SARGUNAN PRAKASH (ES Practice)

Azure

Scenario 1: Your team needs to deploy a virtual machine in azure portal to test a new software application. Here the team has requested both windows and Linux virtual machine.

Question: How could you set up these virtual machines? and what consideration is needed for prizing and OS licensing?

Answer:

Steps to create virtual machine:

1. Go to Home - Microsoft Azure , and on the left sidebar, select Virtual Machines.
2. Click on + Add to create a new VM.
3. Choose a subscription.
4. Select a Resource Group.
5. Configure VM settings:
   a. Give the virtual machine name.
   b. Select the region.
   c. Select the availability Options.
   d. Image: Select the OS (Windows, Linux, etc.).
   e. Size: Choose the size (CPU, RAM).
   f. Authentication type: Choose SSH key (Linux) or password (Windows).
   g. Inbound port rules: Select which ports you want to open (e.g., SSH (Secured Shell) for Linux, RDP (Remote Desktop Protocol) for Windows).
6. Storage Configuration

   Azure VMs use managed disks for storage. Choose between Standard SSD, Premium SSD, or Standard HDD depending on performance needs.
7. Networking

   Choose an existing Virtual Network or create a new one.
8. Review and Create

   Review all your settings and hit Create to deploy the VM.

Pricing Considerations:

- VM size (CPU, RAM) and type (general-purpose, compute-optimized or memory-optimized).

- Operating system: windows (charged for both the compute resource and the Windows license) or Linux (mostly free)
- Licensing models: pay as you go, reserved instances, azure hybrid benefit.
- Storage cost: type (Standard SSD, Premium SSD, or Standard HDD) and disk size (128GB, 512GB)

Scenario 2: The IT security team has requested the sensitive data stored in azure storage account we encrypted to meet compliance requirements.

Question: How could you ensure the data stored in azure storage is encrypted, and what encryption types are available?

Answer:

To ensure the data stored in an Azure Storage Account is encrypted to meet compliance requirements, you can use Azure Storage Encryption. Azure automatically encrypts data at rest using Microsoft-managed keys by default.

Azure Storage Service Encryption (SSE) - Azure automatically encrypts all data at rest using AES-256 encryption. No additional configuration is required for Microsoft-managed Keys.

Encryption Types:

- Microsoft-Managed Keys (MMK)
- Customer-Managed Keys (CMK)
- Client-Side Encryption (CSE)
- Infrastructure Encryption.

Scenario 3: You are responsible for setting up a DevOps pipeline in Azure DevOps for your application. The pipeline must deploy code to an Azure app service and notify the team if the deployment fails.

Question: How could you configure this pipeline to meet this requirement?

Answer:

Step 1: Go to Azure DevOps and login

Step 2: Click New Project and Enter the name of the project.
Step 3: Select Private/Public repo, Version Control and Work Item.
Step 4: Click Create
Step 5: Navigate to your project, Import the repo and push the code
Step 6: Go to Pipelines and Click New Pipeline.
Step 7: Select the repository
Step 8: Choose “Starter Pipeline”, if existing then “Existing YAML”
Step 9: Navigate to Azure DevOps and select Project Settings.
Step 10: Click on New Service Connection and Select Azure Resource Manager.
Step 11: Choose Service Principle
Step 12: Select your Subscription and App Service
Step 13: Click Save button
Step 14: Again, go to Project Settings and navigate to Notifications
Step 15: Click New Subscription
Step 16: Select Build Completed
Step 17: Set the condition to trigger only on failures
Step 18: Add team’s email addresses
Step 19: Click Save
Step 20: Go to Pipelines and select the pipeline
Step 21: Click Run C Check logs
Step 22: If a failure occurs, email notification will be sent.

Scenario 4: Your organization is moving its premises SQL database to Azure. The database must remain accessible during migration with minimal downtime.

Question: Which Azure service could you use, and how could you perform the migration?

Answer:

Azure Service: Use Azure Database Migration Service (DMS) to migrate the SQL database with minimal downtime.

Step 1: Ensure on-premises SQL server is running and accessible
Step 2: Take backup as a precaution
Step 3: Enable Transaction Log Backups for minimal downtime
Step 4: Choose Azure SQL Database as a destination
Step 5: Create an Azure SQL server and configure network settings
Step 6: Deploy Azure Database Migration Service in Azure portal
Step 7: Choose Online Migration option for minimal downtime
Step 8: Connect the source SQL server and destination Azure SQL Database
Step 9: Start the migration process using DMS

Step 10: Monitor the progress through Azure portal Step 11: Once completed, validate data integrity.