

Practice Test 2

Completed on 14-June-2020



Attempt

01



Marks Obtained

0 / 55



Your score

0.0%



Time Taken

00 H 00 M 02 S



Result

Failed

Domains wise Quiz Performance Report

1

Design for identity and security

18

0

0

18

0

2

Design an infrastructure strategy

14

0

0

14

0

3

Design a business continuity strategy

9

0

0

9

0

4

Design a data platform solution

8

0

0

8

0

5

Determine workload requirements

5

0

0

5

0

6

Design for deployment, migration, and integration

1

0

0

1

0

Total

All Domain

55

0

0

55

0

Review the Answers

Sorting by

All



Question 1

Unattempted

A company currently has an on-premise network. They have an Active directory domain defined as whizlab.com. They recently purchased an Azure AD tenant and now want to synchronize users from their on-premise Active Directory domain to Azure AD. They also want to enable single-sign on the users.

The company decides to setup Active Directory Federation Services and setup a sync with Azure AD.

Would this fulfil the requirement?

- A. Yes
- B. No

Explanation:

Answer – A

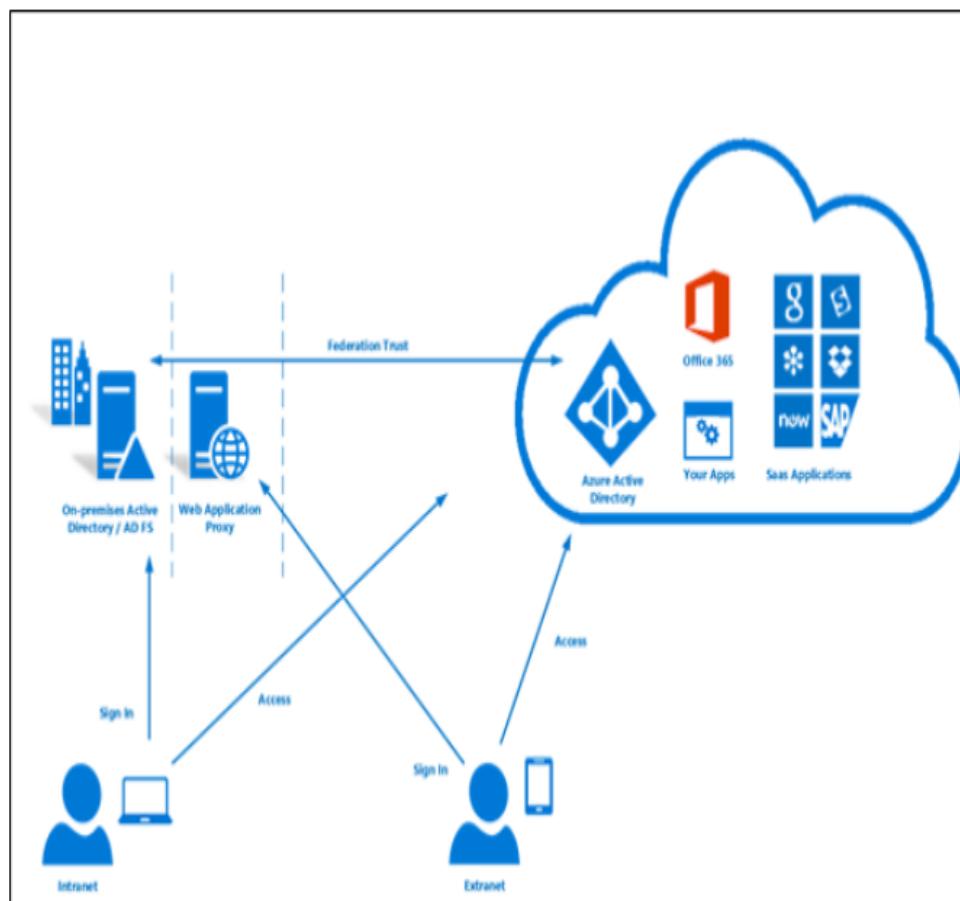
Yes, you can use Active Directory Federation services as well. This is also mentioned in the Microsoft documentation

What is federation with Azure AD?

11/28/2018 • 2 minutes to read • Contributors 

Federation is a collection of domains that have established trust. The level of trust may vary, but typically includes authentication and almost always includes authorization. A typical federation might include a number of organizations that have established trust for shared access to a set of resources.

You can federate your on-premises environment with Azure AD and use this federation for authentication and authorization. This sign-in method ensures that all user authentication occurs on-premises. This method allows administrators to implement more rigorous levels of access control. Federation with AD FS and PingFederate is available.



For more information on hybrid identity, please visit the below URL

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 2

Unattempted

A company currently has an on-premise network. They have an Active directory domain defined as whizlab.com. They recently purchased an Azure AD tenant and now want to synchronize users from their on-premise Active Directory domain to Azure AD. They also want to enable single-sign on the users. The company decides to setup an Active Directory domain on a set of servers in a Virtual Network. They then develop a sync strategy with Azure AD. Would this fulfil the requirement?

- A. Yes
- B. No

Explanation:

Answer – B

Here the primary purpose is to sync on-premise users with Azure AD and not setup a separate domain environment in Azure.

For more information on hybrid identity, please visit the below URL

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity>

[Ask our Experts](#)

Rate this Question?  

[View Queries](#)

open ▾

Question 3

Unattempted

Domain :Design for identity and security

A company currently has an on-premise network. They have an Active directory domain defined as whizlab.com. They recently purchased an Azure AD tenant and now want to synchronize users from their on-premise Active Directory domain to Azure AD. They also want to enable single-sign on the users. The company decides to install Azure AD Connect with pass-through authentication. They then configure Single-Sign in Azure AD Connect. Would this fulfil the requirement?

- A. Yes
- B. No

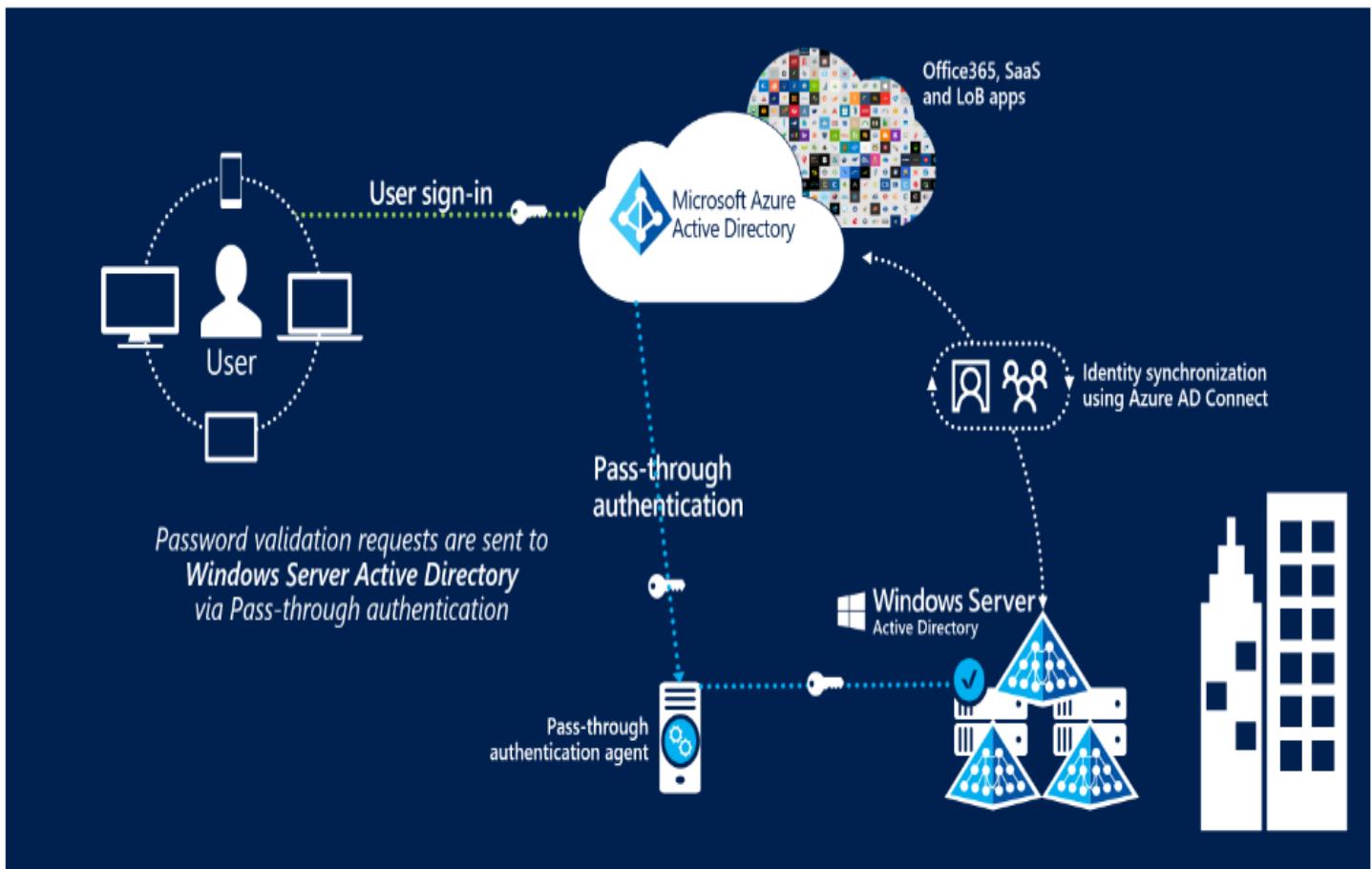
Explanation:

Answer – A

Azure AD connect is a tool that can be used to sync on-premise AD users with Azure AD.

Below is the diagram from the Microsoft documentation that showcases this.

You can also combine this with Single Sign-On as mentioned below.



You can combine Pass-through Authentication with the [Seamless Single Sign-On](#) feature. This way, when your users are accessing applications on their corporate machines inside your corporate network, they don't need to type in their passwords to sign in.

For more information on pass through authentication, please visit the below URL

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-ptt>

Ask our Experts

Rate this Question?

View Queries

open ▾

Question 4

Unattempted

Domain :Design an infrastructure strategy

A company is planning on storing database backups onto Azure. These backups will be individual .bak files. The files need to be stored for compliance reasons. Most likely the data backups will never be used for recovery purposes. You have to decide on which solution to use for the backup data. You have to minimize on costs.

- A. An Azure SQL database
- B. Azure BLOB storage that uses the Archive tier
- C. Azure BLOB storage that uses the Cool tier
- D. A Recovery Services vault

Explanation:

Answer – B

Using BLOB storage for storing files and objects is ideal. You can use the Archive tier to save on storage costs for objects that are not retrieved. The Microsoft documentation mentions the following

Archive access tier

The archive access tier has the lowest storage cost and higher data retrieval costs compared to hot and cool tiers. This tier is intended for data that can tolerate several hours of retrieval latency and will remain in the archive tier for at least 180 days.

While a blob is in archive storage, the blob data is offline and cannot be read, copied, overwritten, or modified. You can't take snapshots of a blob in archive storage. However, the blob metadata remains online and available, allowing you to list the blob and its properties. For blobs in archive, the only valid operations are GetBlobProperties, GetBlobMetadata, ListBlobs, SetBlobTier, and DeleteBlob.

Example usage scenarios for the archive access tier include:

- Long-term backup, secondary backup, and archival datasets
- Original (raw) data that must be preserved, even after it has been processed into final usable form. (*For example*, Raw media files after transcoding into other formats)
- Compliance and archival data that needs to be stored for a long time and is hardly ever accessed. (*For example*, security camera footage, old X-Rays/MRIs for healthcare organizations, audio recordings, and transcripts of customer calls for financial services)

Option A is incorrect since this is a SQL data store and should not be used to file based backups.

Option C is incorrect since using the Archive tier would be a more cost-effective option

Option D is incorrect since this is used when using the Azure Backup and Site Recovery service

For more information on the different storage tiers, please visit the below URL

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

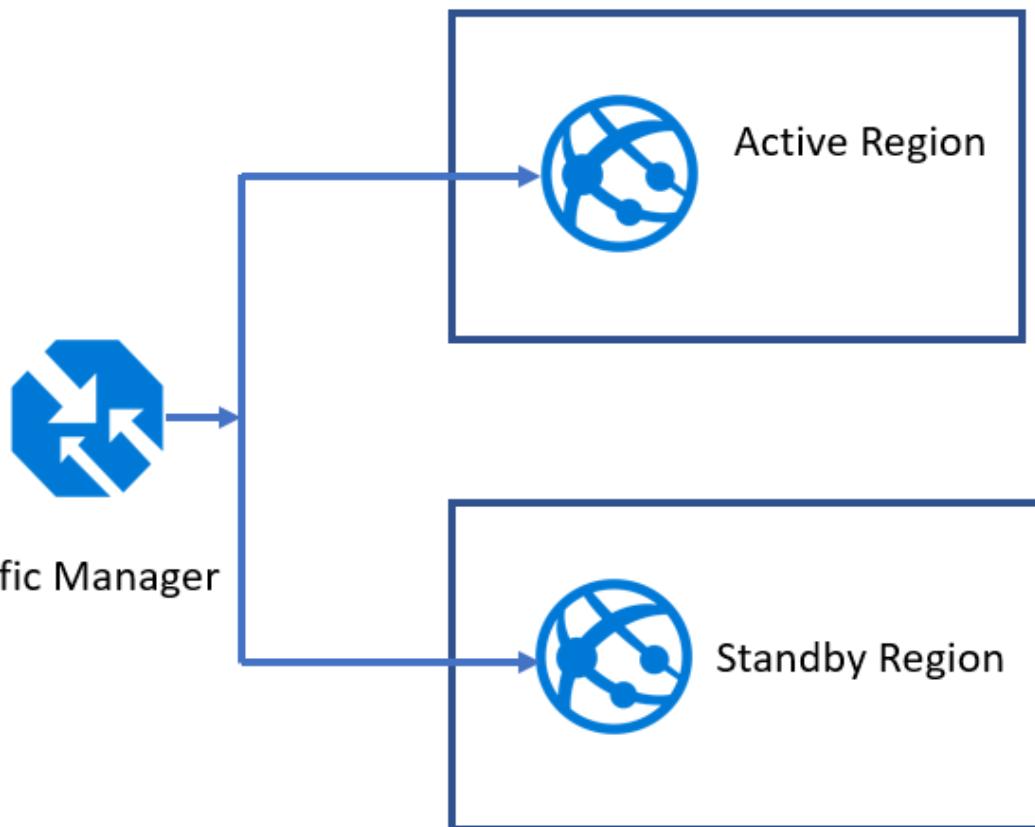
[View Queries](#)

open ▾

Question 5**Unattempted**

Domain :Design a business continuity strategy

A company has deployed a web-based application based on the following architecture



The company now

wants to implement an active-active configuration. Which of the following needs to be done for this requirement?

- A. Add a basic load balancer to the standby region
- B. Add an Application load balancer to the standby region
- C. Add an Application load balancer to the primary region
- D. Modify the Traffic routing method 

Explanation:

Answer – D

You can change the routing method for the Traffic Manager to the Priority routing method for implementing failover. The Microsoft documentation mentions the following on the routing method.

Traffic Manager routing methods

09/17/2018 • 12 minutes to read • Contributors  all

Azure Traffic Manager supports six traffic-routing methods to determine how to route network traffic to the various service endpoints. For any profile, Traffic Manager applies the traffic-routing method associated to it to each DNS query it receives. The traffic-routing method determines which endpoint is returned in the DNS response.

The following traffic routing methods are available in Traffic Manager:

- **Priority:** Select Priority when you want to use a primary service endpoint for all traffic, and provide backups in case the primary or the backup endpoints are unavailable.

The other options are incorrect since Load balancer cannot divert traffic across regions

For more information on Azure Traffic Manager routing methods, please visit the below URL

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

Ask our Experts

Rate this Question?  

View Queries

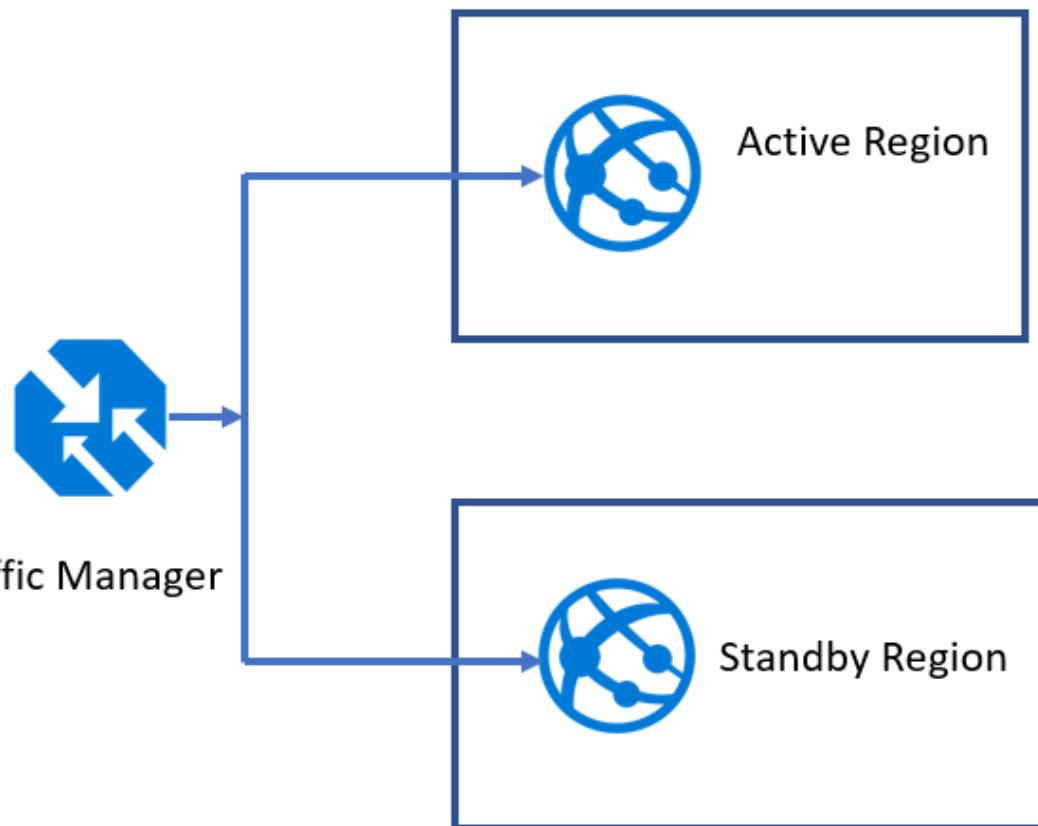
open ▾

Question 6

Unattempted

Domain :Design a business continuity strategy

A company has deployed a web-based application based on the following architecture



The company needs to control the threshold for the failover to the standby region. Which of the following needs to be done for this to happen?

- A. Add an Application Insights test
- B. Make use of Connection Monitor in Azure Network Watcher
- C. Enable SSL on the Load balancer
- D. Modify Endpoint monitor settings in Traffic Manager

Explanation:

Answer – D

Since we are going to be using the Azure Traffic Manager, we can use the Endpoint monitor settings for the Traffic Manager. The Microsoft documentation mentions the following

Traffic Manager endpoint monitoring

12/04/2018 • 14 minutes to read • Contributors  all

Azure Traffic Manager includes built-in endpoint monitoring and automatic endpoint failover. This feature helps you deliver high-availability applications that are resilient to endpoint failure, including Azure region failures.

Since the other settings are not applicable to Azure Traffic Manager, hence the options are incorrect

For more information on Azure Traffic Manager endpoint monitoring, please visit the below URL

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 7

Unattempted

Domain :Design for identity and security

A team is planning on deploying Azure resources by using Resource Manager templates. The templates need to reference secrets that are stored in Azure Key vault. You need to ensure deployments can be made accordingly.

Which of the following would you need to enable in the Azure key vault to ensure the templates can reference the secrets stored in the vault?

- A. Access policies for the Key vault
- B. An Azure policy
- C. Role Based access
- D. Enable "Azure Resource Manager for template Deployment" in Access Policy of Key Vault

Explanation:

Answer – D

This is clearly given in the documentation. In order for Resource Manager templates to access Azure Key vault , you need to enable the setting in the Advanced policy section for the Key vault.

14. Select **Click to show advanced access policies**. Notice **Enable access to Azure Resource Manager for template deployment** is selected. This setting is another condition to make the Key Vault integration to work.

The screenshot shows the 'Access policies' page for a Key Vault named 'mykeyvault0920'. The left sidebar has a red box around the 'Access policies' item. The main area has several checkboxes:

- Click to hide advanced access policies
- Enable access to Azure Virtual Machines for deployment
- Enable access to Azure Resource Manager for template deployment (selected)
- Enable access to Azure Disk Encryption for volume encryption

Below the checkboxes is a 'Add new' button and a list entry for '<Your username> USER'.

Since this is clearly given in the documentation, all other options are invalid

For more information on using the Azure Key vault from Resource Manager templates, please visit the below URL

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-tutorial-use-key-vault>

Ask our Experts

Rate this Question?

View Queries

open ▾

Question 8

Unattempted

Domain :Design for identity and security

A team is planning on deploying Azure resources by using Resource Manager templates. The templates need to reference secrets that are stored in Azure Key vault. You need to ensure deployments can be made accordingly.

Which of the following would you use to restrict access to the secrets in the key vault?

- A. Access policies for the Key vault ✓
- B. An Azure policy
- C. Role Based access
- D. Advanced access policy for the Key vault

Explanation:

Answer – A

Since the question here is referring to restrict access to the secrets in the key vault, we have to work with "Access policies for the Key vault" reason RBAC controls only the management plane, where as access policies control the data plane.

Access model overview

Access to vaults takes place through two interfaces or planes. These planes are the management plane and the data plane.

- The *management plane* is where you manage Key Vault itself and it is the interface used to create and delete vaults. You can also read key vault properties and manage access policies.
- The *data plane* allows you to work with the data stored in a key vault. You can add, delete, and modify keys, secrets, and certificates.

For more information on accessing secrets from Resource Manager templates, please visit the below URL

<https://docs.microsoft.com/en-us/azure/key-vault/general/overview-security>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 9

Unattempted

Domain :Design for identity and security

A company has deployed an API using the API management service. They want to add an OAuth2 service as shown below



Add OAuth2 service

API Management service

* Display name

whizlabs



* Id i

whizlabs



Description

Authorization server description

* Client registration page URL

<http://whizlabs.com/register>



Authorization grant types

Authorization code

Implicit

Resource owner password

Client credentials

* Authorization endpoint URL

<https://login.microsoftonline.com/whizlabs.onmicrosoft.com/a...>



Support state parameter

Authorization request method

GET

POST

Which of the following is

the application/authentication type for which the authorization grant is being used for?

- A. For a background service

- B. For headless device authentication
- C. For a single page application
- D. For Web applications

Explanation:

Answer – D

An example is given in the Microsoft documentation which showcases registering 2 web applications along with the OAuth2 service.

Overview

Here is a quick overview of the steps:

1. Register an application (backend-app) in Azure AD to represent the API.
2. Register another application (client-app) in Azure AD to represent a client application that needs to call the API.
3. In Azure AD, grant permissions to allow the client-app to call the backend-app.
4. Configure the Developer Console to use OAuth 2.0 user authorization.
5. Add the **validate-jwt** policy to validate the OAuth token for every incoming request.

Since this is clearly showcased in the Microsoft documentation, all other options are invalid

For more information on the example itself, please visit the below URL

<https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 10

Unattempted

Domain :Design for identity and security

A company has deployed an API using the API management service. They want to add an OAuth2 service as shown below



Add OAuth2 service

API Management service

* Display name

whizlabs



* Id i

whizlabs



Description

Authorization server description

* Client registration page URL

http://whizlabs.com/register



Authorization grant types

Authorization code

Implicit

Resource owner password

Client credentials

* Authorization endpoint URL

https://login.microsoftonline.com/whizlabs.onmicrosoft.com/a..



Support state parameter

Authorization request method

GET

POST

In order to enable custom data in the grant flow, which of the following should be used to make this happen?

- A. Client Credentials

- B. Implicit
- C. Resource Owner password
- D. Support state parameter

Explanation:

Answer – D

The support state parameter gives a chance for the application to persist data between the user and the application server. Below is what is mentioned in the documentation for OAuth2

state (recommended)

The state parameter serves two functions. When the user is redirected back to your app, whatever value you include as the state will also be included in the redirect. This gives your app a chance to persist data between the user being directed to the authorization server and back again, such as using the state parameter as a session key. This may be used to indicate what action in the app to perform after authorization is complete, for example, indicating which of your app's pages to redirect to after authorization. This also serves as a CSRF protection mechanism. When the user is redirected back to your app, double check that the state value matches what you set it to originally. This will ensure an attacker can't intercept the authorization flow.

Since this is clearly mentioned in the OAuth2 documentation, all other options are invalid

For more information on authorization code for server-side apps, please visit the below URL

<https://www.oauth.com/oauth2-servers/server-side-apps/authorization-code/>

View Queries

open ▾

Question 11

Unattempted

Domain :Design for identity and security

A company named Whizlabs currently has an on-premise Active Directory Forest. They have recently setup an Azure AD tenant and also setup Azure AD Connect. They have currently procured Premium P1 licences. Which of the following features could result in reducing the operational overhead when it comes to managing the user's credentials?

- A. Self-service password reset 
- B. Access review
- C. Password writeback 
- D. Azure AD Privileged Identity Management policies

Explanation:

Answer – A and C

If users get locked or forget their password, you can use the self-service password reset with writeback option. This is also given in the Microsoft documentation. And these features are included as part of Premium P1 licences.

- Self-Service Password Reset/Change/Unlock with on-premises writeback
 - I am a **hybrid user** my on-premises Active Directory user account is synchronized with my Azure AD account using Azure AD Connect. I would like to change my password, have forgotten my password, or been locked out.
 - I would like to change my password or reset it to something I know, or unlock my account, **and** have that change synchronized back to on-premises Active Directory.
 - This functionality is included in Azure AD Premium P1 or P2, or Microsoft 365 Business.

Option B is incorrect since this is only when you want to conduct reviews for existing users.

Option D is incorrect since this requires Premium P2 licensing

For more information on self-service password reset, please visit the below URL

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-licensing>

[Ask our Experts](#)Rate this Question?  [View Queries](#)

open ▾

Question 12**Unattempted****Domain :Design a data platform solution**

A company is planning on migrating their on-premise Microsoft SQL servers to Azure. They need to have a solution in place to host their existing SQL Server Integration Services (SSIS) packages. Which of the following could be used for this purpose?

- A. Azure Data Catalog
- B. SQL Server Migration Assistant (SSMS)
- C. Data Migration Assistant
- D. Azure Data Factory 

Explanation:

Answer – D

This is given in the Microsoft documentation wherein you can use a component from Azure Data Factory for hosting the packages

Architecture of SSIS on Azure

The following table highlights the differences between SSIS on premises and SSIS on Azure.

The most significant difference is the separation of storage from runtime. Azure Data Factory hosts the runtime engine for SSIS packages on Azure. The runtime engine is called the Azure-SSIS Integration Runtime (Azure-SSIS IR). For more info, see [Azure-SSIS Integration Runtime](#).

Location	Storage	Runtime	Scalability
On premises	SQL Server	SSIS runtime hosted by SQL Server	SSIS Scale Out (in SQL Server 2017 and later)
On Azure	SQL Database or SQL Database Managed Instance	Azure-SSIS Integration Runtime, a component of Azure Data Factory	Custom solutions (in prior versions of SQL Server) Scaling options for the Azure-SSIS Integration Runtime

- Option A is incorrect since this is used to organize data sources in Azure
- Options B and C are incorrect since this is used to migrate data between SQL servers.
- For more information on hosting SSIS packages on Azure, please visit the below URL
 - <https://docs.microsoft.com/en-us/sql/integration-services/lift-shift/ssis-azure-lift-shift-ssis-packages-overview?view=sql-server-2017>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 13

Unattempted

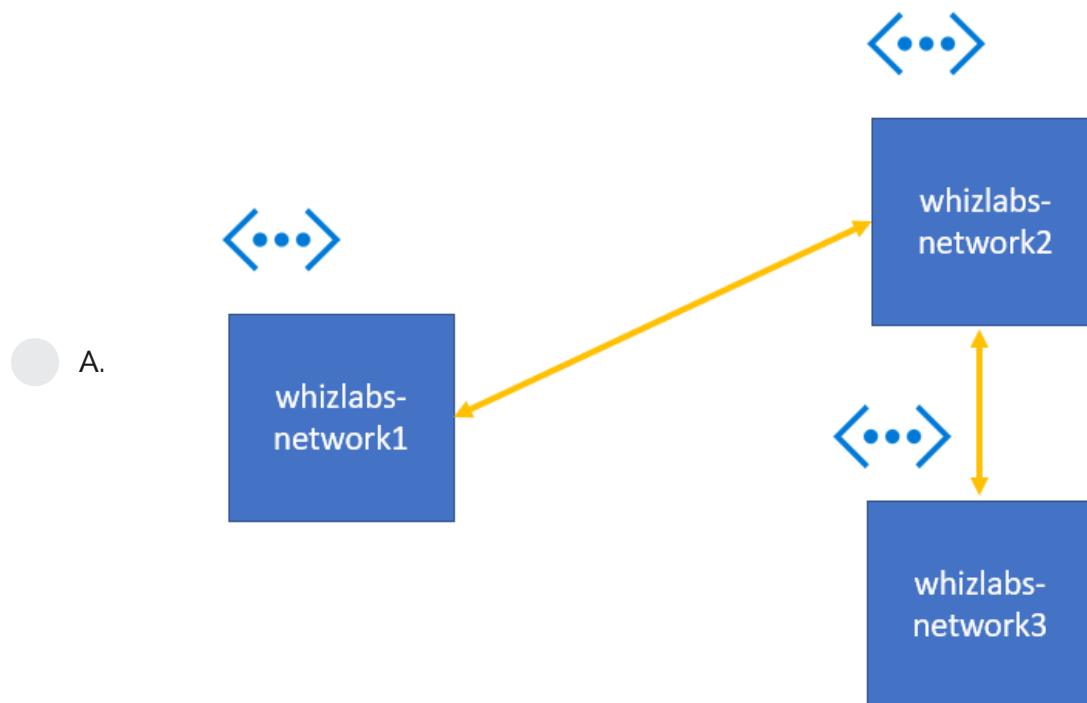
Domain :Design an infrastructure strategy

A company currently has the following networks defined in Azure

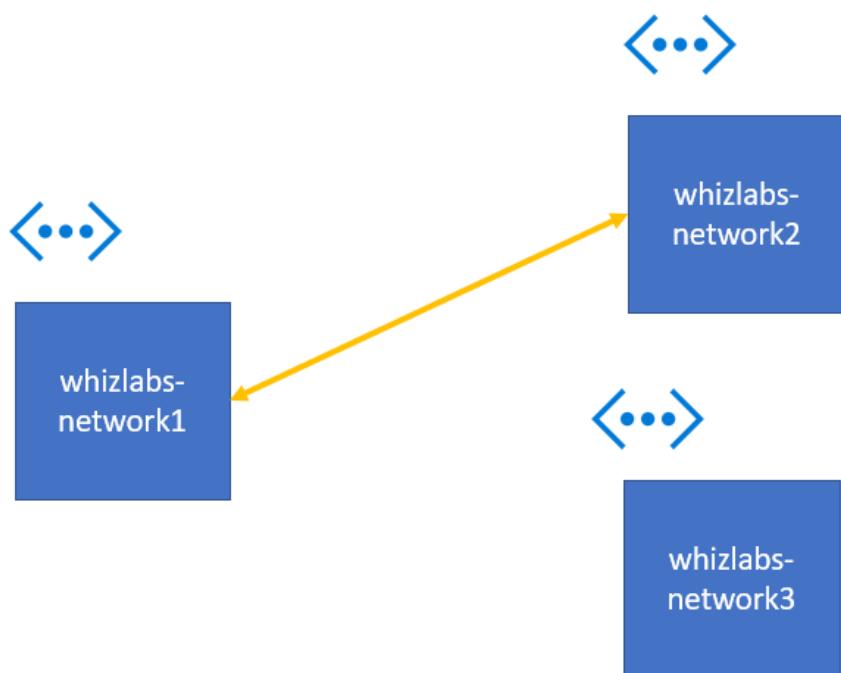
Virtual Network name
Subscription Name
Virtual Network Type
whizlabs-network1
subscriptionA
Classic
whizlabs-network2
subscriptionB
Resource Manager
whizlabs-network3
subscriptionC
Resource Manager

You have to ensure that resources in the virtual networks can communicate with each other. You have to reduce the administrative effort required for the implementation.

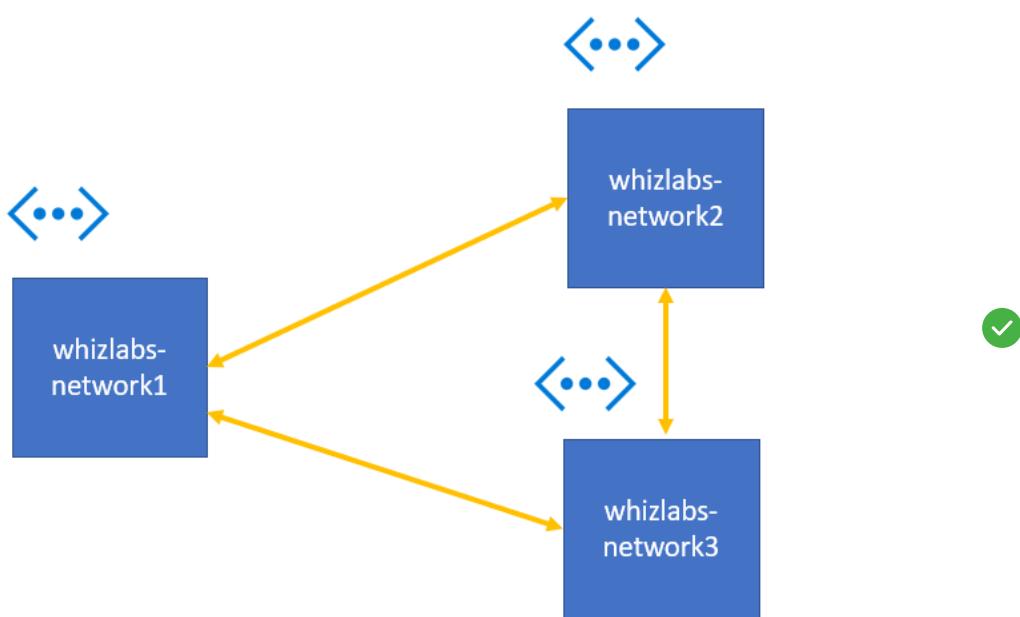
Which Virtual network topology would you recommend for this requirement?



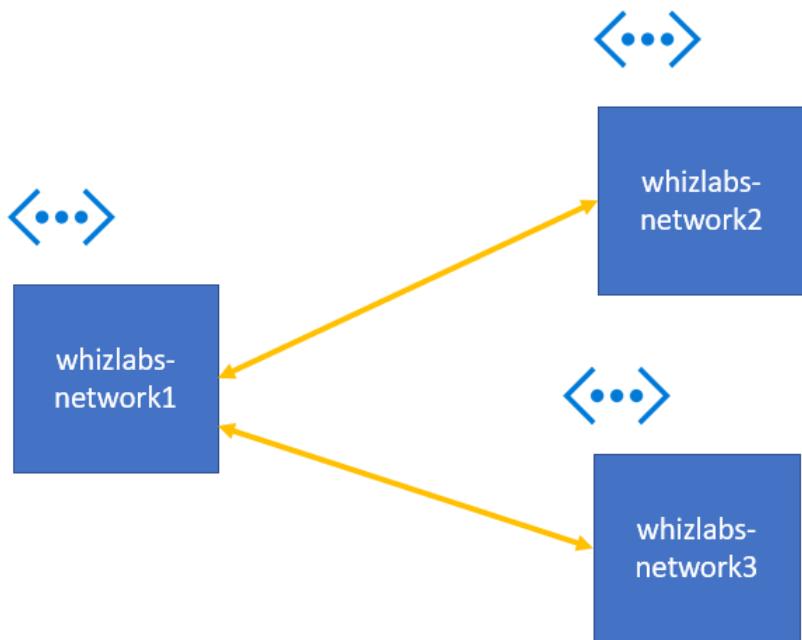
B.



C.



D.



Explanation:

Answer – C

You can create virtual network peering connections between Virtual networks in different subscriptions. You can also create virtual network peering connections between a Classic and Resource Manager Virtual Network. This is mentioned in the Microsoft documentation in the benefits for Virtual Network Peering.

The benefits of using virtual network peering, whether local or global, include:

- Network traffic between peered virtual networks is private. Traffic between the virtual networks is kept on the Microsoft backbone network. No public Internet, gateways, or encryption is required in the communication between the virtual networks.
- A low-latency, high-bandwidth connection between resources in different virtual networks.
- The ability for resources in one virtual network to communicate with resources in a different virtual network, once the virtual networks are peered.
- The ability to transfer data across Azure subscriptions, deployment models, and across Azure regions.
- The ability to peer virtual networks created through the Azure Resource Manager or to peer one virtual network created through Resource Manager to a virtual network created through the classic deployment model. To learn more about Azure deployment models, see [Understand Azure deployment models](#).
- No downtime to resources in either virtual network when creating the peering, or after the peering is created.

Option A is incorrect since there is no peering connection between whizlabs-network1 and whizlabs-network3

Option B is incorrect since there is no peering connection between whizlabs-network1 and whizlabs-network3. There is also no connection between whizlabs-network2 and whizlabs-network3

Option D is incorrect since there is no peering connection between whizlabs-network2 and whizlabs-network3

For more information on Virtual Network peering, please visit the below URL

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 14

Unattempted

Domain :Design a business continuity strategy

A company wants to deploy an application to Azure. The application has the below requirements

- Give the ability to install and provide access to the full .Net framework
- Allow administrative access to the operating system
- Provide a level of redundancy if an Azure region fails

You decide to deploy 2 Azure Virtual Machines in 2 separate regions. And then you create a Traffic Manager Profile

Does this solution meet the requirement?

- A. Yes 
- B. No

Explanation:

Answer - A

Yes, this will meet all the requirements. Since you are using Azure Virtual Machines, IT administrators can get the required access. You can also then get the required access to the underlying software including the .Net framework.

Using a Traffic Manager profile along with the failover routing policy can ensure the requirement for redundancy is fulfilled.

For more information on Azure Traffic Manager, please visit the below URL

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

Ask our Experts

Rate this Question?  

View Queries

open 

Question 15

Unattempted

Domain :Design a business continuity strategy

A company wants to deploy an application to Azure. The application has the below requirements

- Give the ability to install and provide access to the full .Net framework
- Allow administrative access to the operating system
- Provide a level of redundancy if an Azure region fails

You decide to deploy a web app using the Isolated App Service plan

Does this solution meet the requirement?

- A. Yes 
- B. No 

Explanation:

Answer - B

The Isolated App Service Plan provides a dedicated infrastructure, but will not fulfil the key requirements

For more information on the Isolated App Service Plan, please visit the below URL

<https://azure.microsoft.com/en-us/blog/announcing-app-service-isolated-more-power-scale-and-ease-of-use/>

[Ask our Experts](#)

Rate this Question?  

View Queries

[open ▾](#)

Question 16

Unattempted

Domain :Design a business continuity strategy

A company wants to deploy an application to Azure. The application has the below requirements

- Give the ability to install and provide access to the full .Net framework
- Allow administrative access to the operating system
- Provide a level of redundancy if an Azure region fails

You decide to deploy 2 Azure Virtual Machines in 2 separate regions. And then you create an Azure Load balancer

Does this solution meet the requirement?

A. Yes

B. No 

Explanation:

Answer – B

A Load balancer can't distribute traffic across regions and hence this solution will not meet the requirement for redundancy.

For more information on the Azure Load Balancer, please visit the below URL

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

[View Queries](#)

open ▾

Question 17**Unattempted**

Domain :Design a data platform solution

[View Case Study](#)

Which of the following should be recommended for the database backups?

- A. Long term retention for the database 
- B. Use Azure Site Recovery for the database
- C. Configure geo-replication for the database
- D. Configure Azure backup for the database

Explanation:

Answer – A

You can use the long-term retention feature as mentioned in the Microsoft documentation below

Store Azure SQL Database backups for up to 10 years

04/23/2019 • 3 minutes to read • Contributors  all

Many applications have regulatory, compliance, or other business purposes that require you to retain database backups beyond the 7-35 days provided by Azure SQL Database [automatic backups](#). By using the long-term retention (LTR) feature, you can store specified SQL database full backups in [RA-GRS](#) blob storage for up to 10 years. You can then restore any backup as a new database.

Since this is clearly mentioned in the Microsoft documentation, all other options are incorrect

For more information on database long term retention, please visit the below URL

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

View Queries

open ▾

Question 18

Unattempted

Domain :Design a data platform solution

View Case Study

You need to recommend a solution for encrypting data at rest for the database. Which of the following would you recommend?

- A. Transparent data encryption 
- B. Always Encrypted
- C. Azure storage encryption
- D. SSL certificates

Explanation:

Correct Answer: Option A : Transparent Data encryption

The requirement is encrypt the data at rest for

The data store for the transactional query system will be move from
Azure Table storage to a CosmosDB account ?

- Option A: Transparent Data encryption
- Please refer to <https://docs.microsoft.com/en-us/azure/sql-database/transparent-data-encryption-azure-sql#manage-transparent-data-encryption-by-using-transact-sql>

This encryption is for data at Rest but can be managed by T-SQL

Manage transparent data encryption by using Transact-SQL

Connect to the database by using a login that is an administrator or member of the **dbmanager** role in the master database.

[ALTER DATABASE \(Azure SQL Database\)](#)

`SET ENCRYPTION ON/OFF` encrypts or decrypts a database

[sys.dm_database_encryption_keys](#)

Returns information about the encryption state of a database and its associated database encryption keys

sys.dm_pdw_nodes_database_encryption_keys

Returns information about the encryption state of each data warehouse node and its associated database encryption keys

You can't switch the transparent data encryption protector to a key from Key Vault by using Transact-SQL. Use PowerShell or the Azure portal.

- Option B: Always Encrypted

This is done on Column/Field of a table. All data in a particular field/column of a table within a database is encrypted.

So this is not the correct solution

- Option C: Azure Data Storage Encryption

This encryption is for data at Rest but can not be managed by T-SQL, hence wrong answer

- Option D: SSL Certificate

SSL is not for encryption of data at Rest and hence the wrong answer

Ask our Experts

Rate this Question?

View Queries

open ▾

Question 19

Unattempted

Domain :Design for identity and security

View Case Study

Azure AD Connect will be installed to implement the synchronize the identities between Azure AD and the on-premise Active Directory. Which of the following would need to be configured in Azure AD Connect?

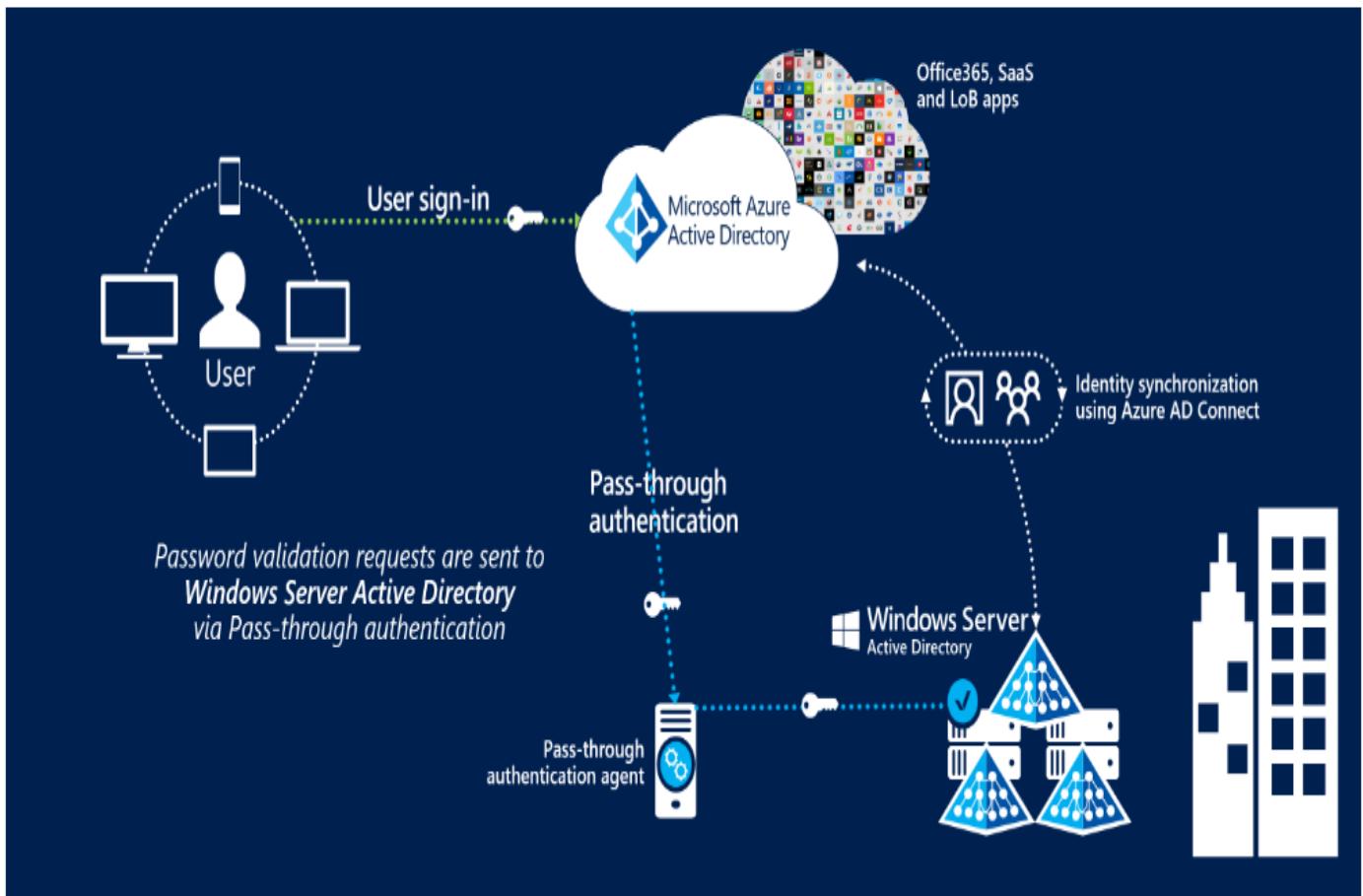
- A. Federation with AD FS
- B. Pass-through Authentication
- C. Federation with AD
- D. Password hash synchronization

Explanation:

Answer – B

A key requirement for the case study is to ensure that the identities are authenticated via the on-premise AD, and this is done with Pass-through Authentication. The Microsoft documentation mentions the following.

This feature is an alternative to [Azure AD Password Hash Synchronization](#), which provides the same benefit of cloud authentication to organizations. However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead. Review [this guide](#) for a comparison of the various Azure AD sign-in methods and how to choose the right sign-in method for your organization.



Options A and C are incorrect since you don't need to do a federation

Option D is incorrect since you need to implement Pass-through Authentication to ensure that identities are authenticated by the on-premise AD

Ask our Experts

Rate this Question?

[View Queries](#)

open ▾

Question 20

Unattempted

[View Case Study](#)

You need to recommend an availability solution for the Web tier of the Financial Processing System application when it is moved to Azure. Which of the following would you recommend?

- A. Standard Load Balancer
- B. Traffic Manager
- C. Basic Load Balancer
- D. Application Gateway

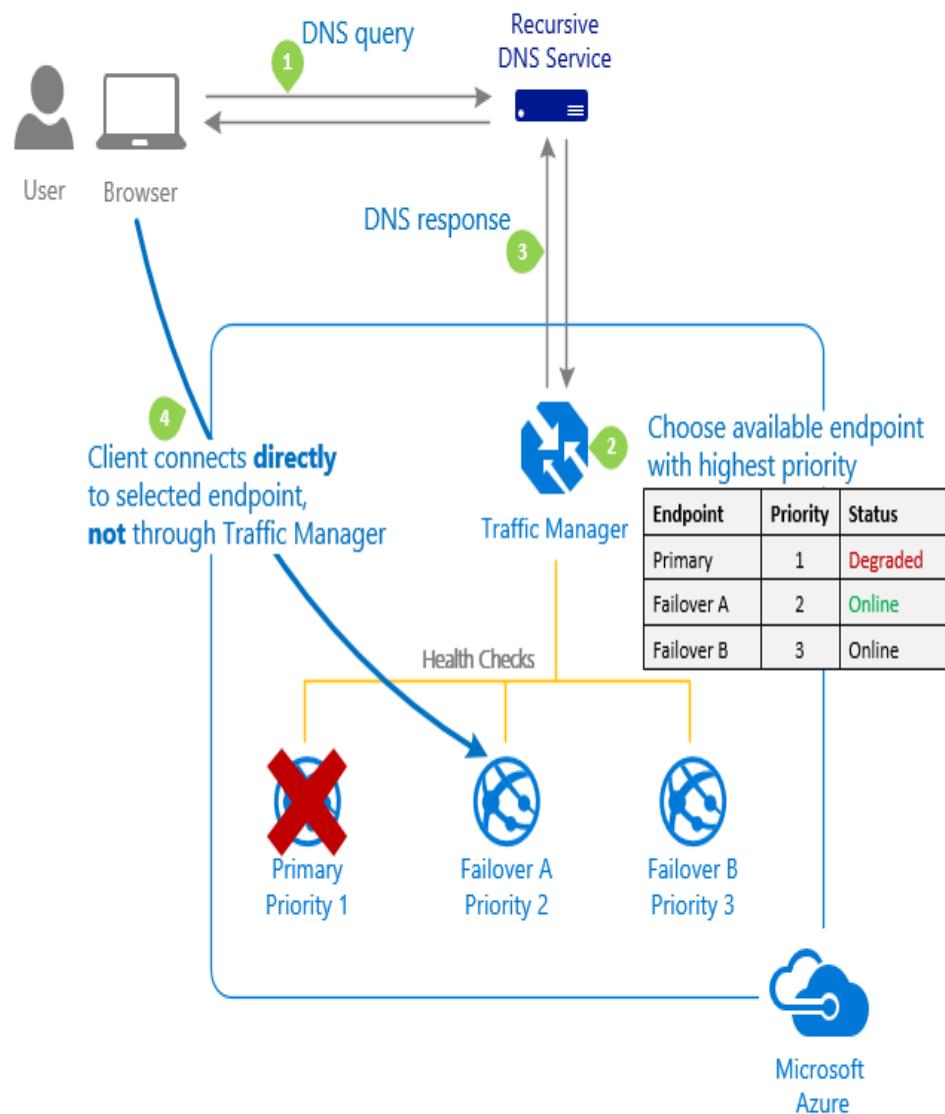
Explanation:

Answer – B

The case study calls for infrastructure availability if a region fails. This can be done with the Traffic Manager. For this you can use the priority routing method as stated below in the Microsoft documentation

Priority traffic-routing method

Often an organization wants to provide reliability for its services by deploying one or more backup services in case their primary service goes down. The 'Priority' traffic-routing method allows Azure customers to easily implement this failover pattern.



The Traffic Manager profile contains a prioritized list of service endpoints. By default, Traffic Manager sends all traffic to the primary (highest-priority) endpoint. If the primary endpoint is not available, Traffic Manager routes the traffic to the second endpoint. If both the primary and secondary endpoints are not available, the traffic goes to the third, and so on. Availability of the endpoint is based on the configured status (enabled or disabled) and the ongoing endpoint monitoring.

The other options are incorrect since they cannot be used to perform disaster recovery if a region fails.

For more information on the Traffic Manager, please visit the below URL

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

Ask our Experts

Rate this Question?

[View Case Study](#)

You need to meet the following requirement of the case study

"Collect windows security logs from the Middle tier and retain the logs for 2 years"

Which of the following would you use for this purpose?

- A. Azure Notification Hubs
- B. Azure Diagnostics agent
- C. Azure Event Hubs
- D. Azure Log Analytics agent

Explanation:

Answer – D

You can use Log Analytics to get event data from Virtual Machines. The Log Analytics workspace can also retain data indefinitely. The Microsoft documentation mentions the following

Collect event and performance data

Log Analytics can collect events from the Windows event logs or Linux Syslog and performance counters that you specify for longer term analysis and reporting, and take action when a particular condition is detected. Follow these steps to configure collection of events from the Windows system log and Linux Syslog, and several common performance counters to start with.

Option A is incorrect since this is only used for notifications

Option B is partially correct, but due to the aspect of the data being collected and the data retention required, you should choose Log Analytics

Option C is incorrect since this is used as a Big data ingestion service

For more information on collecting performance data, please visit the below URL

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm>

[Ask our Experts](#)

Rate this Question?  

View Case Study

You need to recommend the right solution for configuring Multi-Factor Authentication in Azure. Which of the following would you recommend for licensing in Azure?

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

Explanation:

Answer – D

To implement conditional access policies, you can opt for Premium P1 licences, but in our business scenario since we need to raise MFA request for suspicious action, and for this we need to work with AD Identity Protection Service, and this is part of Premium licences P2 licences. The Microsoft documentation mentions the following

License requirements for using conditional access

Using conditional access requires an Azure AD Premium license. To find the right license for your requirements, see [Comparing generally available features of the Free, Basic, and Premium editions](#).

Options A and B are incorrect since these editions don't give access to conditional access policies

Option C is incorrect since we need to work AD Identity Protection Service.

For more information on conditional access, please visit the below URL

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

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

Ask our Experts

Rate this Question?  

[View Case Study](#)

You need to recommend the right solution for configuring Multi-Factor Authentication in Azure. How would you address the access control for the sign-in risk policy?

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

Explanation:

Answer – A

Since the case study says to ensure that conditional access request for MFA, but still allow access we need to choose Option A. In the Grant section, ensure to choose the option of "Require multi-factor authentication"

[Info](#) [Delete](#)

* Name

whizlabpolicy

Assignments

Users and groups [i](#) >

Specific users included

Cloud apps or actions [i](#) >

1 app included

Conditions [i](#) >

0 conditions selected

Access controls

Grant [i](#) >

1 control selected

Session [i](#) >

0 controls selected

Enable policy

[On](#) [Off](#)[Save](#)

Select the controls to be enforced.

 Block access Grant access [Require multi-factor authentication](#) [i](#) [Require device to be marked as compliant](#) [i](#) [Require Hybrid Azure AD joined device](#) [i](#) [Require approved client app](#) [i](#)
[See list of approved client apps](#) [Require app protection policy \(preview\)](#) [i](#)
[See list of policy protected client apps](#)

For multiple controls

 [Require all the selected controls](#) [Require one of the selected controls](#)[Ask our Experts](#)Rate this Question?  

Domain :Design a business continuity strategy

View Case Study

You have to recommend a solution for catering to the high availability requirements for the middle tier of the Financial Processing system. Which of the following would you implement?

- A. The Premium App Service Plan
- B. The Isolated App Service Plan
- C. Use of Availability sets
- D. Use of Availability Zones

Explanation:

Answer – D

Since the requirement is for availability of middle tier, and working with Availability Zones is the correct option. By using this, even if one zone gets failed, availability of other zones is still available and the application is working. In this business scenario, we should ignore the SLA mentioned, reason SLA for AZ is 99.99%.

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

Ask our ExpertsRate this Question?  **View Queries**

open ▾

Domain :Design for identity and security

View Case Study

You need to manage secure access between the .Net service and the CosmosDB account. What would the CosmosDB account be used for in such a scenario

- 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

Explanation:

Answer - B

The CosmosDB account will be used to create the users. The following code snippet from the Microsoft documentation mentions on how you can create CosmosDB account users

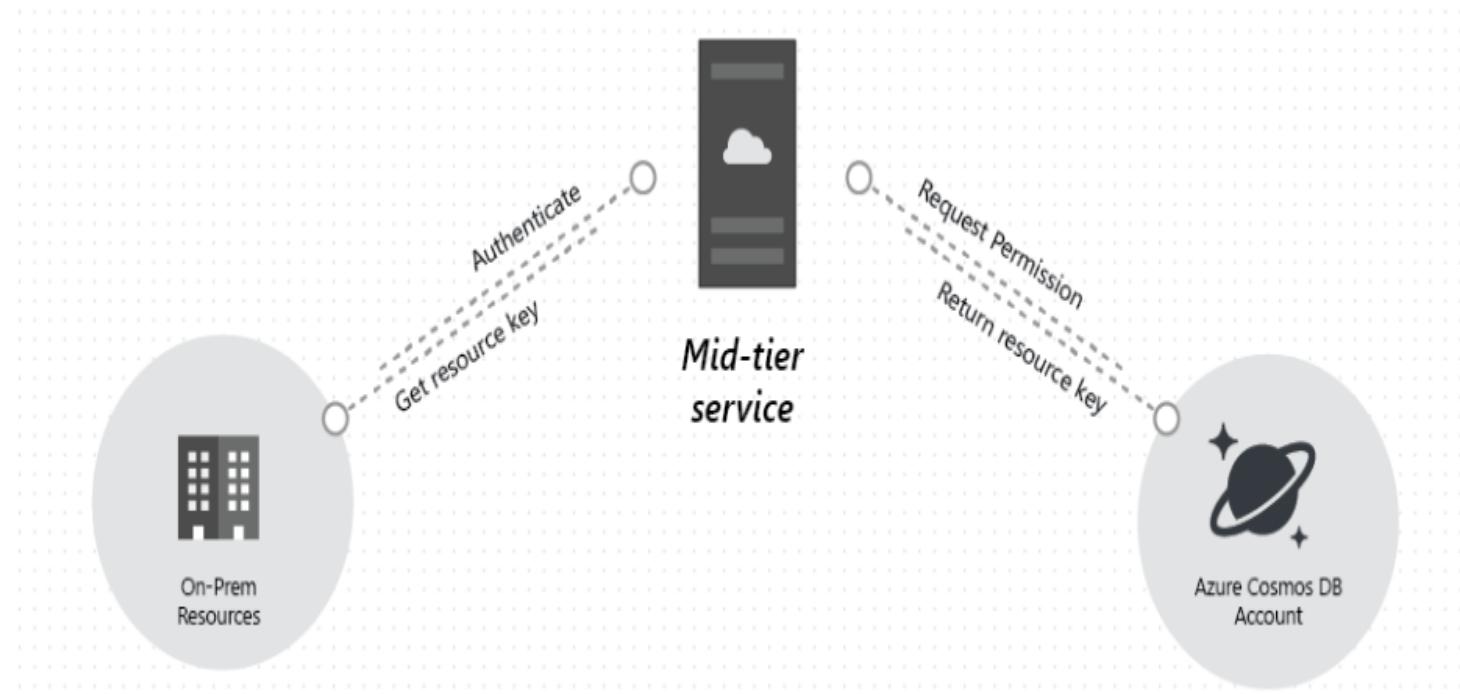
Users

Cosmos DB users are associated with a Cosmos DB database. Each database can contain zero or more Cosmos DB users. The following code sample shows how to create a Cosmos DB user resource.

```
C#  
  
//Create a user.  
User docUser = new User  
{  
    Id = "mobileuser"  
};  
  
docUser = await client.CreateUserAsync(UriFactory.CreateDatabaseUri("db"), docUser);  
  
Copy
```

Next, if the CosmosDB account needs to be accessed,

CosmosDB would request for the right resource tokens to ensure that access could be granted. The Microsoft documentation also mentions an example workflow for a service that would make use of request tokens for CosmosDB



Since this is clearly given in the documentation, all other options are incorrect

For more information on secure access to CosmosDB, please visit the below URL

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

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 26

Unattempted

Domain :Design for identity and security

View Case Study

You need to manage secure access between the .Net service and the CosmosDB account. What would the .Net service be used for in such a scenario?

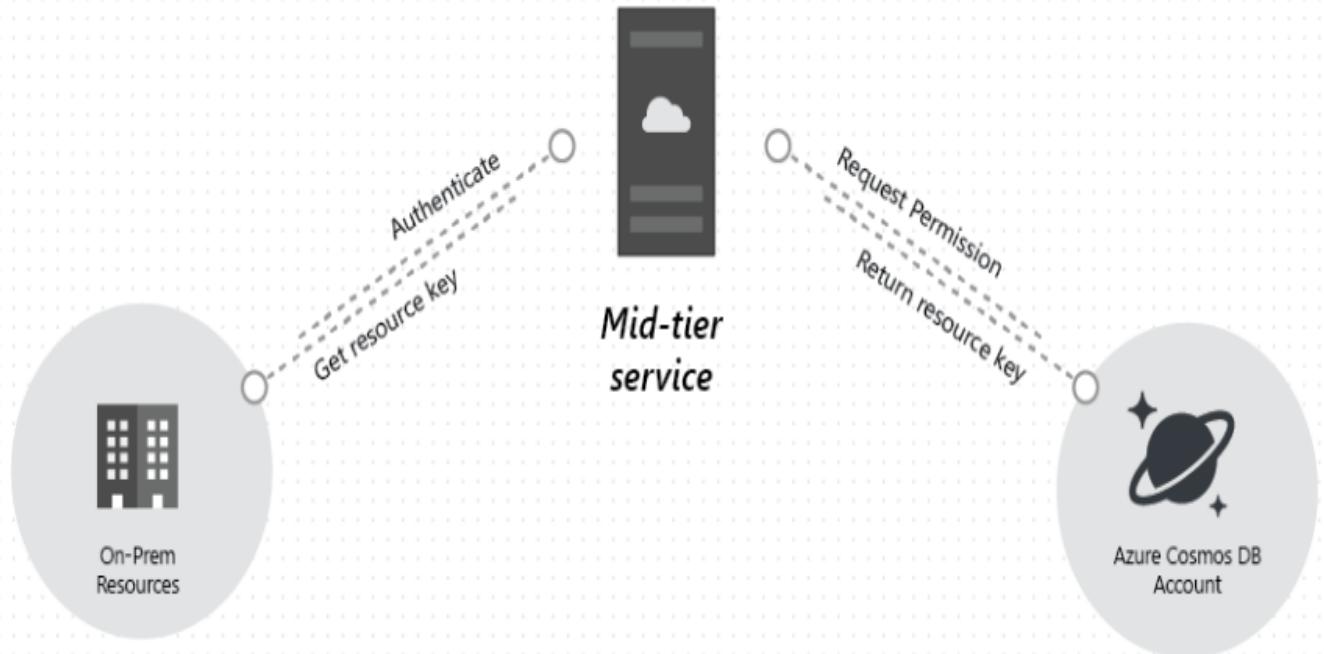
- A. Create users and generate resource tokens
- B. Create users and request resource tokens
- C. Generate resource tokens and perform authentication
- D. Request resource tokens and perform authentication

Explanation:

Answer – C

The .Net service will be used to generate the resource tokens and perform the required authentication.

The Microsoft documentation also mentions an example workflow for a service that would make use of request tokens for CosmosDB



Since this is clearly given in the documentation, all other options are incorrect

For more information on secure access to CosmosDB, please visit the below URL

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

Ask our Experts

Rate this Question?

View Queries

open ▾

Question 27

Unattempted

Domain :Design a business continuity strategy

View Case Study

You have to recommend a strategy for the compute solution for the Financial Processing System. Which of the following would you recommend?

- A. Azure Kubernetes Service
- B. Virtual machine scale sets
- C. Availability sets
- D. App Service Environments

Explanation:

Answer – B

Since we need to cater to the below requirement of the case study

"The number of instances assigned to the front and middle tiers should be adjusted automatically based on the CPU utilization"

We have to use Virtual Machine scale sets for our compute solution. The Microsoft documentation mentions the following

What are virtual machine scale sets?

03/27/2018 • 3 minutes to read • Contributors 

Azure virtual machine scale sets let you create and manage a group of identical, load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs. With virtual machine scale sets, you can build large-scale services for areas such as compute, big data, and container workloads.

Option A is incorrect since there is no mention of orchestrating docker containers for the application

Option C is incorrect since this is used for achieving high availability of the solution

Option D is incorrect since this is used for the Azure Web App service

For more information on virtual machine scale sets, please visit the below URL

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

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 28

Unattempted

Domain :Design an infrastructure strategy

A company has an application running as part of Azure Web Apps. A database is being hosted in a Virtual Network. There is a requirement to ensure that the web app can access the database without the need of exposing a public endpoint.

You decide to implement Web jobs for the Azure Web App

Does this meet the requirement?

A. Yes

B. No 

Explanation:

Answer – B

The Web jobs feature is used to run background tasks and hence cannot be used for this requirement

For more information on Web jobs, please visit the below URL

<https://docs.microsoft.com/en-us/azure/app-service/webjobs-create>

[Ask our Experts](#)

Rate this Question?  

[View Queries](#)

open ▾

Question 29

Unattempted

Domain :Design an infrastructure strategy

A company has an application running as part of Azure We Apps. A database is being hosted in a Azure SQL. There is a requirement to ensure that the web app can access the database without the need of exposing a public endpoint.

You decide to implement Hybrid connections for the Azure Web App

Does this meet the requirement?

A. Yes

B. No

Explanation:

Answer – B

The Hybrid connection is normally used to connect to a single TCP host and port combination. Since Azure SQL does not provide an IP address or Port number, it will not work.

For more information on App Service Hybrid connections, please visit the below URL

<https://docs.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections>

[Ask our Experts](#)

Rate this Question?  

[View Queries](#)

open ▾

Domain :Design an infrastructure strategy

A company has an application running as part of Azure We Apps. A database is being hosted in a Virtual Network. There is a requirement to ensure that the web app can access the database without the need of exposing a public endpoint.

You decide to implement VNET Integration for the Azure Web App

Does this meet the requirement?

A. Yes 

B. No

Explanation:

Answer – A

This is the ideal solution. The Microsoft documentation mentions the following

VNet Integration is often used to enable access from apps to databases and web services running in your VNet. With VNet Integration, you don't need to expose a public endpoint for applications on your VM but can use the private non-internet routable addresses instead.

The VNet Integration feature:

- requires a Standard, Premium, or PremiumV2 pricing plan
- works with Classic or Resource Manager VNet
- supports TCP and UDP
- works with Web, Mobile, API apps, and Function apps
- enables an app to connect to only 1 VNet at a time
- enables up to five VNets to be integrated with in an App Service Plan
- allows the same VNet to be used by multiple apps in an App Service Plan
- requires a Virtual Network Gateway that is configured with Point to Site VPN
- supports a 99.9% SLA due to the SLA on the gateway

For more information on integrating an app using VNET integration, please visit the below URL

- <https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet>

Ask our Experts

Rate this Question?  

Question 31

Unattempted

Domain :Design an infrastructure strategy

A company is planning on deploying the following set of resources to Azure

- A set of virtual machines hosting an internal application
- An Azure Web app used for hosting a production-based application

The company has the following monitoring requirements.

- Understand the failures and performance issues for the application hosted in the Azure Web App service
- The IT Admin staff should be notified if any infrastructure level changes are made to the Virtual Machine
- Be informed if there are any issues with the underlying Azure services.

Which of the following would be best suited to fulfil the requirement?

"Understand the failures and performance issues for the application hosted in the Azure Web App service"

- A. Azure Log Analytics
- B. Application Insights
- C. Azure AD Connect health
- D. Microsoft System Center

Explanation:

Answer – B

You can use Application Insights for this purpose. This is also given in the Microsoft documentation

Deep diagnostics for web apps and services with Application Insights

12/21/2018 • 10 minutes to read • Contributors 

Why do I need Application Insights?

Application Insights monitors your running web app. It tells you about failures and performance issues, and helps you analyze how customers use your app. It works for apps running on many platforms (ASP.NET, Java EE, Node.js, ...) and is hosted either in the Cloud or on-premises.

Since this is clearly given in the Microsoft documentation, all other options are incorrect

For more information on Application Insights, please visit the below URL

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/devops>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 32

Unattempted

Domain :Design an infrastructure strategy

A company is planning on deploying the following set of resources to Azure

- A set of virtual machines hosting an internal application
- An Azure Web app used for hosting a production-based application

The company has the following monitoring requirements.

- Understand the failures and performance issues for the application hosted in the Azure Web App service
- The IT Admin staff should be notified if any infrastructure level changes are made to the Virtual Machine
- Be informed if there are any issues with the underlying Azure services.

Which of the following would be best suited to fulfil the requirement?

"The IT Admin staff should be notified if any infrastructure level changes are made to the Virtual Machine"

- A. Azure Log Analytics
- B. Application Insights
- C. Azure Monitor Alerts 
- D. Azure Service Health

Explanation:

Answer – C

This can be done with Azure Monitor alerts. The following is mentioned in the Microsoft documentation.

Create, view, and manage activity log alerts using Azure Monitor

09/15/2018 • 6 minutes to read • Contributors  all

Overview

Activity log alerts are the alerts that get activated when a new activity log event occurs that matches the conditions specified in the alert.

These alerts are for Azure resources, can be created by using an Azure Resource Manager template. They also can be created, updated, or deleted in the Azure portal. Typically, you create activity log alerts to receive notifications when specific changes occur on resources in your Azure subscription, often scoped to particular resource groups or resource. For example, you might want to be notified when any virtual machine in (sample resource group) `myProductionResourceGroup` is deleted, or you might want to get notified if any new roles are assigned to a user in your subscription.

Since this is clearly given in the Microsoft documentation, all other options are incorrect

For more information on Activity Log alerts, please visit the below URL

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 33

Unattempted

Domain :Design an infrastructure strategy

A company is planning on deploying the following set of resources to Azure

- A set of virtual machines hosting an internal application
- An Azure Web app used for hosting a production-based application

The company has the following monitoring requirements.

- Understand the failures and performance issues for the application hosted in the Azure Web App service
- The IT Admin staff should be notified if any infrastructure level changes are made to the Virtual Machine
- Be informed if there are any issues with the underlying Azure services.

Which of the following would be best suited to fulfil the requirement?

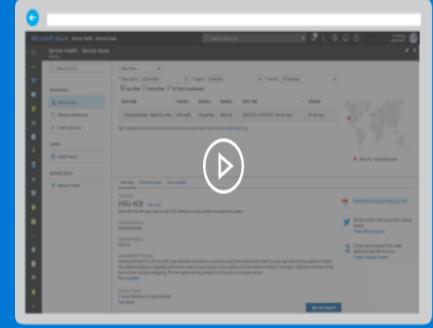
"Be informed if there are any issues with the underlying Azure services."

- A. Azure Log Analytics
- B. Application Insights
- C. Azure Monitor Alerts
- D. Azure Service Health

Explanation:

Answer – D

Azure Service Health is the service that should be used. The following is mentioned in the Microsoft documentation.



Azure Service Health provides personalized alerts and guidance when Azure service issues affect you. It can notify you, help you understand the impact of issues, and keep you updated as the issue resolves. It can also help you prepare for planned maintenance and changes that could affect the availability of your resources.



Access a personalised dashboard

Find timely information about service issues, planned maintenance, and health advisories for your resources directly from the Azure portal, and pin a filtered view that helps you focus on what's important.



Set up targeted notifications

Azure Service Health integrates into Azure Monitor to alert you and your teams via email, text message and webhook notification when your business-critical resources are affected.



Receive guidance and support

When an Azure issue affects your resources, Service Health helps you diagnose it and get support. You'll receive updates on how Azure is fixing the issue until everything is resolved.



Share details and updates easily

Get a link for the issue to use in your problem management system, and download a PDF summary of the issue to share with people who don't have access to the Azure portal.

Since this is clearly given in the Microsoft documentation, all other options are incorrect

For more information on Azure Service Health, please visit the below URL

<https://azure.microsoft.com/en-gb/features/service-health/>

Ask our Experts

Rate this Question?

View Queries

open

Domain :Design a data platform solution

A company is going to be deploying an Azure SQL Database instance to the Central US region. They have the following requirements when it comes to the security for the database instance

- Only select workstations with static Public IP addresses should be allowed to connect and perform administration on the database
- An Application hosted in a Virtual Network on a Virtual machine would need to interact with the Azure SQL database

A function is implemented which hides the Social Security Numbers column in the Person table in the database

Which of the following would be best suited to fulfil the requirement?

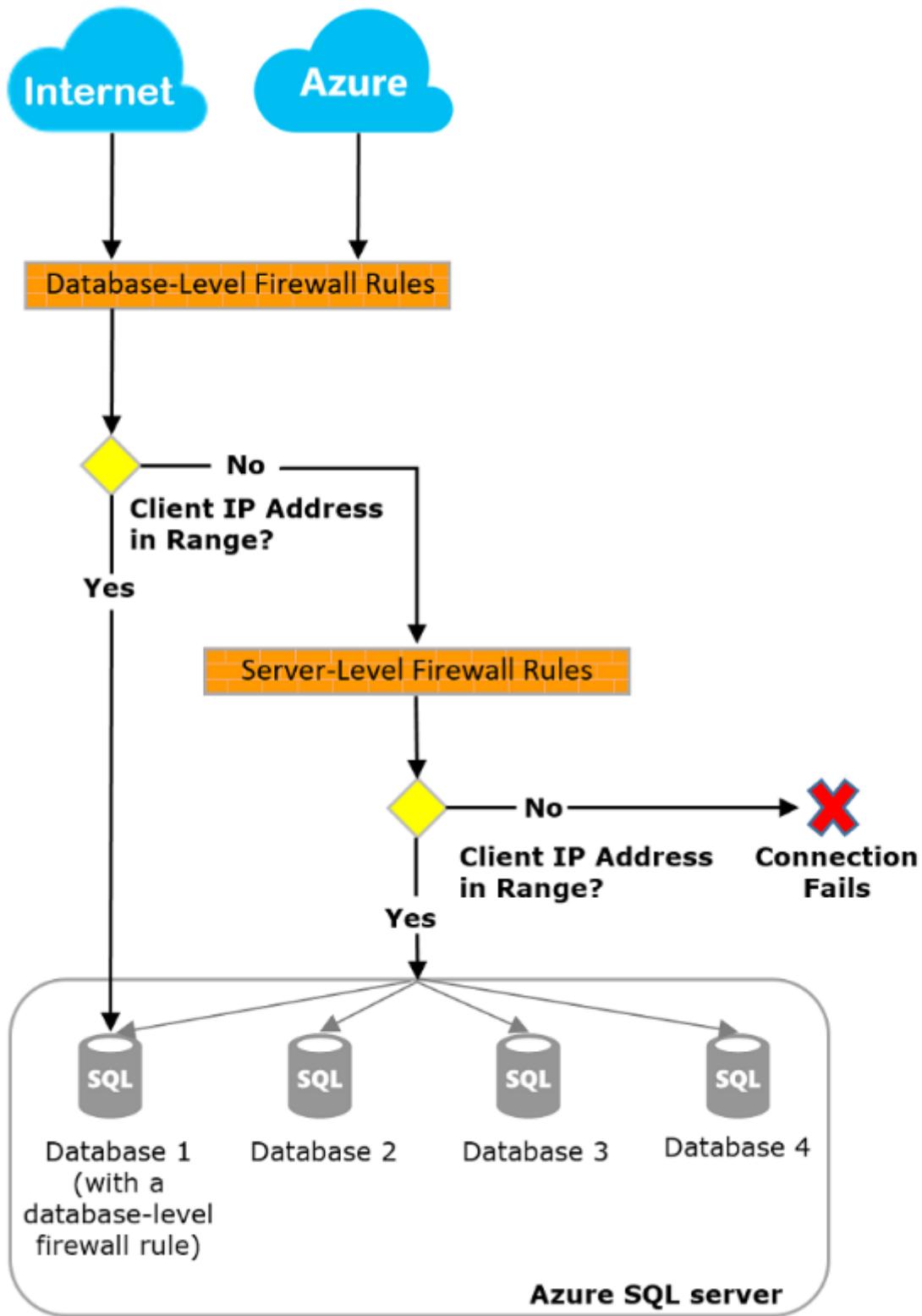
"Only select workstations with static Public IP addresses should be allowed to connect and perform administration on the database"

- A. Azure Network Watcher
- B. Server Level IP Firewall rules
- C. Network Security Groups
- D. Application Security Groups

Explanation:

Answer - B

You can use as shown in the Microsoft documentation below



- **Server-level IP firewall rules:**

These rules enable clients to access your entire Azure SQL server, that is, all the databases within the same SQL Database server. These rules are stored in the **master** database. Server-level IP firewall rules can be configured by using the portal or by using Transact-SQL statements. To create server-level IP firewall rules using the Azure portal or PowerShell, you must be the subscription owner or a subscription contributor. To create a server-level IP firewall rule using Transact-SQL, you must connect to the SQL Database instance as the server-level principal login or the Azure Active Directory administrator (which means that a server-level IP firewall rule must first be created by a user with Azure-level permissions).

Since this is clearly given in the Microsoft documentation, all other options are incorrect

For more information on configuring the firewall for Azure SQL database, please visit the below URL

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-firewall-configure>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 35

Unattempted

Domain :Design a data platform solution

A company is going to be deploying an Azure SQL Database instance to the Central US region. They have the following requirements when it comes to the security for the database instance

- Only select workstations with static Public IP addresses should be allowed to connect and perform administration on the database
- An Application hosted in a Virtual Network on a Virtual machine would need to interact with the Azure SQL database

A function is implemented which hides the Social Security Numbers column in the Person table in the database

Which of the following would be best suited to fulfil the requirement?

"An Application hosted in a Virtual Network on a Virtual machine would need to interact with the Azure SQL database securely"

- A. Azure Network Watcher
- B. Server Level IP Firewall rules
- C. Virtual Network Service Endpoints 
- D. Virtual Network peering

Explanation:

Answer – C

By using Virtual Network Service Endpoints, you can ensure that traffic from the Virtual Network can reach the Azure SQL database via the Azure Backbone network. The Microsoft documentation mentions the following

Virtual Network Service Endpoints

08/15/2018 • 10 minutes to read • Contributors  all

Virtual Network (VNet) service endpoints extend your virtual network private address space and the identity of your VNet to the Azure services, over a direct connection. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Traffic from your VNet to the Azure service always remains on the Microsoft Azure backbone network.

This feature is available for the following Azure services and regions:

Generally available

- [Azure Storage](#): Generally available in all Azure regions.
- [Azure SQL Database](#): Generally available in all Azure regions.
- [Azure SQL Data Warehouse](#): Generally available in all Azure regions.
- [Azure Database for PostgreSQL server](#): Generally available in Azure regions where database service is available.
- [Azure Database for MySQL server](#): Generally available in Azure regions where database service is available.
- [Azure Database for MariaDB](#): Generally available in Azure regions where database service is available.
- [Azure Cosmos DB](#): Generally available in all Azure regions.
- [Azure Key Vault](#): Generally available in all Azure regions.
- [Azure Service Bus](#): Generally available in all Azure regions.
- [Azure Event Hubs](#): Generally available in all Azure regions.
- [Azure Data Lake Store Gen 1](#): Generally available in all Azure regions where ADLS Gen1 is available.

Since this is clearly given in the Microsoft documentation, all other options are incorrect

For more information on virtual network service endpoints, please visit the below URL

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

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 36

Unattempted

Domain :Design a data platform solution

A company is going to be deploying an Azure SQL Database instance to the Central US region. They have the following requirements when it comes to the security for the database instance

- Only select workstations with static Public IP addresses should be allowed to connect and perform administration on the database

- An Application hosted in a Virtual Network on a Virtual machine would need to interact with the Azure SQL database
- A function is implemented which hides the Social Security Numbers column in the Person table in the database

Which of the following would be best suited to fulfil the requirement “A function is implemented which hides the Social Security Numbers column in the Person table in the database”?

- A. Server Level IP firewall
- B. Dynamic Data masking
- C. Azure AD Authentication
- D. Managed Service Identity

Explanation:

Answer – B

This can be managed by using Dynamic Data masking. The Microsoft documentation mentions the following

SQL Database dynamic data masking

03/04/2019 • 3 minutes to read • Contributors  all

SQL Database dynamic data masking limits sensitive data exposure by masking it to non-privileged users.

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

For example, a service representative at a call center may identify callers by several digits of their credit card number, but those data items should not be fully exposed to the service representative. A masking rule can be defined that masks all but the last four digits of any credit card number in the result set of any query. As another example, an appropriate data mask can be defined to protect personally identifiable information (PII) data, so that a developer can query production environments for troubleshooting purposes without violating compliance regulations.

Since this is clearly given in the Microsoft documentation, all other options are incorrect

For more information on dynamic data masking in SQL database, please visit the below URL

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-dynamic-data-masking-get-started>

Ask our Experts

Rate this Question?  

Question 37

Unattempted

Domain :Design an infrastructure strategy

A company is planning on hosting a set of servers in Azure. Some of these servers will run SQL Server 2016. These servers will be deployed to different data centers in the same Azure region. These will be part of an Always On availability group

The data on the servers will be backed up by using the SQL IaaS Agent Extension

Below are the key requirements for the storage for the different components of the Virtual Machine

- Operating System - Speed and availability for the storage priority
- Database and logs - Speed and availability for the storage priority
- Backups - This should use the lowest cost option for storage

You have to decide what is the ideal storage requirement for each component

Which of the following would you implement for the Operating System?

- A. Geo redundant storage account
- B. Premium managed disk
- C. Standard managed disk
- D. Read Access Geo redundant storage account

Explanation:

Answer – B

Make use of premium storage for high performance. Below is what the Microsoft documentation mentions

High-performance Premium Storage and managed disks for VMs

03/30/2018 • 22 minutes to read • Contributors  all

Azure Premium Storage delivers high-performance, low-latency disk support for virtual machines (VMs) with input/output (I/O)-intensive workloads. VM disks that use Premium Storage store data on solid-state drives (SSDs). To take advantage of the speed and performance of premium storage disks, you can migrate existing VM disks to Premium Storage.

Option C is incorrect since Standard storage offers less faster access than Premium storage

The Microsoft documentation mentions that we should not use geo-redundant storage accounts for SQL Servers as mentioned below. So, options A and D are incorrect.

In addition, we recommend that you create your Azure storage account in the same data center as your SQL Server virtual machines to reduce transfer delays. When creating a storage account, disable geo-replication as consistent write order across multiple disks is not guaranteed. Instead, consider configuring a SQL Server disaster recovery technology between two Azure data centers. For more information, see [High Availability and Disaster Recovery for SQL Server in Azure Virtual Machines](#).

For more information on SQL performance on VM's and Premium storage, please go ahead and visit the below URL

<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>

Ask our Experts

Rate this Question?

View Queries

open ▾

Question 38

Unattempted

Domain :Design an infrastructure strategy

A company is planning on hosting a set of servers in Azure. Some of these servers will run SQL Server 2016. These servers will be deployed to different data centers in the same Azure region. These will be part of an Always On availability group

The data on the servers will be backed up by using the SQL IaaS Agent Extension

Below are the key requirements for the storage for the different components of the Virtual Machine

- Operating System - Speed and availability for the storage priority
- Database and logs - Speed and availability for the storage priority
- Backups - This should use the lowest cost option for storage

You have to decide what is the ideal storage requirement for each component

Which of the following would you implement for the Database and Logs?

- A. Geo redundant storage account
- B. Premium managed disk
- C. Standard managed disk
- D. Read Access Geo redundant storage account

Explanation:

Answer – B

High-performance Premium Storage and managed disks for VMs

03/30/2018 • 22 minutes to read • Contributors  all

Azure Premium Storage delivers high-performance, low-latency disk support for virtual machines (VMs) with input/output (I/O)-intensive workloads. VM disks that use Premium Storage store data on solid-state drives (SSDs). To take advantage of the speed and performance of premium storage disks, you can migrate existing VM disks to Premium Storage.

Option C is incorrect since Standard storage offers less faster access than Premium storage

The Microsoft documentation mentions that we should not use geo-redundant storage accounts for SQL Servers as mentioned below. So, options A and D are incorrect.

In addition, we recommend that you create your Azure storage account in the same data center as your SQL Server virtual machines to reduce transfer delays. When creating a storage account, disable geo-replication as consistent write order across multiple disks is not guaranteed. Instead, consider configuring a SQL Server disaster recovery technology between two Azure data centers. For more information, see [High Availability and Disaster Recovery for SQL Server in Azure Virtual Machines](#).

For more information on SQL performance on VM's and Premium storage, please go ahead and visit the below URL

<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>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 39

Unattempted

Domain :Design an infrastructure strategy

A company is planning on hosting a set of servers in Azure. Some of these servers will run SQL Server 2016. These servers will be deployed to different data centers in the same Azure region. These will be part of an Always On availability group

The data on the servers will be backed up by using the SQL IaaS Agent Extension

Below are the key requirements for the storage for the different components of the Virtual Machine

- Operating System - Speed and availability for the storage priority

- Database and logs - Speed and availability for the storage priority
- Backups - This should use the lowest cost option for storage

You have to decide what is the ideal storage requirement for each component

Which of the following would you implement for the Backups?

- A. Geo redundant storage account
- B. Premium managed disk
- C. Standard managed disk
- D. Read Access Geo redundant storage account

Explanation:

Answer - C

With Standard Disks, you can achieve lower costs as mentioned below in the Microsoft documentation

Cost-effective Standard Storage and unmanaged and managed Azure VM disks

06/13/2017 • 8 minutes to read • Contributors 

Azure Standard Storage delivers reliable, low-cost disk support for VMs running latency-insensitive workloads. It also supports blobs, tables, queues, and files. With **Standard Storage**, the data is stored on hard disk drives (HDDs). When working with VMs, you can use standard SSD and HDD disks for Dev/Test scenarios and less critical workloads, and premium SSD disks for mission-critical production applications. Standard Storage is available in all Azure regions.

The Microsoft documentation mentions that we should not use geo-redundant storage accounts for SQL Servers as mentioned below. So, options A and D are incorrect.

In addition, we recommend that you create your Azure storage account in the same data center as your SQL Server virtual machines to reduce transfer delays. When creating a storage account, disable geo-replication as consistent write order across multiple disks is not guaranteed. Instead, consider configuring a SQL Server disaster recovery technology between two Azure data centers. For more information, see [High Availability and Disaster Recovery for SQL Server in Azure Virtual Machines](#).

For more information on Standard storage, please go ahead and visit the below URL

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/standard-storage>

View Queries

open ▾

Question 40

Unattempted

Domain :Design an infrastructure strategy

A team has just setup an Azure SQL database. They are planning on enabling the diagnostics for the underlying Azure SQL server as shown below

* Name

whizlabsetting

 Archive to a storage account

Storage account

whizlabstore

 Stream to an event hub Send to Log Analytics

Subscription

Pay-As-You-Go

Log Analytics Workspace

whizlablog (centralus)

LOG

 SQLInsights

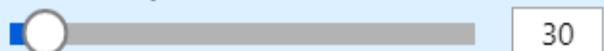
Retention (days)



90

 AutomaticTuning

Retention (days)



30

What is the amount of time SQLInsights data will be stored in BLOB storage?

 A. 30 days B. 90 days C. 700 days

D. indefinite

Explanation:

Answer – B

Since the retention for SQLInsights is specified as 90 days , hence the data will be stored for that duration of time.

* Name
whizlabsetting 

Archive to a storage account

Storage account
whizlabstore 

Stream to an event hub

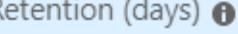
Send to Log Analytics

Subscription
Pay-As-You-Go 

Log Analytics Workspace
whizlablog (centralus) 

LOG

SQLInsights 
Retention (days)   90

AutomaticTuning 
Retention (days)   30

Since this is clear from the above representation, all other options are incorrect

For more information on SQL Server database metrics, please go ahead and visit the below URL

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-metrics-diag-logging>

Ask our Experts

Rate this Question?  

Question 41

Unattempted

Domain :Design an infrastructure strategy

A team has just setup an Azure SQL database. They are planning on enabling the diagnostics for the underlying Azure SQL server as shown below

* Name

whizlabsetting

 Archive to a storage account

Storage account

whizlabstore

 Stream to an event hub Send to Log Analytics

Subscription

Pay-As-You-Go



Log Analytics Workspace

whizlablog (centralus)



LOG

 SQLInsights

Retention (days)



90

 AutomaticTuning

Retention (days)



30

What is the maximum amount of time that SQLInsights data can be stored in Azure Log Analytics?

- A. 30 days
- B. 90 days
- C. 700 days
- D. 730 days

**Explanation:**

The limit for storing data is 730 days.

How long is the data kept?

Raw data points (that is, items that you can query in Analytics and inspect in Search) are kept for up to 730 days. You can [select a retention duration](#) of 30, 60, 90, 120, 180, 270, 365, 550 or 730 days. If you need to keep data longer than 730 days, you can use [Continuous Export](#) to copy it to a storage account during data ingestion.

Data kept longer than 90 days will incur additional charges. Learn more about Application Insights pricing on the [Azure Monitor pricing page](#).

Aggregated data (that is, counts, averages and other statistical data that you see in Metric Explorer) are retained at a grain of 1 minute for 90 days.

[Debug snapshots](#) are stored for 15 days. This retention policy is set on a per-application basis. If you need to increase this value, you can request an increase by opening a support case in the Azure portal.

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/data-retention-privacy>

Ask our Experts

Rate this Question?  

[View Queries](#)

open ▾

Question 42

Unattempted

Domain :Design for identity and security

A company has an Azure subscription named whizlab. The subscription contains resources for an application named whizlab-app. An Azure AD group named whizlab-admin is in place to manage the resources assigned to the application.

The company now wants to deploy a new application named whizlab-app-staging. The development team for the application will be part of a new Azure AD group called whizlab-dev.

The company has the following requirements

- The members of the whizlab-dev group should be able to create resources in Azure which are required by the whizlab-app-staging application
- The members of the whizlab-dev group should not be able to make any changes to the role assignments in Azure
- The role assignments for the whizlab-app-staging application should be performed by the members of the whizlab-admin group

You decide to implement the following solution

Create a new Azure subscription named whizlab-app-staging. Assign the whizlab-admin group as the Owner of the new subscription. Assign the Contributor role to the whizlab-dev group for the subscription

Does this fulfill the requirement?

A. Yes

B. No

Explanation:

Answer – A

Yes, this is one possible isolation of resources. You have the resources in different subscriptions.

Assigning the Owner privilege for the whizlab-admin group would fulfil the requirement of "**The role assignments for the whizlab-app-staging application should be performed by the members of the whizlab-admin group**"

Assigning the contributor role to the whizlab-dev group will ensure the below constraint is met, "**The members of the whizlab-dev group should not be able to make any changes to the role assignments in Azure**"

For more information on organizing subscriptions, please go ahead and visit the below URL

<https://azure.microsoft.com/en-us/blog/organizing-subscriptions-and-resource-groups-within-the-enterprise/>

Ask our Experts

Rate this Question?  

View Queries

open 

Question 43

Unattempted

Domain :Design for identity and security

A company has an Azure subscription named whizlab. The subscription contains resources for an application named whizlab-app. An Azure AD group named whizlab-admin is in place to manage the resources assigned to the application.

The company now wants to deploy a new application named whizlab-app-staging. The development team for the application will be part of a new Azure AD group called whizlab-dev.

The company has the following requirements

- The members of the whizlab-dev group should be able to create resource in Azure which are required by the whizlab-app-staging application
- The members of the whizlab-dev group should not be able to make any changes to the role assignments in Azure
- The role assignments for the whizlab-app-staging application should be performed by the members of the whizlab-admin group

You decide to implement the following solution

Create a new Azure subscription named whizlab-app-staging. Assign the whizlab-admin group the User Access Administrator role for the new subscription. Assign the Owner role to the whizlab-dev group for the subscription

Does this fulfil the requirement?

A. Yes

B. No

Explanation:

Answer – B

Here the role assignments are incorrect.

Assigning the User Access Administrator role to the whizlab-admin group will not enable the assignment of roles

Assigning the Owner role to the whizlab-dev group will break the requirement of **"The members of the whizlab-dev group should not be able to make any changes to the role assignments in Azure"**

For more information on in-built access roles, please go ahead and visit the below URL

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 44

Unattempted

Domain :Design for identity and security

A company has an Azure subscription named whizlab. The subscription contains resources for an application named whizlab-app. An Azure AD group named whizlab-admin is in place to manage the resources assigned to the application.

The company now wants to deploy a new application named whizlab-app-staging. The development team for the application will be part of a new Azure AD group called whizlab-dev.

The company has the following requirements

- The members of the whizlab-dev group should be able to create resource in Azure which are required by the whizlab-app-staging application
- The members of the whizlab-dev group should not be able to make any changes to the role assignments in Azure
- The role assignments for the whizlab-app-staging application should be performed by the members of the whizlab-admin group

You decide to implement the following solution

Create a new resource group named whizlab-app-staging in the current subscription. Assign the whizlab-admin group as the Owner of resource group. Assign the Contributor role to the whizlab-dev group for the subscription.

Does this fulfil the requirement?

A. Yes

B. No

Explanation:

Answer – A

The best solution is to create a new resource group for the resources for the whizlab-app-staging application. You can then go to IAM for the resource group and assign the Owner privilege for the whizlab-admin group. This will fulfil the requirement of **“The role assignments for the whizlab-app-staging application should be performed by the members of the whizlab-admin group”**

Assigning the contributor role to the whizlab-dev group will ensure the below constraint is met, **“The members of the whizlab-dev group should not be able to make any changes to the role assignments in Azure”**

whizlabs-rg - Access control (IAM)

Resource group

Search (Ctrl+ /)

Add Edit columns Refresh Remove

Check access Role assignments Deny assignments Classic administrators Roles

Manage access to Azure resources for users, groups, service principals and managed identities at this scope by creating role assignments. [Learn more](#)

Name	Type	Role
Search by name or email	All	Virtual Machine Contributor
Scope	Group by	
All scopes	Role	

1 items (1 Users)

NAME	TYPE	ROLE	SCOPE
whizlabusr whizlabusr@demo...	User	Virtual Machine Contributor	This resource

For more information on in-built access roles, please go ahead and visit the below URL

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

Ask our Experts

Rate this Question?

Question 45

Unattempted

Domain :Determine workload requirements

Your company has a set of VMware virtual machines that need to be migrated onto Azure. As the architect you have to present an estimation on the cost for the migrating the machines onto Azure. You plan to use the Azure Migrate assessment tool for this. Which of the following costs would be given as part of the assessment tool? Choose 2 answers from the options given below

- A. Network cost
- B. Bandwidth cost
- C. Compute cost
- D. Storage cost

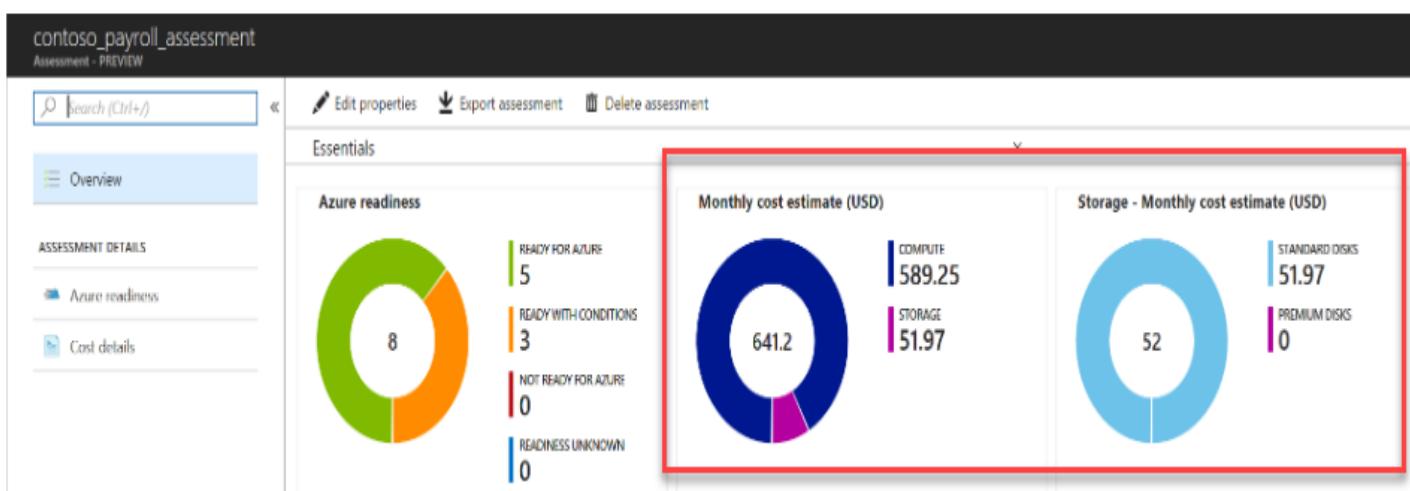
Explanation:

Answer – C and D

This is given in the Microsoft documentation. The assessment tool would give the Compute and storage costs as shown below.

Assessment details

An assessment includes information about whether the on-premises VMs are compatible for Azure, what would be the right VM size for running the VM in Azure and the estimated monthly Azure costs.



Since this is clearly mentioned in the Microsoft documentation, all other options are incorrect

For more information on the assessment tool, please go ahead and visit the below URL

<https://docs.microsoft.com/en-us/azure/migrate/tutorial-assessment-vmware>

View Queries

open ▾

Question 46

Unattempted

Domain :Determine workload requirements

A company has just setup an Azure subscription and an Azure AD tenant. The company wants to enforce the following requirements

- Virtual Machines should only be created in specific regions
- Only Virtual Machines of specific sizes can be created

Which of the following would you use for this requirement?

- A. Conditional access policies
- B. Azure Policies 
- C. Azure Resource Manager templates
- D. Role-based access control (RBAC)

Explanation:

Answer – B

This can be done with the help of Azure Policies. The Microsoft documentation mentions the following

Overview of the Azure Policy service

12/06/2018 • 9 minutes to read • Contributors 

Governance validates that your organization can achieve its goals through an effective and efficient use of IT. It meets this need by creating clarity between business goals and IT projects.

Does your company experience a significant number of IT issues that never seem to get resolved? Good IT governance involves planning your initiatives and setting priorities on a strategic level to help manage and prevent issues. This strategic need is where Azure Policy comes in.

Azure Policy is a service in Azure that you use to create, assign, and manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service level agreements. Azure Policy meets this need by evaluating your resources for non-compliance with assigned policies. For example, you can have a policy to allow only a certain SKU size of virtual machines in your environment. Once this policy is implemented, new and existing resources are evaluated for compliance. With the right type of policy, existing resources can be brought into compliance. Later in this documentation, we'll go over more details on how to create and implement policies with Azure Policy.

Since this is clearly given in the Microsoft documentation, all other options are incorrect

For more information on Azure policies, please go ahead and visit the below URL

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

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 47

Unattempted

Domain :Determine workload requirements

A company has setup an Azure subscription and an Azure tenant. You need to provide the development team to be able to start and stop Virtual Machines. The access needs to be granted for **time-bound** period. You need to ensure the permission gets assigned for a period of start and end dates and use the principle of least privilege. You also need to minimize costs.

Which of the following would you use for the Azure AD license?

- A. Free
- B. Basic

C. Premium P1

D. Premium P2 

Explanation:

Answer – D

Assign **time-bound** access to resources using start and end dates feature is available only in PIM of Azure AD, which is available in Premium P2 edition.

Premium P2 license : <https://azure.microsoft.com/en-in/pricing/details/active-directory/>

time-bound access to resources using start and end dates: <https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-configure>

For this requirement, we need to use Privileged Identity Management and for this we need to have Premium P2 licences.

Prerequisites

To use PIM, you must have one of the following paid or trial licenses. For more information, see [What is Azure Active Directory?](#).

- Azure AD Premium P2
- Enterprise Mobility + Security (EMS) E5



Because of the license requirements mentioned in the documentation, the other options are incorrect

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-configure>

Ask our Experts

Rate this Question?  

View Queries

open 

Question 48

Unattempted

Domain :Determine workload requirements

A company has setup an Azure subscription and an Azure tenant. You need to provide the development team to be able to start and stop Virtual Machines. The access needs to be granted on specific occasions only. You need to ensure the permission gets assigned and use the principle of least privilege. You also need to minimize costs.

Which of the following security feature would you use for the requirement?

- A. Conditional Access policy
- B. Azure Policies
- C. Just in time VM access
- D. Privileged Identity Management

Explanation:

Answer – D

With Privileged Identity Management, you can implement just in time privileges for Azure resources.

What can I do with PIM?

PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Here are some of the key features of PIM:

- Provide **just-in-time** privileged access to Azure AD and Azure resources
- Assign **time-bound** access to resources using start and end dates
- Require **approval** to activate privileged roles
- Enforce **multi-factor authentication** to activate any role
- Use **justification** to understand why users activate
- Get **notifications** when privileged roles are activated
- Conduct **access reviews** to ensure users still need roles
- Download **audit history** for internal or external audit

Since this is clearly given in the Microsoft documentation, all other options are incorrect

For more information on Privileged Identity Management, please go ahead and visit the below URL

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

Ask our Experts

Rate this Question?  

Domain :Design for identity and security

A team has a .Net application that needs to run on a Virtual machine. The application on the Virtual machine must authenticate using the same Azure AD Identity.

Which of the following would be done to provision the Azure AD Identity?

- A. Create a system-assigned Managed Service Identity ✓
- B. Register a web application in Azure AD
- C. Register an Enterprise application in Azure AD
- D. Create a user-assigned Managed Service Identity

Explanation:

Answer – A

Here we can simply use a system assigned Managed Service Identity. This can be done for the Virtual machine. The Microsoft documentation mentions the following

The managed identities for Azure resources feature in Azure Active Directory (Azure AD) solves this problem. The feature provides Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code.

- A **system-assigned managed identity** is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Azure AD tenant that's trusted by the subscription of the instance. After the identity is created, the credentials are provisioned onto the instance. The lifecycle of a system-assigned identity is directly tied to the Azure service instance that it's enabled on. If the instance is deleted, Azure automatically cleans up the credentials and the identity in Azure AD.



Option D is incorrect since we just have a single virtual machine that needs an identity provisioned in Azure AD.

Options B and C are incorrect because you need to use Managed service identities.

For more information on Managed service identities, please go ahead and visit the below URL

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

View Queries

open ▾

Question 50

Unattempted

Domain :Design for identity and security

A team has a .Net application that needs to run on a Virtual machine. The application on the Virtual machine must authenticate using the same Azure AD Identity.

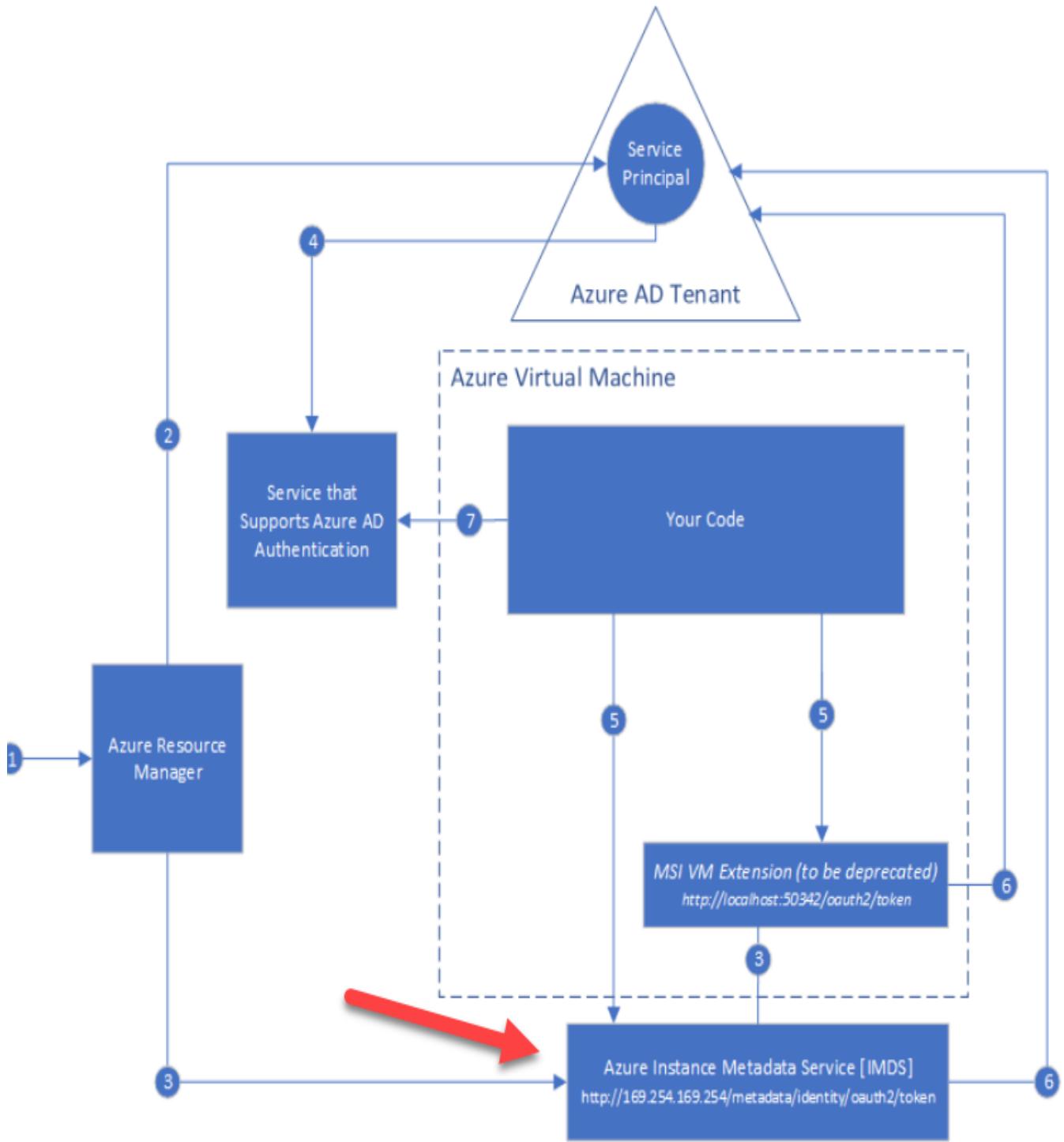
In order to generate a request token, which of the following would be used?

- A. Azure AD v1.0 endpoint
- B. Azure AD v2.0 endpoint
- C. OAuth2 endpoint
- D. Azure Instance Metadata Service Identity 

Explanation:

Answer – D

To generate the token, you have to use the Azure Instance Metadata Service Identity. The workflow is also given in the Microsoft documentation



Since this is clearly given in the Microsoft documentation, all other options are incorrect

For more information on Managed service identities, please go ahead and visit the below URL

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

Ask our Experts

Rate this Question? 😊 😐

View Queries

open ✓

Question 51

Unattempted

A company is developing an application that will consist of different modules. The different modules need to communicate asynchronously with each other. Which of the following is the ideal service to use for this requirement?

- A. Azure Table storage
- B. Azure Notification Hubs
- C. Azure Blob storage
- D. Azure Queue storage

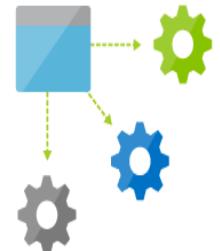
Explanation:

Answer – D

Azure Queue Storage is the perfect solution for decoupling components of an application. The Microsoft documentation mentions the following on Azure Queue storage

Decouple components

Use Azure Queue Storage to build flexible applications and separate functions for better durability across large workloads. When you design applications for scale, application components can be decoupled, so that they can scale independently. Queue storage gives you asynchronous message queueing for communication between application components, whether they are running in the cloud, on the desktop, on-premises, or on mobile devices.



Option A is incorrect because this is ideal for table storage

Option B is incorrect because this is a notification service

Option C is incorrect because this is ideal for object level storage

For more information on Azure queue storage, please go ahead and visit the below URL

<https://azure.microsoft.com/en-us/services/storage/queues/>

Ask our Experts

Rate this Question?

View Queries

open ▾

Question 52

Unattempted

Domain :Design an infrastructure strategy

A team has an Azure CosmosDB account. A solution needs to be in place to generate an alert from Azure Log Analytics when a query request charge exceeds 40 units more than 10 times during a 10-minute window. Which of the following would you recommend? Choose 2 answers from the options given below

- A. Create a search query to identify when the requestCharge_s exceeds 40. ✓
- B. Create a search query to identify when the requestCharge_s exceeds 10.
- C. Create a search query to identify when the duration_s exceeds 10.
- D. Configure a period of 10 and a frequency of 10. ✓

Explanation:

Answer - A and D

If you look at the table for the log entries in Azure Log Analytics, you can see that in order to monitor the request unit rate, we have to check for the requestCharge_s log entry.

Azure Storage field or property	Azure Monitor logs property	Description
time	TimeGenerated	The date and time (UTC) when the operation occurred.
resourceId	Resource	The Azure Cosmos DB account for which logs are enabled.
category	Category	For Azure Cosmos DB logs, DataPlaneRequests is the only available value.
operationName	OperationName	Name of the operation. This value can be any of the following operations: Create, Update, Read, ReadFeed, Delete, Replace, Execute, SqlCommand, Query, JQuery, Head, HeadFeed, or Upsert.
properties	n/a	The contents of this field are described in the rows that follow.
activityId	activityId_g	The unique GUID for the logged operation.
userAgent	userAgent_s	A string that specifies the client user agent that's performing the request. The format is {user agent name}/{version}.
request ResourceType	request ResourceType_s	The type of the resource accessed. This value can be any of the following resource types: Database, Container, Document, Attachment, User, Permission, StoredProcedure, Trigger, UserDefinedFunction, or Offer.
statusCode	statusCode_s	The response status of the operation.
request resourceId	ResourceId	The resourceId that pertains to the request. The value may point to databaseId, collectionId, or documentId depending on the operation performed.
clientIpAddress	clientIpAddress_s	The client's IP address.
requestCharge	requestCharge_s	The number of RUs that are used by the operation

You can then generate alerts in Azure Monitor based on the period and frequency

Option B is incorrect since the question states to check if the request charge exceeds 40 units

Option C is incorrect since this is the wrong metric to monitor

For more information on CosmosDB logging, please go ahead and visit the below URL

<https://docs.microsoft.com/en-us/azure/cosmos-db/logging>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 53

Unattempted

Domain :Design a data platform solution

Your team needs to deploy a Virtual machine that will host a SQL Server. The Virtual machine will have 2 data disks, one for the log file and the other for the data files. You need to recommend a caching policy for each disk

Which of the following would you recommend for the data disk containing the logs?

- A. None 
- B. ReadOnly
- C. WriteOnly
- D. ReadWrite

Explanation:

Answer – A

This is clearly mentioned in the Microsoft documentation

Disks - Use a minimum of 2 P30 disks (1 for log files and 1 for data files including TempDB). For workloads requiring ~50,000 IOPS, consider using an Ultra SSD.

- Avoid using operating system or temporary disks for database storage or logging.

- Enable read caching on the disk(s) hosting the data files and TempDB data files.

- Do not enable caching on disk(s) hosting the log file. Important: Stop the SQL Server service when changing the cache settings for an Azure VM disk.

- Stripe multiple Azure data disks to get increased IO throughput.

- Format with documented allocation sizes.

- Place TempDB on local SSD for mission critical SQL Server workloads (after choosing correct VM size).

Since this is clearly mentioned, all other options are incorrect

For more information on the performance guidelines for SQL Server on Virtual Machines, please go ahead and visit the below URL

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

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 54

Unattempted

Domain :Design a data platform solution

Your team needs to deploy a Virtual machine that will host a SQL Server. The Virtual machine will have 2 data disks, one for the log file and the other for the data files. You need to recommend a caching policy for each disk

Which of the following would you recommend for the data disk containing the data?

A. **None**

B. **ReadOnly** 

C. **WriteOnly**

D. **ReadWrite**

Explanation:

Answer – B

This is clearly mentioned in the Microsoft documentation

Disks - Use a minimum of 2 P30 disks (1 for log files and 1 for data files including TempDB). For workloads requiring ~50,000 IOPS, consider using an Ultra SSD.

- Avoid using operating system or temporary disks for database storage or logging.

- Enable read caching on the disk(s) hosting the data files and TempDB data files.

- Do not enable caching on disk(s) hosting the log file. Important: Stop the SQL Server service when changing the cache settings for an Azure VM disk.

- Stripe multiple Azure data disks to get increased IO throughput.

- Format with documented allocation sizes.

- Place TempDB on local SSD for mission critical SQL Server workloads (after choosing correct VM size).

Since this is clearly mentioned, all other options are incorrect

For more information on the performance guidelines for SQL Server on Virtual Machines, please go ahead and visit the below URL

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

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 55

Unattempted

Domain :Design a business continuity strategy

A company needs to move a web application onto Azure. Below are the main requirements for the application

- The application must be available to users even if an Azure data center becomes unavailable.
- Costs must be minimized.

Which of the following would you recommend?

- A. Deploy a load balancer and the web application in 2 Azure regions

- B. Deploy a Traffic Manager and the web application in 2 Azure regions
- C. Deploy a load balancer and a virtual machine scale set in 2 Azure regions
- D. Deploy a load balancer and a virtual machine scale set across two availability zones ✓

Explanation:

Answer - D

A Data center corresponds to the concept of availability zones.

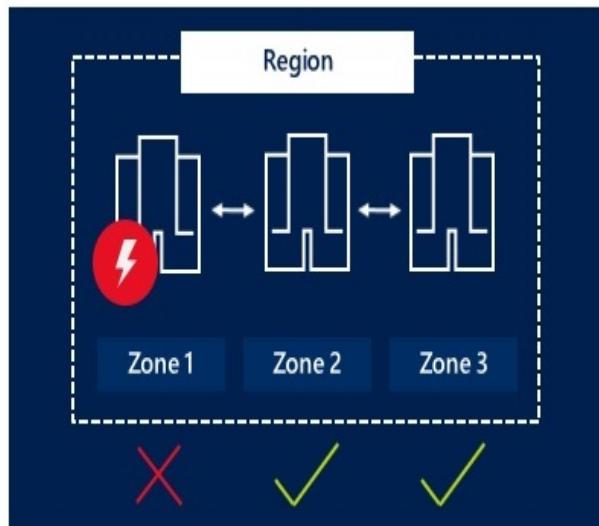
The Microsoft documentation mentions the following with respect to availability sets

Use availability zones to protect from datacenter level failures 🔗

[Availability zones](#) expand the level of control you have to maintain the availability of the applications and data on your VMs. Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there are a minimum of three separate zones in all enabled regions. The physical separation of Availability Zones within a region protects applications and data from datacenter failures. Zone-redundant services replicate your applications and data across Availability Zones to protect from single-points-of-failure.

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

With Availability Zones, Azure offers [industry best 99.99% VM uptime SLA](#). By architecting your solutions to use replicated VMs in zones, you can protect your applications and data from the loss of a datacenter. If one zone is compromised, then replicated apps and data are instantly available in another zone.



Learn more about deploying a [Windows](#) or [Linux](#) VM in an Availability Zone.

All other options are invalid, since you need to minimize on costs, and you don't need to deploy resources across regions

For more information on availability sets, please go ahead and visit the below URL

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability#use-availability-zones-to-protect-from-datacenter-level-failures>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Finish Review

Certification

Cloud Certification

Java Certification

PM Certification

Big Data Certification

Company

Support

Discussions

Blog

Business

Follow us



© Copyright 2020. Whizlabs Software Pvt. Ltd. All Right Reserved.