### **Scenario 1.**

### **Your team needs to deploy a virtual machine in Azure to test a new software application.**

### **Here, a team requested both windows and Linux virtual machine.**

### **Question?**

### **How could u set up these virtual machines and what considerations are needed for pricing and OS licensing? Steps to Set Up the Virtual Machines**

1. **Access Azure Portal:**
   1. Log in to the Azure portal.
2. **Create a Resource Group:**
   1. Go to "Resource Groups" and create a new resource group to organize the resources for both VMs.
   2. Choose an appropriate name and region (e.g., "test-environment" in "South India").
3. **Deploy the Windows Virtual Machine:**
   1. Go to **"Create a resource" > Compute > Windows Virtual Machine.**
   2. Select:
      1. **Image**: Choose a Windows OS (e.g., Windows Server 2022 Datacenter).
      2. **Size**: Select a VM size based on application requirements (e.g., Standard\_B2s for testing purposes).
      3. **Licensing**: Enable Azure Hybrid Benefit if you already own Windows Server licenses (covered below).
      4. Configure **networking** and enable any specific ports (e.g., RDP - 3389 for Windows).
4. **Deploy the Linux Virtual Machine:**
   1. Go to **"Create a resource" > Compute > Linux Virtual Machine.**
   2. Select:
      1. **Image**: Choose a Linux distribution (e.g., Ubuntu, CentOS, or Red Hat).
      2. **Size**: Use similar or different sizing as needed.
      3. Configure **networking** and enable SSH (default port 22) for secure access.
5. **Post-Deployment Configuration:**
   1. Set up additional disk storage if needed.
   2. Configure monitoring using Azure Monitor to track performance and diagnostics.
   3. Secure both VMs using **Azure Bastion** or by limiting IP ranges for RDP/SSH access.

### **Pricing Considerations**

1. **VM Size (SKU):**
   1. Pricing varies by VM size and region. For testing purposes, choose smaller, cost-effective sizes like **B-series (Burstable VMs)** or **D-series**.
2. **Region:**
   1. Select regions with lower costs if latency isn’t a concern. For example, West US might have different pricing than East US.
3. **Reserved Instances:**
   1. Use **Pay-As-You-Go** for short-term testing or consider Reserved Instances if this testing will persist for months.
4. **Storage:**
   1. Use **Standard SSD** or **Standard HDD** disks for cost efficiency unless high performance is needed.
5. **Data Transfer Costs:**
   1. Outbound data transfer (to the internet) incurs additional charges. Keep testing workloads within Azure or limit internet-bound traffic.

### **OS Licensing Considerations**

1. **Windows VM Licensing:**
   1. Azure pricing for Windows VMs includes the OS licensing cost.
   2. If your organization has **existing Windows Server licenses with Software Assurance**, you can enable the **Azure Hybrid Benefit** to reduce costs.
2. **Linux VM Licensing:**
   1. Most Linux distributions (e.g., Ubuntu, CentOS) are free to use in Azure.
   2. For paid distributions like Red Hat Enterprise Linux (RHEL) or SUSE Linux Enterprise Server (SLES), additional costs apply.

### **Other Considerations**

1. **Testing Requirements:**
   1. Confirm if the software requires specific CPU, memory, or disk performance.
   2. Ensure that the chosen VMs meet minimum application requirements.
2. **Scalability:**
   1. Use **Virtual Machine Scale Sets (VMSS)** if you anticipate scaling during testing.
3. **Automation:**
   1. Use Azure CLI, Azure PowerShell, or an ARM template to automate the VM creation process for consistency.
4. **Security:**
   1. Apply Network Security Groups (NSGs) to control inbound and outbound traffic.
   2. Consider using Azure Key Vault to securely store credentials.

### **Scenario 2.**

### **The IT security team requested the sensitive data stored in a azure storage account the encrypted to meet compliance requirements.**

### **Question?**

### **How could you ensure the data stored in azure is encrepted, and what encryption types are available?**

### **Steps to Ensure Data Encryption in Azure**

1. **Enable Azure Storage Encryption (Default Behavior):**
   1. Azure Storage encrypts all data at rest by default, regardless of the service used (Blobs, Files, Queues, or Tables).
   2. Encryption is **transparent** to users, meaning data is automatically encrypted when stored and decrypted during retrieval.
   3. No manual setup is needed for this default encryption, which uses **Microsoft-Managed Keys (MMK)**.
2. **Switch to Customer-Managed Keys (CMKs) for Compliance:**
   1. If compliance requirements mandate control over encryption keys, you can switch to **CMKs**.
   2. **Steps:**
      1. Create or import an encryption key in **Azure Key Vault**.
      2. Go to the Azure portal, navigate to the **Storage Account** settings, and select the **Encryption** blade.
      3. Choose **Customer-Managed Keys** and specify the Key Vault and key to use.
   3. Benefits:
      1. You can control key rotation policies.
      2. It offers an added layer of security as you maintain control over the keys.
3. **Enable Azure Disk Encryption for Virtual Machine Data:**
   1. If sensitive data resides on disks attached to Azure VMs:
      1. For **Windows VMs**, Azure uses **BitLocker** to encrypt the OS and data disks.
      2. For **Linux VMs**, Azure uses **DM-Crypt** for encryption.
   2. **Steps:**
      1. Navigate to the VM's settings in the Azure portal.
      2. Enable **Azure Disk Encryption** under the **Disks** section.
      3. Use Azure Key Vault to manage encryption keys.
4. **Secure Data in Transit:**
   1. Ensure all data being transferred to and from Azure is encrypted:
      1. Enable the **"Secure transfer required"** setting on your storage account to enforce HTTPS connections.
      2. Use SMB 3.0 encryption for Azure Files.
   2. Example: If you are uploading data to Azure Blob Storage, ensure you use HTTPS endpoints.
5. **Transparent Data Encryption (TDE) for Databases:**
   1. If the sensitive data is stored in Azure SQL Database, Azure Synapse Analytics, or Azure Managed Instances:
      1. Enable **TDE**, which encrypts the data and log files at rest using AES-256.
   2. TDE is enabled by default for new databases, but you can confirm this by checking the database's encryption settings.
6. **Implement Client-Side Encryption for Additional Control:**
   1. For highly sensitive scenarios, encrypt the data on the client-side before uploading it to Azure.
   2. Tools like the **Azure Storage SDK** provide libraries for client-side encryption, allowing you to manage the keys and encryption process locally.

### **Types of Encryptions Available in Azure**

#### **1. Encryption at Rest**

* **Server-Side Encryption (SSE):**
  + Automatically encrypts data when it is stored in Azure and decrypts it when accessed.
  + Options:
    - **Microsoft-Managed Keys (MMK):**
      * Default option, where Microsoft manages the keys for you.
      * Suitable for most general-purpose workloads.
    - **Customer-Managed Keys (CMK):**
      * Use your own encryption keys stored in Azure Key Vault.
      * Ideal for regulatory compliance where organizations need to control and rotate keys.
    - **Customer-Provided Keys (CPK):**
      * You provide encryption keys at the time of data upload.
      * Gives complete control over the encryption process.
* **Azure Disk Encryption:**
  + Encrypts virtual machine disks using BitLocker (Windows) or DM-Crypt (Linux).

#### **2. Encryption in Transit**

* Protects data being transmitted to and from Azure services.
* Enforced through:
  + **TLS/HTTPS**: Encrypts data during transport.
  + **SMB 3.0 Encryption**: Secures Azure Files during access.
* Azure also provides options for **private endpoints**, ensuring data never leaves Microsoft's internal network.

#### **3. Client-Side Encryption**

* Data is encrypted by the client application before being uploaded to Azure.
* Provides end-to-end control over encryption keys and ensures Azure only stores already-encrypted data.
* Example: Use the **Azure Storage SDK** for Java, .NET, Python, or JavaScript to encrypt data locally before uploading.

#### **4. Double Encryption**

* Applies to services like Azure Managed Disks or SQL databases where encryption occurs twice:
  + Once with **infrastructure encryption**.
  + Once with **data encryption**.
* Ensures compliance with highly stringent data protection standards.

### **Best Practices for Compliance**

1. **Key Management with Azure Key Vault:**
   1. Use Key Vault for securely managing keys and secrets.
   2. Implement policies for key expiration and rotation.
2. **Enforce Secure Connections:**
   1. Always enable the **Secure transfer required** option in storage accounts to force HTTPS.
3. **Monitor Encryption Status:**
   1. Use **Azure Security Center** and **Azure Monitor** to ensure compliance with encryption policies.
   2. Set up alerts for non-compliance.
4. **Apply Azure Policies:**
   1. Use **Azure Policy** to enforce encryption standards across your environment.
   2. Examples:
      1. Require all storage accounts to use CMKs.
      2. Enforce "Secure transfer required."
5. **Backups and Snapshots:**
   1. Ensure that backups of data (e.g., Azure Blob Storage snapshots or SQL database backups) are also encrypted.
   2. Verify backup policies and encryption settings.

### **Example Use Case: Secure Storage for Sensitive Files**

Let’s say you need to store healthcare data that requires encryption for compliance with regulations like **HIPAA**:

1. Create a Storage Account with **CMKs** in Azure Key Vault.
2. Enable "Secure transfer required" to force HTTPS.
3. Use **Azure Blob Storage** for storing sensitive files and configure the lifecycle policy to delete outdated data.
4. Use **Azure Monitor** and **Azure Security Center** to audit encryption compliance.

### **Scenario 3.**

### 

### **You're responsible for setting up Devops pipeline in azure Devops for your application.**

### **The pipeline must deploy code to an app service and notify the team if the deployment fails.**

### 

### **Question?**

### **How could you configure this pipeline to meet the requirements?**

### **Detailed Steps to Configure the Pipeline**

#### **1. Set Up Azure DevOps Project and Repository**

* Log in to **Azure DevOps** and navigate to your organization or project.
* If the application code is not already in Azure DevOps, import it into a repository. You can link to external repositories like GitHub or Bitbucket if needed.

#### **2. Create and Configure a New Azure DevOps Pipeline**

* Go to the **Pipelines** tab in Azure DevOps.
* Select **Create Pipeline**.
* Choose the source repository where the application code resides.
* Use the **YAML pipeline** for flexibility and scalability.

#### **3. Define the YAML Pipeline to Deploy to Azure App Service**

Here’s a comprehensive YAML pipeline with additional steps and improvements:

trigger:  
 branches:  
 include:  
 - main # Trigger the pipeline when changes are pushed to the 'main' branch.  
variables:  
 azureSubscription: "<Your Azure Service Connection>" # Azure service connection name  
 appServiceName: "<Your App Service Name>" # Azure App Service name  
 slackWebhookUrl: "$(SlackWebhookUrl)" # Slack webhook stored in pipeline secrets  
 teamEmail: "[team@example.com](mailto:team@example.com)" # Team email for notifications  
 artifactPath: "$(System.DefaultWorkingDirectory)/\*\*/\*.zip" # Path to build artifact  
  
stages:  
- stage: Build  
 displayName: "Build Stage"  
 jobs:  
 - job: BuildJob  
 displayName: "Build the Application"  
 pool:  
 vmImage: "ubuntu-latest"  
 steps:  
 - task: UseDotNet@2  
 inputs:  
 packageType: sdk  
 version: "6.x" # Replace with the required version of .NET or relevant SDK  
 - script: |  
 dotnet restore  
 dotnet build --configuration Release  
 displayName: "Restore and Build"  
 - task: PublishBuildArtifacts@1  
 inputs:  
 pathToPublish: "$(System.DefaultWorkingDirectory)/bin/Release"  
 artifactName: "drop"  
 displayName: "Publish Build Artifacts"  
  
- stage: Deploy  
 displayName: "Deploy Stage"  
 dependsOn: Build  
 jobs:  
 - deployment: DeployJob  
 displayName: "Deploy to Azure App Service"  
 environment: "Production" # Name the environment (can be Dev, Staging, or Production)  
 pool:  
 vmImage: "ubuntu-latest"  
 strategy:  
 runOnce:  
 deploy:  
 steps:  
 - task: AzureWebApp@1  
 inputs:  
 azureSubscription: "$(azureSubscription)"  
 appType: "webApp"  
 appName: "$(appServiceName)"  
 package: "$(artifactPath)"  
 - script: |  
 echo "Verifying deployment..."  
 curl -f https://$(appServiceName).azurewebsites.net || exit 1  
 displayName: "Verify Deployment"  
  
- stage: Notify  
 displayName: "Notification Stage"  
 condition: failed() # This stage runs only if a previous stage fails  
 jobs:  
 - job: NotifyTeam  
 displayName: "Notify Team of Failure"  
 pool:  
 vmImage: "ubuntu-latest"  
 steps:  
 - task: SlackNotification@1 # Using a Slack task for notifications  
 inputs:  
 slackWebhookUrl: "$(slackWebhookUrl)"  
 message: |  
 Deployment failed for $(Build.Repository.Name) on branch $(Build.SourceBranch).  
 Check the Azure DevOps pipeline logs for details: $(System.TeamFoundationCollectionUri)$(System.TeamProject)/\_build/results?buildId=$(Build.BuildId)  
 - task: Email@1  
 inputs:  
 to: "$(teamEmail)"  
 subject: "Deployment Failure Alert: $(Build.Repository.Name)"  
 body: |  
 Hello Team,  
 The deployment of the application $(Build.Repository.Name) to Azure App Service ($(appServiceName)) has failed.  
 Please investigate the issue. Access the pipeline logs here: $(System.TeamFoundationCollectionUri)$(System.TeamProject)/\_build/results?buildId=$(Build.BuildId)

### **Detailed Explanation of Each Section**

#### **Trigger Configuration**

* Specifies that the pipeline will run automatically whenever there is a push to the main branch.
* You can adjust the trigger to include or exclude specific branches.

#### **Variables**

* Define reusable variables for important parameters, such as the Azure service connection name, App Service name, Slack webhook URL, team email, and artifact paths.

#### **Build Stage**

* **Objective:** Compile the application and prepare artifacts for deployment.
* Key Steps:
  + Use the UseDotNet@2 task (or a language-specific equivalent) to install the required SDK/runtime.
  + Restore dependencies and build the project.
  + Publish the compiled application as an artifact for the next stage.

#### **Deploy Stage**

* **Objective:** Deploy the compiled application to Azure App Service.
* Key Steps:
  + Use the AzureWebApp@1 task to deploy the application artifact to the specified App Service.
  + Verify the deployment with a curl command to ensure the application is reachable.

#### **Notification Stage**

* **Objective:** Notify the team in case of deployment failure.
* Key Details:
  + **Slack Notifications:** Send a Slack message with deployment failure details.
  + **Email Notifications:** Send an email alert to the team, including a direct link to the pipeline logs for troubleshooting.

### **Key Considerations for a Robust Pipeline**

#### **1. Authentication with Azure**

* Use a **Service Connection** in Azure DevOps to authenticate and deploy resources securely.
* Ensure the service principal associated with the service connection has adequate permissions (e.g., **Contributor** or **App Service Contributor** role).

#### **2. Artifact Management**

* Ensure the PublishBuildArtifacts task is configured to store build outputs.
* Use consistent naming for artifacts and ensure the Deploy stage references the correct artifact paths.

#### **3. Deployment Verification**

* Add a verification step (e.g., curl) to confirm the app is live after deployment.
* Optionally, run integration tests post-deployment to ensure functionality.

#### **4. Error Handling**

* Use the condition: failed() clause to trigger the notification stage only if earlier stages fail.
* Include detailed logs and pipeline information in notifications to aid troubleshooting.

#### **5. Security**

* Store sensitive information, like Slack webhook URLs or email credentials, as pipeline secrets or environment variables in Azure DevOps.

#### **6. Continuous Deployment**

* Integrate this pipeline with your **CI/CD** workflow for automatic deployment after successful builds.
* Use deployment slots (e.g., **staging**) to test before production deployment.

### **Monitoring and Improving the Pipeline**

#### **1. Monitoring Deployment**

* Use **Azure Monitor** and **Application Insights** to track application health after deployment.
* Enable diagnostics logs on the App Service for troubleshooting.

#### **2. Azure DevOps Insights**

* Review pipeline execution statistics to identify bottlenecks.
* Use pipeline analytics to improve success rates and optimize runtimes.

#### **3. Rollback Plan**

* Implement a rollback mechanism to redeploy the last successful build if the new deployment fails.

### **Scenario 4.**

### **Your organization is moving its on premises SQL database to Azure the database must remain accessible while migrating with minimal downtime.**

### **Question?**

### **Which Azure service do you use and how do you perform the migration?**

### **1. Choosing the Appropriate Azure SQL Service**

Azure offers several SQL services. The choice depends on your application requirements, database size, and desired level of control.

**Options:**

1. **Azure SQL Database**:
   1. A fully managed PaaS offering ideal for modern cloud-native applications.
   2. Automatically scales and includes built-in backups, updates, and high availability.
   3. Suitable if your application requires only a single database instance.
2. **Azure SQL Managed Instance**:
   1. A managed database service that provides near 100% compatibility with on-premises SQL Server, including SQL Agent, cross-database queries, and CLR.
   2. Ideal for organizations looking to move legacy applications with minimal changes.
3. **Azure SQL Virtual Machine**:
   1. An IaaS offering that allows you to run SQL Server on an Azure VM.
   2. Provides full control over the SQL Server environment and is suitable for highly customized setups.

#### **Factors to Consider:**

* **Compatibility**: Use Azure SQL Managed Instance if you're on-premises database relies on advanced SQL Server features.
* **Scaling Needs**: Azure SQL Database offers easy scaling for modern apps.
* **Operational Control**: Choose Azure SQL Virtual Machine for full control over OS and SQL Server configurations.

### **2. Preparation Phase**

Proper preparation ensures a smooth migration process and reduces potential risks.

#### **a. Assess the On-Premises Database**

* Use the **Data Migration Assistant (DMA)** to:
  + Analyze compatibility issues with the target Azure SQL service.
  + Identify unsupported features or required schema modifications.
  + Assess database readiness for migration.

#### **b. Set Up the Target Azure SQL Environment**

* **Provision the Target Database**:
  + Log in to the Azure Portal.
  + Create the Azure SQL Database, Managed Instance, or Virtual Machine.
  + Configure computer and storage based on database size and workload needs.
* **Enable Security Features**:
  + Configure **firewall rules** or use **virtual network integration** to secure access.
  + Enable **Transparent Data Encryption (TDE)** to protect data at rest.

#### **c. Configure Network Connectivity**

* Set up reliable and secure network connections between your on-premises environment and Azure:
  + Use **ExpressRoute** for low-latency, private connections.
  + Alternatively, use **Site-to-Site VPN** for encrypted communication over the internet.
* Test connectivity to ensure the on-premises database can communicate with Azure.

#### **d. Back Up the Database**

* Take a full backup of the on-premises SQL database to safeguard against data loss.
* Store the backup in a secure location (e.g., Azure Blob Storage).

### **3. Migration Phase**

To ensure minimal downtime, use **Azure Database Migration Service (DMS)** with the **online migration** option.

#### **Step-by-Step Migration Using Azure Database Migration Service (DMS):**

##### **a. Provision Azure Database Migration Service**

* In the Azure Portal:
  + Search for **Database Migration Service** and create a new instance.
  + Choose the pricing tier based on the size and complexity of your database.

##### **b. Configure the Migration Project**

* In the DMS interface:
  + Create a new migration project.
  + Select the **online migration** option for continuous replication.
  + Specify the source (on-premises SQL Server) and the target (Azure SQL Database, Managed Instance, or Virtual Machine).

##### **c. Perform Schema Migration**

* Use the **Data Migration Assistant (DMA)** to:
  + Export the database schema from the on-premises environment.
  + Apply the schema to the target Azure SQL Database.

##### **d. Perform Data Migration**

* In the DMS migration project:
  + Specify the tables or databases to migrate.
  + Start the initial data migration, which replicates the current data to Azure.
  + Enable continuous replication to keep the source and target databases in sync.

### **4. Cutover Phase**

The cutover phase involves switching the application to the Azure database while minimizing downtime.

#### **Steps to Perform the Cutover:**

1. **Pause Writes to the Source Database**
   1. Schedule a maintenance window to pause any write operations on the on-premises database.
   2. This ensures no new data is written to the source database during the final sync.
2. **Perform Final Synchronization**
   1. In the Azure Database Migration Service:
      1. Trigger the final synchronization to replicate any remaining changes to the Azure database.
3. **Redirect Application Connections**
   1. Update application connection strings to point to the Azure database.
   2. Test application functionality to ensure everything works as expected.

### **5. Post-Migration Tasks**

#### **a. Validate the Migration**

* Compare the source and target databases to ensure data consistency and accuracy.
* Use query testing tools or run application-specific tests.

#### **b. Optimize the Target Database**

* Scale up or down based on workload requirements.
* Optimize database performance using indexing, partitioning, and query tuning.

#### **c. Implement Monitoring and Alerts**

* Enable **Azure Monitor** and **Application Insights** to track database performance and detect issues.
* Configure alerts for key metrics such as CPU usage, query response time, and storage utilization.

#### **d. Enable Backups**

* Configure automated backups for the Azure database:
  + Point-in-Time Restore for Azure SQL Database and Managed Instance.
  + Full and incremental backups for SQL Virtual Machines.

#### **e. Decommission On-Premises Database**

* After confirming the success of the migration, decommission the on-premises SQL Server to free up resources.

### **Key Considerations for a Successful Migration**

#### **1. Minimal Downtime**

* Online migration ensures the database remains accessible during the process, reducing downtime to a few minutes during the cutover.

#### **2. Secure Data Transfer**

* Use **encrypted connections** (e.g., SSL/TLS) to secure data in transit.
* Configure **Azure Private Link** or **ExpressRoute** for enhanced security.

#### **3. Scalability**

* Ensure the Azure database tier and compute/storage configurations can handle future workload growth.

#### **4. High Availability**

* Enable high availability features such as **Auto-Failover Groups** or **Zone-Redundant Configurations** to minimize disruptions in case of failures.

#### **5. Cost Management**

* Use Azure Cost Management to monitor and control expenses during and after migration.
* Scale resources as needed to optimize costs.