Answer Sheet

Q1)

A company currently has an on-premise network. They have an Active directory domain defined as XYZ.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?

- Correct
- ✓ Incorrect

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

Q2)

A company currently has an on-premise network. They have an Active directory domain defined as XYZ.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?

- ✓ Correct

Explanation:-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.

- Incorrect

Q3)

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.

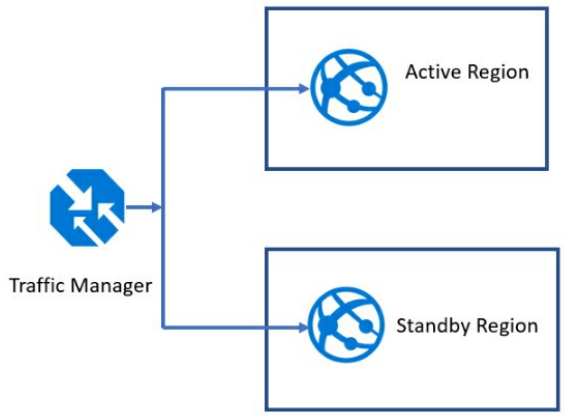
- An Azure SQL database
- ✓ Azure BLOB storage that uses the Archive tier

Explanation:-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

- Azure BLOB storage that uses the Cool tier
- A Recovery Services vault

Q4)

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?

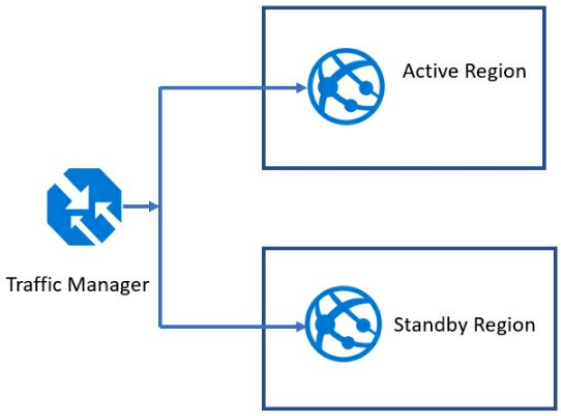
- Add a basic load balancer to the standby region
- Add an Application load balancer to the standby region
- ✓ Modify the Traffic routing method

Explanation:-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.

- Add an Application load balancer to the Primary region

Q5)

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?

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

Explanation:-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

---

Q6)

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?

- ✅ Enable "Azure Resource Manager for template Deployment" in Access Policy of Key Vault

Explanation:-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.

- Role based access
- An Azure policy
- Access policy for Key vaut

Q7)

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?

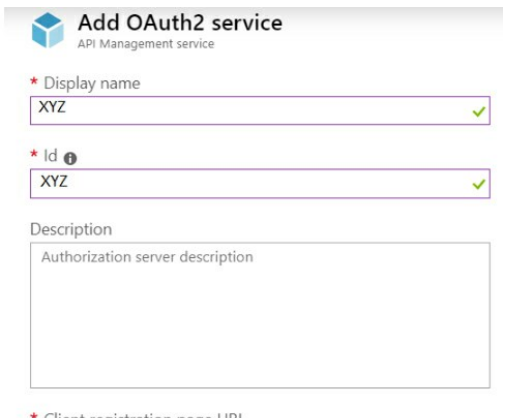
- Access policy for Key vault
- An Azure policy
- ✅ Role based access

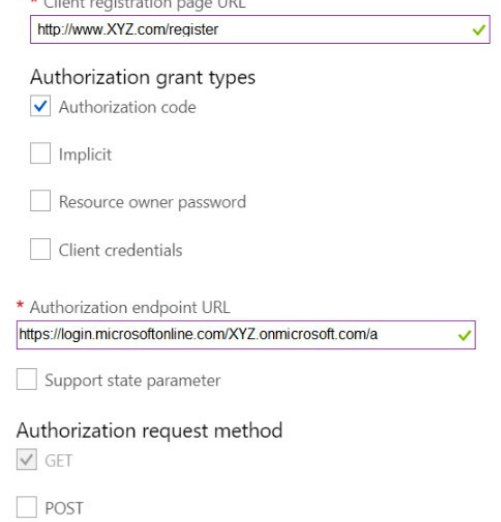
Explanation:-The Microsoft documentation clearly gives the steps for this. One of them is to ensure the identity deploying the template has the right permissions. This can be done with the help of Role based access.

- Advanced access policy

Q8)

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





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

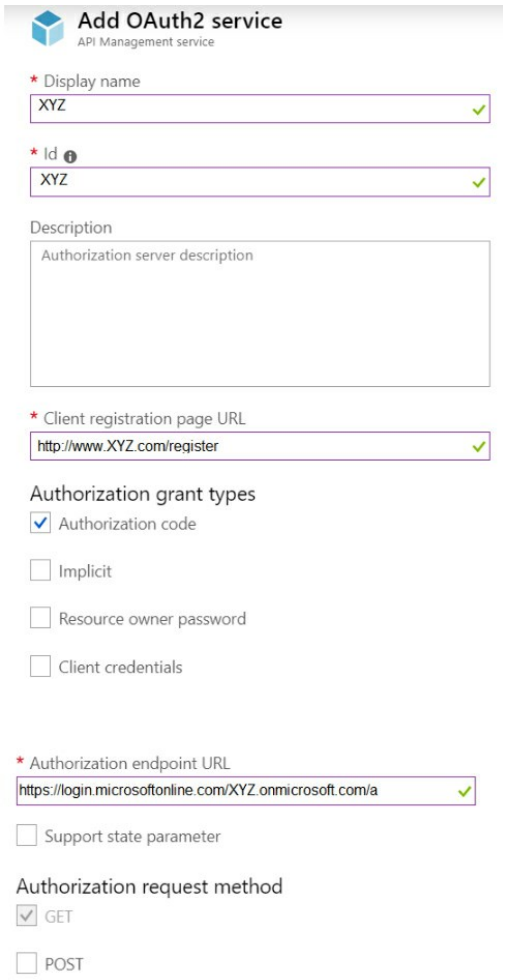
- ✅ For web application

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

- For a background service
- For headless device authentication
- For a single page application

Q9)

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



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

- Client credentials
- Implicit
- Resource owner Password
- ✅ Support state parameter

Explanation:-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

Q10)

A company named XYZ 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?

✅ Self-Service password reset

Explanation:-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.

⚪ Access review

✅ Password writeback

Explanation:-

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.

⚪ Azure AD privilege policies

Q11) 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?

⚪ Azure data catalog

⚪ SQL Migration Assistant (SSMs)

⚪ Data migration assistant

✅ Azure data factory

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

---

Q12)

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

1)Give the ability to install and provide access to the full .Net framework

2)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?

✅ Correct

Explanation:-

Correct, 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.

⚪ Incorrect

Q13)

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

1) Give the ability to install and provide access to the full .Net framework

2) 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?

⚪ Correct

✅ Incorrect

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

---

Q14)

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

1) Give the ability to install and provide access to the full .Net framework

2) 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?

Correct

Incorrect

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

Q15)

Overview

XYZ is an online training provider.

Current System - Financial Processing

XYZ currently has a system that consists of 3 tiers

- Front end Web App
- Middle tier API
- Back end data store

Below is the current set of the system

- The backend is running on Microsoft SQL server 2016
- All servers are running on Windows
- The Front and Middle tiers are written in C# and hosted on Internet Information Services
- The database is currently 1 TB in size. The growth of the database is not expected to grow beyond 3 TB.

The system currently has the following requirements

- All data must be encrypted in rest and in transit
- The front and middle tier components currently make use of encryption keys to protect the data store. Only these tiers should have the capability to access the encryption keys.
- Database backups need to be maintained in 2 separate locations that are at least 100 miles apart
- Database backups need to be stored for up to 7 years
- Traffic to the servers needs to be controlled via source IP address and port no
- Access to the system should only be via the internal network of XYZ
- The Security team needs to be able to inspect all inbound and outbound traffic

Current System - Transactional Query System

XYZ also has a Transaction Query system built on .Net. The data is stored in Azure Table storage. This .Net service currently runs on a client computer

Planned Changes

XYZ wants to migrate the Financial Processing system to Azure

Key requirements

- Infrastructure services must remain available if a region or a data center fails.
- Failover must occur without any administrative intervention
- Wherever possible, Azure managed services must be used to management overhead
- Whenever possible, costs must be minimized.
- Collect windows security logs from the Middle tier and retain the logs for several year
- Generate alerts if any unauthorized access to the backend Virtua machines are detected.
- The number of instances assigned to the front and middle tiers should be adjusted automatically based on the CPU utilization
- An SLA of 99.95% must be guaranteed on the Infrastructure for the front and middle tier systems
- Identity management must be performed via Active directory and all password hashes must be stored on the on-premise environment.
- If there are any suspicious attempts for authentication, then that should trigger multi-factor authentication. Access should be allowed if the authentication attempt is successful.
- The data store for the transactional query system will be move from Azure Table storage to a CosmosDB account

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

Long term retention for the database

Explanation:-

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

- Use Azure Site Recovery for the database
- Configure geo-replication for the database
- Configure Azure backup for the database

Q16)

Overview

XYZ is an online training provider.

Current System - Financial Processing

XYZ currently has a system that consists of 3 tiers

- Front end Web App
- Middle tier API
- Back end data store

Below is the current set of the system

- The backend is running on Microsoft SQL server 2016
- All servers are running on Windows
- The Front and Middle tiers are written in C# and hosted on Internet Information Services
- The database is currently 1 TB in size. The growth of the database is not expected to grow beyond 3 TB.

The system currently has the following requirements

- All data must be encrypted in rest and in transit
- The front and middle tier components currently make use of encryption keys to protect the data store. Only these tiers should have the capability to access the encryption keys.
- Database backups need to be maintained in 2 separate locations that are at least 100 miles apart
- Database backups need to be stored for up to 7 years
- Traffic to the servers needs to be controlled via source IP address and port no
- Access to the system should only be via the internal network of XYZ
- The Security team needs to be able to inspect all inbound and outbound traffic

Current System - Transactional Query System

XYZ also has a Transaction Query system built on .Net. The data is stored in Azure Table storage. This .Net service currently runs on a client computer

Planned Changes

XYZ wants to migrate the Financial Processing system to Azure

Key requirements

- Infrastructure services must remain available if a region or a data center fails.
- Failover must occur without any administrative intervention
- Wherever possible, Azure managed services must be used to management overhead
- Whenever possible, costs must be minimized.
- Collect windows security logs from the Middle tier and retain the logs for several year
- Generate alerts if any unauthorized access to the backend Virtua machines are detected.

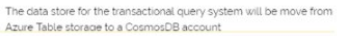
- The number of instances assigned to the front and middle tiers should be adjusted automatically based on the CPU utilization
- An SLA of 99.95% must be guaranteed on the Infrastructure for the front and middle tier systems
- Identity management must be performed via Active directory and all password hashes must be stored on the on-premise environment.
- If there are any suspicious attempts for authentication, then that should trigger multi-factor authentication. Access should be allowed if the authentication attempt is successful.
- The data store for the transactional query system will be move from Azure Table storage to a CosmosDB account

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

✅ Transparent data encryption

Explanation:-

The requirement is encrypt the data at rest for



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.

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.

- Always Encrypted
- Azure storage encryption
- SSL certificates

Q17)

Overview

XYZ is an online training provider.

Current System - Financial Processing

XYZ currently has a system that consists of 3 tiers

- Front end Web App
- Middle tier API
- Back end data store

Below is the current set of the system

- The backend is running on Microsoft SQL server 2016
- All servers are running on Windows
- The Front and Middle tiers are written in C# and hosted on Internet Information Services
- The database is currently 1 TB in size. The growth of the database is not expected to grow beyond 3 TB.

The system currently has the following requirements

- All data must be encrypted in rest and in transit
- The front and middle tier components currently make use of encryption keys to protect the data store. Only these tiers should have the capability to access the encryption keys.
- Database backups need to be maintained in 2 separate locations that are at least 100 miles apart
- Database backups need to be stored for up to 7 years
- Traffic to the servers needs to be controlled via source IP address and port no
- Access to the system should only be via the internal network of XYZ
- The Security team needs to be able to inspect all inbound and outbound traffic

Current System - Transactional Query System

XYZ also has a Transaction Query system built on .Net. The data is stored in Azure Table storage. This .Net service currently runs on a client computer

Planned Changes

XYZ wants to migrate the Financial Processing system to Azure

Key requirements

- Infrastructure services must remain available if a region or a data center fails.
- Failover must occur without any administrative intervention
- Wherever possible, Azure managed services must be used to management overhead
- Whenever possible, costs must be minimized.
- Collect windows security logs from the Middle tier and retain the logs for several year
- Generate alerts if any unauthorized access to the backend Virtua machines are detected.
- The number of instances assigned to the front and middle tiers should be adjusted automatically based on the CPU utilization
- An SLA of 99.95% must be guaranteed on the Infrastructure for the front and middle tier systems

- Identity management must be performed via Active directory and all password hashes must be stored on the on-premise environment.
- If there are any suspicious attempts for authentication, then that should trigger multi-factor authentication. Access should be allowed if the authentication attempt is successful.
- The data store for the transactional query system will be move from Azure Table storage to a CosmosDB account

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?

- Federation AD FS
- ✅ Pass-through Authentication

Explanation:-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.

- Federation with AD
- Password hash synchronization

Q18) 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?

- Standard Load Balancer
- ✅ Traffic Manager

Explanation:-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

- Basic Load Balancer
- Application gateway

Q19)

Overview

XYZ is an online training provider.

Current System - Financial Processing

XYZ currently has a system that consists of 3 tiers

- Front end Web App
- Middle tier API
- Back end data store

Below is the current set of the system

- The backend is running on Microsoft SQL server 2016
- All servers are running on Windows
- The Front and Middle tiers are written in C# and hosted on Internet Information Services
- The database is currently 1 TB in size. The growth of the database is not expected to grow beyond 3 TB.

Current System - Transactional Query System

XYZ also has a Transaction Query system built on .Net. The data is stored in Azure Table storage. This .Net service currently runs on a client computer

Planned Changes

XYZ wants to migrate the Financial Processing system to Azure

Key requirements

- Infrastructure services must remain available if a region or a data center fails.
- Failover must occur without any administrative intervention
- Wherever possible, Azure managed services must be used to management overhead
- Whenever possible, costs must be minimized.
- Collect windows security logs from the Middle tier and retain the logs for several year
- Generate alerts if any unauthorized access to the backend Virtua machines are detected.

The system currently has the following requirements

- All data must be encrypted in rest and in transit
- The front and middle tier components currently make use of encryption keys to protect the data store. Only these tiers should have the capability to access the encryption keys.
- Database backups need to be maintained in 2 separate locations that are at least 100 miles apart

- Database backups need to be stored for up to 7 years
- Traffic to the servers needs to be controlled via source IP address and port no
- Access to the system should only be via the internal network of XYZ
- The Security team needs to be able to inspect all inbound and outbound traffic

- The number of instances assigned to the front and middle tiers should be adjusted automatically based on the CPU utilization
- An SLA of 99.95% must be guaranteed on the Infrastructure for the front and middle tier systems
- Identity management must be performed via Active directory and all password hashes must be stored on the on-premise environment.
- If there are any suspicious attempts for authentication, then that should trigger multi-factor authentication. Access should be allowed if the authentication attempt is successful.
- The data store for the transactional query system will be move from Azure Table storage to a CosmosDB account

You need to meet the following requirement of the case study

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

Which of the following would you use for this purpose?

- Azure Notification Hub
- Azure Diagnostic agent
- Azure event Hub
- ✅ Azure Log Analytics agent

Explanation:-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

---

Q20)

Overview

XYZ is an online training provider.

Current System - Financial Processing

XYZ currently has a system that consists of 3 tiers

- Front end Web App
- Middle tier API
- Back end data store

Below is the current set of the system

- The backend is running on Microsoft SQL server 2016
- All servers are running on Windows
- The Front and Middle tiers are written in C# and hosted on Internet Information Services
- The database is currently 1 TB in size. The growth of the database is not expected to grow beyond 3 TB.

The system currently has the following requirements

- All data must be encrypted in rest and in transit
- The front and middle tier components currently make use of encryption keys to protect the data store. Only these tiers should have the capability to access the encryption keys.
- Database backups need to be maintained in 2 separate locations that are at least 100 miles apart
- Database backups need to be stored for up to 7 years
- Traffic to the servers needs to be controlled via source IP address and port no
- Access to the system should only be via the internal network of XYZ
- The Security team needs to be able to inspect all inbound and outbound traffic

Current System - Transactional Query System

XYZ also has a Transaction Query system built on .Net. The data is stored in Azure Table storage. This .Net service currently runs on a client computer

Planned Changes

XYZ wants to migrate the Financial Processing system to Azure

Key requirements

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

- Wherever possible, Azure managed services must be used to management overhead
- Whenever possible, costs must be minimized.
- Collect windows security logs from the Middle tier and retain the logs for several year
- Generate alerts if any unauthorized access to the backend Virtua machines are detected.

- The number of instances assigned to the front and middle tiers should be adjusted automatically based on the CPU utilization
- An SLA of 99.95% must be guaranteed on the Infrastructure for the front and middle tier systems
- Identity management must be performed via Active directory and all password hashes must be stored on the on-premise environment.
- If there are any suspicious attempts for authentication, then that should trigger multi-factor authentication. Access should be allowed if the authentication attempt is successful.
- The data store for the transactional query system will be move from Azure Table storage to a CosmosDB account

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?

- Basic
- ✅ Premium P1

Explanation:-To implement conditional access policies, you can opt for Premium P1 licences. Premium licences are required for conditional access policies. And Premium P1 would be less expensive than Premium P2 licences. The Microsoft documentation mentions the following

- Free
- Premium P2

Q21)

Overview

XYZ is an online training provider.

Current System - Financial Processing

XYZ currently has a system that consists of 3 tiers

- Front end Web App
- Middle tier API
- Back end data store

Below is the current set of the system

- The backend is running on Microsoft SQL server 2016
- All servers are running on Windows
- The Front and Middle tiers are written in C# and hosted on Internet Information Services
- The database is currently 1 TB in size. The growth of the database is not expected to grow beyond 3 TB.

The system currently has the following requirements

- All data must be encrypted in rest and in transit
- The front and middle tier components currently make use of encryption keys to protect the data store. Only these tiers should have the capability to access the encryption keys.
- Database backups need to be maintained in 2 separate locations that are at least 100 miles apart
- Database backups need to be stored for up to 7 years
- Traffic to the servers needs to be controlled via source IP address and port no
- Access to the system should only be via the internal network of XYZ
- The Security team needs to be able to inspect all inbound and outbound traffic

Current System - Transactional Query System

XYZ also has a Transaction Query system built on .Net. The data is stored in Azure Table storage. This .Net service currently runs on a client computer

Planned Changes

XYZ wants to migrate the Financial Processing system to Azure

Key requirements

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

- Wherever possible. Azure managed services must be used to management overhead
- Whenever possible. costs must be minimized.
- Collect windows security logs from the Middle tier and retain the logs for several year
- Generate alerts if any unauthorized access to the backend Virtua machines are detected.

- The number of instances assigned to the front and middle tiers should be adjusted automatically based on the CPU utilization
- An SLA of 99.95% must be guaranteed on the Infrastructure for the front and middle tier systems
- Identity management must be performed via Active directory and all password hashes must be stored on the on-premise environment.
- If there are any suspicious attempts for authentication, then that should trigger multi-factor authentication. Access should be allowed if the authentication attempt is successful.
- The data store for the transactional query system will be move from Azure Table storage to a CosmosDB account

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?

✅ Allow access and require multi-factor authentication

Explanation:-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”

- Allow access and require Azure MFA registration
- Block access and require multi-factor authentication
- Block access and require Azure MFA registration

Q22)

Overview

XYZ is an online training provider.

Current System - Financial Processing

XYZ currently has a system that consists of 3 tiers

- Front end Web App
- Middle tier API
- Back end data store

Below is the current set of the system

- The backend is running on Microsoft SQL server 2016
- All servers are running on Windows
- The Front and Middle tiers are written in C# and hosted on Internet Information Services
- The database is currently 1 TB in size. The growth of the database is not expected to grow beyond 3 TB.

The system currently has the following requirements

- All data must be encrypted in rest and in transit
- The front and middle tier components currently make use of encryption keys to protect the data store. Only these tiers should have the capability to access the encryption keys.
- Database backups need to be maintained in 2 separate locations that are at least 100 miles apart
- Database backups need to be stored for up to 7 years
- Traffic to the servers needs to be controlled via source IP address and port no
- Access to the system should only be via the internal network of XYZ
- The Security team needs to be able to inspect all inbound and outbound traffic

Current System - Transactional Query System

XYZ also has a Transaction Query system built on .Net. The data is stored in Azure Table storage. This .Net service currently runs on a client computer

Planned Changes

XYZ wants to migrate the Financial Processing system to Azure

Key requirements

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

- Wherever possible. Azure managed services must be used to management overhead
- Whenever possible. costs must be minimized.
- Collect windows security logs from the Middle tier and retain the logs for several year
- Generate alerts if any unauthorized access to the backend Virtua machines are detected.

- The number of instances assigned to the front and middle tiers should be adjusted automatically based on the CPU utilization
- An SLA of 99.95% must be guaranteed on the Infrastructure for the front and middle tier systems
- Identity management must be performed via Active directory and all password hashes must be stored on the on-premise environment.
- If there are any suspicious attempts for authentication. then that should trigger multi-factor authentication. Access should be allowed if the authentication attempt is successful.
- The data store for the transactional query system will be move from Azure Table storage to a CosmosDB account

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?

- The premium app service plan
- The isolated app service plan
- ✅ Use of availability sets

Explanation:-
Using Availability sets is the ideal solution for achieving 99.95% availability for your infrastructure. The Microsoft documentation mentions the following

Configure multiple virtual machines in an availability set for redundancy

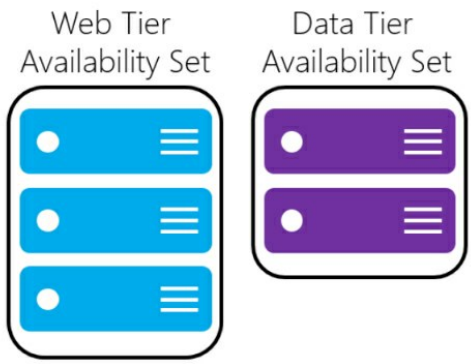
To provide redundancy to your application, we recommend that you group two or more virtual machines in an availability set. This configuration within a datacenter ensures that during either a planned or unplanned maintenance event, at least one virtual machine is available and meets the 99.95% Azure SLA. For more information, see the SLA for Virtual Machines.

You can also configure availability sets for each of the tier's , the web and front end tier.

Configure each application tier into separate availability sets

If your virtual machines are all nearly identical and serve the same purpose for your application, we recommend that you configure an availability set for each tier of your application. If you place two different tiers in the same availability set, all virtual machines in the same application tier can be rebooted at once. By configuring at least two virtual machines in an availability set for each tier, you guarantee that at least one virtual machine in each tier is available.

For example, you could put all the virtual machines in the front end of your application running IIS, Apache, Nginx in a single availability set. Make sure that only front-end virtual machines are placed in the same availability set. Similarly, make sure that only data-tier virtual machines are placed in their own availability set, like your replicated SQL Server virtual machines, or your MySQL virtual machines.



- Use of availability zones

Q23)

Overview

XYZ is an online training provider.

Current System - Financial Processing

XYZ currently has a system that consists of 3 tiers

- Front end Web App
- Middle tier API
- Back end data store

Below is the current set of the system

- The backend is running on Microsoft SQL server 2016

- All servers are running on Windows
- The Front and Middle tiers are written in C# and hosted on Internet Information Services
- The database is currently 1 TB in size. The growth of the database is not expected to grow beyond 3 TB.

The system currently has the following requirements

- All data must be encrypted in rest and in transit
- The front and middle tier components currently make use of encryption keys to protect the data store. Only these tiers should have the capability to access the encryption keys.
- Database backups need to be maintained in 2 separate locations that are at least 100 miles apart
- Database backups need to be stored for up to 7 years
- Traffic to the servers needs to be controlled via source IP address and port no
- Access to the system should only be via the internal network of XYZ
- The Security team needs to be able to inspect all inbound and outbound traffic

Current System - Transactional Query System

XYZ also has a Transaction Query system built on .Net. The data is stored in Azure Table storage. This .Net service currently runs on a client computer

Planned Changes

XYZ wants to migrate the Financial Processing system to Azure

Key requirements

- Infrastructure services must remain available if a region or a data center fails.
- Failover must occur without any administrative intervention
- Wherever possible, Azure managed services must be used to management overhead
- Whenever possible, costs must be minimized.
- Collect windows security logs from the Middle tier and retain the logs for several year
- Generate alerts if any unauthorized access to the backend Virtua machines are detected.

- The number of instances assigned to the front and middle tiers should be adjusted automatically based on the CPU utilization
- An SLA of 99.95% must be guaranteed on the Infrastructure for the front and middle tier systems
- Identity management must be performed via Active directory and all password hashes must be stored on the on-premise environment.
- If there are any suspicious attempts for authentication, then that should trigger multi-factor authentication. Access should be allowed if the authentication attempt is successful.
- The data store for the transactional query system will be move from Azure Table storage to a CosmosDB account

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

✅ Create users and request resource token

Explanation:-

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

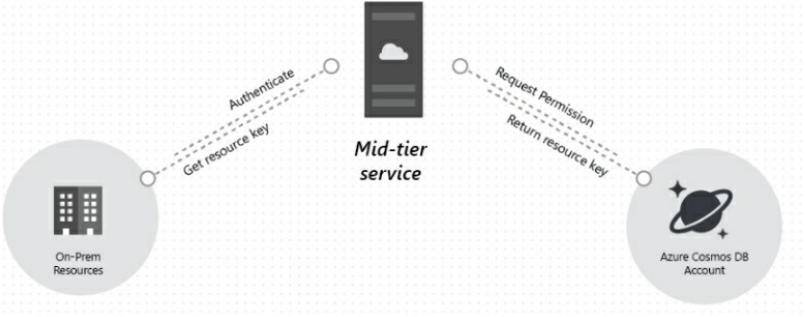
Cosmos DB users are associated with a Cosmos DB database. Each database can contain zero or more Cosmos DB users. The following code sample shows how to create a Cosmos DB user resource.

C# Copy

```
//Create a user.
User docUser = new User
{
    Id = "mobileuser"
};

docUser = await client.CreateUserAsync(UriFactory.CreateDatabaseUri("db"), docUser);
```

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.



- Create users and generate resource token
- Generate resource tokens and perform authentication
- Request resource tokens and perform authentication

Q24)

Overview

XYZ is an online training provider.

Current System - Financial Processing

XYZ currently has a system that consists of 3 tiers

- Front end Web App
- Middle tier API
- Back end data store

Below is the current set of the system

- The backend is running on Microsoft SQL server 2016
- All servers are running on Windows
- The Front and Middle tiers are written in C# and hosted on Internet Information Services
- The database is currently 1 TB in size. The growth of the database is not expected to grow beyond 3 TB.

The system currently has the following requirements

- All data must be encrypted in rest and in transit
- The front and middle tier components currently make use of encryption keys to protect the data store. Only these tiers should have the capability to access the encryption keys.
- Database backups need to be maintained in 2 separate locations that are at least 100 miles apart
- Database backups need to be stored for up to 7 years
- Traffic to the servers needs to be controlled via source IP address and port no
- Access to the system should only be via the internal network of XYZ.
- The Security team needs to be able to inspect all inbound and outbound traffic

Current System - Transactional Query System

XYZ also has a Transaction Query system built on .Net. The data is stored in Azure Table storage. This .Net service currently runs on a client computer

Planned Changes

XYZ wants to migrate the Financial Processing system to Azure

Key requirements

- Infrastructure services must remain available if a region or a data center fails.
- Failover must occur without any administrative intervention
- Wherever possible, Azure managed services must be used to management overhead
- Whenever possible, costs must be minimized.
- Collect windows security logs from the Middle tier and retain the logs for several year
- Generate alerts if any unauthorized access to the backend Virtua machines are detected.
- The number of instances assigned to the front and middle tiers should be adjusted automatically based on the CPU utilization
- An SLA of 99.95% must be guaranteed on the Infrastructure for the front and middle tier systems
- Identity management must be performed via Active directory and all password hashes must be stored on the on-premise environment.
- If there are any suspicious attempts for authentication, then that

- If there are any suspicious attempts for authentication, then that should trigger multi-factor authentication. Access should be allowed if the authentication attempt is successful.
- The data store for the transactional query system will be move from Azure Table storage to a CosmosDB account

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?

- Create users and request resource tokens
- ✅ Generate resource tokens and perform authentication

Explanation:-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.

- Create users and generate resource tokens
- Request resource tokens and perform authentication

Q25)

Overview

XYZ is an online training provider.

Current System - Financial Processing

XYZ currently has a system that consists of 3 tiers

- Front end Web App
- Middle tier API
- Back end data store

Below is the current set of the system

- The backend is running on Microsoft SQL server 2016
- All servers are running on Windows
- The Front and Middle tiers are written in C# and hosted on Internet Information Services
- The database is currently 1 TB in size. The growth of the database is not expected to grow beyond 3 TB.

The system currently has the following requirements

- All data must be encrypted in rest and in transit
- The front and middle tier components currently make use of encryption keys to protect the data store. Only these tiers should have the capability to access the encryption keys.
- Database backups need to be maintained in 2 separate locations that are at least 100 miles apart
- Database backups need to be stored for up to 7 years
- Traffic to the servers needs to be controlled via source IP address and port no
- Access to the system should only be via the internal network of XYZ
- The Security team needs to be able to inspect all inbound and outbound traffic

Current System - Transactional Query System

XYZ also has a Transaction Query system built on .Net. The data is stored in Azure Table storage. This .Net service currently runs on a client computer

Planned Changes

XYZ wants to migrate the Financial Processing system to Azure

Key requirements

- Infrastructure services must remain available if a region or a data center fails.
- Failover must occur without any administrative intervention
- Wherever possible, Azure managed services must be used to management overhead
- Whenever possible, costs must be minimized.
- Collect windows security logs from the Middle tier and retain the logs for several year
- Generate alerts if any unauthorized access to the backend Virtua machines are detected.

- The number of instances assigned to the front and middle tiers should be adjusted automatically based on the CPU utilization
- An SLA of 99.95% must be guaranteed on the Infrastructure for the front and middle tier systems
- Identity management must be performed via Active directory and all password hashes must be stored on the on-premise environment.
- If there are any suspicious attempts for authentication, then that should trigger multi-factor authentication. Access should be allowed if the authentication attempt is successful.

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

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

- Availability sets
- ✅ Virtual machine scale sets

Explanation:-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

- Azure Kubernetes Services
- App Service Environments

Q26)

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 Webjobs for the Azure Web App. Does this meet the requirement?

- Correct
- ✅ Incorrect

Explanation:-The Webjobs feature is used to run background tasks and hence cannot be used for this requirement

---

Q27)

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 Hybrid connections for the Azure Web App. Does this meet the requirement?

- Correct
- ✅ Incorrect

Explanation:-The Hybrid connection is normally used to connect to a single TCP host and port combination.

Q28)

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?

- ✅ Correct

Explanation:-This is the ideal solution. The Microsoft documentation mentions the following

- Incorrect

Q29)

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.

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

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

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

- Azure AD Connect Health
- ✅ Application Insight

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

- Azure Log Analytics
- Microsoft System Center

Q30)

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

1) A set of virtual machines hosting an internal application

2) An Azure Web app used for hosting a production-based application

The company has the following monitoring requirements.

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

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

3) 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"

- Azure Log Analytics
- Application Insight
- ✅ Azure Monitor Alerts

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

- Azure Service Health

Q31)

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

1) A set of virtual machines hosting an internal application

2) An Azure Web app used for hosting a production-based application

The company has the following monitoring requirements.

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

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

3) 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."

- Azure Log Analytics
- Application Insight
- Azure Monitor Alerts
- ✅ Azure Service Health

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

Q32)

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.

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

2) 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"

- Azure Network Watcher
- ✅ Server Level IP Firewalls rules

Explanation:-
You can use as shown in the Microsoft documentation below

- Network Security Groups
- Application Security Groups

Q33)

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.

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

2) 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"

- Azure Network Watcher
- Server Level IP Firewall rules
- ✅ Virtual Network Service Endpoints

Explanation:-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 Peering

Q34)

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.

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

2) 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”?

- Server Level IP Firewall
- ✅ Dynamic Data Masking

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

- Azure AD authentication
- Managed Service Identity

Q35)

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

1) Operating System - Speed and availability for the storage priority

2) Database and logs - Speed and availability for the storage priority

3) 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?

- Geo redundant storage account
- ✅ Premium managed disk
- Standard managed disk
- Read Access Geo redundant storage account

Q36)

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

1) Operating System - Speed and availability for the storage priority

2) Database and logs - Speed and availability for the storage priority

3) 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?

- Geo redundant account
- ✅ Premium managed disk

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

- Standard managed disk
- Read Access Geo redundant account

Q37)

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

1) Operating System - Speed and availability for the storage priority

2) Database and logs - Speed and availability for the storage priority

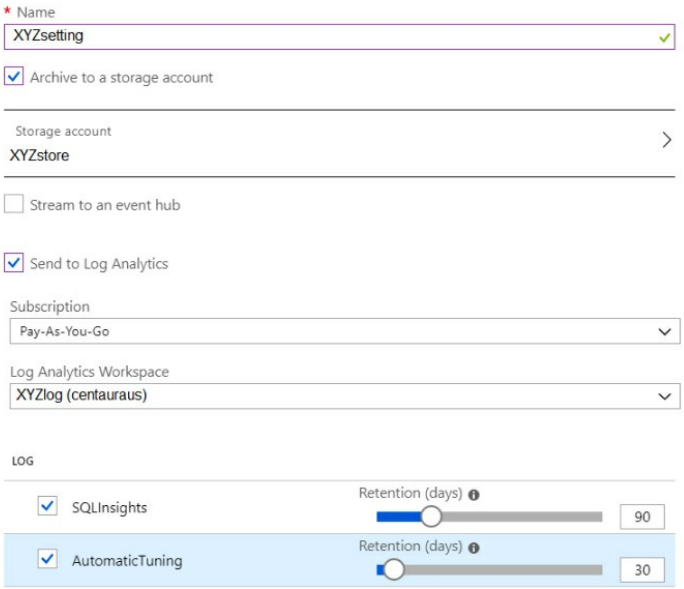
3) Backups - This should use the lowest cost option for storage

You have to decide what is the ideal storage requirement for each component. Which of the following would you implement for the Backups?

- Geo redundant account
- Premium managed disk
- ✅ Standard managed disk
- Read Access Geo redundant storage account

Q38)

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.



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

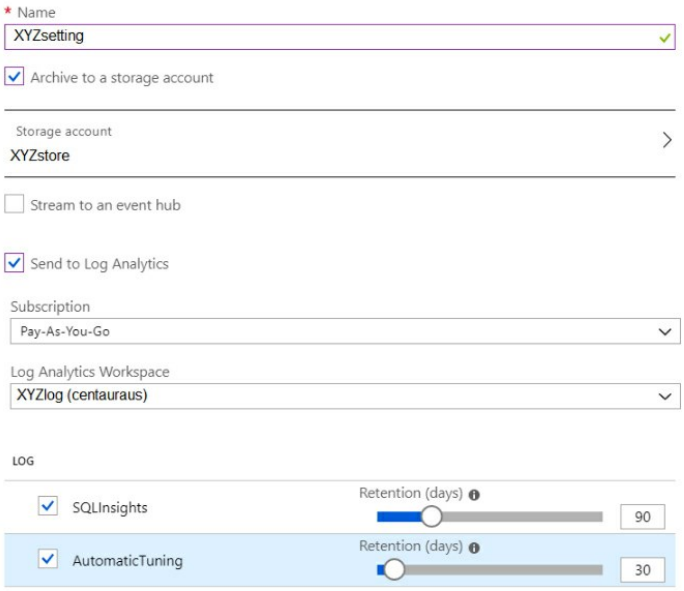
- 700 days
- 90 days

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

- 30 days
- indefinite

Q39)

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.



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

- 30 days
- 90 days
- 700 days
- indefinite

Explanation:-

There is no limit on the amount or retention of data in Azure Log Analytics. In Azure Log Analytics, you get charged for the data ingestion and retention. But the service itself is automatically scalable in terms of storage requirements.

The data retention policy only refers when sending logs to Event Hubs or to a storage account. This is also given in the Microsoft documentation

---

Q40)

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

The company now wants to deploy a new application named awza-app-staging. The development team for the application will be part of a new Azure

AD group called awza-dev.

The Company has the following requirements

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

You decide to implement the following solution

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

Does this fulfill the requirement?

✅ Correct
Explanation:-this is one possible isolation of resources. You have the resources in different subscriptions. Assigning the Owner privilege for the awza-admin group would fulfil the requirement of "The role assignments for the awza-app-staging application should be performed by the members of the awza-admin group".
Assigning the contributor role to the awza-dev group will ensure the below constraint is met, "The members of the awza-dev group should not be able to make any changes to the role assignments in Azure"
⚪ Incorrect

Q41)

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

The company now wants to deploy a new application named awza-app-staging. The development team for the application will be part of a new Azure

AD group called awza-dev.

The company has the following requirements

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

You decide to implement the following solution. Create a new Azure subscription named awza-app-staging. Assign the awza-admin group the User Access Administrator role for the new subscription. Assign the Owner role to the awza-dev group for the subscription.

Does this fulfil the requirement?

⚪ Correct
✅ Incorrect
Explanation:-Assigning the User Access Administrator role to the awza-admin group will not enable the assignment of roles. Assigning the Owner role to the awza-dev group will break the requirement of "The members of the awza-dev group should not be able to make any changes to the role assignments in Azure"

Q42)

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

The company now wants to deploy a new application named awza-app-staging. The development team for the application will be part of a new Azure

AD group called awza-dev.

The company has the following requirements

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

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

Does this fulfill the requirements?

⚪ Incorrect
✅ Correct
Explanation:-
The best solution is to create a new resource group for the resources for the awza-app-staging application. You can then go to IAM for the resource group and assign the Owner privilege for the awza-admin group. This will fulfill the requirement of "The role assignments for the awza-app-staging application should be performed by the members of the awza-admin group".

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

Q43)

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

- Network Cost
- Bandwidth Cost
- ✅ Compute Cost

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

- ✅ Storage Cost

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

Q44)

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

1) Virtual Machines should only be created in specific regions

2) Only Virtual Machines of specific sizes can be created

Which of the following would you use for this requirement?

- Role Based Access Control (RBAC)
- Azure Resources Manager Templates
- ✅ Azure Policies

Explanation:-This can be done with the help of Azure Policies. The Microsoft documentation mentions the following
- Conditional Access Policies

Q45)

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?

- Free
- Basic
- Premium P1
- ✅ Premium P2

Explanation:-
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.

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

Q46)

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?

- Conditional Access Policies
- Azure Policies
- Just in Time VM access
- ✅ Privileged Identity Management

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

Q47)

A company has set up a set of virtual machine in a network in Azure. They have connected the virtual network to their on-premise network using Express route.

There is an issue with an application hosted on the virtual machines in the network a team need.to inspect the packet flowing into the virtual machine The company decides to use Azure advisor for the packet analysis. Would this fulfill the requirement?

- Correct
- ✅ Incorrect

Explanation:-Azure Advisor is a recommendation based tool and can't be used to perform the packet analysis

---

Q48)

A company has set up a set of virtual machine in a network in Azure. They have connected the virtual network to their on-premise network using Express route.

There is an issue with an application hosted on the virtual machines in the network a team need.to inspect the packet flowing into the virtual machine .

The company decides to use Azure Traffic Analysis for the packet analysis. Would this fulfill the requirement?

Correct

Explanation:-Azure traffic analytics is used for traffic monitoring and is the correct solution to this business scenario.

Incorrect

Q49)

A company has set up a set of virtual machine in a network in Azure. They have connected the virtual network to their on-premise network using Express route.

There is an issue with an application hosted on the virtual machines in the network a team need.to inspect the packet flowing into the virtual machine .

The company decides to use Azure Traffic Manager for the packet analysis. Would this fulfill the requirement?

Correct

Incorrect

Explanation:-Azure traffic manager Is a DNS based Load balancing tool and can't be used for the purpose of Network capture.

Q50)

A company is planning on deploying and as your web app to 2 regions. one of the key requirements is to ensure that the web app is always running if an Azure region fails.

You need to ensure deployment costs are minimized. which of the following service would you include in the deployment of the solution ?

Azure function

Azure traffic manager

Explanation:-You can use the Azure traffic manager to switch traffic over failover region. The Microsoft documentation mention the following on the Azure traffic manager.

Azure application gateway

Azure Load Balancer

Q51)

A company is planning on deploying and as your web app to 2 regions. one of the key requirements is to ensure that the web app is always running if an Azure region fails. You need to ensure deployment costs are minimized.

Which of the following feature would be used to ensure failover in the service?

Season affinity

Performance based routing

Priority routing

Explanation:-You can change the routing method for the traffic manager to the Priority routing method for implementing failover. The Microsoft documentation mention the following on the routing method

URL routing

Q52)

A company currently has an on-premise network with an IP address space of of 18.1 .0.0 / 1. The company is going to deploy 20 virtual machines to Azure. The virtual machines will be placed in a subnet in an Azure virtual network. The requirement is to ensure the on-premise service can communicate with the virtual machines hosted in Azure via a site-to-site VPN connection.

You have to design the subnet for the virtual network in Azure which will be used to host the virtual machine. Which of the following address space would you assign for the subnet in the virtual network?

18 6.1 6.0.0 / 16

18 6.1 6.1.0 / 28

192.168.0.0 / 24

Explanation:-The address space for the virtual network should not conflict with the address space for the on-premises network. So. in this case the ideal option to choose as the address space is 192.168.0.0 / 24. Also if you look at the question clearly it mentions about having “20 VMs will be deployed in Azure” taking this into consideration option C is the correct reason we get 256 IP addresses to work with.

192 .168. 1.0 / 28

Q53)

A company currently has an on-premise network with an IP address space of of 186.1 6.0.0 / 16. The company is going to deploy 20 virtual machines to Azure. The virtual machines will be placed in a subnet in an Azure virtual network. The requirement is to ensure the on-premise service can communicate with the virtual machines hosted in Azure via a site-to-site VPN connection.

You have to design the subnet for the virtual network in Azure which will be used to host the virtual machine. Which of the following address space would you assign for the gateway subnet in the virtual network?

18 6.1 6.0.0 / 16

18 6.1 6.1.0 / 28

192.168.0.0 / 24

192 .168. 1.0 / 28

Explanation:-The address space for the virtual network should not conflict with the address space for the on-premises network. So. in this case the ideal option to choose as the address space is 192.168.0.0 / 24 for the subnet in the virtual network. And then use 192.168.1. 0/28 as the address space for the Gateway subnet.

Q54) Company has an API service that currently returns XML data to its internal users. the API is going to be migrated on Azure it will sit behind an API management instance. Below are the requirements for the API when it is move to azure:
1) the API must send data in JSON format to its internal user.
2) when external consultants access the API, the header information must be stripped before the data is received.
What is the minimum number of API's that need to be added to Azure API management

✅ 1
Explanation:-Since you have just one API. you can place that behind the API management instance.
2
3
4

Q55)

Company has an API service that currently returns XML data to its internal users. the API is going to be migrated on Azure it will sit behind an API management instance. Below are the requirements for the API when it is move to Azure:

1) The API must send data in JSON format to its internal user.

2) When external consultants access the API, the header information must be stripped before the data is received.

What is the minimum number of products to publish in Azure API management ?

✅ 1
Explanation:-You can have one product that is published for the internet development team.
2
3
4

Q56)

Company has an API service that currently returns XML data to its internal users. the API is going to be migrated on Azure it will sit behind an API management instance. Below are the requirements for the API when it is move to Azure:

1) the API must send data in JSON format to its internal user.

2) when external consultants access the API, the header information must be stripped before the data is received.

What is the minimum number of policy elements that need to be added to the API?

1
✅ 2
Explanation:-You can have one policy element to ensure that XML data is transform to JS0N for the internal users when it is published to azure
3
4

Q57)

A Company currently has resource deployed to on premise network and to Azure AD.

There is a requirement to ensure that the Azure AD tenant can only be managed from workstations on the on premise network.

Which of the following needs to be part of the implementation of this requirement?

Azure ADroles and administrator
✅ Conditional access policy
Explanation:-This can be managed by conditional access policy ensuring that the locations is set in the policy
Role based access control
Azure AD privilege identity management

Q58)

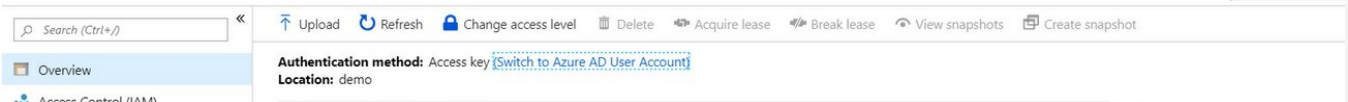
A team has an application that receives data from iot based devices. That I send to CosmosDB which uses the SQL API. A notification needs to be sent when data is received from the iot devices which of the following Can be part of the implementation?

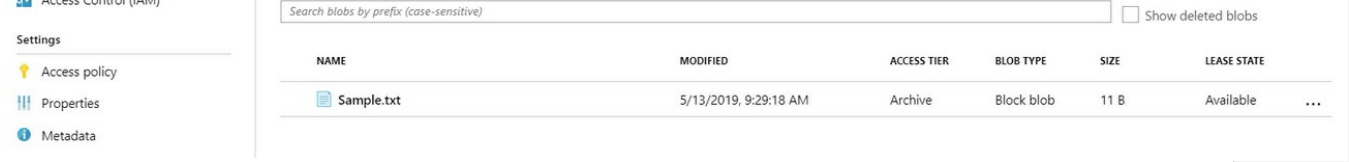
Choose 2 answers from the options given below

✅ deploy an Azure logic app that has an Azure CosmosDB connector
Explanation:-You can use the CosmosDB connector for azure logic app to Trigger a workflow when data is send to CosmosDB
deploy a function app that has an Azure CosmosDB connector
✅ ensure the Azure logic app uses a sendgrid action
Explanation:-You can use the CosmosDB connector for azure logic app to Trigger a workflow when data is send to CosmosDB
ensure the Azure function app uses a sendgrid action

Q59)

A team has created a storage account in Azure they also have the following object available in the storage account





In order to access the sample txt file which of the following must be done first

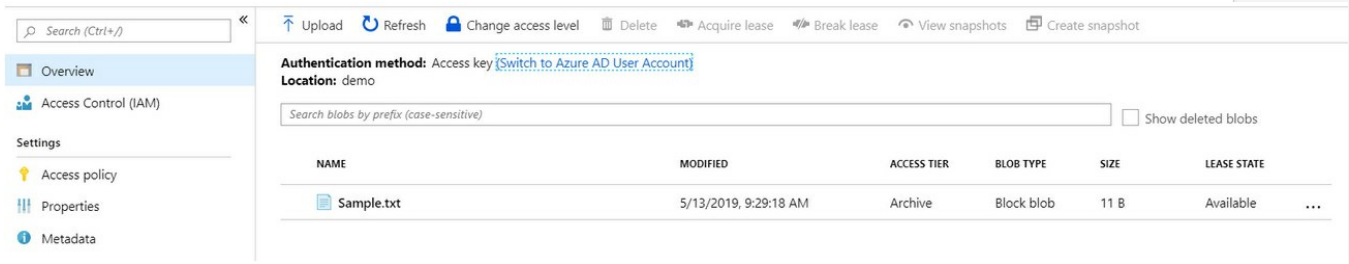
- generate a snapshot
- ✓ modify the access tier

Explanation:-In order to access the BLOB. send it is in the archive access tier. you need to first change the access tier for the blob object.

- generate a shared access signature
- modify the type of blob

Q60)

A team has created a storage account in Azure they also have the following object available in the storage account



The object available in the storage account are _____.

- at a highest storage cost
- ✓ at a lowest storage cost
- at a lowest data retrieval cost
- at a premium storage cost
