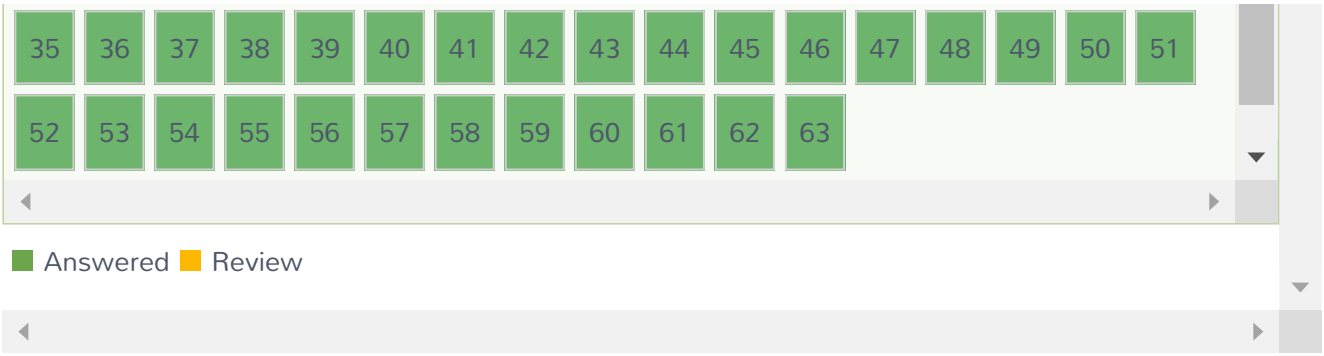


You can review your answers by clicking on “View Answers” option.

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 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 Databases and logs?

- 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 requirement for database and logs is Speed and availability. Azure premium SSDs deliver high-performance and low-latency disk support for virtual machines (VMs) with input/output (IO)-intensive workloads. To take advantage of the speed and performance of premium storage disks, you can migrate existing VM disks to Premium SSDs. Premium SSDs are suitable for mission-critical production applications.

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/windows/disks-types#premium-ssd

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

Premium SSD

Azure premium SSDs deliver high-performance and low-latency disk support for virtual machines (VMs) with input/output (IO)-intensive workloads. To take advantage of the speed and performance of premium storage disks, you can migrate existing VM disks to Premium SSDs. Premium SSDs are suitable for mission-critical production applications. Premium SSDs can only be used with VM series that are premium storage-compatible.

To learn more about individual VM types and sizes in Azure for Windows or Linux, including which sizes are premium storage-compatible, see Sizes for virtual machines in Azure. From this article, you need to check each individual VM size article to determine if it is premium storage-compatible.

2. 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 backups?

- A. A geo-redundant storage (GRS) account
- B. A locally-redundant storage (LRS) account
- C. A premium managed disk
- D. A standard managed disk

Incorrect

Automated Backup v2 automatically configures Managed Backup to Microsoft Azure for all existing and new databases on an Azure VM running SQL Server 2016/2017 Standard, Enterprise, or Developer editions. This enables you to configure regular database backups that utilize durable Azure blob storage.

LRS is cheaper than GRS

Incorrect Answers:

A. A geo-redundant storage (GRS) account

The requirement for backup storage is low-cost. GRS is costlier than LRS.

C. A premium managed disk

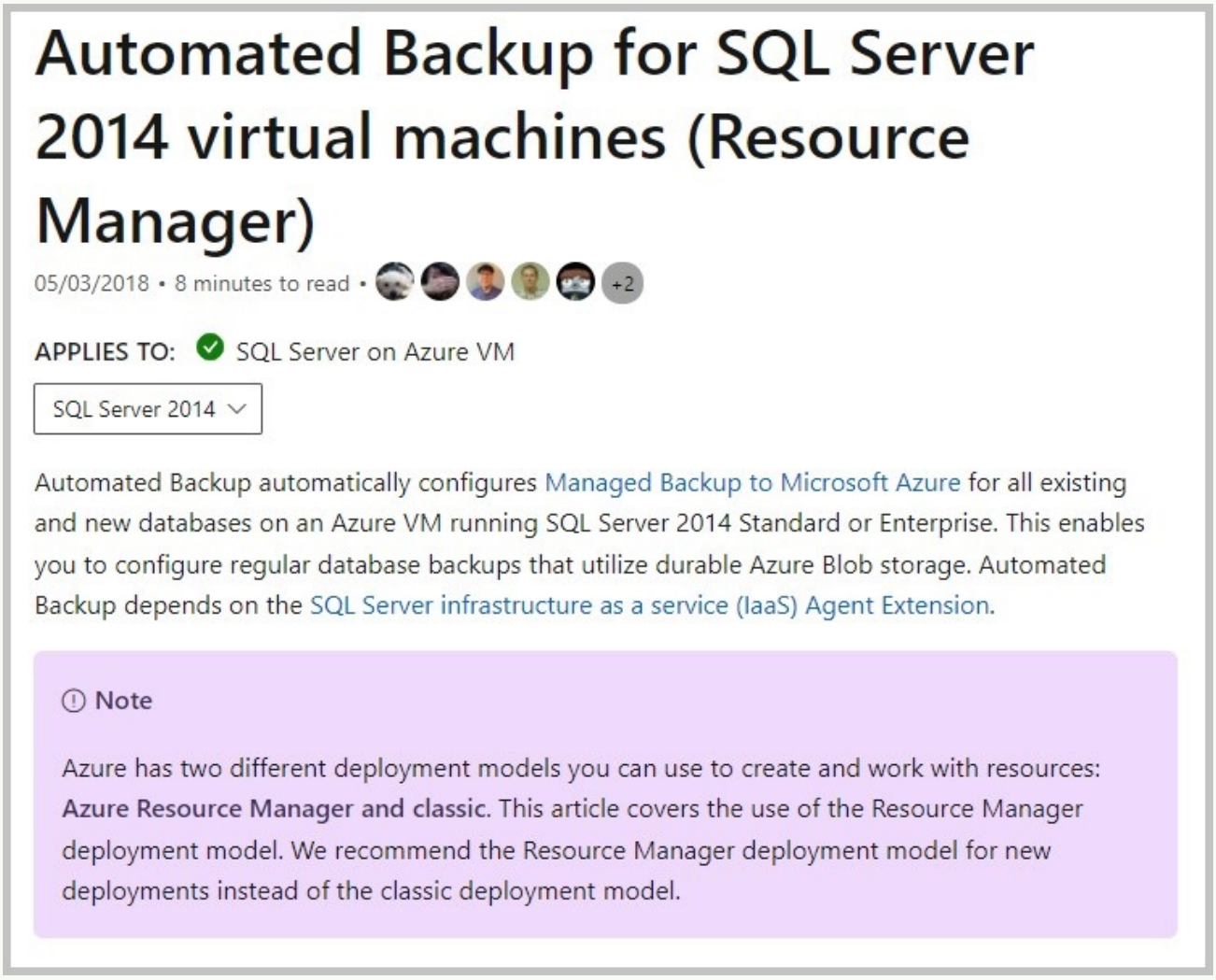
The automated backups feature uses an Azure storage account to store backups.

D. A standard managed disk

The automated backups feature uses an Azure storage account to store backups.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/automated-backup-sql-2014



Automated Backup for SQL Server 2014 virtual machines (Resource Manager)

05/03/2018 • 8 minutes to read • +2

APPLIES TO: SQL Server on Azure VM

SQL Server 2014

Automated Backup automatically configures Managed Backup to Microsoft Azure for all existing and new databases on an Azure VM running SQL Server 2014 Standard or Enterprise. This enables you to configure regular database backups that utilize durable Azure Blob storage. Automated Backup depends on the SQL Server infrastructure as a service (IaaS) Agent Extension.

Note

Azure has two different deployment models you can use to create and work with resources: **Azure Resource Manager and classic**. This article covers the use of the Resource Manager deployment model. We recommend the Resource Manager deployment model for new deployments instead of the classic deployment model.

3. Question

You have an Azure subscription that contains two applications named App1 and App2. App1 is a sales processing application. When a transaction in App1 requires shipping, a message is added to an Azure Storage account queue, and then App2 listens to the queue for relevant transactions.

In the future, additional applications will be added that will process some of the shipping requests based on the specific details of the transactions.

You need to recommend a replacement for the storage account queue to ensure that each additional application will be able to read the relevant transactions.

What should you recommend?

- A. one Azure Service Bus topic
- B. multiple storage account queues
- C. one Azure Data Factory pipeline
- D. one Azure Service Bus queue

Correct

A queue allows processing of a message by a single consumer. In contrast to queues, topics and subscriptions provide a one-to-many form of communication in a publish and subscribe pattern. It's useful for scaling to large numbers of recipients. Each published message is made available to each subscription registered with the topic. Publisher sends a message to a topic and one or more subscribers receive a copy of the message, depending on filter rules set on these subscriptions.

Reference:

https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-queues-topics-subscriptions

Service Bus queues, topics, and subscriptions

08/27/2021 • 6 minutes to read • +3

Azure Service Bus supports a set of cloud-based, message-oriented middleware technologies including reliable message queuing and durable publish/subscribe messaging. These brokered messaging capabilities can be thought of as decoupled messaging features that support publish-subscribe, temporal decoupling, and load-balancing scenarios using the Service Bus messaging workload. Decoupled communication has many advantages. For example, clients and servers can connect as needed and do their operations in an asynchronous fashion.

The messaging entities that form the core of the messaging capabilities in Service Bus are **queues**, **topics and subscriptions**, and rules/actions.

4. Question

You have an Azure subscription that contains a Basic Azure virtual WAN named VirtualWAN1 and the virtual hubs shown in the following table.

Name	Azure Region
Hub1	US East
Hub2	US West

You have an ExpressRoute circuit in the US East region.

You need to create an ExpressRoute association to VirtualWAN1.

What should you do first?

- A. Upgrade VirtualWAN1 to Standard
- B. Create a gateway on Hub1
- C. Create a hub virtual network in US East
- D. Enable the ExpressRoute premium add-on

Incorrect

Basic azure virtual WAN doesn‘t support express route, only site-to-site VPN. You have to upgrade to standard

Incorrect Answers:

B. Create a gateway on Hub1

Create a gateway on Hub1 You can create gateway while creating Hub. As question doesn‘t say if Hub has gateway, this option is not 100% correct

C. Create a hub virtual network in US East

Create a hub virtual network in US East. Obviously it‘s wrong

D. Enable the ExpressRoute premium add-on

Firstly, question doesn‘t say Express route is standard or premium. Also the ExpressRoute location does not need to match the Azure region. ExpressRoute Standard or Premium circuits that are in ExpressRoute Global Reach-supported locations can connect to a Virtual WAN ExpressRoute gateway and enjoy all Virtual WAN transit capabilities (VPN-to-VPN, VPN, and ExpressRoute transit)

Reference:

https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about#basicstandard

Basic and Standard virtual WANs

There are two types of virtual WANs: Basic and Standard. The following table shows the available configurations for each type.

Virtual WAN type	Hub type	Available configurations
Basic	Basic	Site-to-site VPN only
Standard	Standard	ExpressRoute User VPN (P2S) VPN (site-to-site) Inter-hub and VNet-to-VNet transiting through the virtual hub Azure Firewall NVA in a virtual WAN

Note

You can upgrade from Basic to Standard, but cannot revert from Standard back to Basic.

5. Question

You plan to deploy an API by using Azure API Management.

You need to recommend a solution to protect the API from a distributed denial of service (DDoS) attack.

What should you recommend?

- A. Strip the Powered-By response header
- B. Enable rate limiting
- C. Enable quotas
- D. Create network security groups (NSGs)

Correct

A rate limiting solution measures the amount of time between each request from each IP address, and also measures the number of requests within a specified timeframe. If there are too many requests from a single IP within the given timeframe, the rate limiting solution will not fulfill the IP address's requests for a certain amount of time.

Note:

As of today, the best answer would be Enable Azure DDoS Protection Standard on the Vnet associated with your API Management deployment to protect from distributed denial of service (DDoS) attacks.

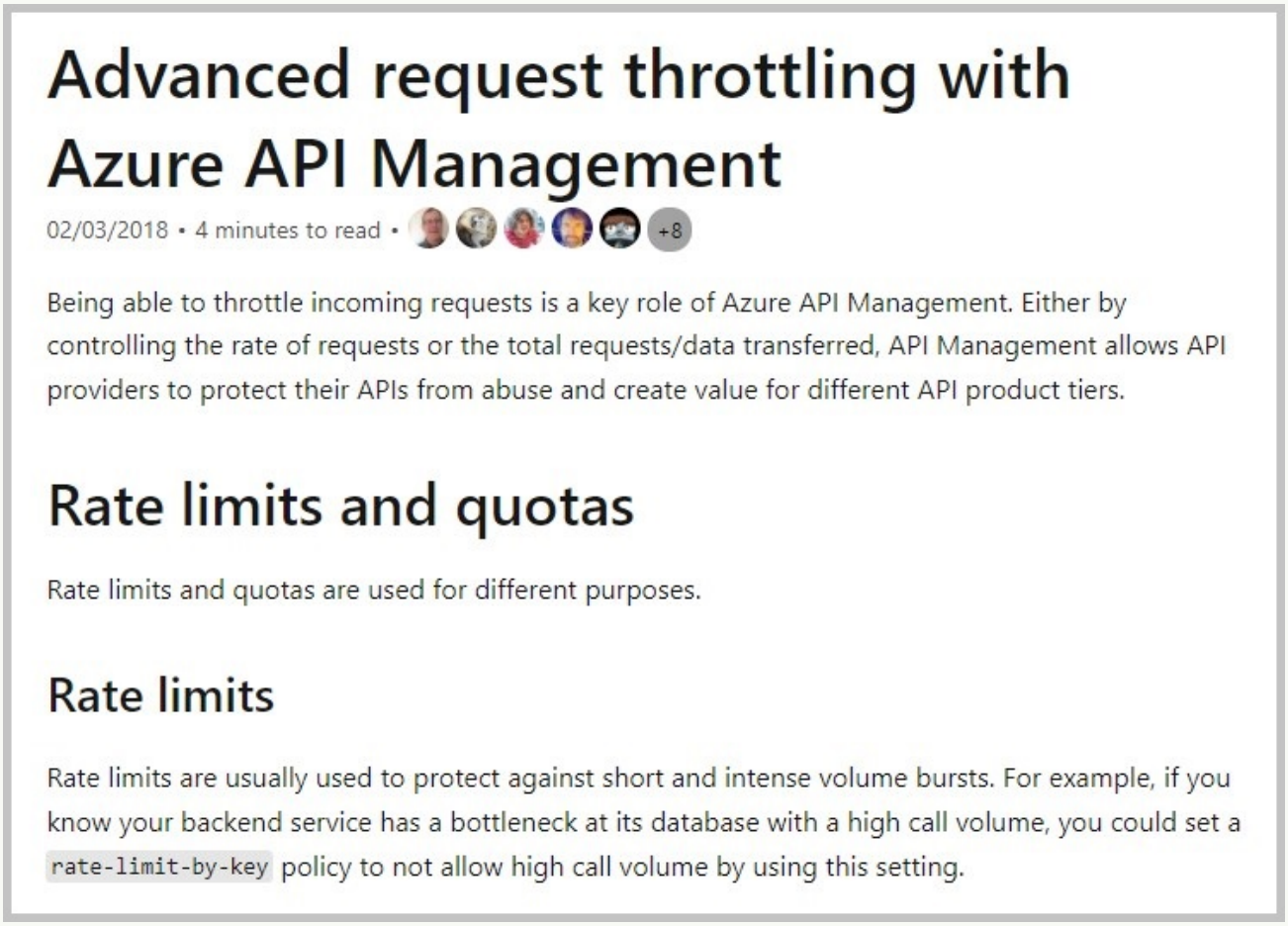
But as this is not in the answers, so rate limit is the best choice. It has more options to control DDoS attacks in a world open scenario where legitimate requests can come from everywhere

Reference:

https://docs.microsoft.com/en-us/azure/api-management/api-management-sample-flexible-throttling

https://docs.microsoft.com/en-us/azure/api-management/api-management-access-restriction-policies

https://docs.microsoft.com/en-us/azure/api-management/security-baseline



Advanced request throttling with Azure API Management

02/03/2018 • 4 minutes to read • +8

Being able to throttle incoming requests is a key role of Azure API Management. Either by controlling the rate of requests or the total requests/data transferred, API Management allows API providers to protect their APIs from abuse and create value for different API product tiers.

Rate limits and quotas

Rate limits and quotas are used for different purposes.

Rate limits

Rate limits are usually used to protect against short and intense volume bursts. For example, if you know your backend service has a bottleneck at its database with a high call volume, you could set a `rate-limit-by-key` policy to not allow high call volume by using this setting.

6. Question

You have 100 Standard_F2s_v2 Azure virtual machines. Each virtual machine has two network adapters. You need to increase the network performance of the workloads running on the virtual machines. The solution must meet the following requirements:

? The CPU-to-memory ratio must remain the same.

? The solution must minimize costs.

What should you do?

- A. Configure NIC teaming
- **B. Enable Accelerated Networking**
- C. Enable RDMA over InfiniBand
- D. Install an additional network adapter

Correct

Accelerated networking enables single root I/O virtualization (SR-IOV) to a VM, greatly improving its networking performance. This high-performance path bypasses the host from the datapath, reducing latency, jitter, and CPU utilization, for use with the most demanding network workloads on supported VM types.

Incorrect Answers:

A. Configure NIC teaming

NIC Teaming allows you to group between one and 32 physical Ethernet network adapters into one or more software-based virtual network adapters. These virtual network adapters provide fast performance and fault tolerance in the event of a network adapter failure.

C. Enable RDMA over InfiniBand

The RDMA capability boosts the scalability and performance of distributed-node HPC

D. Install an additional network adapter

This helps as a dedicated network backup solution.

Reference:

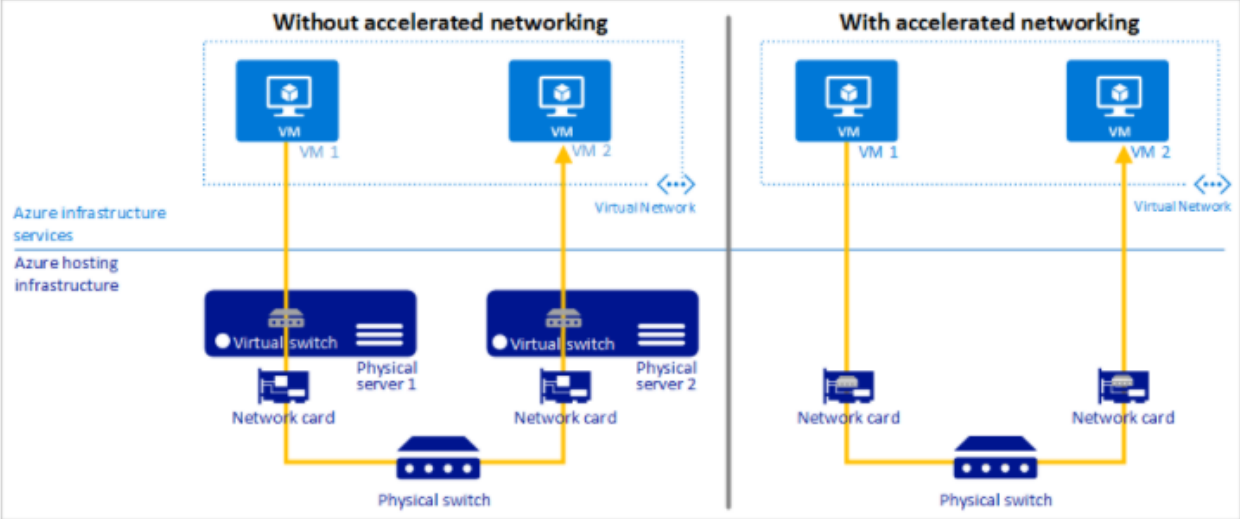
https://docs.microsoft.com/en-us/azure/virtual-network/create-vm-accelerated-networking-cli

https://docs.microsoft.com/en-us/azure/site-recovery/azure-vm-disaster-recovery-with-accelerated-networking

Accelerated Networking with Azure virtual machine disaster recovery

04/08/2019 • 3 minutes to read •

Accelerated Networking enables single root I/O virtualization (SR-IOV) to a VM, greatly improving its networking performance. This high-performance path bypasses the host from the datapath, reducing latency, jitter, and CPU utilization, for use with the most demanding network workloads on supported VM types. The following picture shows communication between two VMs with and without accelerated networking:



Azure Site Recovery enables you to utilize the benefits of Accelerated Networking, for Azure virtual machines that are failed over to a different Azure region. This article describes how you can enable Accelerated Networking for Azure virtual machines replicated with Azure Site Recovery.

7. 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. General Overview

Litware, Inc. is a medium-sized finance company.

Overview. Physical Locations

Litware has a main office in Boston.

?? Existing Environment

? Identity Environment

? The network contains an Active Directory forest named Litware.com that is linked to an Azure Active Directory (Azure AD) tenant named Litware.com. All users have Azure Active Directory Premium P2 licenses.

? Litware has a second Azure AD tenant named dev.Litware.com that is used as a development environment.

? The Litware.com tenant has a conditional ac?ess policy named capolicy1. Capolicy1 requires that when users manage the Azure subscription for a production environment by using the Azure portal, they must connect from a hybrid Azure AD-joined device.

? Azure Environment

? Litware has 10 Azure subscriptions that are linked to the Litware.com tenant and five Azure subscriptions that are linked to the dev.Litware.com tenant. All the subscriptions are in an Enterprise Agreement (EA).

? The Litware.com tenant contains a custom Azure role-based access control (Azure RBAC) role named Role1 that grants the DataActions read permission to the blobs and files in Azure Storage.

? On-premises Environment

The on-premises network of Litware contains the resources shown in the following table.

Name	Type	Configuration
SERVER1 SERVER2 SERVER3	Ubuntu 18.04 virtual machines hosted on Hyper-V	The virtual machines host a third-party app named App1. App1 uses an external storage solution that provides Apache Hadoop-compatible data storage. The data storage supports POSIX access control list (ACL) file-level permissions.
SERVER10	Server that runs Windows Server 2016	The server contains a Microsoft SQL Server instance that hosts two databases named DB1 and DB2.

? Network Environment

Litware has ExpressRoute connectivity to Azure.

?? Planned Changes and Requirements.

? Planned Changes

Litware plans to implement the following changes:

? Migrate DB1 and DB2 to Azure.

? Migrate App1 to Azure virtual machines.

? Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.

? Authentication and Authorization Requirements

Litware identifies the following authentication and authorization requirements:

? Users that manage the production environment by using the Azure portal must connect from a hybrid Azure AD-joined device and authenticate by using Azure Multi-Factor Authentication (MFA).

? The Network Contributor built-in RBAC role must be used to grant permission to all the virtual networks in all the Azure subscriptions.

? To access the resources in Azure, App1 must use the managed identity of the virtual machines that will

host the app.

? Role1 must be used to assign permissions to the storage accounts of all the Azure subscriptions.

? RBAC roles must be applied at the highest level possible.

? Resiliency Requirements

Litware identifies the following resiliency requirements:

? Once migrated to Azure, DB1 and DB2 must meet the following requirements:

? Maintain availability if two availability zones in the local Azure region fail.

? Fail over automatically.

? Minimize I/O latency.

? App1 must meet the following requirements:

? Be hosted in an Azure region that supports availability zones.

? Be hosted on Azure virtual machines that support automatic scaling.

? Maintain availability if two availability zones in the local Azure region fail.

? Security and Compliance Requirements

Litware identifies the following security and compliance requirements:

? Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.

? On-premises users and services must be able to access the Azure Storage account that will host the data in App1.

? Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.

? All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.

? App1 must not share physical hardware with other workloads.

? Business Requirements

Litware identifies the following business requirements:

? Minimize administrative effort.

? Minimize costs.

Question

You plan to migrate App1 to Azure.

You need to recommend a network connectivity solution for the Azure Storage account that will host the App1 data. The solution must meet the security and compliance requirements.

What should you include in the recommendation?

- A. a private endpoint
- B. a service endpoint that has a service endpoint policy
- C. Azure public peering for an ExpressRoute circuit
- D. Microsoft peering for an ExpressRoute circuit

Incorrect

By default, Azure service resources secured to virtual networks aren't reachable from on-premises networks. If you want to allow traffic from on-premises, you must also allow public (typically, NAT) IP addresses from your on-premises or ExpressRoute. You can add these IP addresses through the IP firewall configuration for Azure service resources.

You can use ExpressRoute for public peering and Microsoft peering.

Scenario:

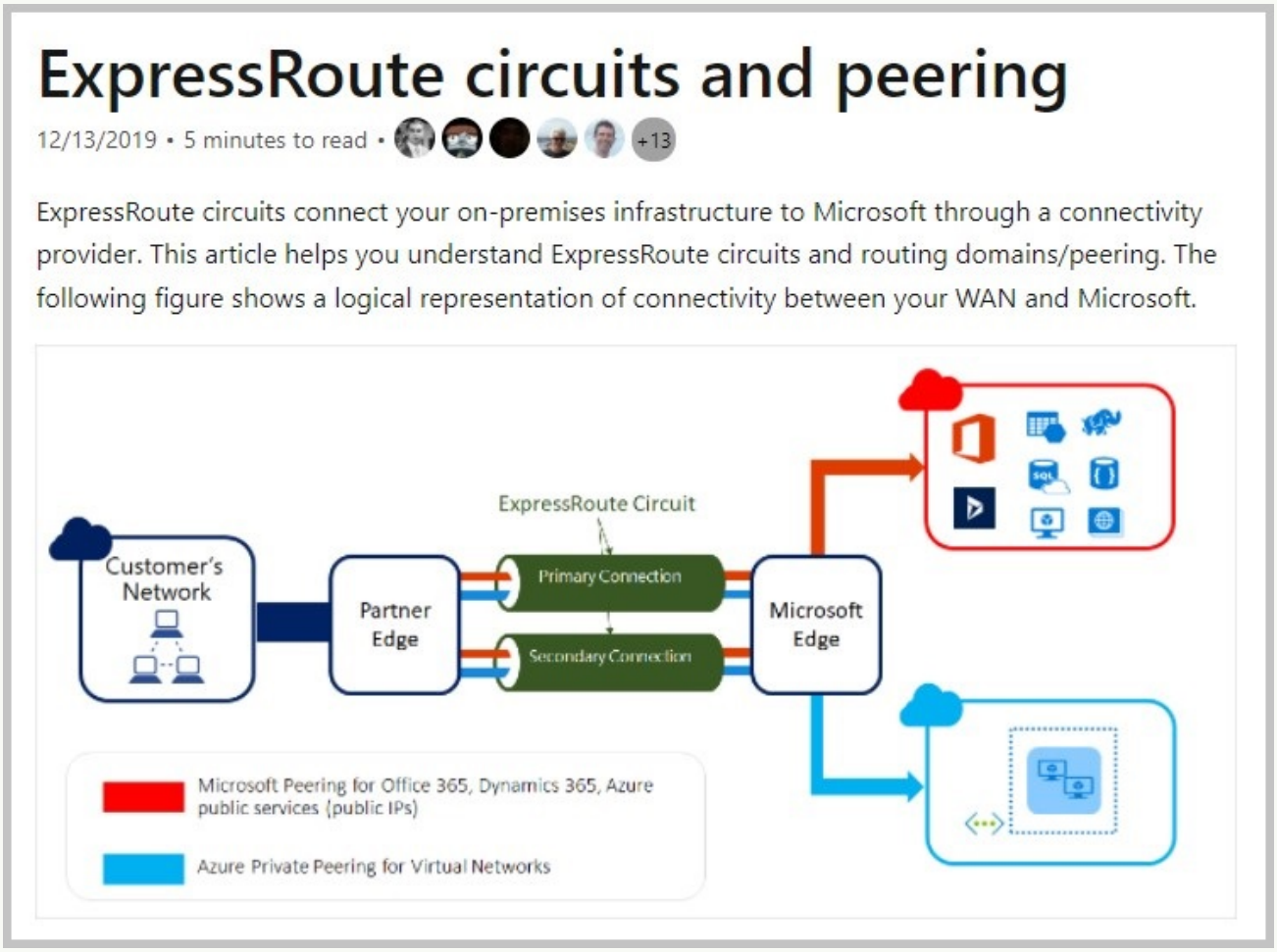
? On-premises users and services must be able to access the Azure Storage account that will host the data in App1.

? Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings



8. 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. General Overview

Litware, Inc. is a medium-sized finance company.

Overview. Physical Locations

Litware has a main office in Boston.

?? Existing Environment

? Identity Environment

? The network contains an Active Directory forest named Litware.com that is linked to an Azure Active Directory (Azure AD) tenant named Litware.com. All users have Azure Active Directory Premium P2 licenses.

? Litware has a second Azure AD tenant named dev.Litware.com that is used as a development environment.

? The Litware.com tenant has a conditional ac?ess policy named capolicy1. Capolicy1 requires that when users manage the Azure subscription for a production environment by using the Azure portal, they must connect from a hybrid Azure AD-joined device.

? Azure Environment

? Litware has 10 Azure subscriptions that are linked to the Litware.com tenant and five Azure subscriptions that are linked to the dev.Litware.com tenant. All the subscriptions are in an Enterprise Agreement (EA).

? The Litware.com tenant contains a custom Azure role-based access control (Azure RBAC) role named Role1 that grants the DataActions read permission to the blobs and files in Azure Storage.

? On-premises Environment

The on-premises network of Litware contains the resources shown in the following table.

Name	Type	Configuration
SERVER1 SERVER2 SERVER3	Ubuntu 18.04 virtual machines hosted on Hyper-V	The virtual machines host a third-party app named App1. App1 uses an external storage solution that provides Apache Hadoop-compatible data storage. The data storage supports POSIX access control list (ACL) file-level permissions.
SERVER10	Server that runs Windows Server 2016	The server contains a Microsoft SQL Server instance that hosts two databases named DB1 and DB2.

? Network Environment

Litware has ExpressRoute connectivity to Azure.

?? Planned Changes and Requirements.

? Planned Changes

Litware plans to implement the following changes:

? Migrate DB1 and DB2 to Azure.

? Migrate App1 to Azure virtual machines.

? Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.

? Authentication and Authorization Requirements

Litware identifies the following authentication and authorization requirements:

? Users that manage the production environment by using the Azure portal must connect from a hybrid Azure AD-joined device and authenticate by using Azure Multi-Factor Authentication (MFA).

? The Network Contributor built-in RBAC role must be used to grant permission to all the virtual networks in all the Azure subscriptions.

? To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.

? Role1 must be used to assign permissions to the storage accounts of all the Azure subscriptions.

? RBAC roles must be applied at the highest level possible.

? Resiliency Requirements

Litware identifies the following resiliency requirements:

? Once migrated to Azure, DB1 and DB2 must meet the following requirements:

? Maintain availability if two availability zones in the local Azure region fail.

? Fail over automatically.

? Minimize I/O latency.

? App1 must meet the following requirements:

? Be hosted in an Azure region that supports availability zones.

? Be hosted on Azure virtual machines that support automatic scaling.

? Maintain availability if two availability zones in the local Azure region fail.

? Security and Compliance Requirements

Litware identifies the following security and compliance requirements:

? Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.

? On-premises users and services must be able to access the Azure Storage account that will host the data in App1.

? Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.

? All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.

? App1 must not share physical hardware with other workloads.

? Business Requirements

Litware identifies the following business requirements:

? Minimize administrative effort.

? Minimize costs.

Question

You plan to migrate App1 to Azure. The solution must meet the authentication and authorization

requirements.

Which type of endpoint should App1 use to obtain an access token?

- A. Azure Instance Metadata Service (IMDS)
- B. Azure AD
- C. Azure Service Management
- D. Microsoft identity platform

Correct

Of course, that is somehow a part of “Microsoft Identity Platform,“ but you‘d clearly use Azure Instance Metadata service to “obtain the token.“

A managed identity, assigned by the system, can be enabled on the VM. You can also assign one or more user-assigned managed identities to the VM. You can then request tokens for managed identities from IMDS. Use these tokens to authenticate with other Azure services, such as Azure Key Vault.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/instance-metadata-service?tabs=windows#managed-identity

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-to-use-vm-token

Azure Instance Metadata Service (Windows)

04/16/2021 • 33 minutes to read • +31

Applies to: ✔ Windows VMs

The Azure Instance Metadata Service (IMDS) provides information about currently running virtual machine instances. You can use it to manage and configure your virtual machines. This information includes the SKU, storage, network configurations, and upcoming maintenance events. For a complete list of the data available, see the Endpoint Categories Summary.

IMDS is available for running instances of virtual machines (VMs) and virtual machine scale set instances. All endpoints support VMs created and managed by using Azure Resource Manager. Only the Attested category and Network portion of the Instance category support VMs created by using the classic deployment model. The Attested endpoint does so only to a limited extent.

IMDS is a REST API that's available at a well-known, non-routable IP address (`169.254.169.254`). You can only access it from within the VM. Communication between the VM and IMDS never leaves the host. Have your HTTP clients bypass web proxies within the VM when querying IMDS, and treat `169.254.169.254` the same as 168.63.129.16.

9. 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. General Overview

Litware, Inc. is a medium-sized finance company.

Overview. Physical Locations

Litware has a main office in Boston.

?? Existing Environment

? Identity Environment

? The network contains an Active Directory forest named Litware.com that is linked to an Azure Active Directory (Azure AD) tenant named Litware.com. All users have Azure Active Directory Premium P2 licenses.

? Litware has a second Azure AD tenant named dev.Litware.com that is used as a development environment.

? The Litware.com tenant has a conditional ac?ess policy named capolicy1. Capolicy1 requires that when users manage the Azure subscription for a production environment by using the Azure portal, they must connect from a hybrid Azure AD-joined device.

? Azure Environment

? Litware has 10 Azure subscriptions that are linked to the Litware.com tenant and five Azure subscriptions that are linked to the dev.Litware.com tenant. All the subscriptions are in an Enterprise Agreement (EA).

? The Litware.com tenant contains a custom Azure role-based access control (Azure RBAC) role named Role1 that grants the DataActions read permission to the blobs and files in Azure Storage.

? On-premises Environment

The on-premises network of Litware contains the resources shown in the following table.

Name	Type	Configuration
SERVER1 SERVER2 SERVER3	Ubuntu 18.04 virtual machines hosted on Hyper-V	The virtual machines host a third-party app named App1. App1 uses an external storage solution that provides Apache Hadoop-compatible data storage. The data storage supports POSIX access control list (ACL) file-level permissions.
SERVER10	Server that runs Windows Server 2016	The server contains a Microsoft SQL Server instance that hosts two databases named DB1 and DB2.

? Network Environment

Litware has ExpressRoute connectivity to Azure.

?? Planned Changes and Requirements.

? Planned Changes

Litware plans to implement the following changes:

? Migrate DB1 and DB2 to Azure.

? Migrate App1 to Azure virtual machines.

? Deploy the Azure virtual machines that will host App1 to Azure dedicated hosts.

? Authentication and Authorization Requirements

Litware identifies the following authentication and authorization requirements:

? Users that manage the production environment by using the Azure portal must connect from a hybrid Azure AD-joined device and authenticate by using Azure Multi-Factor Authentication (MFA).

? The Network Contributor built-in RBAC role must be used to grant permission to all the virtual networks in all the Azure subscriptions.

? To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.

? Role1 must be used to assign permissions to the storage accounts of all the Azure subscriptions.

? RBAC roles must be applied at the highest level possible.

? Resiliency Requirements

Litware identifies the following resiliency requirements:

? Once migrated to Azure, DB1 and DB2 must meet the following requirements:

? Maintain availability if two availability zones in the local Azure region fail.

? Fail over automatically.

? Minimize I/O latency.

? App1 must meet the following requirements:

? Be hosted in an Azure region that supports availability zones.

? Be hosted on Azure virtual machines that support automatic scaling.

? Maintain availability if two availability zones in the local Azure region fail.

? Security and Compliance Requirements

Litware identifies the following security and compliance requirements:

? Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.

? On-premises users and services must be able to access the Azure Storage account that will host the data in App1.

? Access to the public endpoint of the Azure Storage account that will host the App1 data must be prevented.

? All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.

? App1 must not share physical hardware with other workloads.

? Business Requirements

Litware identifies the following business requirements:

? Minimize administrative effort.

? Minimize costs.

Question

You need to configure an Azure policy to ensure that the Azure SQL databases have TDE enabled. The solution must meet the security and compliance requirements.

Which three actions should you perform in sequence?

? Create an Azure policy definition that uses the deployIfNotExists effect.

? Create a user-assigned managed identity.

? Invoke a remediation task.

? Create an Azure policy assignment.

? Create an Azure policy definition that uses the Modify effect

- (●) 1 -> 4 -> 3
- ( ) 2 -> 4 -> 3
- ( ) 4 -> 1 -> 3
- ( ) 5 -> 3 -> 4

Correct

Scenario: All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.

Step 1: Create an Azure policy definition that uses the deployIfNotExists identity.

The first step is to define the roles that deployIfNotExists and modify needs in the policy definition to successfully deploy the content of your included template.

Step 2: Create an Azure policy assignment

When creating an assignment using the portal, Azure Policy both generates the managed identity and grants it the roles defined in roleDefinitionIds.

Step 3: Invoke a remediation task

Resources that are non-compliant to a deployIfNotExists or modify policy can be put into a compliant state through Remediation. Remediation is accomplished by instructing Azure Policy to run the deployIfNotExists effect or the modify operations of the assigned policy on your existing resources and

subscriptions, whether that assignment is to a management group, a subscription, a resource group, or an individual resource.

During evaluation, the policy assignment with deployIfNotExists or modify effects determines if there are non-compliant resources or subscriptions. When non-compliant resources or subscriptions are found, the details are provided on the Remediation page.

Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

Remediate non-compliant resources with Azure Policy

08/17/2021 • 7 minutes to read •

Resources that are non-compliant to a **deployIfNotExists** or **modify** policy can be put into a compliant state through **Remediation**. Remediation is accomplished by instructing Azure Policy to run the **deployIfNotExists** effect or the **modify operations** of the assigned policy on your existing resources and subscriptions, whether that assignment is to a management group, a subscription, a resource group, or an individual resource. This article shows the steps needed to understand and accomplish remediation with Azure Policy.

10. 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 solution for implementing the back-end tier of the payment processing system in Azure.

What should you include in the recommendation?

- A. an Azure SQL Database managed instance
- B. a SQL Server database on an Azure virtual machine
- C. an Azure SQL Database single database
- D. an Azure SQL Database elastic pool

Correct

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

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

SQL Managed Instance has near 100% compatibility with the latest SQL Server (Enterprise Edition) database engine. So you can migrate application with minimal effort.

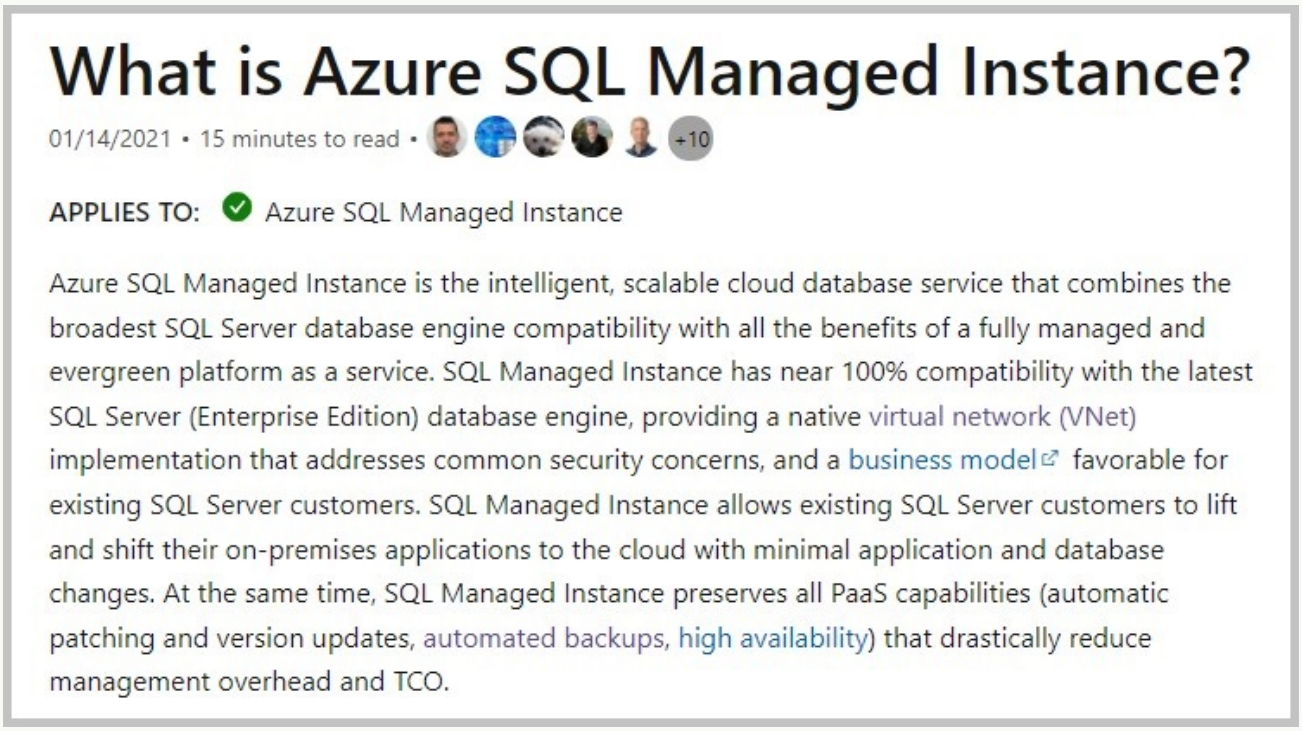
Using SQL Server Agent in SQL Server and SQL Managed Instance, you can create and schedule jobs

that could be periodically executed against one or many databases to run Transact-SQL (T-SQL) queries and perform maintenance tasks.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview

https://docs.microsoft.com/en-us/azure/azure-sql/database/job-automation-managed-instances



What is Azure SQL Managed Instance?

01/14/2021 • 15 minutes to read • +10

APPLIES TO: Azure SQL Managed Instance

Azure SQL Managed Instance is the intelligent, scalable cloud database service that combines the broadest SQL Server database engine compatibility with all the benefits of a fully managed and evergreen platform as a service. SQL Managed Instance has near 100% compatibility with the latest SQL Server (Enterprise Edition) database engine, providing a native virtual network (VNet) implementation that addresses common security concerns, and a business model favorable for existing SQL Server customers. SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.

11. Question

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager resource deployments in your subscription.

What should you include in the recommendation?

- A. Azure Advisor
- B. Azure Analysis Services
- C. Azure Monitor action groups
- **D. Azure Log Analytics**

Incorrect

Log Analytics is a tool in the Azure portal used to edit and run log queries with data in Azure Monitor Logs. You may write a simple query that returns a set of records and then use features of Log Analytics to sort, filter, and analyze them. Or you may write a more advanced query to perform statistical analysis and visualize the results in a chart to identify a particular trend.

Incorrect Answers:

A. Azure Advisor

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

B. Azure Analysis Services

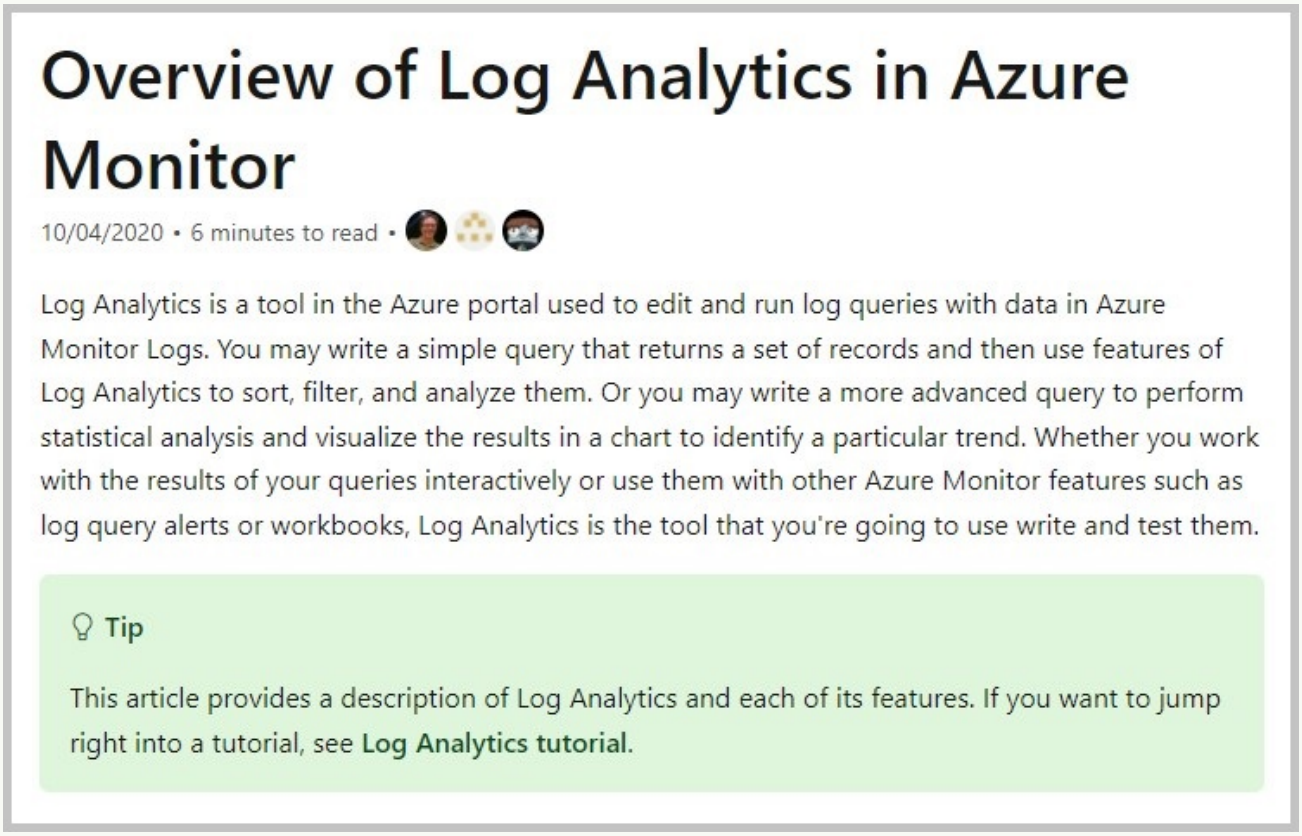
Azure Analysis Services is a fully managed platform as a service (PaaS) that provides enterprise-grade data models in the cloud.

C. Azure Monitor action groups

An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor, Service Health and Azure Advisor alerts use action groups to notify users that an alert has been triggered.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview



Overview of Log Analytics in Azure Monitor

10/04/2020 • 6 minutes to read •

Log Analytics is a tool in the Azure portal used to edit and run log queries with data in Azure Monitor Logs. You may write a simple query that returns a set of records and then use features of Log Analytics to sort, filter, and analyze them. Or you may write a more advanced query to perform statistical analysis and visualize the results in a chart to identify a particular trend. Whether you work with the results of your queries interactively or use them with other Azure Monitor features such as log query alerts or workbooks, Log Analytics is the tool that you're going to use write and test them.

Tip

This article provides a description of Log Analytics and each of its features. If you want to jump right into a tutorial, see **Log Analytics tutorial**.

12. Question

A company has a hybrid ASP.NET Web API application that is based on a software as a service (SaaS) offering.

Users report general issues with the data. You advise the company to implement live monitoring and use ad hoc queries on stored JSON data. You also advise the company to set up smart alerting to detect anomalies in the data.

You need to recommend a solution to set up smart alerting.

What should you recommend?

- A. Azure Site Recovery and Azure Monitor Logs

B. Azure Data Lake Analytics and Azure Monitor Logs

C. Azure Application Insights and Azure Monitor Logs

D. Azure Security Center and Azure Data Lake Store

Incorrect

Application Insights, a feature of Azure Monitor, is an extensible Application Performance Management (APM) service for developers and DevOps professionals. Use it to monitor your live applications. It will automatically detect performance anomalies, and includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app. It's designed to help you continuously improve performance and usability. It works for apps on a wide variety of platforms including .NET, Node.js, Java, and Python hosted on-premises, hybrid, or any public cloud. It integrates with your DevOps process, and has connection points to a variety of development tools. It can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center.

Incorrect Answers:

A. Azure Site Recovery and Azure Monitor Logs

Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages.

B. Azure Data Lake Analytics and Azure Monitor Logs

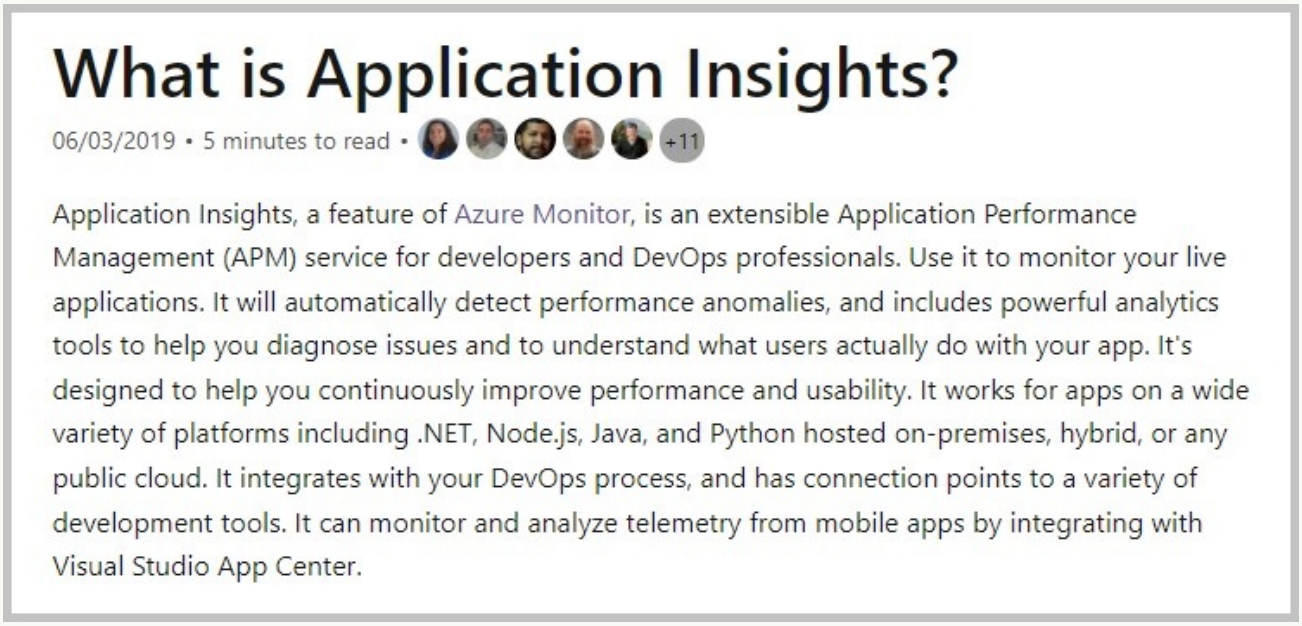
Azure Data Lake Analytics is an on-demand analytics job service that simplifies big data. It is not used to alerting.

D. Azure Security Center and Azure Data Lake Store

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud. It is used for security related alerts. Not to debug application specific issues.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview



What is Application Insights?

06/03/2019 • 5 minutes to read • +11

Application Insights, a feature of Azure Monitor, is an extensible Application Performance Management (APM) service for developers and DevOps professionals. Use it to monitor your live applications. It will automatically detect performance anomalies, and includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app. It's designed to help you continuously improve performance and usability. It works for apps on a wide variety of platforms including .NET, Node.js, Java, and Python hosted on-premises, hybrid, or any public cloud. It integrates with your DevOps process, and has connection points to a variety of development tools. It can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center.

13. Question

You have an Azure subscription.

You need to recommend a solution to provide developers with the ability to provision Azure virtual machines. The solution must meet the following requirements:

? Only allow the creation of the virtual machines in specific regions.

? Only allow the creation of specific sizes of virtual machines.

What should you include in the recommendation?

- A. Azure Resource Manager templates
- **B. Azure Policy**
- C. conditional access policies
- D. role-based access control (RBAC)

Correct

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management

Incorrect Answers:

A. Azure Resource Manager templates

Using ARM templates, you can automate deployments and use the practice of infrastructure as code.

C. conditional access policies

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action.

D. role-based access control (RBAC)

Azure role-based access control (Azure RBAC) helps you manage who has access to Azure resources.

Reference:

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

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/manage/azure-server-management/common-policies#restrict-vm-size

What is Azure Policy?

07/27/2021 • 11 minutes to read • +4

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management. Policy definitions for these common use cases are already available in your Azure environment as built-ins to help you get started.

All Azure Policy data and objects are encrypted at rest. For more information, see Azure data encryption at rest.

14. 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 solution for the data store of the historical transaction query system.

Which of the following should you choose as the sizing requirements?

- A. A table that has unlimited capacity
- B. A table that has a fixed capacity
- C. Multiple tables that have unlimited capacity
- **D. Multiple tables that have fixed capacity**

Incorrect

Here the issue is that the queries are based on different attributes of the item. Hence it would be ideal to create multiple tables. Each table can have the same values and specify a different partition key. Even though in Azure Cosmos DB , you can have virtually unlimited capacity, you can choose to limit the capacity since the data size is not going to increase for the system.

Multiple tables, because of the 20GB Maximum storage across all items per (logical) partition.

Reference:

https://docs.microsoft.com/en-us/azure/cosmos-db/table-api-faq#does-the-table-api-index-all-attributes-of-an-entity-by-default

https://docs.microsoft.com/en-us/azure/cosmos-db/concepts-limits#provisioned-throughput

https://docs.microsoft.com/en-us/azure/cosmos-db/table-storage-design-guide

Design scalable and performant tables

03/09/2020 • 8 minutes to read • 

Tip

The content in this article applies to the original Azure Table storage. However, the same concepts apply to the newer Azure Cosmos DB Table API. The Cosmos DB Table API offers higher performance and availability, global distribution, and automatic secondary indexes. It is also available in a consumption-based **serverless** mode. There are some **feature differences** between Table API in Azure Cosmos DB and Azure table storage. For more information, see **Azure Cosmos DB Table API**. For ease of development, we now provide a unified **Azure Tables SDK** that can be used to target both the original Table storage as well as the Cosmos DB Table API.

To design scalable and performant tables, you must consider factors such as performance, scalability, and cost. If you have previously designed schemas for relational databases, these considerations are familiar, but while there are some similarities between the Azure Table service storage model and relational models, there are also important differences. These differences typically lead to different designs that may look counter-intuitive or wrong to someone familiar with relational databases, yet make sense if you are designing for a NoSQL key/value store such as the Azure Table service. Many of your design differences reflect the fact that the Table service is designed to support cloud-scale applications that can contain billions of entities (or rows in relational database terminology) of data or for datasets that must support high transaction volumes. Therefore, you must think differently about how you store your data and understand how the Table service works. A well-designed NoSQL data store can enable your solution to scale much further and at a lower cost than a solution that uses a relational database. This guide helps you with these topics.

15. 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 solution for the data store of the historical transaction query system.

Which of the following would you choose as the right option for implementing resiliency?

- A. An additional read region
- B. An Availability Set
- C. An Availability Zone

Correct

In Azure Cosmos DB , you can implement a new read region. This would ensure the data is available in another region in case of a region wide failure to the primary region.

Reference:

https://docs.microsoft.com/en-us/azure/cosmos-db/table/table-api-faq#does-the-table-api-index-all-attributes-of-an-entity-by-default

16. 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 solution for protecting the content of the payment processing system.

What should you include in the recommendation?

- A. Always Encrypted with deterministic encryption
- B. Always Encrypted with randomized encryption
- C. Transparent Data Encryption (TDE)
- D. Azure Storage Service Encryption

Incorrect

Using the Always Encrypted with deterministic encryption feature would allow for data to be encrypted at rest and in transit. Transparent Data Encryption would only encrypt data at rest. Data Masking will only hide sensitive data. Azure Storage Service Encryption is used for encrypting data in storage accounts.

Deterministic encryption always generates the same encrypted value for any given plain text value. Using deterministic encryption allows point lookups, equality joins, grouping and indexing on encrypted columns. However, it may also allow unauthorized users to guess information about encrypted values by examining patterns in the encrypted column, especially if there's a small set of possible encrypted values, such as True/False, or North/South/East/West region. Deterministic encryption must use a column collation with a binary2 sort order for character columns.

Randomized encryption uses a method that encrypts data in a less predictable manner. Randomized encryption is more secure, but prevents searching, grouping, indexing, and joining on encrypted columns.

Reference:

https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-ver15#selecting—deterministic-or-randomized-encryption

Selecting Deterministic or Randomized Encryption

The Database Engine never operates on plaintext data stored in encrypted columns, but it still supports some queries on encrypted data, depending on the encryption type for the column. Always Encrypted supports two types of encryption: randomized encryption and deterministic encryption.

- Deterministic encryption always generates the same encrypted value for any given plain text value. Using deterministic encryption allows point lookups, equality joins, grouping and indexing on encrypted columns. However, it may also allow unauthorized users to guess information about encrypted values by examining patterns in the encrypted column, especially if there's a small set of possible encrypted values, such as True/False, or North/South/East/West region. Deterministic encryption must use a column collation with a binary2 sort order for character columns.

- Randomized encryption uses a method that encrypts data in a less predictable manner. Randomized encryption is more secure, but prevents searching, grouping, indexing, and joining on encrypted columns.

Use deterministic encryption for columns that will be used as search or grouping parameters. For example, a government ID number. Use randomized encryption for data such as confidential investigation comments, which aren't grouped with other records and aren't used to join tables. For details on Always Encrypted cryptographic algorithms, see Always Encrypted cryptography.

17. Question

You are designing a virtual machine that will run Microsoft SQL Server and will contain two data disks. The first data disk will store log files, and the second data disk will store data. Both disks are P40 managed disks.

You need to recommend a caching policy for each disk. The policy must provide the best overall performance for the virtual machine while preserving integrity of the SQL data and logs.

Which caching policy should you recommend for each disk?

- [x] Log: None
- [ ] Log: ReadOnly
- [ ] Log: ReadWrite
- [ ] Data: None
- [x] Data: ReadOnly
- [ ] Data: ReadWrite

Correct

You can apply these guidelines to SQL Server running on Premium Storage by doing the following,

1. Configure “ReadOnly“ cache on premium storage disks hosting data files.

a. The fast reads from cache lower the SQL Server query time since data pages are retrieved much faster from the cache compared to directly from the data disks.

b. Serving reads from cache, means there is additional Throughput available from premium data disks. SQL Server can use this additional Throughput towards retrieving more data pages and other operations like backup/restore, batch loads, and index rebuilds.

2. Configure “None“ cache on premium storage disks hosting the log files.

a. Log files have primarily write-heavy operations. Therefore, they do not benefit from the ReadOnly cache.

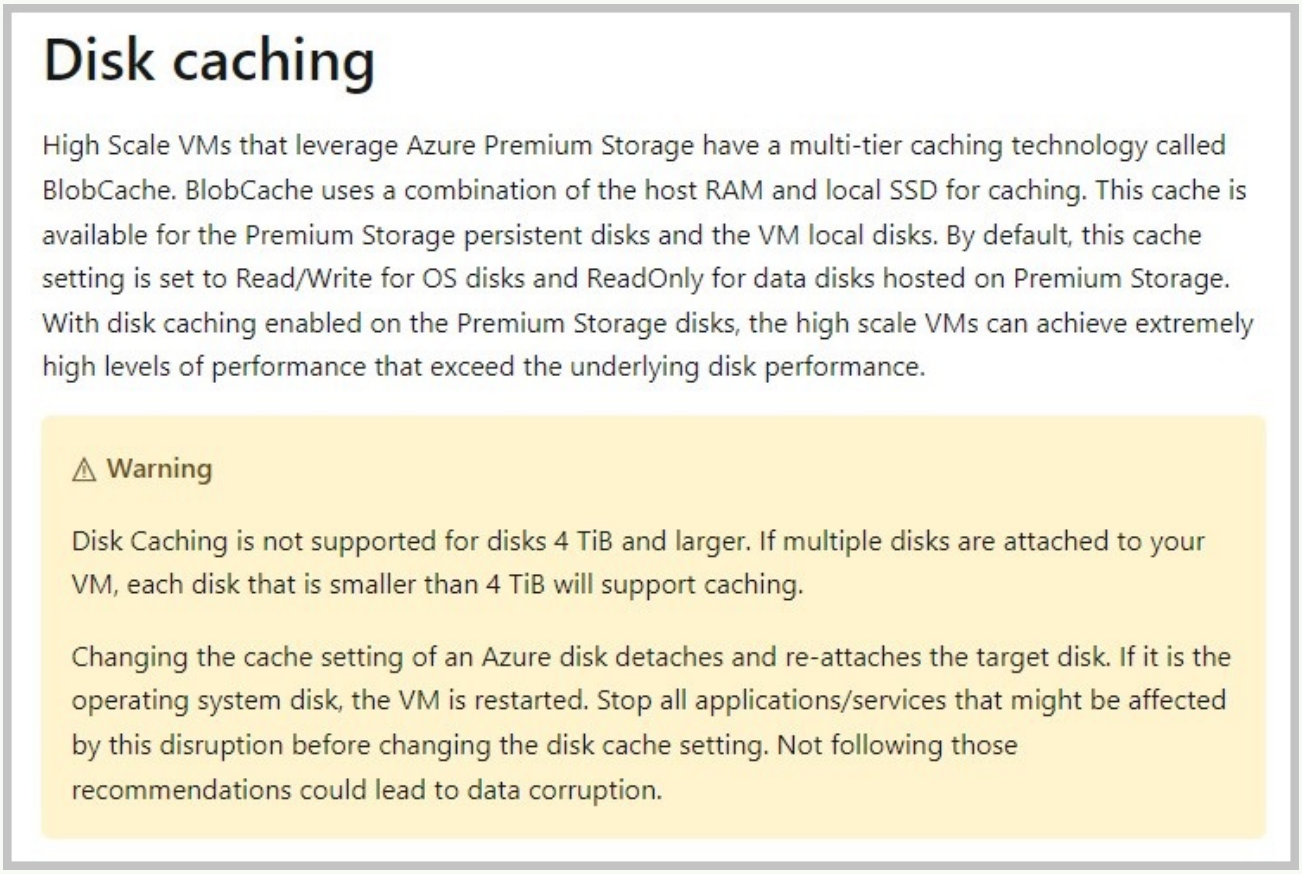
Note: If you are using separate disks for data and log files, enable read caching on the data disks hosting your data files and TempDB data files. This can result in a significant performance benefit. Do not enable caching on the disk holding the log file as this causes a minor decrease in performance.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sql/virtual-machines-windows-sql-performance

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/premium-storage-performance#disk-caching

https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices



Disk caching

High Scale VMs that leverage Azure Premium Storage have a multi-tier caching technology called BlobCache. BlobCache uses a combination of the host RAM and local SSD for caching. This cache is available for the Premium Storage persistent disks and the VM local disks. By default, this cache setting is set to Read/Write for OS disks and ReadOnly for data disks hosted on Premium Storage. With disk caching enabled on the Premium Storage disks, the high scale VMs can achieve extremely high levels of performance that exceed the underlying disk performance.

⚠ **Warning**

Disk Caching is not supported for disks 4 TiB and larger. If multiple disks are attached to your VM, each disk that is smaller than 4 TiB will support caching.

Changing the cache setting of an Azure disk detaches and re-attaches the target disk. If it is the operating system disk, the VM is restarted. Stop all applications/services that might be affected by this disruption before changing the disk cache setting. Not following those recommendations could lead to data corruption.

Currently, **None** is only supported on data disks. It is not supported on OS disks. If you set **None** on an OS disk it will override this internally and set it to **ReadOnly**.

As an example, you can apply these guidelines to SQL Server running on Premium Storage by doing the following,

1. Configure "ReadOnly" cache on premium storage disks hosting data files.
   a. The fast reads from cache lower the SQL Server query time since data pages are retrieved much faster from the cache compared to directly from the data disks.
   b. Serving reads from cache, means there is additional Throughput available from premium data disks. SQL Server can use this additional Throughput towards retrieving more data pages and other operations like backup/restore, batch loads, and index rebuilds.
2. Configure "None" cache on premium storage disks hosting the log files.
   a. Log files have primarily write-heavy operations. Therefore, they do not benefit from the ReadOnly cache.

18. Question

You plan to move a web application named App! from an on-premises data center 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 data center becomes unavailable.

? Costs must be minimized.

What should you include in the recommendation?

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

Correct

You must migrate the application to a virtual machine due to the dependency on COM component.

Availability Zones are unique physical locations with independent power, network, and cooling. Each Availability Zone is comprised of one or more datacenters and houses infrastructure to support highly available, mission critical applications. Availability Zones are tolerant to datacenter failures through redundancy and logical isolation of services.

Incorrect Answers:

A. In two Azure regions, deploy a load balancer and a virtual machine scale set.

As we are not having two independent web applications and we don‘t have any further details about the architecture of App1 this can be ruled out as well.

B. In two Azure regions, deploy a Traffic Manager profile and a web app

Azure App Service doesn't support COM components

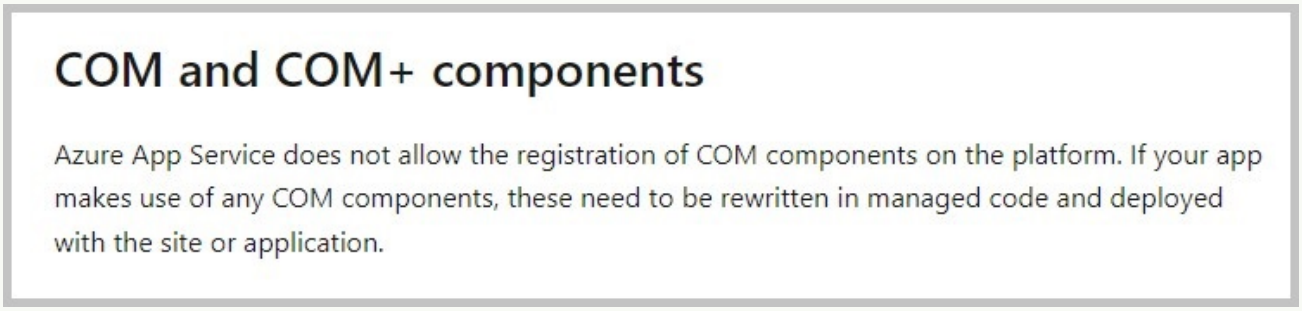
C. In two Azure regions, deploy a load balancer and a web app.

Can be ruled out, as Azure App Service doesn't support COM components

Reference:

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

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



19. Question

Your network contains an on-premises Active Directory forest.

You discover that when users change jobs within your company, the membership of the user groups are not being updated. As a result, the users can access resources that are no longer relevant to their job.

You plan to integrate Active Directory and Azure Active Directory (Azure AD) by using Azure AD Connect.

You need to recommend a solution to ensure that group owners are emailed monthly about the group memberships they manage.

What should you include in the recommendation?

- A. Azure AD Identity Protection
- **B. Azure AD access reviews**
- C. Tenant Restrictions
- D. conditional access policies

Correct

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Incorrect Answers:

A. Azure AD Identity Protection

Identity Protection is a tool that allows organizations to accomplish automated detection and remediation of of identity based risks.

C. Tenant Restrictions

With tenant restrictions, organizations can control access to SaaS cloud applications, based on the Azure

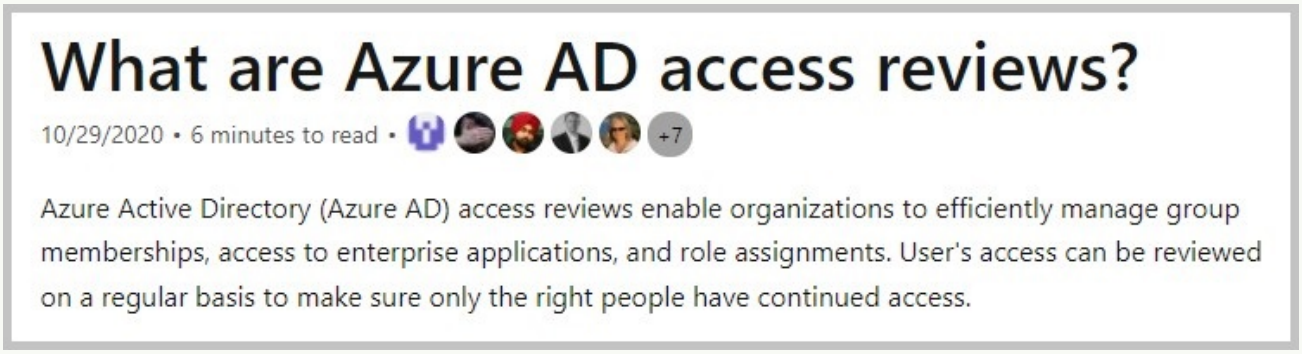
AD tenant the applications use for single sign-on. Organizations can specify the list of tenants that their users are permitted to access.

D. conditional access policies

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.

Reference:

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



20. Question

Your company has an on-premises Windows HPC cluster. The cluster runs a parallel, compute-intensive workload that performs financial risk modeling.

You plan to migrate the workload to Azure Batch.

You need to design a solution that will support the workload. The solution must meet the following requirements:

? Support the large-scale parallel execution of Azure Batch jobs.

? Minimize cost.

What should you include in the solution?

- A. burstable virtual machines
- B. low-priority virtual machines
- C. Azure virtual machine sizes that support the Message Passing Interface (MPI) API
- D. Basic A-series virtual machines

Correct

Batch works well with intrinsically parallel (also known as “embarrassingly parallel“) workloads.

Intrinsically parallel workloads have applications which can run independently, with each instance completing part of the work. When the applications are executing, they might access some common data, but they don‘t communicate with other instances of the application.

To reduce the costs we can choose low-priority virtual machines.

Incorrect Answers:

A. burstable virtual machines

These are ideal for workloads that do not need the full performance of the CPU continuously, like web servers, small databases and development and test environments.

C. Azure virtual machine sizes that support the Message Passing Interface (MPI) API

This can be a correct answer if costs are not a constraint.

D. Basic A-series virtual machines

Recommended for dev/test environments

Reference:

https://docs.microsoft.com/en-us/azure/batch/batch-technical-overview#how-it-works

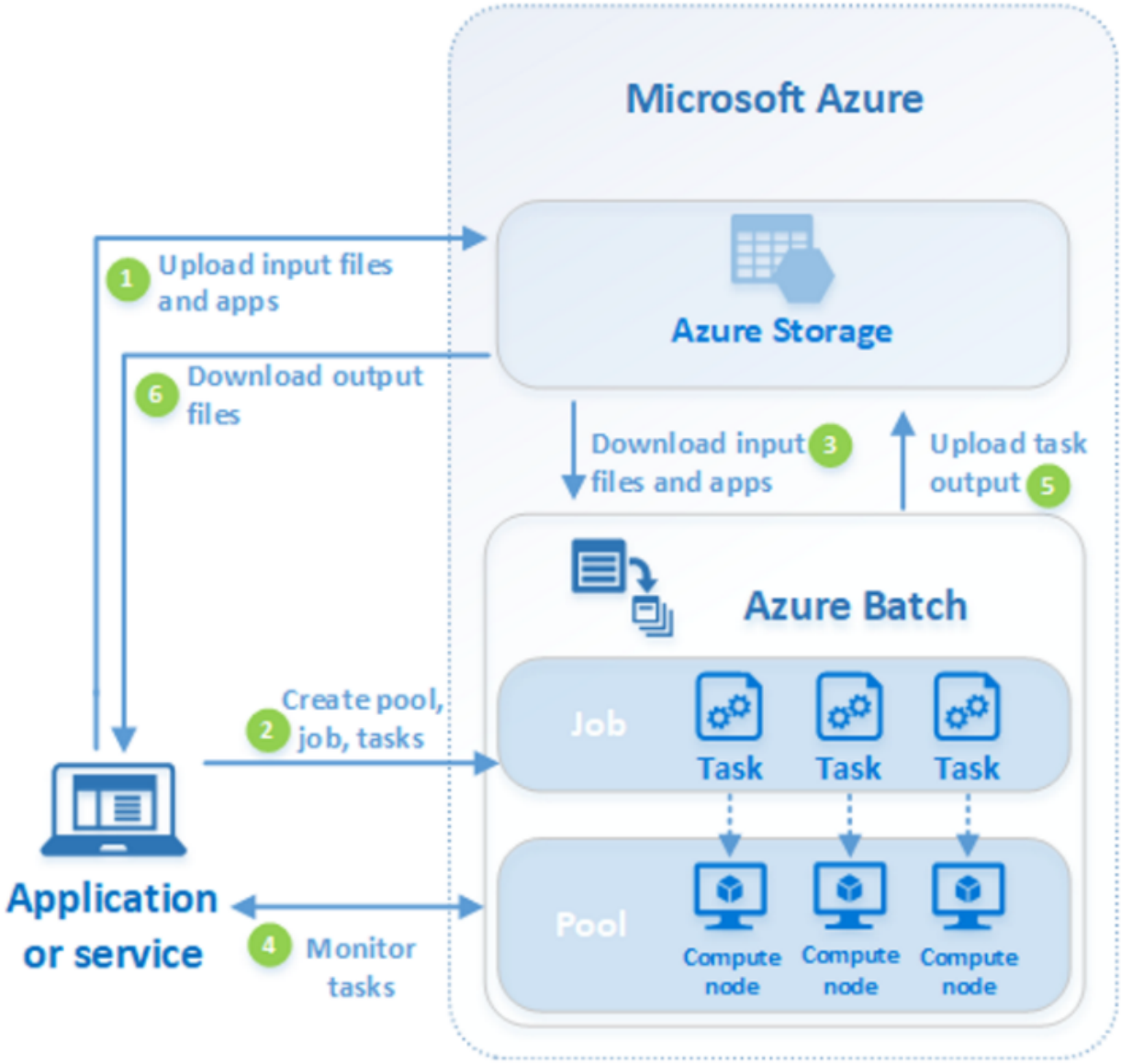
https://docs.microsoft.com/en-us/azure/batch/batch-low-pri-vms

https://azure.microsoft.com/en-us/pricing/details/batch/

How it works

A common scenario for Batch involves scaling out intrinsically parallel work, such as the rendering of images for 3D scenes, on a pool of compute nodes. This pool can be your "render farm" that provides tens, hundreds, or even thousands of cores to your rendering job.

The following diagram shows steps in a common Batch workflow, with a client application or hosted service using Batch to run a parallel workload.



21. 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.

Your company plans to deploy various Azure App Service instances that will use Azure SQL databases. The App Service instances will be deployed at the same time as the Azure SQL databases.

The company has a regulatory requirement to deploy the App Service instances only to specific Azure

regions. The resources for the App Service instances must reside in the same region.

You need to recommend a solution to meet the regulatory requirement.

Solution: You recommend using the Regulatory compliance dashboard in Azure Security Center.

Does this meet the goal?

- A. Yes
- **B. No**

Correct

The Regulatory compliance dashboard in Azure Security Center is not used for regional compliance. Instead use Azure Policy. Azure Policy helps to enforce organizational standards and to assess compliance at-scale.

Reference:

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

https://azure.microsoft.com/en-us/blog/regulatory-compliance-dashboard-in-azure-security-center-now-available/

22. 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.

Your company plans to deploy various Azure App Service instances that will use Azure SQL databases. The App Service instances will be deployed at the same time as the Azure SQL databases.

The company has a regulatory requirement to deploy the App Service instances only to specific Azure regions. The resources for the App Service instances must reside in the same region.

You need to recommend a solution to meet the regulatory requirement.

Solution: You recommend using an Azure policy to enforce the resource group location.

Does this meet the goal?

- **A. Yes**
- B. No

Correct

Azure Resource Policy Definitions can be used which can be applied to a specific Resource Group with the App Service instances.

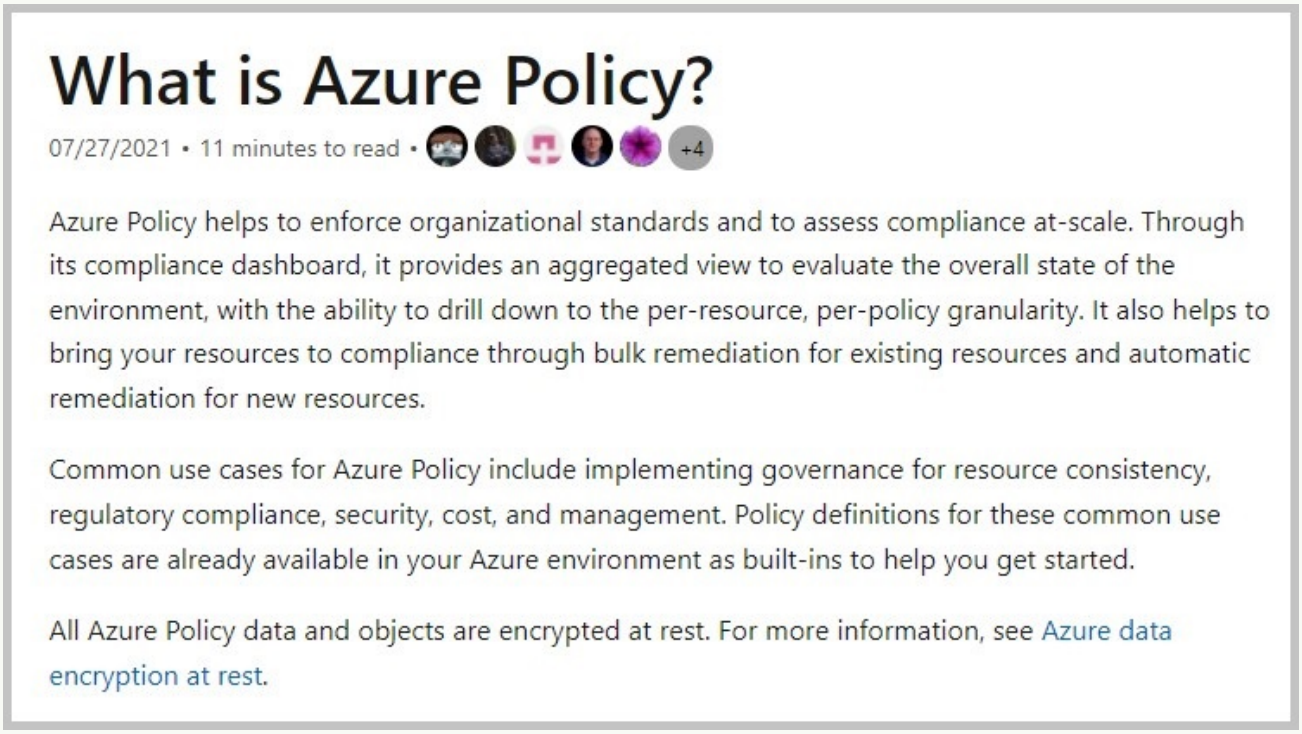
Note: An assignment is a policy definition or initiative that has been assigned to take place within a specific scope. This scope could range from a management group to an individual resource. The term scope refers to all the resources, resource groups, subscriptions, or management groups that the

definition is assigned to. Assignments are inherited by all child resources. This design means that a definition applied to a resource group is also applied to resources in that resource group. However, you can exclude a subscope from the assignment.

Reference:

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

https://docs.microsoft.com/en-us/azure/governance/policy/overview#assignments



What is Azure Policy?

07/27/2021 • 11 minutes to read • +4

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management. Policy definitions for these common use cases are already available in your Azure environment as built-ins to help you get started.

All Azure Policy data and objects are encrypted at rest. For more information, see Azure data encryption at rest.

23. 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.

Your company plans to deploy various Azure App Service instances that will use Azure SQL databases. The App Service instances will be deployed at the same time as the Azure SQL databases.

The company has a regulatory requirement to deploy the App Service instances only to specific Azure regions. The resources for the App Service instances must reside in the same region.

You need to recommend a solution to meet the regulatory requirement.

Solution: You recommend creating resource groups based on locations and implementing resource locks on the resource groups.

Does this meet the goal?

- A. Yes
- B. No

Correct

Resource locks are not used for compliance purposes. Resource locks prevent changes from being made to resources.

Instead use Azure Policy. Azure Policy helps to enforce organizational standards and to assess compliance at-scale.

Reference:

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

24. Question

You deploy two instances of an Azure web app. One instance is in the East US Azure region and the other instance is in the West US Azure region. The web app uses Azure Blob storage to deliver large files to end users.

You need to recommend a solution for delivering the files to the users. The solution must meet the following requirements:

? Ensure that the users receive files from the same region as the web app that they access.

? Ensure that the files only need to be uploaded once.

? Minimize costs.

What should you include in the recommendation?

- A. Distributed File System (DFS)
- **B. read-access geo-redundant storage (RA-GRS)**
- C. Azure File Sync
- D. geo-redundant storage (GRS)

Incorrect

Geo-redundant storage (with GRS or GZRS) replicates your data to another physical location in the secondary region to protect against regional outages. However, that data is available to be read only if the customer or Microsoft initiates a failover from the primary to secondary region. When you enable read access to the secondary region, your data is available to be read at all times, including in a situation where the primary region becomes unavailable. For read access to the secondary region, enable read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS).

When read access to the secondary is enabled, your application can be read from the secondary endpoint as well as from the primary endpoint. The secondary endpoint appends the suffix secondary to the account name. For example, if your primary endpoint for Blob storage is myaccount.blob.core.windows.net, then the secondary endpoint is myaccount-secondary.blob.core.windows.net. The account access keys for your storage account are the same for both the primary and secondary endpoints.

Incorrect Answers:

A. Distributed File System (DFS)

The Distributed File System (DFS) functions provide the ability to logically group shares on multiple servers and to transparently link shares into a single hierarchical namespace.

C. Azure File Sync

Azure File Sync transforms Windows Server into a quick cache of your Azure file share.

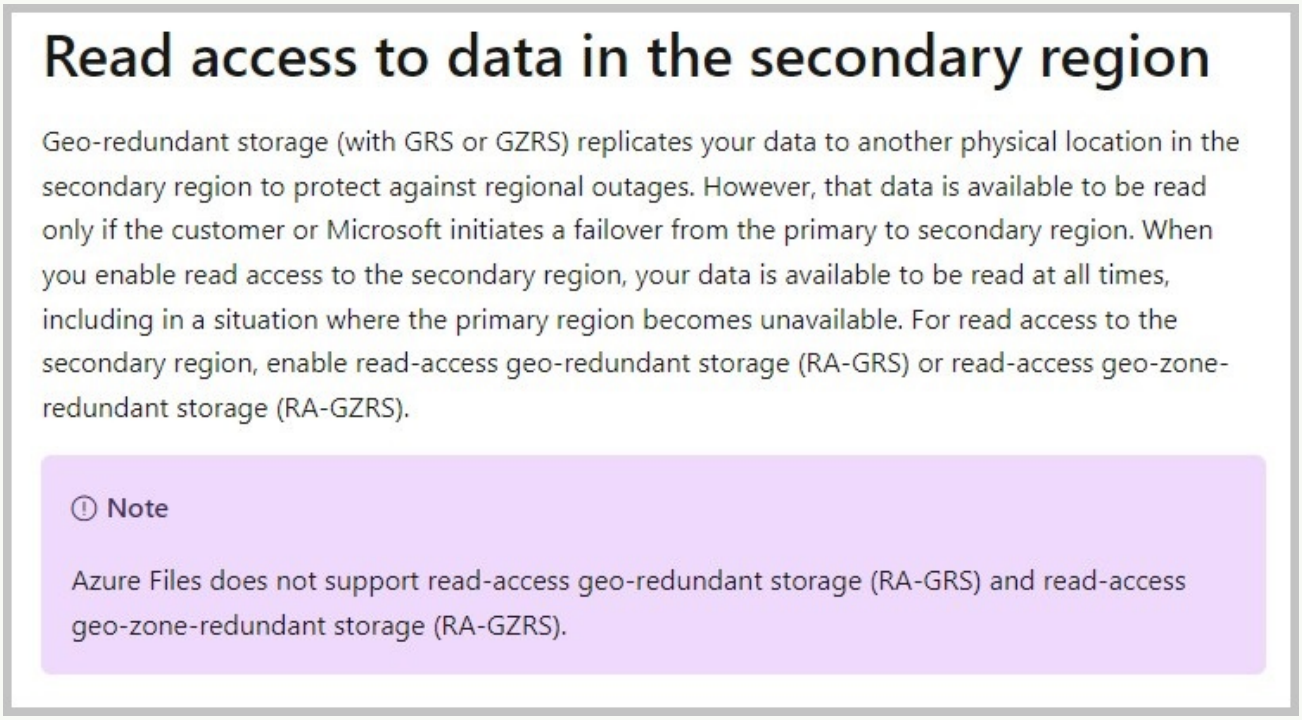
D. geo-redundant storage (GRS)

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/storage/common/storage-redundancy#read-access-to-data-in-the-secondary-region

https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#geo-redundant-storage



Read access to data in the secondary region

Geo-redundant storage (with GRS or GZRS) replicates your data to another physical location in the secondary region to protect against regional outages. However, that data is available to be read only if the customer or Microsoft initiates a failover from the primary to secondary region. When you enable read access to the secondary region, your data is available to be read at all times, including in a situation where the primary region becomes unavailable. For read access to the secondary region, enable read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS).

Note

Azure Files does not support read-access geo-redundant storage (RA-GRS) and read-access geo-zone-redundant storage (RA-GZRS).

25. Question

You are developing a web application that provides streaming video to users. You configure the application to use continuous integration and deployment.

The app must be highly available and provide a continuous streaming experience for users.

You need to recommend a solution that allows the application to store data in a geographical location that is closest to the user.

What should you recommend?

- A. Azure Content Delivery Network (CDN)
- B. Azure Redis Cache
- C. Azure App Service Web Apps

D. Azure App Service Isolated

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.

Incorrect Answers:

B. 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.

C. Azure App Service Web Apps

This option provides compute to host your web application. It does not provide caching capabilities.

D. Azure App Service Isolated

This option provides network isolation for your compute. It does not provide caching capabilities.

Reference:

https://docs.microsoft.com/en-in/azure/cdn/

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

What is a content delivery network on Azure?

05/09/2018 • 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.

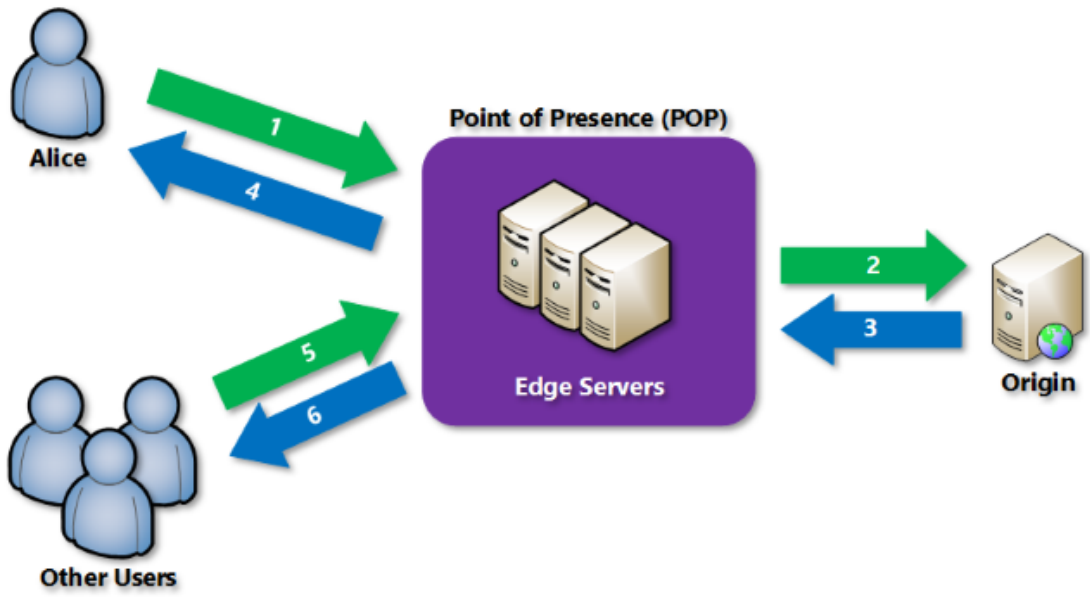
Azure Content Delivery Network (CDN) offers developers a global solution for rapidly delivering high-bandwidth content to users by caching their content at strategically placed physical nodes across the world. Azure CDN can also accelerate dynamic content, which cannot be cached, by leveraging various 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



26. 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 need to deploy resources to host a stateless web app in an Azure subscription. The solution must meet the following requirements:

? Provide access to the full .NET framework.

? Provide redundancy if an Azure region fails.

? Grant administrators access to the operating system to install custom application dependencies.

Solution: You deploy a virtual machine scale set that uses autoscaling.

Does this meet the goal?

- A. Yes
- B. No

Correct

Virtual machine scale sets are used to auto scale virtual machine instances based on traffic or load. Instead, you deploy two Azure virtual machines to two Azure regions, and create a Traffic Manager profile.

Reference:

https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/overview

27. 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 need to deploy resources to host a stateless web app in an Azure subscription. The solution must meet the following requirements:

? Provide access to the full .NET framework.

? Provide redundancy if an Azure region fails.

? Grant administrators access to the operating system to install custom application dependencies.

Solution: You deploy two Azure virtual machines to two Azure regions, and you deploy an Azure Application Gateway.

Does this meet the goal?

- A. Yes
- B. No

Incorrect

Azure application gateway is a regional service. It cannot load balance the virtual machines across regions.

Instead, you deploy two Azure virtual machines to two Azure regions, and create a Traffic Manager profile

Note: Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.

Reference:

https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview

28. 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 need to deploy resources to host a stateless web app in an Azure subscription. The solution must meet the following requirements:

? Provide access to the full .NET framework.

? Provide redundancy if an Azure region fails.

? Grant administrators access to the operating system to install custom application dependencies.

Solution: You deploy a web app in an Isolated App Service plan.

Does this meet the goal?

- A. Yes
- B. No

Correct

Instead, you deploy two Azure virtual machines to two Azure regions, and create a Traffic Manager profile

Reference:

https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview

29. 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 need to deploy resources to host a stateless web app in an Azure subscription. The solution must

meet the following requirements:

? Provide access to the full .NET framework.

? Provide redundancy if an Azure region fails.

? Grant administrators access to the operating system to install custom application dependencies.

Solution: You deploy two Azure virtual machines to two Azure regions, and create a Traffic Manager profile.

Does this meet the goal?

- A. Yes
- B. No

Correct

Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.

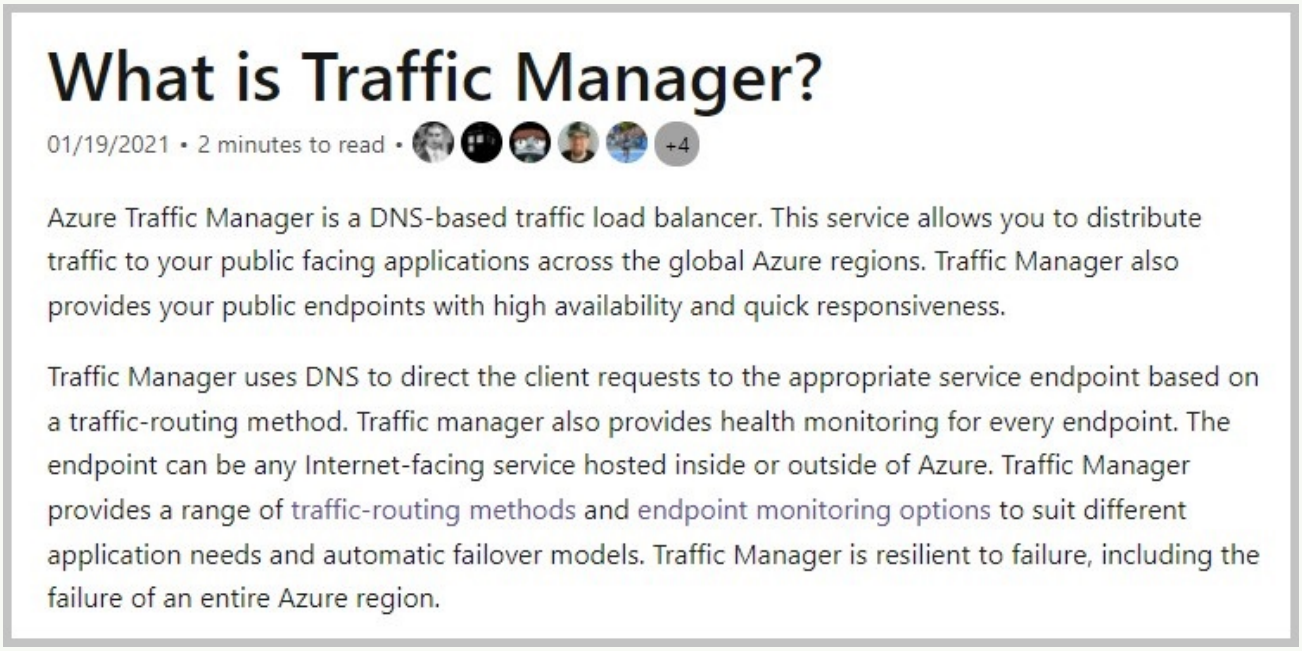
Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints. An endpoint is any Internet-facing service hosted inside or outside of Azure.

Reference:

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

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods

https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview



What is Traffic Manager?

01/19/2021 • 2 minutes to read • +4

Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness.

Traffic Manager uses DNS to direct the client requests to the appropriate service endpoint based on a traffic-routing method. Traffic manager also provides health monitoring for every endpoint. The endpoint can be any Internet-facing service hosted inside or outside of Azure. Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

30. Question

You are developing a sales application that will contain several Azure cloud services and will handle different components of a transaction. Different cloud services will process customer orders, billing, payment, inventory, and shipping.

You need to recommend a solution to enable the cloud services to asynchronously communicate transaction information by using REST messages.

What should you include in the recommendation?

- A. Azure Service Fabric
- B. Azure Blob storage
- **C. Azure Queue storage**
- D. Azure Traffic Manager

Correct

Azure Queue Storage is a service for storing large numbers of messages. You access messages from anywhere in the world via authenticated calls using HTTP or HTTPS. A queue message can be up to 64 KB in size. A queue may contain millions of messages, up to the total capacity limit of a storage account. Queues are commonly used to create a backlog of work to process asynchronously.

Incorrect Answers:

A. Azure Service Fabric

Azure Service Fabric is a distributed systems platform that makes it easy to package, deploy, and manage scalable and reliable microservices and containers.

B. Azure Blob storage

Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data.

D. Azure Traffic Manager

It is a load balancing solution.

Reference:

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

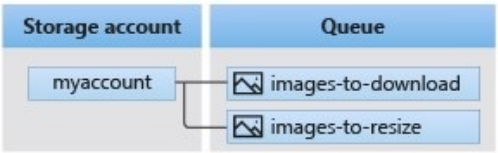
What is Azure Queue Storage?

03/18/2020 • 2 minutes to read • +8

Azure Queue Storage is a service for storing large numbers of messages. You access messages from anywhere in the world via authenticated calls using HTTP or HTTPS. A queue message can be up to 64 KB in size. A queue may contain millions of messages, up to the total capacity limit of a storage account. Queues are commonly used to create a backlog of work to process asynchronously.

Queue Storage concepts

Queue Storage contains the following components:



31. Question

You architect a solution that calculates 3D geometry from height-map data.

You have the following requirements:

Perform calculations in Azure.

? Each node must communicate data to every other node.

? Maximize the number of nodes to calculate multiple scenes as fast as possible.

? Require the least amount of effort to implement.

You need to recommend a solution.

Which two actions should you recommend?

- [x] A. Create a render farm that uses Azure Batch
- [ ] B. Create a render farm that uses virtual machines (VMs)
- [x] C. Enable parallel task execution on compute nodes
- [ ] D. Create a render farm that uses virtual machine (VM) scale sets
- [ ] E. Enable parallel file systems on Azure

Correct

Rendering is the process of taking 3D models and converting them into 2D images. 3D scene files are authored in applications such as Autodesk 3ds Max, Autodesk Maya, and Blender.

The process of rendering is computationally intensive; there can be many frames/images to produce and each image can take many hours to render. Rendering is therefore a perfect batch processing workload that can leverage Azure and Azure Batch to run many renders in parallel.

Incorrect Answers:

B. Create a render farm that uses virtual machines (VMs)

Can be possible with high GPU machines, however it requires lot of effort to implement as compared with Azure Batch.

D. Create a render farm that uses virtual machine (VM) scale sets

VMSS is used to scale-out instance based on metrics. Scaling out VM's does not provide faster rendering of 3D models.

E. Enable parallel file systems on Azure

Not a valid option. There is no option like parallel file system.

Reference:

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

https://docs.microsoft.com/en-us/azure/batch/batch-parallel-node-tasks#enable-parallel-task-execution

https://docs.microsoft.com/en-us/azure/batch/batch-rendering-applications

https://docs.microsoft.com/en-us/azure/batch/batch-mpi

https://docs.microsoft.com/en-us/azure/batch/batch-rendering-service

Run parallel workloads

Batch works well with intrinsically parallel (also known as "embarrassingly parallel") workloads. These workloads have applications which can run independently, with each instance completing part of the work. When the applications are executing, they might access some common data, but they don't communicate with other instances of the application. Intrinsically parallel workloads can therefore run at a large scale, determined by the amount of compute resources available to run applications simultaneously.

Some examples of intrinsically parallel workloads you can bring to Batch:

- Financial risk modeling using Monte Carlo simulations
- VFX and 3D image rendering
- Image analysis and processing
- Media transcoding
- Genetic sequence analysis
- Optical character recognition (OCR)
- Data ingestion, processing, and ETL operations
- Software test execution

You can also use Batch to run tightly coupled workloads, where the applications you run need to communicate with each other, rather than running independently. Tightly coupled applications normally use the Message Passing Interface (MPI) API. You can run your tightly coupled workloads with Batch using Microsoft MPI or Intel MPI. Improve application performance with specialized HPC and GPU-optimized VM sizes.

Some examples of tightly coupled workloads:

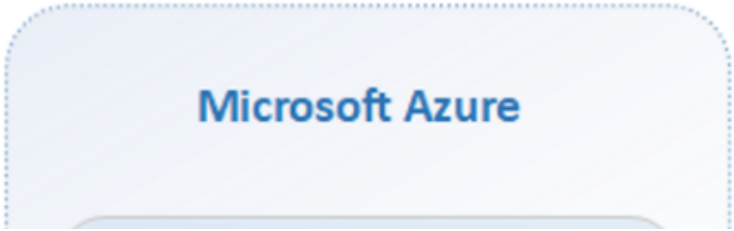
- Finite element analysis
- Fluid dynamics
- Multi-node AI training

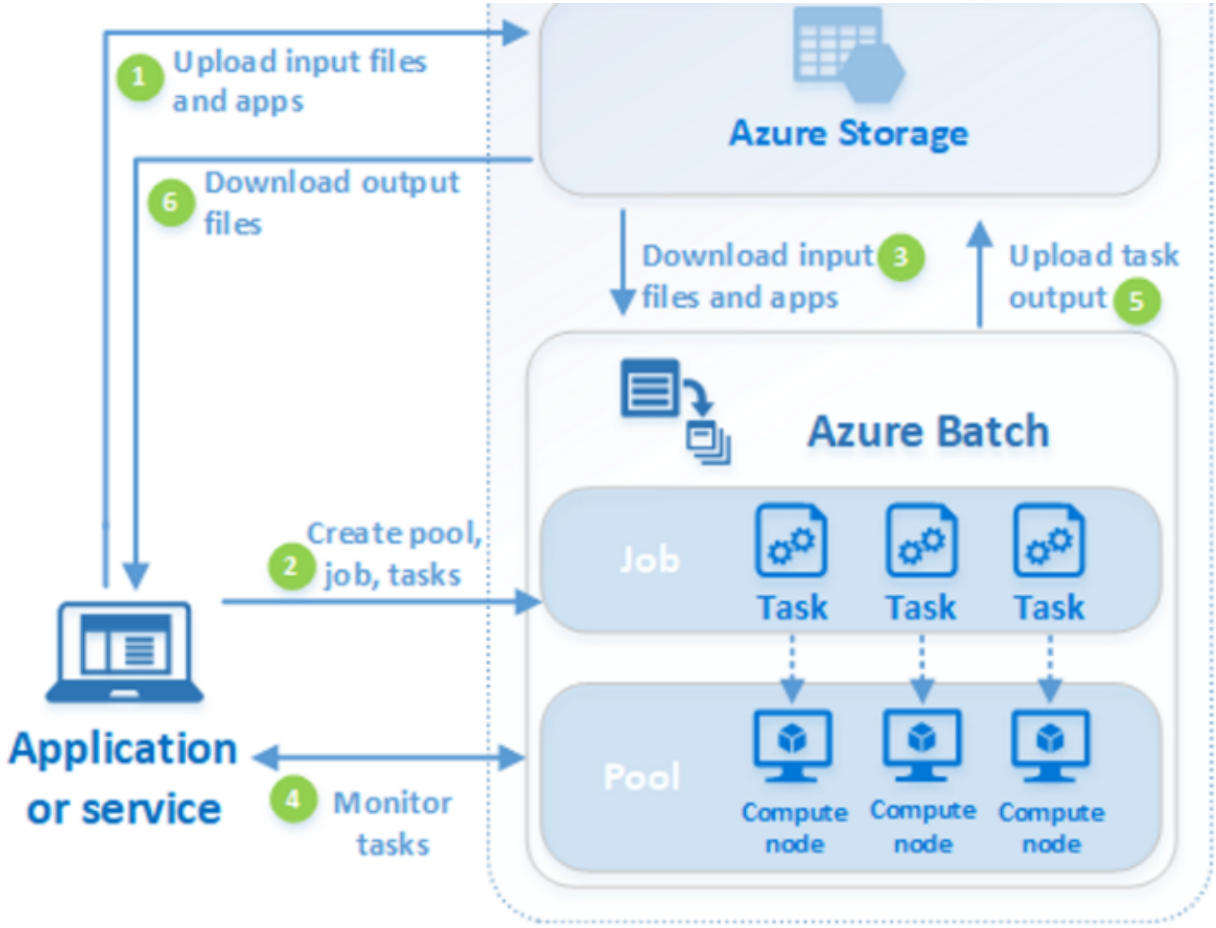
Many tightly coupled jobs can be run in parallel using Batch. For example, you can perform multiple simulations of a liquid flowing through a pipe with varying pipe widths.

How it works

A common scenario for Batch involves scaling out intrinsically parallel work, such as the rendering of images for 3D scenes, on a pool of compute nodes. This pool can be your "render farm" that provides tens, hundreds, or even thousands of cores to your rendering job.

The following diagram shows steps in a common Batch workflow, with a client application or hosted service using Batch to run a parallel workload.





Step	Description
1. Upload **input files** and the **applications** to process those files to your Azure Storage account.	The input files can be any data that your application processes, such as financial modeling data, or video files to be transcoded. The application files can include scripts or applications that process the data, such as a media transcoder.
2. Create a Batch **pool** of compute nodes in your Batch account, a **job** to run the workload on the pool, and **tasks** in the job.	Compute nodes are the VMs that execute your tasks. Specify properties for your pool, such as the number and size of the nodes, a Windows or Linux VM image, and an application to install when the nodes join the pool. Manage the cost and size of the pool by using low-priority VMs or by automatically scaling the number of nodes as the workload changes. When you add tasks to a job, the Batch service automatically schedules the tasks for execution on the compute nodes in the pool. Each task uses the application that you uploaded to process the input files.
3. Download **input files** and the **applications** to Batch	Before each task executes, it can download the input data that it will process to the assigned node. If the application isn't already installed on the pool nodes, it can be downloaded here instead. When the downloads from Azure Storage complete, the task executes on the assigned node.
4. Monitor **task execution**	As the tasks run, query Batch to monitor the progress of the job and its tasks. Your client application or service communicates with the Batch service over HTTPS. Because you may be monitoring thousands of tasks running on thousands of compute nodes, be sure to query the Batch service efficiently.
5. Upload **task output**	As the tasks complete, they can upload their result data to Azure Storage. You can also retrieve files directly from the file system on a compute node.

6. Download **output files**	When your monitoring detects that the tasks in your job have completed, your client application or service can download the output data for further processing.

Pre-installed applications on Batch rendering VM images

03/12/2021 • 3 minutes to read •

It's possible to use any rendering applications with Azure Batch. However, Azure Marketplace VM images are available with common applications pre-installed.

Where applicable, pay-for-use licensing is available for the pre-installed rendering applications. When a Batch pool is created, the required applications can be specified and both the cost of VM and applications will be billed per minute. Application prices are listed on the Azure Batch pricing page.

Some applications only support Windows, but most are supported on both Windows and Linux.

Important

The rendering VM images and pay-for-use licensing have been **deprecated and will be retired on February 29, 2024**. To use Batch for rendering, **a custom VM image and standard application licensing should be used.**

32. Question

You need to recommend a solution to deploy containers that run an application. The application has two tiers. Each tier is implemented as a separate Docker Linux-based image. The solution must meet the following requirements:

? The front-end tier must be accessible by using a public IP address on port 80.

? The backend tier must be accessible by using port 8080 from the front-end tier only.

? Both containers must be able to access the same Azure file share.

? If a container fails, the application must restart automatically.

? Costs must be minimized.

What should you recommend using to host the application?

- A. Azure Kubernetes Service (AKS)
- B. Azure Service Fabric
- C. Azure Container instances

Correct

Azure Container Instances enables a layered approach to orchestration, providing all of the scheduling and management capabilities required to run a single container, while allowing orchestrator platforms to manage multi-container tasks on top of it.

Because the underlying infrastructure for container instances is managed by Azure, an orchestrator platform does not need to concern itself with finding an appropriate host machine on which to run a single container.

Azure Container Instances can schedule both Windows and Linux containers with the same API.

Orchestration of container instances exclusively

Because they start quickly and bill by the second, an environment based exclusively on Azure Container Instances offers the fastest way to get started and to deal with highly variable workloads.

Incorrect Answers:

A. Azure Kubernetes Service (AKS)

Azure Kubernetes Service (AKS) simplifies deploying a managed Kubernetes cluster in Azure by offloading the operational overhead to Azure.

B. Azure Service Fabric

Azure Service Fabric is a distributed systems platform that makes it easy to package, deploy, and manage scalable and reliable microservices and containers.

Reference:

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

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-orchestrator-relationship

What is Azure Container Instances?

03/22/2021 • 3 minutes to read • +8

Containers are becoming the preferred way to package, deploy, and manage cloud applications. Azure Container Instances offers the fastest and simplest way to run a container in Azure, without having to manage any virtual machines and without having to adopt a higher-level service.

Azure Container Instances is a great solution for any scenario that can operate in isolated containers, including simple applications, task automation, and build jobs. For scenarios where you need full container orchestration, including service discovery across multiple containers, automatic scaling, and coordinated application upgrades, we recommend Azure Kubernetes Service (AKS).

33. Question

You plan to deploy a network-intensive application to several Azure virtual machines.

You need to recommend a solution that meets the following requirements:

? Minimizes the use of the virtual machine processors to transfer data

? Minimizes network latency

Which virtual machine size should you use?

A. Compute optimized Standard_F8s

B. General purpose Standard_B8ms

C. High performance compute Standard_H16r

D. Memory optimized Standard_E16s_v3

Correct

Most of the HPC VM sizes feature a network interface for remote direct memory access (RDMA) connectivity. Selected N-series sizes designated with ‘r‘ are also RDMA-capable. This interface is in addition to the standard Azure Ethernet network interface available in the other VM sizes.

This secondary interface allows the RDMA-capable instances to communicate over an InfiniBand (IB) network, operating at HDR rates for HBv3, HBv2, EDR rates for HB, HC, NDv2, and FDR rates for H16r, H16mr, and other RDMA-capable N-series virtual machines. These RDMA capabilities can boost the scalability and performance of Message Passing Interface (MPI) based applications.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-hpc#h-series

https://docs.microsoft.com/en-us/azure/virtual-machines/h-series?toc=/azure/virtual-machines/linux/toc.json&bc=/azure/virtual-machines/linux/breadcrumb/toc.json

RDMA-capable instances

Most of the HPC VM sizes feature a network interface for remote direct memory access (RDMA) connectivity. Selected N-series sizes designated with 'r' are also RDMA-capable. This interface is in addition to the standard Azure Ethernet network interface available in the other VM sizes.

This secondary interface allows the RDMA-capable instances to communicate over an InfiniBand (IB) network, operating at HDR rates for HBv3, HBv2, EDR rates for HB, HC, NDv2, and FDR rates for H16r, H16mr, and other RDMA-capable N-series virtual machines. These RDMA capabilities can boost the scalability and performance of Message Passing Interface (MPI) based applications.

Note

SR-IOV support: In Azure HPC, currently there are two classes of VMs depending on whether they are SR-IOV enabled for InfiniBand. Currently, almost all the newer generation, RDMA-capable or InfiniBand enabled VMs on Azure are SR-IOV enabled except for H16r, H16mr, and NC24r. RDMA is only enabled over the InfiniBand (IB) network and is supported for all RDMA-capable VMs. IP over IB is only supported on the SR-IOV enabled VMs. RDMA is not enabled over the Ethernet network.

34. Question

You plan to deploy a network-intensive application to several Azure virtual machines.

You need to recommend a solution that meets the following requirements:

? Minimizes the use of the virtual machine processors to transfer data

? Minimizes network latency

Which virtual machine feature should you use?

- A. Receive side scaling (RSS)
- B. Remote Direct Memory Access (RDMA)
- C. Single root 1/0 virtualization (SR-IOV)
- D. Virtual Machine Multi-Queue (VMMQ)

Incorrect

Most of the HPC VM sizes feature a network interface for remote direct memory access (RDMA) connectivity. Selected N-series sizes designated with 'r' are also RDMA-capable. This interface is in addition to the standard Azure Ethernet network interface available in the other VM sizes.

This secondary interface allows the RDMA-capable instances to communicate over an InfiniBand (IB) network, operating at HDR rates for HBv3, HBv2, EDR rates for HB, HC, NDv2, and FDR rates for H16r, H16mr, and other RDMA-capable N-series virtual machines. These RDMA capabilities can boost the scalability and performance of Message Passing Interface (MPI) based applications.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-hpc#h-series

https://docs.microsoft.com/en-us/azure/virtual-machines/h-series?toc=/azure/virtual-machines/linux/toc.json&bc=/azure/virtual-machines/linux/breadcrumb/toc.json

RDMA-capable instances

Most of the HPC VM sizes feature a network interface for remote direct memory access (RDMA) connectivity. Selected N-series sizes designated with 'r' are also RDMA-capable. This interface is in addition to the standard Azure Ethernet network interface available in the other VM sizes.

This secondary interface allows the RDMA-capable instances to communicate over an InfiniBand (IB) network, operating at HDR rates for HBv3, HBv2, EDR rates for HB, HC, NDv2, and FDR rates for H16r, H16mr, and other RDMA-capable N-series virtual machines. These RDMA capabilities can boost the scalability and performance of Message Passing Interface (MPI) based applications.

ⓘ Note

SR-IOV support: In Azure HPC, currently there are two classes of VMs depending on whether they are SR-IOV enabled for InfiniBand. Currently, almost all the newer generation, RDMA-capable or InfiniBand enabled VMs on Azure are SR-IOV enabled except for H16r, H16mr, and NC24r. RDMA is only enabled over the InfiniBand (IB) network and is supported for all RDMA-capable VMs. IP over IB is only supported on the SR-IOV enabled VMs. RDMA is not enabled over the Ethernet network.

35. Question

Your company purchases an app named App1.

You need to recommend a solution to ensure that App1 can read and modify access reviews.

What should you recommend?

A. From API Management services, publish the API of App1, and then delegate permissions to the Microsoft Graph API

B. From the Azure Active Directory admin center, register App1. From the Access control (IAM) blade, delegate permissions

C. From the Azure Active Directory admin center, register App1, and then delegate permissions to the Microsoft Graph API

D. From API Management services, publish the API of App1. From the Access control (IAM) blade, delegate permissions

Incorrect

The app must be registered. You can register the application in the Azure Active Directory admin center. The Azure AD access reviews feature has an API in the Microsoft Graph endpoint. You can register an Azure AD application and set it up for permissions to call the access reviews API in Microsoft Graph endpoint.

Incorrect Answers:

A. From API Management services, publish the API of App1, and then delegate permissions to the Microsoft Graph API

API management is not referred in the question. The delegation must be provided to application not API.

B. From the Azure Active Directory admin center, register App1. From the Access control (IAM) blade, delegate permissions

To read of modify Azure AD related services, you need access to Graph API.

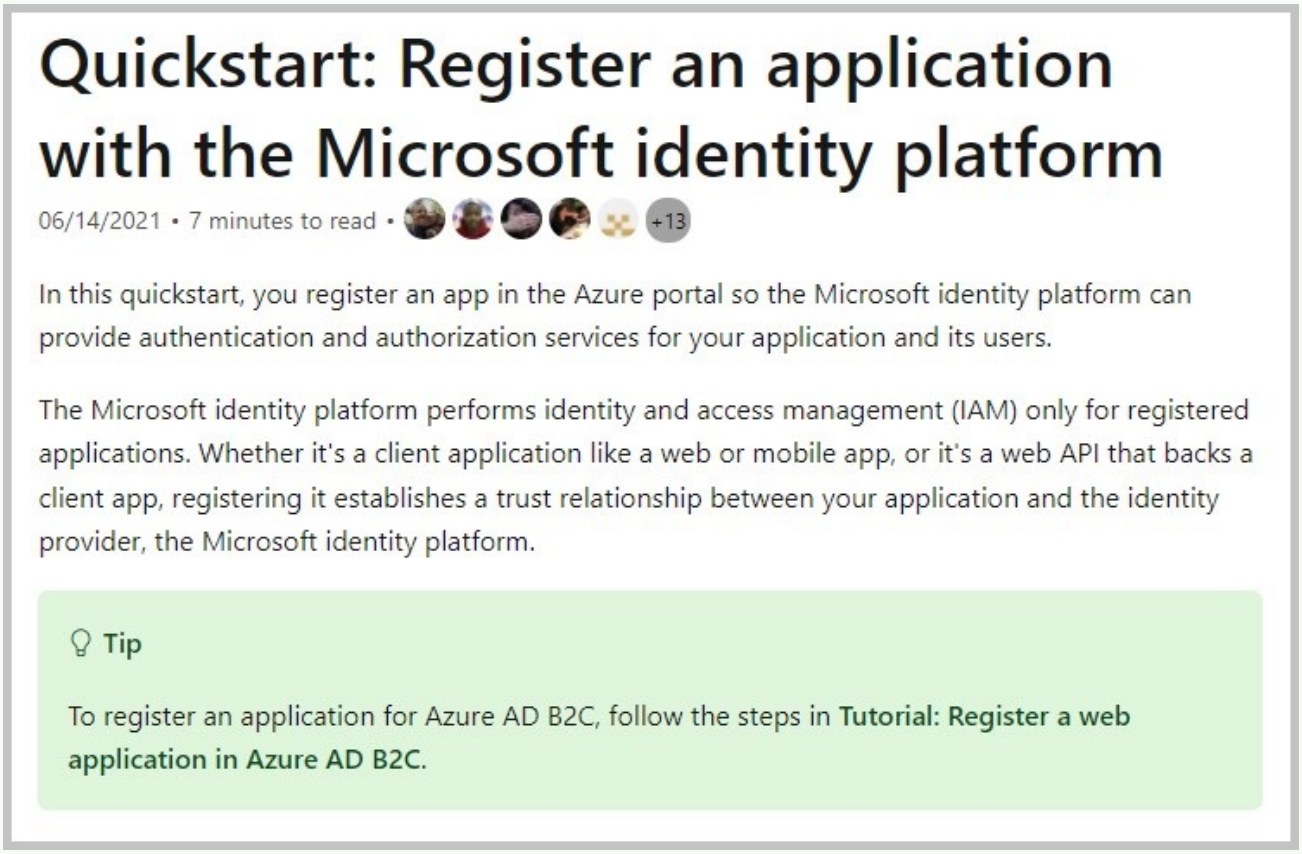
D. From API Management services, publish the API of App1. From the Access control (IAM) blade, delegate permissions

API management is not referred in the question. The delegation must be provided to application not API.

Reference:

https://docs.microsoft.com/en-us/graph/use-the-api

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app



Quickstart: Register an application with the Microsoft identity platform

06/14/2021 • 7 minutes to read • +13

In this quickstart, you register an app in the Azure portal so the Microsoft identity platform can provide authentication and authorization services for your application and its users.

The Microsoft identity platform performs identity and access management (IAM) only for registered applications. Whether it's a client application like a web or mobile app, or it's a web API that backs a client app, registering it establishes a trust relationship between your application and the identity provider, the Microsoft identity platform.

Tip

To register an application for Azure AD B2C, follow the steps in **Tutorial: Register a web application in Azure AD B2C.**

Use the Microsoft Graph API

09/03/2021 • 5 minutes to read • +8

Microsoft Graph is a RESTful web API that enables you to access Microsoft Cloud service resources. After you register your app and get authentication tokens for a user or service, you can make requests to the Microsoft Graph API.

> **Important:** How conditional access policies apply to Microsoft Graph is changing. Applications need to be updated to handle scenarios where conditional access policies are configured. For more information and guidance, see Developer Guidance for Azure Active Directory Conditional Access.

36. Question

You have an Azure Active Directory (Azure AD) tenant.

You plan to provide users with access to shared files by using Azure Storage. The users will be provided with different levels of access to various Azure file shares based on their user account or their group membership.

You need to recommend which additional Azure services must be used to support the planned deployment.

What should you include in the recommendation?

- A. an Azure AD enterprise application
- B. Azure Information Protection
- C. an Azure AD Domain Services (Azure AD DS) instance
- D. an Azure Front Door instance

Incorrect

Azure Files supports identity-based authentication over Server Message Block (SMB) through two types of Domain Services: on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).

Incorrect Answers:

A. an Azure AD enterprise application

This option is used to register an application with Azure AD tenant.

B. Azure Information Protection

Azure Information Protection (AIP) is a cloud-based solution that enables organizations to discover, classify, and protect documents and emails by applying labels to content.

D. an Azure Front Door instance

Azure Front door is a load balancing solution.

Reference:

https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable?tabs=azure-portal

Enable Azure Active Directory Domain Services authentication on Azure Files

07/22/2021 • 13 minutes to read • +6

Azure Files supports identity-based authentication over Server Message Block (SMB) through two types of Domain Services: on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).We strongly recommend you to review the How it works section to select the right domain service for authentication. The setup is different depending on the domain service you choose. This article focuses on enabling and configuring Azure AD DS for authentication with Azure file shares.

If you are new to Azure file shares, we recommend reading our planning guide before reading the following series of articles.

Note

Azure Files supports Kerberos authentication with Azure AD DS with RC4-HMAC and AES-256 encryption.

Azure Files supports authentication for Azure AD DS with full synchronization with Azure AD. If you have enabled scoped synchronization in Azure AD DS which only sync a limited set of identities from Azure AD, authentication and authorization is not supported.

37. Question

Your company has 300 virtual machines hosted in a VMware environment. The virtual machines vary in size and have various utilization levels.

You plan to move all the virtual machines to Azure.

You need to recommend how many and what size Azure virtual machines will be required to move the current workloads to Azure. The solution must minimize administrative effort.

What should you use to make the recommendation?

- A. Azure Pricing calculator
- B. Azure Cost Management
- C. Azure Advisor
- D. Azure Migrate

Correct

Azure Migrate provides a centralized hub to assess and migrate to Azure on-premises servers, infrastructure, applications, and data.

Metadata discovered by the Azure Migrate appliance helps you to figure out whether servers are ready for migration to Azure, right-size servers, plans costs, and analyze application dependencies.

Incorrect Answers:

A. Azure Pricing calculator

Let's you Configure and estimate the costs for Azure products

B. Azure Cost Management

Azure Cost Management helps you understand your Azure invoice (bill), manage your billing account and subscriptions, monitor and control Azure spending and optimize resource use.

C. Azure Advisor

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

Reference:

https://docs.microsoft.com/en-us/azure/migrate/migrate-appliance#collected-data—vmware

https://docs.microsoft.com/en-us/azure/migrate/migrate-services-overview#azure-migrate-server-assessment-tool

https://docs.microsoft.com/en-us/azure/migrate/tutorial-discover-vmware

About Azure Migrate

04/15/2020 • 6 minutes to read • +3

This article provides a quick overview of the Azure Migrate service.

Azure Migrate provides a centralized hub to assess and migrate to Azure on-premises servers, infrastructure, applications, and data. It provides the following:

- **Unified migration platform**: A single portal to start, run, and track your migration to Azure.
- **Range of tools**: A range of tools for assessment and migration. Azure Migrate tools include Azure Migrate: Discovery and assessment and Azure Migrate: Server Migration. Azure Migrate also integrates with other Azure services and tools, and with independent software vendor (ISV) offerings.
- **Assessment and migration**: In the Azure Migrate hub, you can assess and migrate:
  - **Servers, databases, and web apps**: Assess on-premises servers including web apps and SQL Server instances and migrate them to Azure virtual machines or Azure VMware Solution (AVS) (Preview).
  - **Databases**: Assess on-premises databases and migrate them to Azure SQL Database or to SQL Managed Instance.
  - **Web applications**: Assess on-premises web applications and migrate them to Azure App Service.
  - **Virtual desktops**: Assess your on-premises virtual desktop infrastructure (VDI) and migrate it to Windows Virtual Desktop in Azure.
  - **Data**: Migrate large amounts of data to Azure quickly and cost-effectively using Azure Data Box products.

Metadata

Metadata discovered by the Azure Migrate appliance helps you to figure out whether servers are ready for migration to Azure, right-size servers, plans costs, and analyze application dependencies. Microsoft doesn't use this data in any license compliance audit.

38. Question

You have an Azure subscription. The subscription contains an app that is hosted in the East US, Central Europe, and East Asia regions.

You need to recommend a data-tier solution for the app. The solution must meet the following requirements:

? Support multiple consistency levels.

? Be able to store at least 1 TB of data.

? Be able to perform read and write operations in the Azure region that is local to the app instance.

What should you include in the recommendation?

A. an Azure Cosmos DB database

B. a Microsoft SQL Server Always On availability group on Azure virtual machines

C. an Azure SQL database in an elastic pool

D. Azure Table storage that uses geo-redundant storage (GRS) replication

Incorrect

Azure Cosmos DB approaches data consistency as a spectrum of choices. This approach includes more options than the two extremes of strong and eventual consistency. You can choose from five well-defined levels on the consistency spectrum.

With Cosmos DB any write into any region must be replicated and committed to all configured regions within the account.

Incorrect Answers:

B. a Microsoft SQL Server Always On availability group on Azure virtual machines

This option is used for BCDR scenarios.

C. an Azure SQL database in an elastic pool

Azure SQL Database elastic pools are a simple, cost-effective solution for managing and scaling multiple databases that have varying and unpredictable usage demands.

D. Azure Table storage that uses geo-redundant storage (GRS) replication

There are no consistency levels in Azure Table storage and GRS does not provide multi-region write capability.

Reference:

https://docs.microsoft.com/en-us/azure/cosmos-db/consistency-levels

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

Consistency levels in Azure Cosmos DB

09/20/2021 • 13 minutes to read • +11

APPLIES TO: SQL API Cassandra API Gremlin API Table API Azure Cosmos DB API for MongoDB

Distributed databases that rely on replication for high availability, low latency, or both, must make a fundamental tradeoff between the read consistency, availability, latency, and throughput as defined by the PACLC theorem. The linearizability of the strong consistency model is the gold standard of data programmability. But it adds a steep price from higher write latencies due to data having to replicate and commit across large distances. Strong consistency may also suffer from reduced availability (during failures) because data cannot replicate and commit in every region. Eventual consistency offers higher availability and better performance, but its more difficult to program applications because data may not be completely consistent across all regions.

Configure multi-region writes in your applications that use Azure Cosmos DB

01/06/2021 • 3 minutes to read •

APPLIES TO: SQL API

Once an account has been created with multiple write regions enabled, you must make two changes in your application to the ConnectionPolicy for the Cosmos client to enable the multi-region writes in Azure Cosmos DB. Within the ConnectionPolicy, set UseMultipleWriteLocations to true and pass the name of the region where the application is deployed to ApplicationRegion. This will populate the PreferredLocations property based on the geo-proximity from location passed in. If a new region is later added to the account, the application does not have to be updated or redeployed, it will automatically detect the closer region and will auto-home on to it should a regional event occur.

Note

Cosmos accounts initially configured with single write region can be configured to multiple write regions with zero down time. To learn more see, **Configure multiple-write regions**

39. 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 a storage solution to support on-premises resources and Azure-hosted resources.

You need to provide on-premises storage that has built-in replication to Azure.

Solution: You include Azure Blob storage in the design.

Does the solution meet the goal?

- A. Yes
- B. No

Correct

Azure StorSimple replicates to Azure Blob storage.

The solution INCLUDES blob storage as part of the solution. So they mean you have StorSimple and Blob Storage as solution.

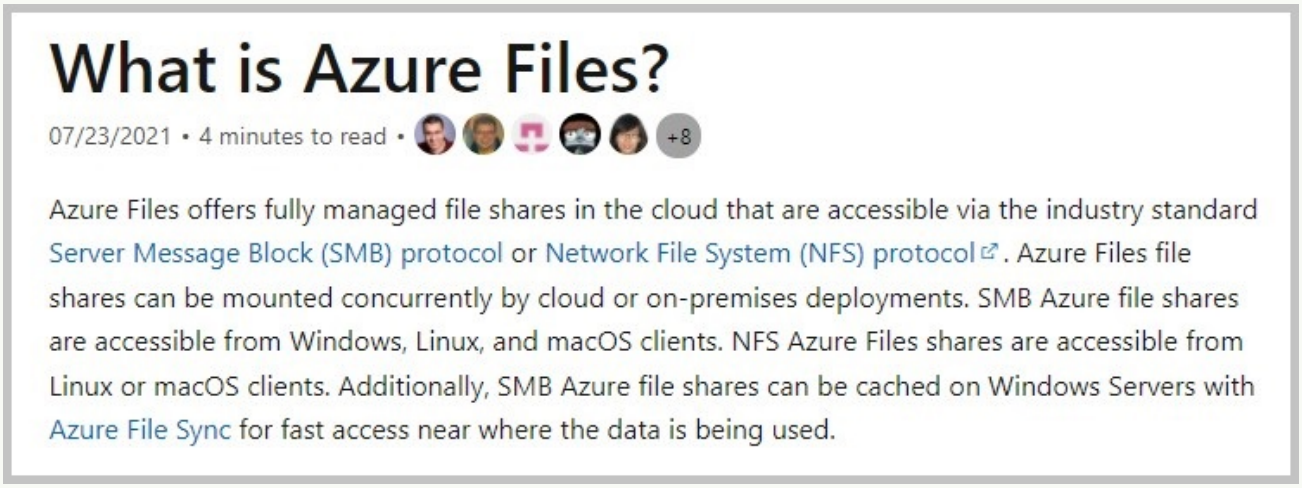
You can also use Azure Files in Azure Storage account.

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.

Use Azure File Sync to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of your Azure file share. You can use any protocol that's available on Windows Server to access your data locally, including SMB, NFS, and FTPS. You can have as many caches as you need across the world.

Reference:

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



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 a storage solution to support on-premises resources and Azure-hosted resources.

You need to provide on-premises storage that has built-in replication to Azure.

Solution: You include Azure Data Lake Storage in the design.

Does the solution meet the goal?

- A. Yes
- B. No

Correct

Instead use Azure Files in Azure Storage account.

Reference:

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

Create and configure a self-hosted integration runtime

09/09/2021 • 23 minutes to read • +30

APPLIES TO: Azure Data Factory Azure Synapse Analytics

The integration runtime (IR) is the compute infrastructure that Azure Data Factory and Synapse pipelines use to provide data-integration capabilities across different network environments. For details about IR, see Integration runtime overview.

A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network. It also can dispatch transform activities against compute resources in an on-premises network or an Azure virtual network. The installation of a self-hosted integration runtime needs an on-premises machine or a virtual machine inside a private network.

This article describes how you can create and configure a self-hosted IR.

Note

This article has been updated to use the Azure Az PowerShell module. The Az PowerShell module is the recommended PowerShell module for interacting with Azure. To get started with the Az PowerShell module, see **Install Azure PowerShell**. To learn how to migrate to the Az PowerShell module, see **Migrate Azure PowerShell from AzureRM to Az**.

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 a storage solution to support on-premises resources and Azure-hosted resources.

You need to provide on-premises storage that has built-in replication to Azure.

Solution: You include Azure Data Table Storage in the design.

Does the solution meet the goal?

- A. Yes
- B. No

Correct

Instead use Azure Files in Azure Storage account.

Reference:

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

42. Question

You have an Azure virtual machine named VM1 that runs Windows Server 2019 and contains 500 GB of data files.

You are designing a solution that will use Azure Data Factory to transform the data files, and then load the files to Azure Data Lake Storage.

What should you deploy on VM1 to support the design?

- A. the Azure Pipelines agent
- B. the Azure File Sync agent
- C. the On-premises data gateway
- **D. the self-hosted integration runtime**

Incorrect

The integration runtime (IR) is the compute infrastructure that Azure Data Factory uses to provide data-integration capabilities across different network environments. For details about IR, see Integration runtime overview.

A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network. It also can dispatch transform activities against compute resources in an on-premises network or an Azure virtual network. The installation of a self-hosted integration runtime needs an on-premises machine or a virtual machine inside a private network.

Note: If your data store is located inside an on-premises network, an Azure virtual network, or Amazon Virtual Private Cloud, you need to configure a self-hosted integration runtime to connect to it.

Incorrect Answers:

A. the Azure Pipelines agent

Azure Pipelines agent is used to build your code or deploy your software using Azure Pipelines.

B. the Azure File Sync agent

The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share.

C. the 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.

Reference:

https://docs.microsoft.com/en-us/azure/data-factory/create-self-hosted-integration-runtime

https://docs.microsoft.com/en-us/azure/data-factory/connector-file-system

43. Question

You plan to store data in Azure Blob storage for many years. The stored data will be accessed rarely.

You need to ensure that the data in Blob storage is always available for immediate access. The solution must minimize storage costs.

Which storage tier should you use?

- A. Cool
- B. Archive
- C. Hot

Correct

Data in the cool access tier can tolerate slightly lower availability, but still requires high durability, retrieval latency, and throughput characteristics similar to hot data. For cool data, a slightly lower availability service-level agreement (SLA) and higher access costs compared to hot data are acceptable trade-offs for lower storage costs.

Incorrect Answers:

B. Archive

Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements, on the order of hours.

C. Hot

Optimized for storing data that is accessed frequently.

Reference:

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

Access tiers for Azure Blob Storage - hot, cool, and archive

03/18/2021 • 13 minutes to read • +17

Azure storage offers different access tiers, allowing you to store blob object data in the most cost-effective manner. Available access tiers include:

- **Hot** - Optimized for storing data that is accessed frequently.
- **Cool** - Optimized for storing data that is infrequently accessed and stored for at least 30 days.
- **Archive** - Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements, on the order of hours.

The following considerations apply to the different access tiers:

- The access tier can be set on a blob during or after upload.
- Only the hot and cool access tiers can be set at the account level. The archive access tier can only be set at the blob level.
- Data in the cool access tier has slightly lower availability, but still has high durability, retrieval latency, and throughput characteristics similar to hot data. For cool data, slightly lower availability and higher access costs are acceptable trade-offs for lower overall storage costs compared to hot data. For more information, see SLA for storage.
- Data in the archive access tier is stored offline. The archive tier offers the lowest storage costs but also the highest access costs and latency.
- The hot and cool tiers support all redundancy options. The archive tier supports only LRS, GRS, and RA-GRS.
- Data storage limits are set at the account level and not per access tier. You can choose to use all of your limit in one tier or across all three tiers.

44. Question

You have an Azure Active Directory (Azure AD) tenant named techzen-az304.com that contains several administrative user accounts.

You need to recommend a solution to identify which administrative user accounts have NOT signed in during the previous 30 days.

Which service should you include in the recommendation?

- A. Azure AD Privileged Identity Management (PIM)
- B. Azure AD Identity Protection
- C. Azure Advisor
- D. Azure Activity Log

Correct

You can use the Privileged Identity Management (PIM) audit history to see all role assignments and activations within the past 30 days for all privileged roles. If you want to see the full audit history of activity in your Azure Active Directory (Azure AD) organization, including administrator, end user, and synchronization activity, you can use the Azure Active Directory security and activity reports.

Incorrect Answers:

B. Azure AD Identity Protection

Identity Protection is a tool that allows organizations to accomplish automatic detection and remediation of identity based risks.

D. Azure Activity Log

The Activity log is a platform log in Azure that provides insight into subscription-level events. This includes such information as when a resource is modified or when a virtual machine is started.

C. Azure Advisor

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

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new

Configure security alerts for Azure AD roles in Privileged Identity Management

06/30/2021 • 5 minutes to read •

Privileged Identity Management (PIM) generates alerts when there is suspicious or unsafe activity in your Azure Active Directory (Azure AD) organization. When an alert is triggered, it shows up on the Privileged Identity Management dashboard. Select the alert to see a report that lists the users or roles that triggered the alert.

45. Question

You deploy an Azure virtual machine that runs an ASP.NET application. The application will be accessed from the internet by the users at your company.

You need to recommend a solution to ensure that the users are pre-authenticated by using their Azure Active Directory (Azure AD) account before they can connect to the ASP.NET application.

What should you include in the recommendation?

- A. a public Azure Load Balancer
- B. Azure Application Gateway
- C. Azure Traffic Manager
- **D. an Azure AD enterprise application**

Correct

You can manage service principals in the Azure portal through the Enterprise Applications experience. Service principals are what govern an application connecting to Azure AD and can be considered the instance of the application in your directory.

Incorrect Answers:

A. a public 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. It is a load balancing solution.

B. Azure Application Gateway

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. It is a load balancing solution.

C. Azure Traffic Manager

Azure Traffic Manager is a DNS-based traffic load balancer. It is a load balancing solution.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

What are service principals and where do they come from?

You can manage service principals in the Azure portal through the Enterprise Applications experience. Service principals are what govern an application connecting to Azure AD and can be considered the instance of the application in your directory. For any given application, it can have at most one application object (which is registered in a "home" directory) and one or more service principal objects representing instances of the application in every directory in which it acts.

The service principal can include:

- A reference back to an application object through the application ID property
- Records of local user and group application-role assignments
- Records of local user and admin permissions granted to the application
  - For example: permission for the application to access a particular user's email
- Records of local policies including Conditional Access policy
- Records of alternate local settings for an application
  - Claims transformation rules
  - Attribute mappings (User provisioning)
  - Directory-specific app roles (if the application supports custom roles)
  - Directory-specific name or logo

Like application objects, service principals can also be created through multiple pathways including:

- When users sign in to a third-party application integrated with Azure AD
  - During sign-in, users are asked to give permission to the application to access their profile and other permissions. The first person to give consent causes a service principal that represents the application to be added to the directory.
- When users sign in to Microsoft online services like Microsoft 365
  - When you subscribe to Microsoft 365 or begin a trial, one or more service principals are created in the directory representing the various services that are used to deliver all of the functionality associated with Microsoft 365.
  - Some Microsoft 365 services like SharePoint create service principals on an ongoing basis to allow secure communication between components including workflows.
- When an admin adds an application from the app gallery (this will also create an underlying app object)
- Add an application to use the Azure AD Application Proxy
- Connect an application for single sign on using SAML or password single sign-on (SSO)
- Programmatically via the Microsoft Graph API or PowerShell

46. Question

You use Azure Application Insights. You plan to use continuous export. You need to store Application Insights data for five years.

Which Azure service should you use?

A. Azure SQL Database

B. Azure Monitor Logs

C. Azure Backup

D. Azure Storage

Incorrect

You can use continuous export to archive telemetry data. You can store it in Azure storage for long term retention.

Create a Continuous Export.

1. In the Application Insights resource for your app under configure on the left, open Continuous Export and choose Add:

2. Choose the telemetry data types you want to export.

3. Create or select an Azure storage account where you want to store the data. Click Add, Export Destination, Storage account, and then either create a new store or choose an existing store.

4. Create or select a container in the storage.

Incorrect Answers:

A. Azure SQL Database

Not an option to store telemetry data.

B. Azure Monitor Logs

Not a recommended option for long term retention.

C. Azure Backup

The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data such as files, folders, disks etc.. and recover it from the Microsoft Azure cloud.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/app/export-telemetry#continuous-export-advanced-storage-configuration

https://docs.microsoft.com/en-us/azure/azure-monitor/app/export-telemetry

Continuous Export advanced storage configuration

Continuous Export **does not support** the following Azure storage features/configurations:

- Use of VNET/Azure Storage firewalls in conjunction with Azure Blob storage.
- Azure Data Lake Storage Gen2.

Create a Continuous Export

> ⓘ Note
>
> An application cannot export more than 3TB of data per day. If more than 3TB per day is exported, the export will be disabled. To export without a limit use **diagnostic settings based export**.

1. In the Application Insights resource for your app under configure on the left, open Continuous Export and choose **Add**:
2. Choose the telemetry data types you want to export.
3. Create or select an Azure storage account where you want to store the data. For more information on storage pricing options, visit the official pricing page.

   Click Add, Export Destination, Storage account, and then either create a new store or choose an existing store.

   > ⚠ Warning
   >
   > By default, the storage location will be set to the same geographical region as your Application Insights resource. If you store in a different region, you may incur transfer charges.

4. Create or select a container in the storage.

> ⓘ Note
>
> Once you've created your export, newly ingested data will begin to flow to Azure Blob storage. Continuous export will only transmit new telemetry that is created/ingested after continuous export was enabled. Any data that existed prior to enabling continuous export will not be exported, and there is no supported way to retroactively export previously created data using continuous export.

There can be a delay of about an hour before data appears in the storage.

47. Question

You have 500 Azure web apps in the same Azure region. The apps use a premium Azure key vault for authentication.

A developer reports that some authentication requests are being throttled.

You need to recommend a solution to increase the available throughput of the key vault. The solution must minimize costs.

What should you recommend?

- A. Change the pricing tier
- B. Configure geo-replication
- C. Configure load balancing for the apps
- **D. Increase the number of key vaults in the subscription**

Correct

Throttling is a process you initiate that limits the number of concurrent calls to the Azure service to prevent overuse of resources. Azure Key Vault (AKV) is designed to handle a high volume of requests. If an overwhelming number of requests occurs, throttling your client's requests helps maintain optimal performance and reliability of the AKV service.

To maximize your Key Vault through put rates, here are some recommended guidelines/best practices for maximizing your throughput:

1. Ensure you have throttling in place. Client must honor exponential back-off policies for 429's and ensure you are doing retries as per the guidance below.

2. Divide your Key Vault traffic amongst multiple vaults and different regions. Use a separate vault for each security/availability domain. If you have five apps, each in two regions, then we recommend 10 vaults each containing the secrets unique to app and region.

Incorrect Answers:

A. Change the pricing tier

Changing the pricing tier of Azure web apps increases compute capacity. This will have no impact on Azure Key Vault. The application is already using premium Azure Key Vault.

B. Configure geo-replication

By default, the contents of your key vault are replicated within the region and to a secondary region at least 150 miles away.

C. Configure load balancing for the apps

A load balancer distribute the incoming to multiple application instances. This does not decrease the traffic to Azure Key Vault.

Reference:

https://docs.microsoft.com/en-us/azure/key-vault/general/overview-throttling#how-does-key-vault-handle-its-limits

How does Key Vault handle its limits?

Service limits in Key Vault prevent misuse of resources and ensure quality of service for all of Key Vault's clients. When a service threshold is exceeded, Key Vault limits any further requests from that client for a period of time, returns HTTP status code 429 (Too many requests), and the request fails. Failed requests that return a 429 do not count towards the throttle limits tracked by Key Vault.

Key Vault was originally designed to be used to store and retrieve your secrets at deployment time. The world has evolved, and Key Vault is being used at run-time to store and retrieve secrets, and often apps and services want to use Key Vault like a database. Current limits do not support high throughput rates.

Key Vault was originally created with the limits specified in Azure Key Vault service limits. To maximize your Key Vault throughput rates, here are some recommended guidelines/best practices for maximizing your throughput:

1. Ensure you have throttling in place. Client must honor exponential back-off policies for 429's and ensure you are doing retries as per the guidance below.
2. Divide your Key Vault traffic amongst multiple vaults and different regions. Use a separate vault for each security/availability domain. If you have five apps, each in two regions, then we recommend 10 vaults each containing the secrets unique to app and region. A subscription-wide limit for all transaction types is five times the individual key vault limit. For example, HSM-other transactions per subscription are limited to 5,000 transactions in 10 seconds per subscription. Consider caching the secret within your service or app to also reduce the RPS directly to key vault and/or handle burst based traffic. You can also divide your traffic amongst different regions to minimize latency and use a different subscription/vault. Do not send more than the subscription limit to the Key Vault service in a single Azure region.

48. Question

You have 100 servers that run Windows Server 2012 R2 and host Microsoft SQL Server 2014 instances.

The instances host databases that have the following characteristics:

? The largest database is currently 3 TB. None of the databases will ever exceed 4 TB.

? Stored procedures are implemented by using CLR.

You plan to move all the data from SQL Server to Azure.

You need to recommend an Azure service to host the databases. The solution must meet the following requirements:

? Whenever possible, minimize management overhead for the migrated databases.

? Minimize the number of database changes required to facilitate the migration.

? Ensure that users can authenticate by using their Active Directory credentials.

What should you include in the recommendation?

- A. Azure SQL Database elastic pools
- B. Azure SQL Database Managed Instance

C. Azure SQL Database single databases

D. SQL Server 2016 on Azure virtual machines

Correct

Azure SQL Managed Instance is the intelligent, scalable cloud database service that combines the broadest SQL Server database engine compatibility with all the benefits of a fully managed and evergreen platform as a service. SQL Managed Instance has near 100% compatibility with the latest SQL Server (Enterprise Edition) database engine, providing a native virtual network (VNet) implementation that addresses common security concerns, and a business model favorable for existing SQL Server customers. SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.

Incorrect Answers:

A. Azure SQL Database elastic pools

CLR integration is not supported in Azure SQL database.

C. Azure SQL Database single databases

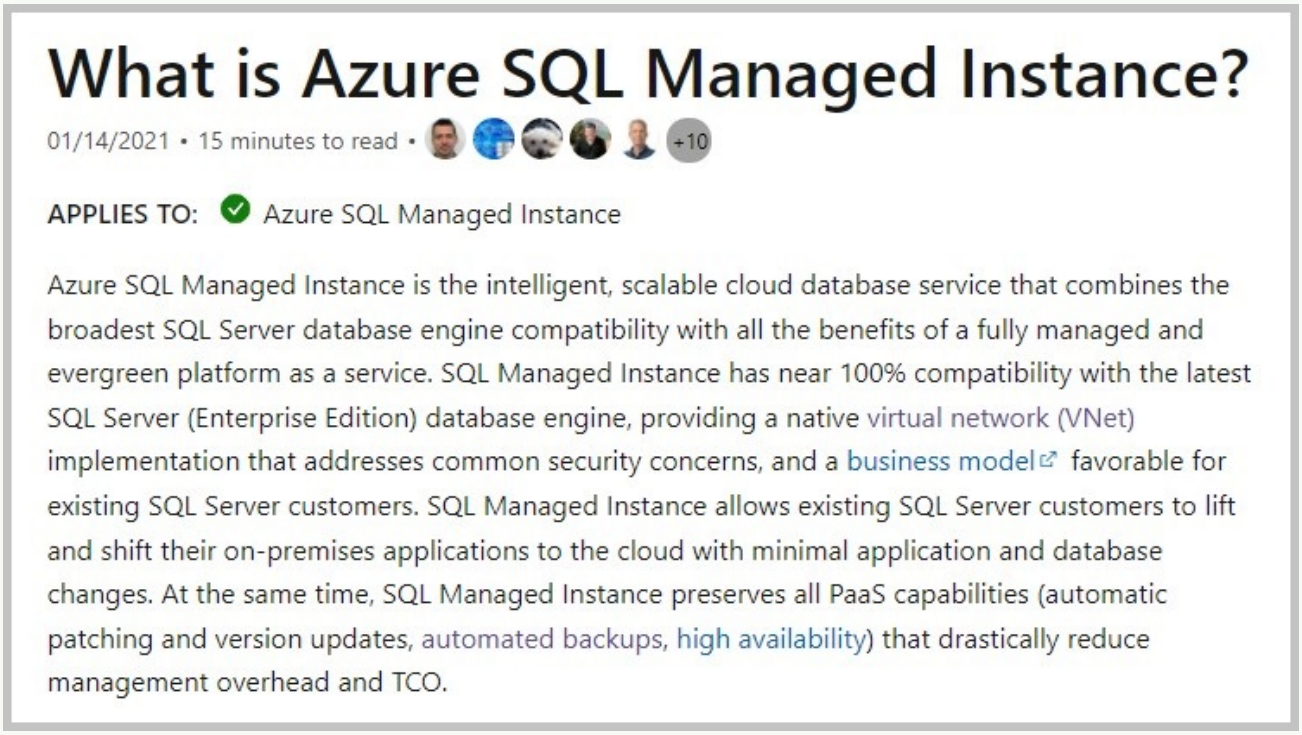
CLR integration is not supported in Azure SQL database.

D. SQL Server 2016 on Azure virtual machines

This option will continue to have management overhead post migration.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview



What is Azure SQL Managed Instance?

01/14/2021 • 15 minutes to read • +10

APPLIES TO: Azure SQL Managed Instance

Azure SQL Managed Instance is the intelligent, scalable cloud database service that combines the broadest SQL Server database engine compatibility with all the benefits of a fully managed and evergreen platform as a service. SQL Managed Instance has near 100% compatibility with the latest SQL Server (Enterprise Edition) database engine, providing a native virtual network (VNet) implementation that addresses common security concerns, and a business model favorable for existing SQL Server customers. SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.

49. Question

You need to design a highly available Azure SQL database that meets the following requirements:

? Failover between replicas of the database must occur without any data loss.

? The database must remain available in the event of a zone outage.

? Costs must be minimized.

Which deployment option should you use?

- A. Azure SQL Database Standard
- B. Azure SQL Database Managed Instance Business Critical
- C. Azure SQL Database Business Critical
- D. Azure SQL Database Basic

Incorrect

Standard geo-replication is available with Standard and General Purpose databases in the current Azure Management Portal and standard APIs.

Note: If you try to create a SQL Database in the portal, you will see that nowdays you can select Zone-redundant backup storage – Preview

Incorrect Answers:

B, C: Business Critical service tier is designed for applications that require low-latency responses from the underlying SSD storage (1-2 ms in average), fast recovery if the underlying infrastructure fails, or need to off-load reports, analytics, and read-only queries to the free of charge readable secondary replica of the primary database.

Note: Azure SQL Database and Azure SQL Managed Instance are both based on SQL Server database engine architecture that is adjusted for the cloud environment in order to ensure 99.99% availability even in the cases of infrastructure failures. There are three architectural models that are used:

? General Purpose/Standard

? Business Critical/Premium

? Hyperscale

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/service-tier-business-critical

Business Critical tier - Azure SQL Database and Azure SQL Managed Instance

12/04/2018 • 4 minutes to read •

APPLIES TO: Azure SQL Database Azure SQL Managed Instance

Note

Business Critical tier is called Premium in the DTU purchasing model. For a comparison of the vCore-based purchasing model with the DTU-based purchasing model, see **Azure SQL Database purchasing models and resources.**

Azure SQL Database and Azure SQL Managed Instance are both based on SQL Server database engine architecture that is adjusted for the cloud environment in order to ensure 99.99% availability even in the cases of infrastructure failures. There are three architectural models that are used:

- General Purpose/Standard
- Business Critical/Premium
- Hyperscale

Premium/Business Critical service tier model is based on a cluster of database engine processes. This architectural model relies on a fact that there is always a quorum of available database engine nodes and has minimal performance impact on your workload even during maintenance activities. The hyperscale service tier is currently only available for Azure SQL Database (not SQL Managed Instance), and is a highly scalable storage and compute performance tier that leverages the Azure architecture to scale out the storage and compute resources for a database in Azure SQL Database substantially beyond the limits available for the General Purpose and Business Critical service tiers.

50. Question

Your company plans to migrate its on-premises data to Azure.

You need to recommend which Azure services can be used to store the data. The solution must meet the following requirements:

? Encrypt all data while at rest.

? Encrypt data only by using a key generated by the company.

Which two possible services can you recommend?

- [ ] A. Azure Table storage
- [x] B. Azure Backup
- [x] C. Azure Blob storage

D. Azure Queue storage

E. Azure Files

Incorrect

Both supports encryption at rest using customer owned key s and can store file share data.

Incorrect Answers:

A. Azure Table storage

It is not possible to store file share data in Azure table storage.

B. Azure Backup

The Azure Backup service provides solutions to back up your data and recover it from the Microsoft Azure cloud.

D. Azure Queue storage

It is not possible to store file share data in Azure Queue storage.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption-customer-managed-keys

https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction?toc=/azure/storage/blobs/toc.json

51. Question

You are planning the implementation of an order processing web service that will contain microservices hosted in an Azure Service Fabric cluster.

You need to recommend a solution to provide developers with the ability to proactively identify and fix performance issues. The developers must be able to simulate user connections to the order processing web service from the Internet, as well as simulate user transactions. The developers must be notified if the goals for the transaction response times are not met.

What should you include in the recommendation?

A. container health

B. Azure Network Watcher

C. Application Insights

D. Service Fabric Analytics

Incorrect

Availability tests in Application Insights are recurring tests that monitor the availability and responsiveness of your application at regular intervals from points around the world. You can create a simple ping test for free or create a sequence of web requests to simulate user transactions which has associated cost.

Note:

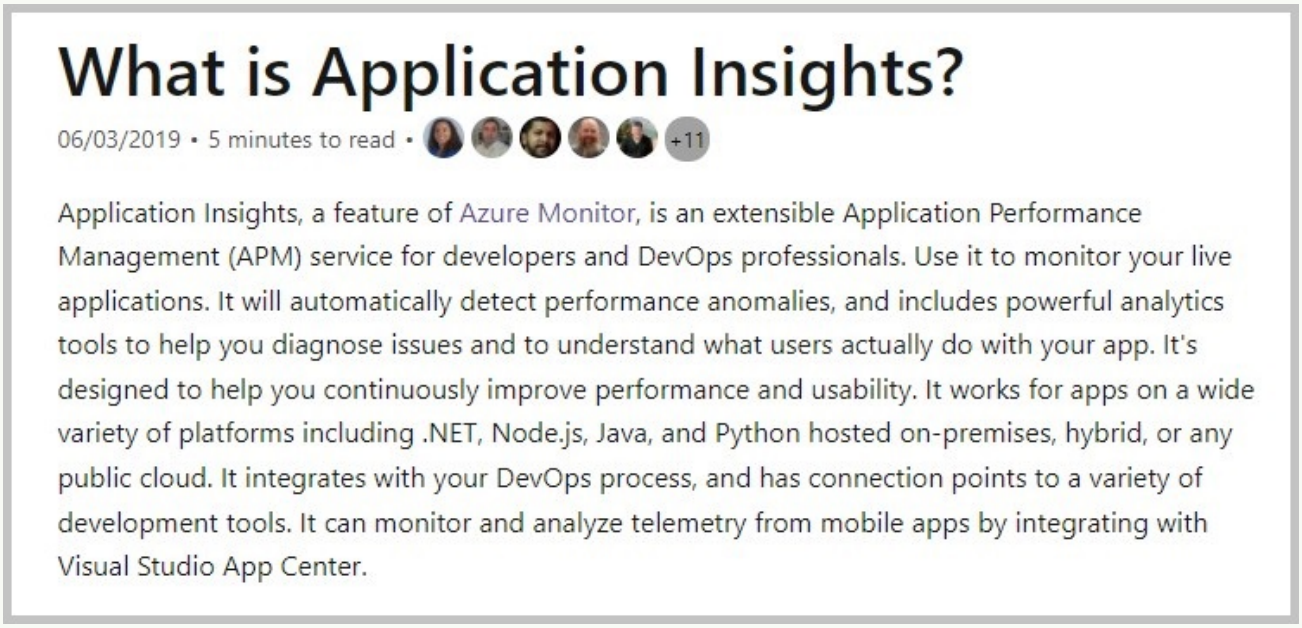
? Application monitoring with Application Insights

? Cluster monitoring with Diagnostics Agent and Azure Monitor logs

? Infrastructure monitoring with Azure Monitor logs

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview



What is Application Insights?

06/03/2019 • 5 minutes to read • +11

Application Insights, a feature of Azure Monitor, is an extensible Application Performance Management (APM) service for developers and DevOps professionals. Use it to monitor your live applications. It will automatically detect performance anomalies, and includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app. It's designed to help you continuously improve performance and usability. It works for apps on a wide variety of platforms including .NET, Node.js, Java, and Python hosted on-premises, hybrid, or any public cloud. It integrates with your DevOps process, and has connection points to a variety of development tools. It can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center.

52. 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.

A company has custom ASP.NET and Java applications that run old versions of Windows and Linux. The company plans to place applications in containers.

You need to design a solution that includes networking, service discovery, and load balancing for the applications. The solution must support storage orchestration.

Solution: You create an Azure virtual network, public IP address, and load balancer. Then add virtual machines (VMs) to the solution and deploy individual containers on them.

Does the solution meet the goal?

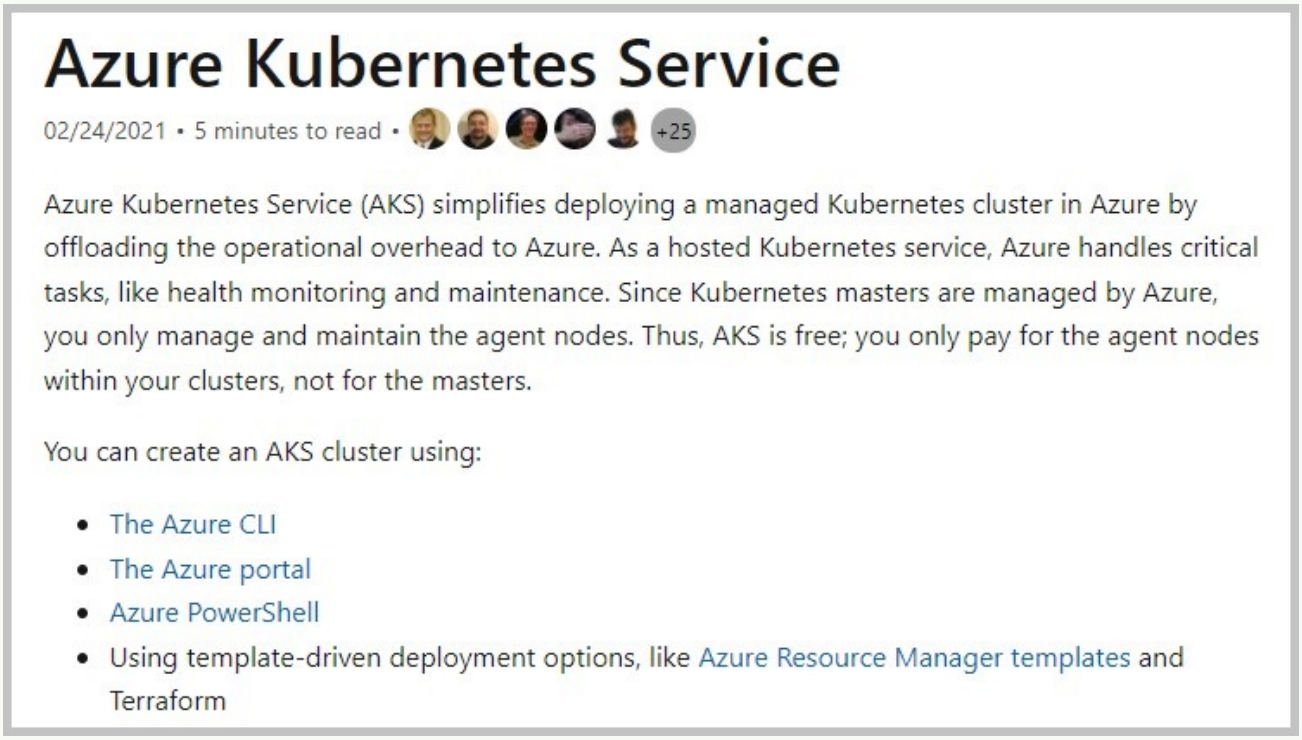
- A. Yes
- B. No

Incorrect

Instead use Azure Kubernetes Service (AKS)

Reference:

https://docs.microsoft.com/en-us/azure/aks/intro-kubernetes



Azure Kubernetes Service

02/24/2021 • 5 minutes to read • +25

Azure Kubernetes Service (AKS) simplifies deploying a managed Kubernetes cluster in Azure by offloading the operational overhead to Azure. As a hosted Kubernetes service, Azure handles critical tasks, like health monitoring and maintenance. Since Kubernetes masters are managed by Azure, you only manage and maintain the agent nodes. Thus, AKS is free; you only pay for the agent nodes within your clusters, not for the masters.

You can create an AKS cluster using:

- The Azure CLI
- The Azure portal
- Azure PowerShell
- Using template-driven deployment options, like Azure Resource Manager templates and Terraform

53. 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.

A company has custom ASP.NET and Java applications that run old versions of Windows and Linux. The company plans to place applications in containers.

You need to design a solution that includes networking, service discovery, and load balancing for the applications. The solution must support storage orchestration.

Solution: Deploy a Kubernetes cluster that has the desired number of instances of the applications.

Does the solution meet the goal?

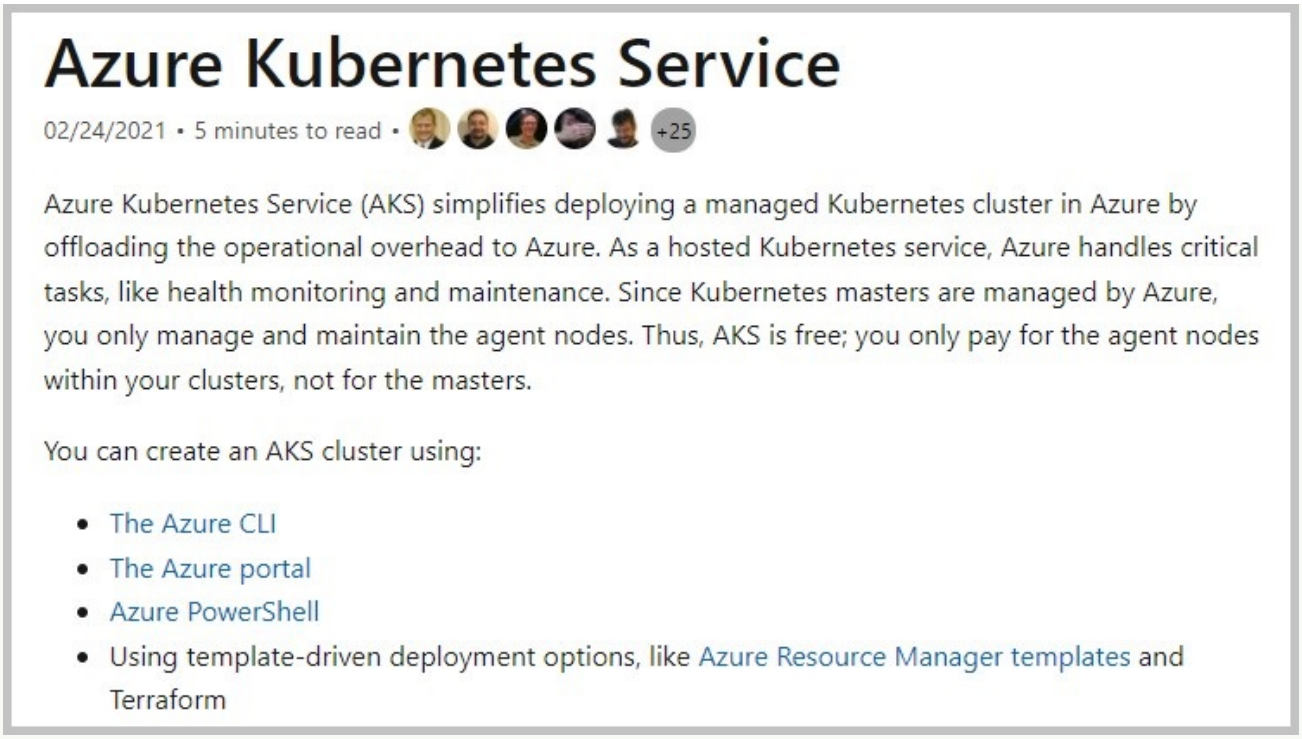
- A. Yes
- B. No

Correct

For scenarios where you need full container orchestration, including service discovery across multiple containers, automatic scaling, and coordinated application upgrades, we (MS) recommend Azure Kubernetes Service (AKS).

Reference:

https://docs.microsoft.com/en-us/azure/aks/intro-kubernetes



Azure Kubernetes Service

02/24/2021 • 5 minutes to read • +25

Azure Kubernetes Service (AKS) simplifies deploying a managed Kubernetes cluster in Azure by offloading the operational overhead to Azure. As a hosted Kubernetes service, Azure handles critical tasks, like health monitoring and maintenance. Since Kubernetes masters are managed by Azure, you only manage and maintain the agent nodes. Thus, AKS is free; you only pay for the agent nodes within your clusters, not for the masters.

You can create an AKS cluster using:

- The Azure CLI
- The Azure portal
- Azure PowerShell
- Using template-driven deployment options, like Azure Resource Manager templates and Terraform

54. 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.

A company has custom ASP.NET and Java applications that run old versions of Windows and Linux. The company plans to place applications in containers.

You need to design a solution that includes networking, service discovery, and load balancing for the applications. The solution must support storage orchestration.

Solution: You deploy each application to an Azure Container instance.

Does the solution meet the goal?

- A. Yes
- B. No

Correct

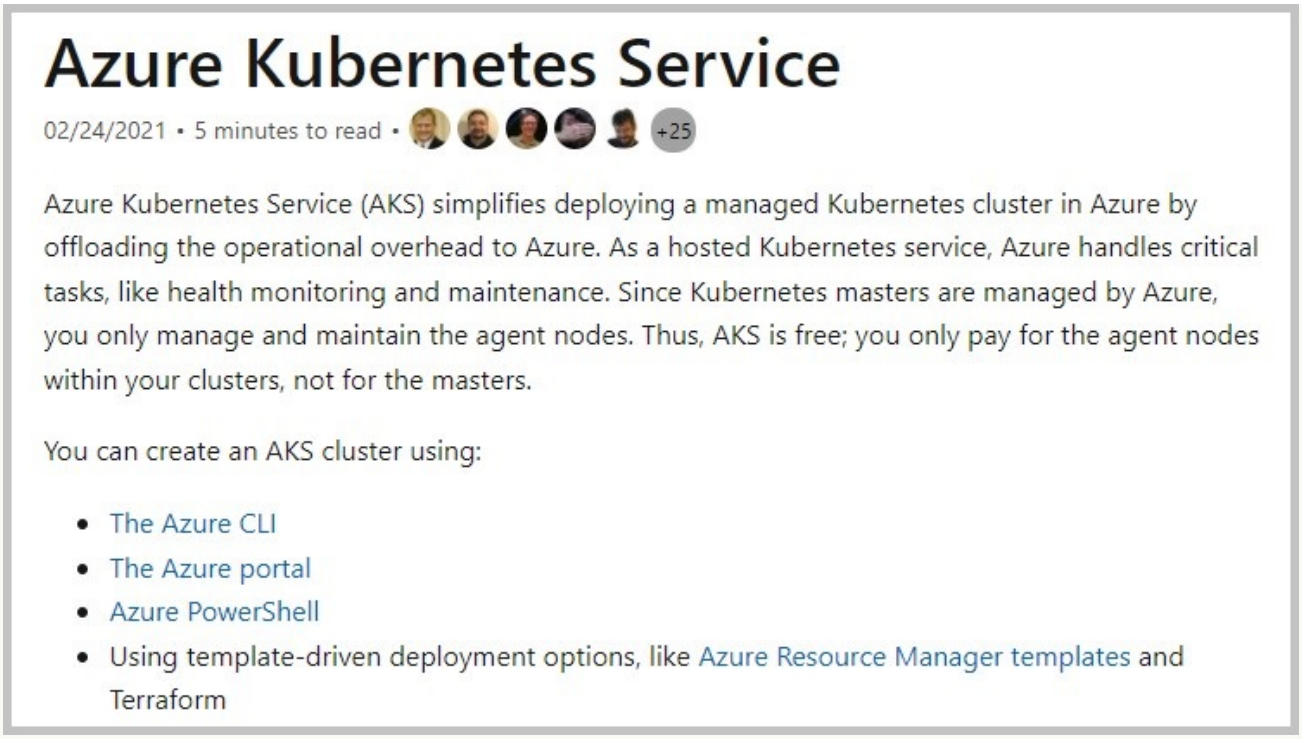
Instead, you can use Azure Kubernetes Service (AKS).

Azure Container Instances is a great solution for any scenario that can operate in isolated containers, including simple applications, task automation, and build jobs. For scenarios where you need full container orchestration, including service discovery across multiple containers, automatic scaling, and coordinated application upgrades, we recommend Azure Kubernetes Service (AKS).

Reference:

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

https://docs.microsoft.com/en-us/azure/aks/intro-kubernetes



Azure Kubernetes Service

02/24/2021 • 5 minutes to read • +25

Azure Kubernetes Service (AKS) simplifies deploying a managed Kubernetes cluster in Azure by offloading the operational overhead to Azure. As a hosted Kubernetes service, Azure handles critical tasks, like health monitoring and maintenance. Since Kubernetes masters are managed by Azure, you only manage and maintain the agent nodes. Thus, AKS is free; you only pay for the agent nodes within your clusters, not for the masters.

You can create an AKS cluster using:

- The Azure CLI
- The Azure portal
- Azure PowerShell
- Using template-driven deployment options, like Azure Resource Manager templates and Terraform

55. 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.

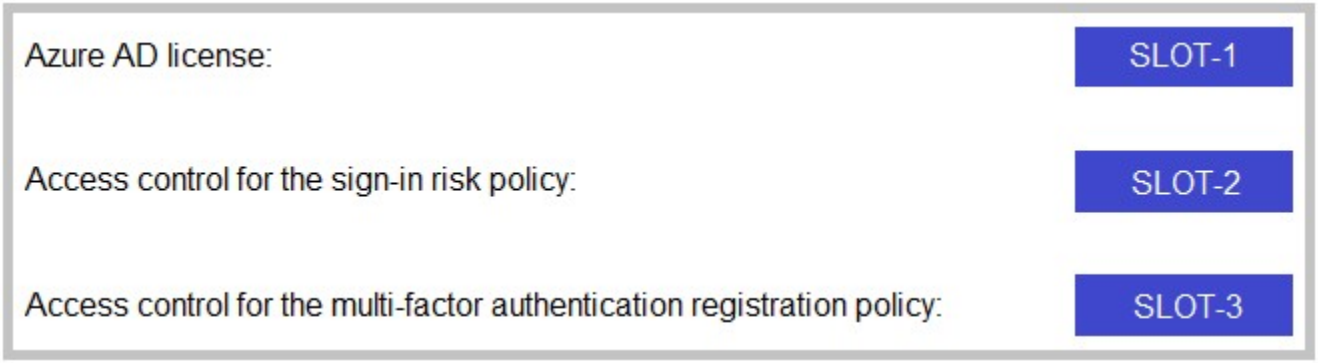
? Information Security Requirements

? 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 solution for configuring the Azure Multi-Factor Authentication (MFA) settings



Which of the following would go into Slot1?

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

Incorrect

Here we need to use Azure Identity Protection and define policies. To define policies, we need to have Azure AD Premium P2 licenses.

56. 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.

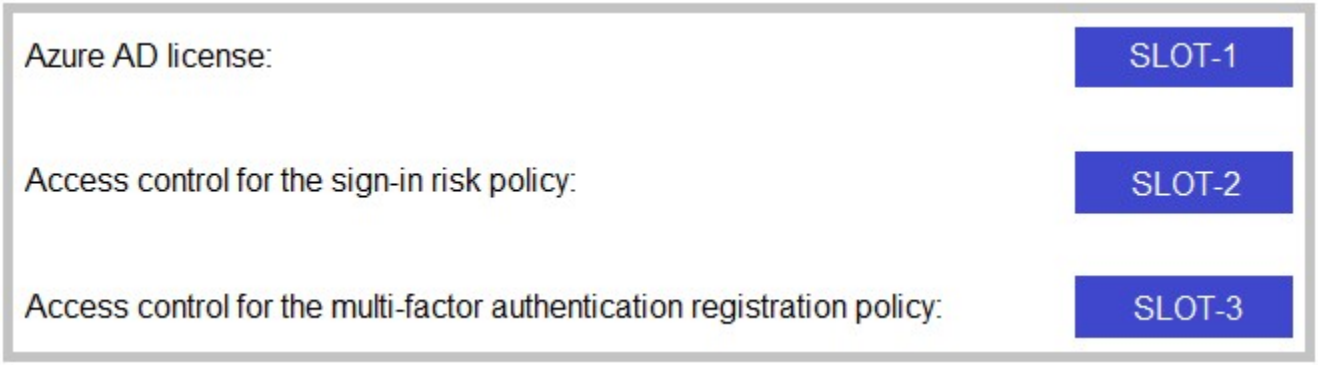
? Information Security Requirements

? 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 solution for configuring the Azure Multi-Factor Authentication (MFA) settings



Which of the following would go into Slot2?

- A. Allow access and require multi-factor authentication
- B. Block access and require multi-factor authentication
- C. Allow access and require Azure MFA registration
- D. Block access

Correct

Here we should define that the user should be granted access after carrying out multi-factor authentication

Reference:

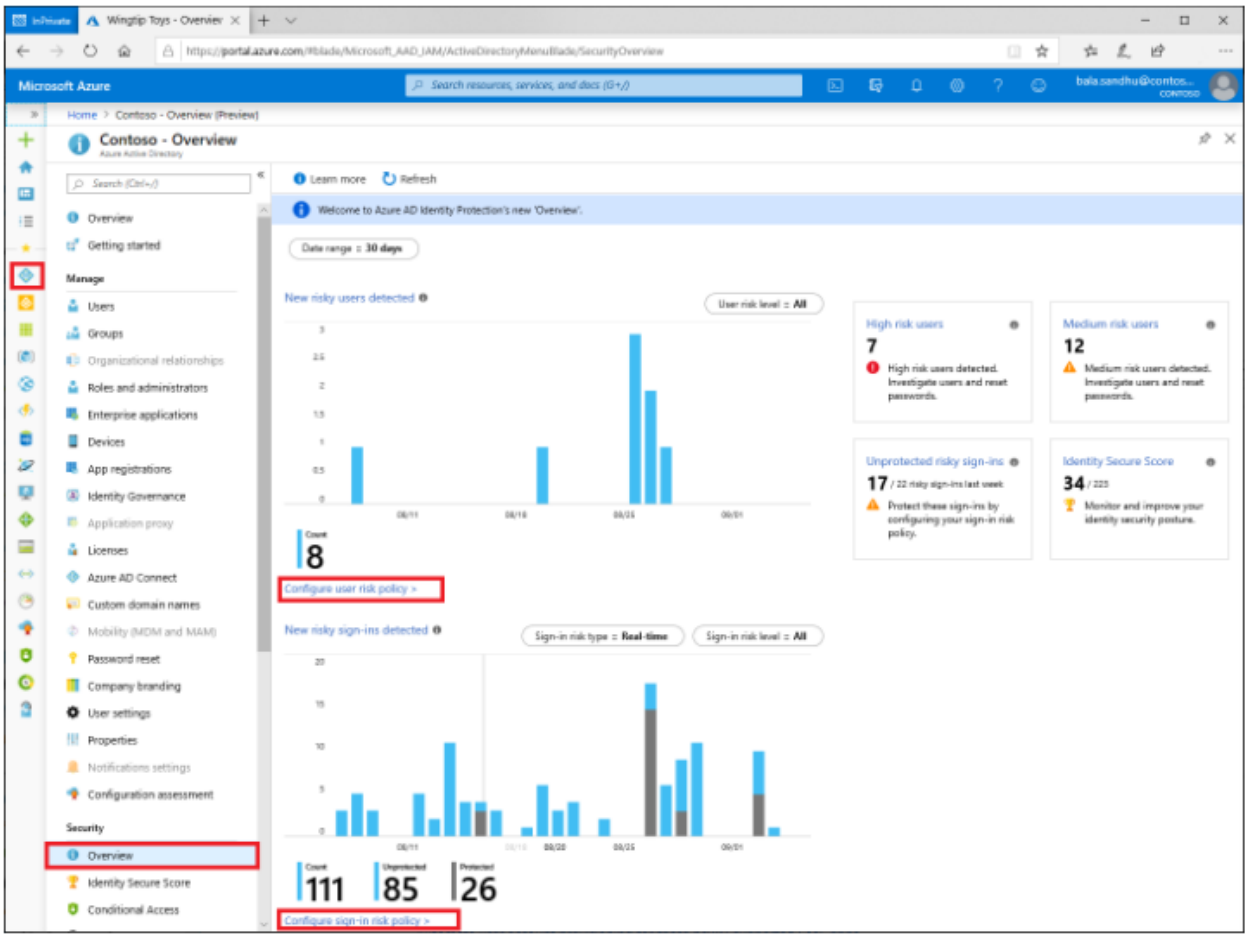
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy

How To: Configure and enable risk policies

05/27/2021 • 3 minutes to read •

As we learned in the previous article, Identity Protection policies we have two risk policies that we can enable in our directory.

- Sign-in risk policy
- User risk policy



Both policies work to automate the response to risk detections in your environment and allow users to self-remediate when risk is detected.

57. 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.

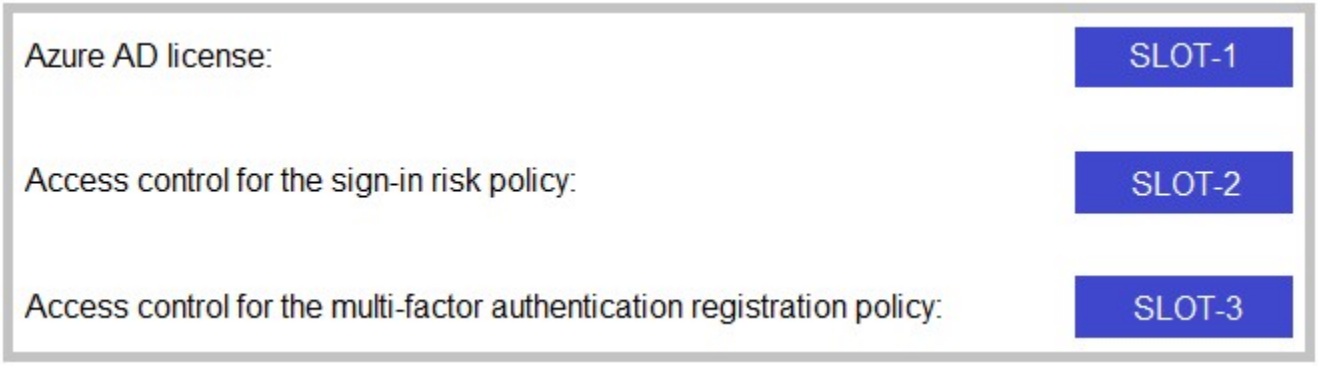
? Information Security Requirements

? 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 solution for configuring the Azure Multi-Factor Authentication (MFA) settings



Which of the following would go into Slot3?

- A. Allow access and require multi-factor authentication
- B. Block access and require multi-factor authentication
- C. Allow access and require Azure MFA registration
- D. Block access

Correct

Here we can define the user will be allowed access with Azure MFA registration

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-mfa-policy

58. 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

Which of the following can be used to collect the security logs from the middle tier system?

- Azure Notification Hubs
- Azure Diagnostics agent
- Azure Event Hubs
- **Azure Log Analytics agent**

Correct

Here the security logs can be sent to a Log Analytics workspace. Hence the Azure Log Analytics agent needs to be installed on the virtual machines hosting the middle tier component.

Incorrect Answers:

A. Azure Notification Hubs

Azure Notification Hubs provide an easy-to-use and scaled-out push engine that enables you to send notifications to any platform (iOS, Android, Windows, etc.) from any back-end (cloud or on-premises).

B. Azure Diagnostics agent

Azure Diagnostics extension is an agent in Azure Monitor that collects monitoring data from the guest operating system of Azure compute resources including virtual machines

C. Azure Event Hubs

Azure Event Hubs is a big data streaming platform and event ingestion service. It can receive and process millions of events per second.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent

Log Analytics agent overview

01/12/2021 • 7 minutes to read •

The Azure Log Analytics agent collects telemetry from Windows and Linux virtual machines in any cloud, on-premises machines, and those monitored by System Center Operations Manager and sends it collected data to your Log Analytics workspace in Azure Monitor. The Log Analytics agent also supports insights and other services in Azure Monitor such as VM insights, Azure Security Center, and Azure Automation. This article provides a detailed overview of the agent, system and network requirements, and deployment methods.

Note

You may also see the Log Analytics agent referred to as the Microsoft Monitoring Agent (MMA).

59. 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.

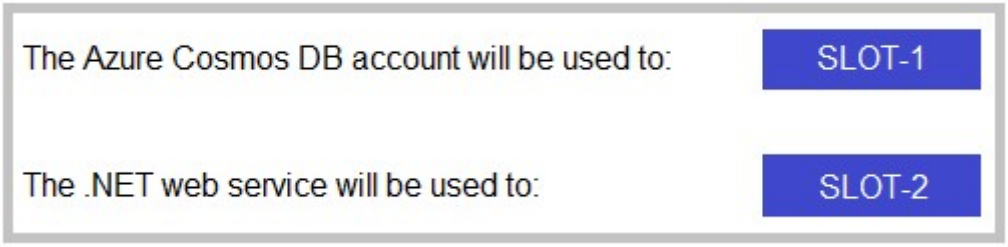
? Information Security Requirements

? 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 design a solution for securing access to the historical transaction data.



Which of the following would go into Slot1?

A. Create users and generate resource tokens

B. Create users and request resource tokens

C. Generate resource tokens and perform authentication

D. Request resource tokens and perform authentication

Incorrect

The Cosmos DB account will be used to create users. Resource tokens can be generated and sent to the .Net web service.

Note: Resource Tokens are a feature of Cosmos DB, which provide a safe alternative to giving out the master key. Our .NET Web Service acts as mid-tier service and is the only component that is going to talk directly to the Cosmos DB (its the only one having the master key). The client app talks to the mid-tier, which in turn performs auth. and requests a resource token from Cosmos DB and returns it back to the client.

Reference:

https://docs.microsoft.com/en-us/azure/cosmos-db/secure-access-to-data#users

https://docs.microsoft.com/en-us/azure/cosmos-db/secure-access-to-data#resource-tokens

https://docs.microsoft.com/en-us/azure/cosmos-db/database-security

Resource tokens

Resource tokens provide access to the application resources within a database. Resource tokens:

- Provide access to specific containers, partition keys, documents, attachments, stored procedures, triggers, and UDFs.
- Are created when a user is granted permissions to a specific resource.
- Are recreated when a permission resource is acted upon on by POST, GET, or PUT call.
- Use a hash resource token specifically constructed for the user, resource, and permission.
- Are time bound with a customizable validity period. The default valid time span is one hour. Token lifetime, however, may be explicitly specified, up to a maximum of five hours.
- Provide a safe alternative to giving out the primary key.
- Enable clients to read, write, and delete resources in the Cosmos DB account according to the permissions they've been granted.

You can use a resource token (by creating Cosmos DB users and permissions) when you want to provide access to resources in your Cosmos DB account to a client that cannot be trusted with the primary key.

Cosmos DB resource tokens provide a safe alternative that enables clients to read, write, and delete resources in your Cosmos DB account according to the permissions you've granted, and without need for either a primary or read only key.

60. 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.

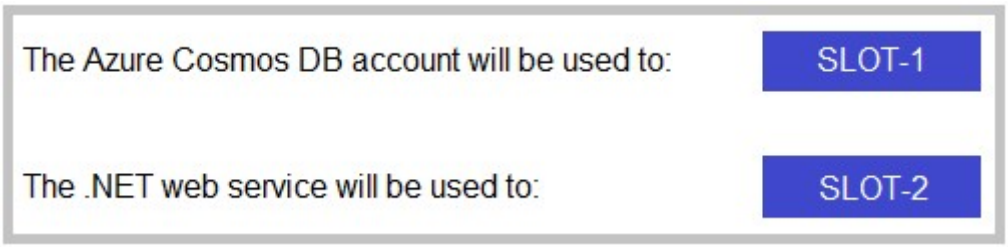
? Information Security Requirements

? 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 design a solution for securing access to the historical transaction data.



Which of the following would go into Slot2?

- A. Create users and generate resource tokens
- B. Create users and request resource tokens
- C. Generate resource tokens and perform authentication
- **D. Request resource tokens and perform authentication**

Incorrect

The .Net service should be used to perform authentication from the clients and request resource tokens from the Cosmos DB account.

Note: Resource Tokens are a feature of Cosmos DB, which provide a safe alternative to giving out the master key. Our .NET Web Service acts as mid-tier service and is the only component that is going to talk directly to the Cosmos DB (its the only one having the master key). The client app talks to the mid-tier, which in turn performs auth. and requests a resource token from Cosmos DB and returns it back to the client.

Reference:

https://docs.microsoft.com/en-us/azure/cosmos-db/secure-access-to-data#users

https://docs.microsoft.com/en-us/azure/cosmos-db/secure-access-to-data#resource-tokens

https://docs.microsoft.com/en-us/azure/cosmos-db/database-security

Resource tokens

Resource tokens provide access to the application resources within a database. Resource tokens:

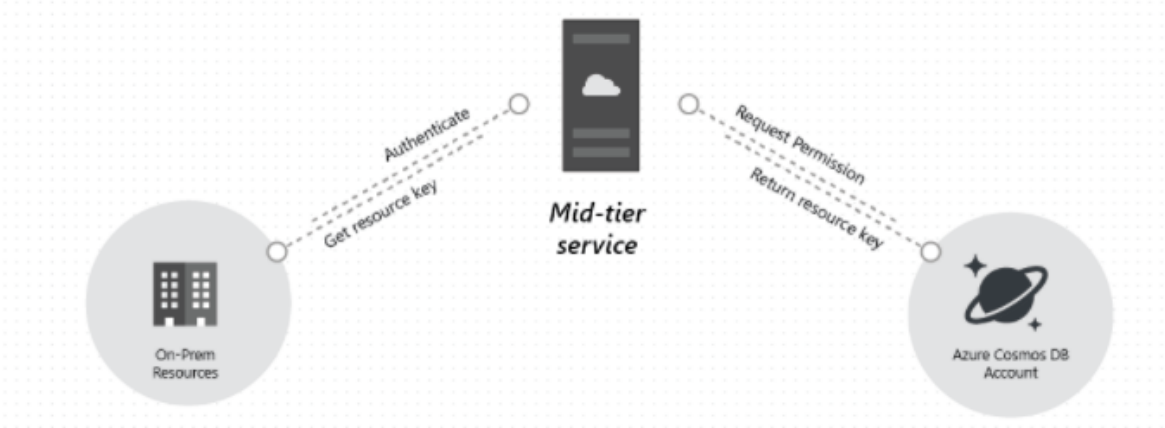
- Provide access to specific containers, partition keys, documents, attachments, stored procedures, triggers, and UDFs.
- Are created when a user is granted permissions to a specific resource.
- Are recreated when a permission resource is acted upon on by POST, GET, or PUT call.
- Use a hash resource token specifically constructed for the user, resource, and permission.
- Are time bound with a customizable validity period. The default valid time span is one hour. Token lifetime, however, may be explicitly specified, up to a maximum of five hours.
- Provide a safe alternative to giving out the primary key.
- Enable clients to read, write, and delete resources in the Cosmos DB account according to the permissions they've been granted.

You can use a resource token (by creating Cosmos DB users and permissions) when you want to provide access to resources in your Cosmos DB account to a client that cannot be trusted with the primary key.

Cosmos DB resource tokens provide a safe alternative that enables clients to read, write, and delete resources in your Cosmos DB account according to the permissions you've granted, and without need for either a primary or read only key.

Here is a typical design pattern whereby resource tokens may be requested, generated, and delivered to clients:

1. A mid-tier service is set up to serve a mobile application to share user photos.
2. The mid-tier service possesses the primary key of the Cosmos DB account.
3. The photo app is installed on end-user mobile devices.
4. On login, the photo app establishes the identity of the user with the mid-tier service. This mechanism of identity establishment is purely up to the application.
5. Once the identity is established, the mid-tier service requests permissions based on the identity.
6. The mid-tier service sends a resource token back to the phone app.
7. The phone app can continue to use the resource token to directly access Cosmos DB resources with the permissions defined by the resource token and for the interval allowed by the resource token.
8. When the resource token expires, subsequent requests receive a 401 unauthorized exception. At this point, the phone app re-establishes the identity and requests a new resource token.



Resource token generation and management are handled by the native Cosmos DB client libraries; however, if you use REST you must construct the request/authentication headers. For more information on creating authentication headers for REST, see Access Control on Cosmos DB Resources or the source code for our .NET SDK or Node.js SDK.

61. 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 solution for the network configuration of the front-end tier of the payment processing.

What should you include in the recommendation?

- A. Azure Application Gateway
- B. Traffic Manager
- C. a Standard Load Balancer

D. a Basic load Balancer

Incorrect

Front-End System:

? Hosted on servers that run Win2012R2, ISS

? Code is written in C# and ASP.NET

Scenario:

? 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.

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

? 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.

? Cost must be minimized

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

With Azure Load Balancer, you can scale your applications and create high availability for your services. Load Balancer supports inbound and outbound scenarios, provides low latency and high throughput, and scales up to millions of flows for all TCP and UDP applications.

Azure Load Balancer is available in two SKUs: Basic and Standard. There are differences in scale, features, and pricing. Standard SLA guarantees a 99.99% for data path with two healthy virtual machines. Basic SLA does not exist.

Incorrect Answers:

A. Application Gateway

? Supports Availability Zones

? Supports Autoscaling

? Provides 99.95% SLA

B. Traffic Manager

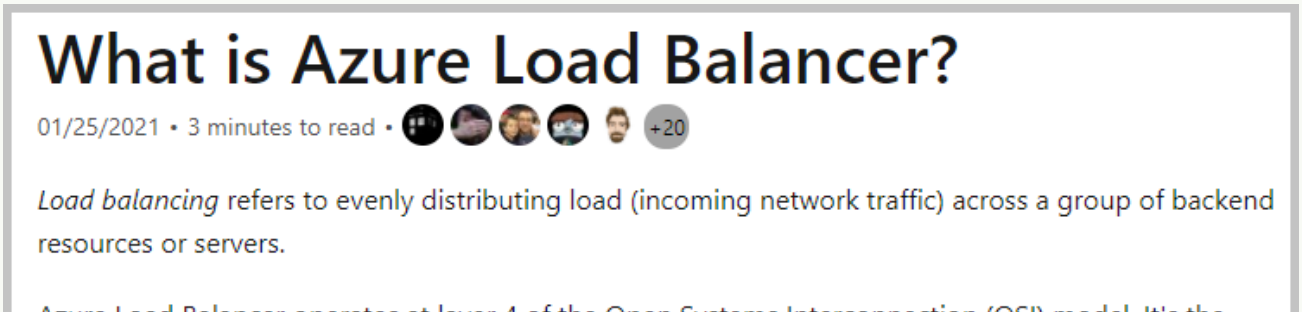
? Doesn't provide a way by itself to scale a group of VMs in or out

D. Load Balancer (Basic SKU)

? Doesn't support Availability Zones and can be ruled out

Reference:

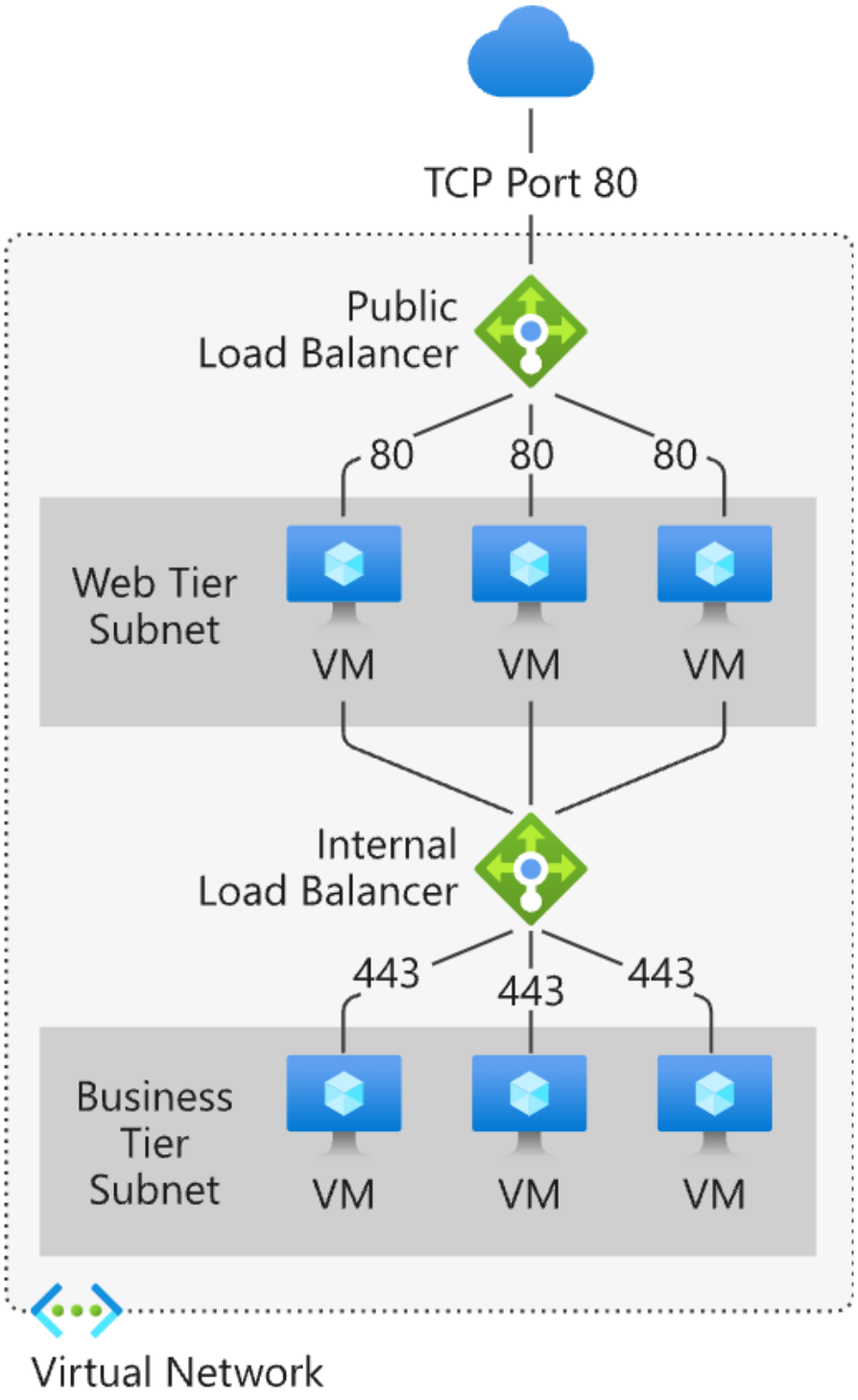
https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview



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. These flows are according to configured load-balancing rules and health probes. The backend pool instances can be Azure Virtual Machines or instances in a virtual machine scale set.

A **public load balancer** can provide outbound connections for virtual machines (VMs) inside your virtual network. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load Balancers are used to load balance internet traffic to your VMs.

An **internal (or private) load balancer** is used where private IPs are needed at the frontend only. Internal load balancers are used to load balance traffic inside a virtual network. A load balancer frontend can be accessed from an on-premises network in a hybrid scenario.



62. Question

You plan to create an Azure Storage account that will host file shares. The shares will be accessed from on-premises applications that are transaction-intensive.

You need to recommend a solution to minimize latency when accessing the file shares. The solution must provide the highest-level of resiliency for the selected storage tier.

What should you include in the Storage tier?

- A. Hot
- **B. Premium**
- C. Transaction optimized

Incorrect

Premium: Premium file shares are backed by solid-state drives (SSDs) and provide consistent high performance and low latency, within single-digit milliseconds for most IO operations, for IO-intensive workloads.

Incorrect Answers:

A. Hot: Hot file shares offer storage optimized for general purpose file sharing scenarios such as team shares. Hot file shares are offered on the standard storage hardware backed by HDDs.

C. Transaction optimized: Transaction optimized file shares enable transaction heavy workloads that don't need the latency offered by premium file shares.

Transaction optimized file shares are offered on the standard storage hardware backed by hard disk drives (HDDs). Transaction optimized has historically been called "standard", however this refers to the storage media type rather than the tier itself (the hot and cool are also "standard" tiers, because they are on standard storage hardware).

Reference:

https://docs.microsoft.com/en-us/azure/storage/files/storage-files-planning#storage-tiers

Storage tiers

Azure Files offers four different tiers of storage, premium, transaction optimized, hot, and cool to allow you to tailor your shares to the performance and price requirements of your scenario:

- **Premium**: Premium file shares are backed by solid-state drives (SSDs) and provide consistent high performance and low latency, within single-digit milliseconds for most IO operations, for IO-intensive workloads. Premium file shares are suitable for a wide variety of workloads like databases, web site hosting, and development environments. Premium file shares can be used with both Server Message Block (SMB) and Network File System (NFS) protocols.
- **Transaction optimized**: Transaction optimized file shares enable transaction heavy workloads that don't need the latency offered by premium file shares. Transaction optimized file shares are offered on the standard storage hardware backed by hard disk drives (HDDs). Transaction optimized has historically been called "standard", however this refers to the storage media type rather than the tier itself (the hot and cool are also "standard" tiers, because they are on standard storage hardware).
- **Hot**: Hot file shares offer storage optimized for general purpose file sharing scenarios such as team shares. Hot file shares are offered on the standard storage hardware backed by HDDs.
- **Cool**: Cool file shares offer cost-efficient storage optimized for online archive storage scenarios. Cool file shares are offered on the standard storage hardware backed by HDDs.

63. Question

You plan to create an Azure Storage account that will host file shares. The shares will be accessed from on-premises applications that are transaction-intensive.

You need to recommend a solution to minimize latency when accessing the file shares. The solution must provide the highest-level of resiliency for the selected storage tier.

What should you include in the Redundancy?

- A. Geo-redundant storage (GRS)
- B. Zone-redundant storage (ZRS)
- C. Locally-redundant storage (LRS)

Incorrect

Premium Azure file shares only support LRS and ZRS.

Zone-redundant storage (ZRS): With ZRS, three copies of each file stored, however these copies are

physically isolated in three distinct storage clusters in different Azure availability zones. Availability zones are unique physical locations within an Azure region. Each zone is made up of one or more data centers equipped with independent power, cooling, and networking. A write to storage is not accepted until it is written to the storage clusters in all three availability zones.

Reference:

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

Redundancy

To protect the data in your Azure file shares against data loss or corruption, all Azure file shares store multiple copies of each file as they are written. Depending on the requirements of your workload, you can select additional degrees of redundancy. Azure Files currently supports the following data redundancy options:

- **Locally-redundant storage (LRS)**: With LRS, every file is stored three times within an Azure storage cluster. This protects against loss of data due to hardware faults, such as a bad disk drive. However, if a disaster such as fire or flooding occurs within the data center, all replicas of a storage account using LRS may be lost or unrecoverable.
- **Zone-redundant storage (ZRS)**: With ZRS, three copies of each file stored, however these copies are physically isolated in three distinct storage clusters in different Azure *availability zones*. Availability zones are unique physical locations within an Azure region. Each zone is made up of one or more data centers equipped with independent power, cooling, and networking. A write to storage is not accepted until it is written to the storage clusters in all three availability zones.
- **Geo-redundant storage (GRS)**: With GRS, you have two regions, a primary and secondary region. Files are stored three times within an Azure storage cluster in the primary region. Writes are asynchronously replicated to a Microsoft-defined secondary region. GRS provides six copies of your data spread between two Azure regions. In the event of a major disaster such as the permanent loss of an Azure region due to a natural disaster or other similar event, Microsoft will perform a failover and the secondary becomes the primary, serving all operations. Since the replication between the primary and secondary regions are asynchronous, in the event of a major disaster, data not yet replicated to the secondary region will be lost. You can also perform a manual failover of a geo-redundant storage account.
- **Geo-zone-redundant storage (GZRS)**: You can think of GZRS as if it were like ZRS but with geo-redundancy. With GZRS, files are stored three times across three distinct storage clusters in the primary region. All writes are then asynchronously replicated to a Microsoft-defined secondary region. The failover process for GZRS works the same as GRS.

Use Last Page number to navigate to Master Cheat Sheet

Pages: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

← Previous Post

Next Post →