Course Title: Microsoft Azure Administrator Associate For Beginner

Module 1: Introduction to Microsoft Azure

- Overview of Cloud Computing
- Introduction to Microsoft Azure
- Azure Services and Solutions

Module 2: Azure Subscriptions and Resource Groups

- Understanding Azure Subscriptions
- Creating and Managing Resource Groups
- Resource Group Best Practices

Hands-On:

- Introduction to Azure Subscriptions
  - Definition and Purpose of Azure Subscriptions
  - Subscription Types and Tiers
  - Subscription Limits and Quotas
- Creating and Managing Azure Subscriptions
  - Creating a New Azure Subscription
  - Subscription Governance and Access Control
  - Subscription Management Best Practices
- Creating and Managing Resource Groups
  - Definition and Purpose of Resource Groups
  - Benefits of Using Resource Groups
  - Scenarios for Resource Group Usage
- Creating Resource Groups
  - Step-by-Step Guide to Creating Resource Groups
  - Naming Conventions and Guidelines
  - Tagging Strategies for Resource Groups

- Managing Resources With in Resource Groups
  - Adding and Removing Resources
  - Moving Resources Between Resource Groups
  - Monitoring and Auditing Resource Group Activities
- Resource Group Best Practices
  - Organizing Resources Based on Functionality
  - Implementing Hierarchical Resource Group Structures
- Security Best Practices for Resource Groups
  - Role-Based Access Control (RBAC) for Resource Groups
  - Implementing Policies and Locks
- Resource Group Cleanup and Optimization
  - Identifying and Decommissioning Unused Resources
  - Implementing Automation for Resource Cleanup
  - Regular Audits and Optimization Strategies
  - Final Project Challenge

Module 3: Azure Virtual Machines

- Deploying Virtual Machines
- Configuring Virtual Networks
- Managing Virtual Machine Storage
- Virtual Machine Scaling and High Availability

Hands-On:

Module 3.1 Virtual Machine Deployment

Objective: Deploy a multi-tier web application on Azure Virtual Machines.

Tasks:

- Choose an appropriate operating system for the virtual machines (e.g., Windows Server, Linux).
- Create and configure virtual machines for each tier (e.g., web server, application server, database server).
- Install necessary software and dependencies on each virtual machine.
- Configure networking to allow communication between the virtual machines.
- Deploy a sample web application to ensure proper functionality.

Module 3.2 Configuring Virtual Networks

Objective: Design and implement a secure virtual network for a business application.

Tasks:

- Create a virtual network with subnets for different components (e.g., frontend, backend, and database).
- Configure Network Security Groups (NSGs) to control traffic between subnets.
- Implement a VPN or Express Route connection for secure on-premises connectivity.
- Set up Azure Bastion for secure remote access to virtual machines.
- Monitor and log network traffic using Azure Network Watcher.

Module 3.3 Managing Virtual Machine Storage

Objective: Optimize storage usage and implement backup strategies for virtual machines.

Tasks:

- Configure Azure Managed Disks for virtual machines.
- Implement Azure Storage features such as Azure Blob Storage for data storage.
- Set up Azure Backup to regularly backup virtual machine data.
- Test the restore process to ensure data recoverability.
- Explore and implement Azure Disk Encryption for enhanced security.

Module 3.4 Virtual Machine Scaling and High Availability

Objective: Design and implement scaling and high availability solutions for a critical application.

Tasks:

- Implement Azure Availability Sets for virtual machines.
- Configure load balancing for distributing traffic across multiple virtual machines.
- Explore and set up auto-scaling based on performance metrics.
- Design and implement a disaster recovery plan using Azure Site Recovery.
- Test failover scenarios to ensure high availability and disaster recovery.

Module 3.5 Monitoring and Optimization

Objective: Monitor and optimize the performance of virtual machines and associated resources.

Tasks:

- Implement Azure Monitor to collect and analyze performance data.
- Set up alerts based on key performance indicators.
- Use Azure Advisor to get recommendations for optimizing virtual machine resources.
- Implement Azure Automation to schedule routine tasks and resource optimization.
- Evaluate and implement best practices for cost management and resource optimization.

Module 4: Azure Storage

- Azure Storage Services Overview
- Blob Storage, Table Storage, File Storage, and Queue Storage
- Azure Storage Security and Encryption

Hands-On:

Module 4.1 Azure Storage Services Overview

Objective: Understand and explore different Azure Storage services.

Tasks:

- Create an Azure Storage account.
- Explore the Azure Storage account dashboard and settings.
- Understand the purpose and use cases of each storage service (Blob, Table, File, and Queue).
- Use Azure Portal, Azure CLI, or Azure PowerShell to interact with storage services.
- Perform basic operations like creating containers, tables, file shares, and queues.

Module 4.2 Blob Storage Operations

Objective: Work with Blob Storage for storing and managing unstructured data.

Tasks:

- Create a Blob Storage container.
- Upload and download files to and from Blob Storage using Azure Portal and Azure Storage Explorer.
- Implement blob versioning for data protection.
- Set up a Content Delivery Network (CDN) for efficient content distribution.
- Explore and implement Azure Blob Storage lifecycle management.

Module 4.3 Table Storage and Queue Storage

Objective: Use Table Storage for NoSQL data and Queue Storage for messaging.

Tasks:

- Create a Table Storage account.
- Design and implement a simple NoSQL database using Table Storage.
- Perform CRUD (Create, Read, Update, and Delete) operations on Table Storage.
- Create a Queue Storage and implement message processing using Azure Functions.
- Explore and implement message expiration and visibility timeout in Queue Storage.

Module 4.4 File Storage Implementation

Objective: Set up and manage File Storage for file sharing in the cloud.

Tasks:

- Create a File Storage account.
- Set up file shares and configure access controls.
- Upload and download files to and from File Storage.
- Implement Azure File Sync for hybrid cloud file sharing.
- Explore and implement Azure File Storage snapshots for data recovery.

Module 4.5 Azure Storage Security and Encryption

Objective: Implement security measures and encryption for Azure Storage.

Tasks:

- Configure Azure Storage account firewalls and virtual networks.
- Implement Shared Access Signatures (SAS) for secure access to Blob Storage.
- Enable encryption at rest for Azure Storage accounts.
- Implement Azure Key Vault integration for managing storage account keys.
- Monitor storage account activities using Azure Storage Analytics.

Module 5: Azure Networking

- Virtual Network Configuration
- Network Security Groups (NSGs)
- Azure Load Balancer
- Azure VPN Gateway

Hands-On:

Module 5.1 Virtual Network Configuration

Objective: Design and implement a virtual network for a multi-tier application.

Tasks:

- Plan and design a virtual network architecture for a multi-tier application (e.g., frontend, backend, and database).
- Define subnet structure and IP address ranges for each tier.
- Create a virtual network in Azure.
- Configure subnets based on the designed architecture.
- Implement Network Security Groups (NSGs) to control inbound and outbound traffic.
- Test connectivity between different subnets within the virtual network.
- Set up a private DNS zone for the virtual network.
- Configure DNS records for internal communication.
- Deploy virtual machines in each subnet.
- Test connectivity between virtual machines in different subnets.
- Validate DNS resolution within the virtual network.

Module 5.2 Network Security Groups (NSGs)

Objective: Implement and manage Network Security Groups for traffic control.

Tasks:

- NSG Rules Setup:
- Create NSGs for different subnets within the virtual network.
- Define and implement inbound and outbound security rules for each NSG.
- Application Security Groups (ASGs):
- Implement ASGs to simplify NSG management.
- Assign virtual machines to appropriate ASGs.
- Rule Testing:
- Test NSG rules by attempting to connect to virtual machines from different subnets.
- Validate that NSG rules are effectively filtering traffic.
- NSG Logging:
- Enable NSG flow logs.
- Analyze flow logs to understand network traffic patterns.
- Dynamic Rule Updates:
- Explore and implement dynamic NSG rules based on tags or labels.
- Test dynamic rule updates and observe their impact.

Module 5.3 Azure Load Balancer

Objective: Configure Azure Load Balancer for high availability and load distribution.

Tasks:

- Basic Load Balancer Setup:
- Set up a basic Azure Load Balancer.
- Configure backend pools and health probes.
- Load Balancing Rules:
- Implement load balancing rules for different application services.
- Test the load balancing functionality with multiple virtual machines.
- Inbound NAT Rules:
- Explore and configure inbound NAT rules for specific services.
- Test access to individual virtual machines through NAT rules.

- Health Monitoring:
- Monitor backend pool health using Azure Monitor.
- Configure alerts for load balancer health.
- Traffic Distribution:
- Implement session persistence for specific applications.
- Test and observe the distribution of traffic among backend resources.

Module 5.4 Azure VPN Gateway

Objective: Establish a secure connection between on-premises networks and Azure using VPN Gateway.

Tasks:

- Virtual Network Gateway Setup:
- Set up a Virtual Network Gateway for site-to-site VPN.
- Configure the local network gateway to represent the on-premises network.
- Connection Establishment:
- Establish a connection between the on-premises network and Azure using VPN.
- Verify the VPN connection status.
- Traffic Routing:
- Configure and test routing between on-premises and Azure networks.
- Ensure secure and reliable communication.
- Point-to-Site VPN:
- Implement Point-to-Site VPN for secure remote access to the virtual network.
- Test remote access connectivity.
- Monitoring and Logging:
- Monitor VPN Gateway performance and connection logs.
- Set up alerts for VPN connection status changes.

Module 6: Identity and Access Management

- Azure Active Directory (AD)
- Azure AD Users and Groups
- Role-Based Access Control (RBAC)
- Multi-Factor Authentication (MFA)

Hands-On:

Module 6.1 Azure Active Directory (AD) Setup

Objective: Set up and configure Azure Active Directory.

Tasks:

- Azure AD Creation:
- Create an Azure AD instance in the Azure Portal.
- Configure basic settings such as domain names and synchronization options.
- Directory Users:
- Add users to the Azure AD directory.
- Configure user attributes and profile settings.
- External Identity Providers:
- Integrate external identity providers (e.g., Microsoft accounts, Google) with Azure AD.
- Enable users to sign in using external accounts.
- Self-Service Password Reset:
- Configure self-service password reset options for Azure AD users.
- Test and validate the password reset process.

Module 6.2 Azure AD Users and Groups

Objective: Manage users and groups in Azure Active Directory.

Tasks:

- User Group Creation:
- Create different user groups based on roles or departments.
- Assign users to appropriate groups.
- Group-Based Access Control:
- Implement group-based access control for Azure resources.
- Test access permissions based on group membership.
- User Attributes and Claims:
- Customize user attributes and claims.
- Use custom attributes for user-specific information.
- Dynamic Group Memberships:
- Create dynamic user groups based on user attributes.
- Test automatic membership changes based on user attributes.

Module 6.3 Role-Based Access Control (RBAC)

Objective: Implement RBAC for controlling access to Azure resources.

Tasks:

- Role Assignment:
- Create custom roles or use built-in roles in Azure RBAC.
- Assign roles to users or groups for specific resources.
- Scope Management:
- Implement RBAC at different scopes (subscription, resource group, resource).
- Test and validate access permissions based on the assigned roles.
- Azure Policy Integration:
- Integrate Azure Policy with RBAC for additional governance.
- Enforce compliance and security policies using RBAC.

Module 6.4 Multi-Factor Authentication (MFA)

Objective: Enhance security with Multi-Factor Authentication.

Tasks:

- MFA Setup:
- Enable Multi-Factor Authentication for Azure AD users.
- Choose and configure MFA methods (e.g., phone call, text message, and mobile app).
- Conditional Access Policies:
- Implement conditional access policies that require MFA under specific conditions.
- Test the application of conditional access policies.
- User Enrollment:
- Guide users through the process of enrolling in Multi-Factor Authentication.
- Communicate the importance of MFA for enhanced security.
- Monitoring and Reporting:
- Monitor MFA usage and success/failure rates.
- Set up reporting for MFA-related events and alerts.

Module 6.5 Identity and Access Management Automation

Objective: Automate identity and access management tasks.

Tasks:

- Azure AD PowerShell Automation:
- Use Azure PowerShell to automate user and group management tasks.
- Create scripts for bulk operations on Azure AD objects.
- Role Assignment Automation:

- Automate the process of assigning roles to users or groups using Azure Automation.
- Implement scheduled role assignments based on specific criteria.
- MFA Policy Automation:
- Use Azure Policy and PowerShell to automate the enforcement of MFA policies.
- Implement automated responses to MFA-related events.

Module 7: Azure Virtual Network Connectivity

- Site-to-Site and Point-to-Site Connectivity
- Express Route
- VNet Peering

Hands-On:

Module 7.1 Site-to-Site Connectivity

Objective: Establish a secure connection between on-premises and Azure virtual networks.

Tasks:

- Network Design:
- Design a network architecture with on-premises and Azure components.
- Define IP addressing and subnets for on-premises and Azure networks.
- VPN Gateway Configuration:
- Set up a Virtual Network Gateway for Site-to-Site VPN.
- Configure the local network gateway to represent the on-premises network.
- Connection Establishment:
- Establish a secure connection between the on-premises network and Azure using Site-to-Site VPN.
- Validate connectivity by sending traffic between on-premises and Azure resources.
- Monitoring and Optimization:
- Monitor VPN Gateway performance and connection logs.
- Optimize the VPN connection for better performance.

Module 7.2 Point-to-Site Connectivity

Objective: Enable secure remote access to the Azure virtual network.

Tasks:

- VPN Client Configuration:
- Configure and distribute VPN client configurations to on-premises devices.
- Test the ability to establish a secure Point-to-Site VPN connection.
- Conditional Access Policies:
- Implement conditional access policies for Point-to-Site VPN.
- Enforce additional security measures for remote access.
- Monitoring and Reporting:
- Monitor Point-to-Site VPN usage and connection logs.
- Set up reporting and alerts for Point-to-Site VPN-related events.

Module 7.3 Express Route Connectivity

Objective: Establish a private, high-throughput connection between on-premises and Azure using Express Route.

Tasks:

- Express Route Circuit Setup:
- Provision an Express Route circuit with the required bandwidth and configuration.
- Establish a connection between the on-premises network and Azure using Express Route.
- Route Configuration:
- Configure BGP routing between on-premises and Azure networks.
- Ensure proper route propagation and network reachability.
- Monitoring and Troubleshooting:
- Monitor Express Route circuit performance using Azure Monitor.
- Implement troubleshooting steps for connectivity issues.

Module 7.4 VNet Peering

Objective: Enable communication between Azure virtual networks using VNet Peering.

Tasks:

- VNet Creation:

- Create two separate Azure virtual networks with different subnets.
- VNet Peering Configuration:
- Configure VNet Peering between the two virtual networks.
- Define and implement peering rules for traffic flow.
- Testing Connectivity:
- Deploy virtual machines in each virtual network.
- Test connectivity between virtual machines in different virtual networks.
- Security Considerations:
- Implement Network Security Groups (NSGs) to control traffic between peered virtual networks.
- Ensure that only necessary traffic is allowed between the networks.

Module 7.5 Advanced Connectivity Scenarios

Objective: Implement advanced connectivity scenarios to meet specific business requirements.

Tasks:

- Hub-and-Spoke Architecture:
- Design and implement a hub-and-spoke architecture using virtual networks.
- Configure VNet Peering to connect spokes to the hub.
- Transit Network:
- Design and implement a transit virtual network for routing traffic between different connected networks.
- Utilize Azure Route Tables for efficient routing.
- Global VNet Peering:
- Extend connectivity globally using Global VNet Peering.
- Connect virtual networks in different Azure regions.
- Express Route Global Reach:
- Explore and implement Express Route Global Reach for connecting on-premises networks globally.
- Test and validate global network connectivity.

Module 8: Monitoring and Diagnostics

- Azure Monitor Overview
- Log Analytics and Application Insights
- Azure Metrics and Alerts

Hands-On:

Module 8.1 Azure Monitor Overview

Objective: Implement basic monitoring and gain insights into Azure resources.

Tasks:

- Azure Monitor Setup:
- Set up Azure Monitor for the subscription.
- Configure basic monitoring settings for resource health.
- Activity Log Analysis:
- Explore and analyze activities logged in the Azure Activity Log.
- Identify and understand critical events related to resource changes.
- Diagnostic Settings:
- Configure diagnostic settings for key Azure resources.
- Stream resource logs to Azure Monitor for central analysis.
- Dashboard Creation:
- Create a custom Azure Dashboard to visualize key metrics.
- Add relevant charts and graphs for quick resource status assessment.

Module 8.2 Log Analytics and Application Insights

Objective: Utilize Log Analytics and Application Insights for in-depth analysis.

Tasks:

- Log Analytics Workspace Setup:
- Create a Log Analytics workspace.
- Configure data sources for Log Analytics.
- Query Language Exploration:
- Learn and practice Kusto Query Language (KQL) for Log Analytics.
- Write queries to extract meaningful insights from log data.
- Custom Log Searches:
- Implement custom log searches based on specific resource requirements.
- Save and schedule log searches for regular monitoring.
- Application Insights Integration:
- Set up Application Insights for a web application.
- Analyze application performance and user interactions.

Module 8.3 Azure Metrics and Alerts

Objective: Utilize Azure Metrics and Alerts for proactive monitoring.

Tasks:

- Metric Exploration:
- Explore Azure Metrics for different resources.

- Identify key performance indicators and metrics.
- Alert Rule Creation:
- Create alert rules based on specific metric thresholds.
- Configure alert actions, such as sending emails or triggering Azure Automation Runbooks.
- Auto-Scaling with Metrics:
- Implement auto-scaling based on Azure Metrics.
- Configure scaling rules to adjust resources dynamically.
- Metric Visualization:
- Visualize metrics data using Azure Monitor charts and graphs.
- Customize metric dashboards based on resource importance.

Module 8.4 Advanced Monitoring Scenarios

Objective: Implement advanced monitoring scenarios for complex environments.

Tasks:

- Log Analytics Workbooks:
- Design and create Log Analytics workbooks for advanced visualizations.
- Customize workbooks for specific monitoring needs.
- Distributed Tracing with Application Insights:
- Implement distributed tracing in Application Insights.
- Analyze end-to-end transaction traces for a comprehensive view.
- Azure Monitor Logs Integration:
- Integrate Azure Monitor Logs with other Azure services (e.g., Azure Security Center).
- Correlate logs from multiple sources for advanced analysis.
- Incident Response and Automation:
- Set up incident response plans based on alerts.
- Implement Azure Automation Runbooks for automatic remediation.

Module 8.5 Monitoring Governance and Compliance

Objective: Establish monitoring governance and ensure compliance.

Tasks:

- Azure Policy for Monitoring:
- Implement Azure Policy for enforcing monitoring standards.
- Ensure that all resources comply with required monitoring settings.
- Log Retention and Archiving:
- Configure log retention settings for compliance requirements.
- Implement log archiving to external storage for long-term storage.
- Security Monitoring:

- Set up Azure Security Center for advanced security monitoring.
- Implement security alerts and recommendations.
- Cost Management with Monitoring:
- Integrate Azure Cost Management with Azure Monitor.
- Monitor and analyze resource costs for optimization.

Module 9: Data Protection and Management

- Azure Backup and Restore
- Azure Site Recovery
- Azure Backup Policies

Hands-On:

Module 9.1 Azure Backup and Restore

Objective: Implement data backup and restoration strategies for Azure resources.

Tasks:

- Azure Backup Setup:
- Set up Azure Backup for key resources (e.g., virtual machines, databases).
- Configure backup policies based on retention requirements.
- Backup and Restore Test:
- Perform a backup of a sample virtual machine.
- Simulate a data loss scenario and restore the virtual machine from the backup.
- Azure Backup for Databases:
- Implement Azure Backup for databases (e.g., Azure SQL Database).
- Configure backup policies for automated database backups.
- Azure Backup Vaults:
- Explore and configure Azure Backup Vaults.
- Implement secure backup storage settings.

Module 9.2 Azure Site Recovery

Objective: Set up disaster recovery solutions using Azure Site Recovery.

Tasks:

- Site Recovery Setup:
- Set up Azure Site Recovery for a virtual machine or an entire application.
- Configure replication settings and target regions.
- Disaster Recovery Test:

- Simulate a disaster scenario by triggering a failover.
- Verify the successful failover and functionality of the replicated resources.
- Application Consistency:
- Ensure application consistency during failover.
- Implement pre- and post-failover scripts for application-specific tasks.
- Cross-Region Replication:
- Explore cross-region replication capabilities of Azure Site Recovery.
- Set up a disaster recovery plan for resources across different Azure regions.

Module 9.3 Azure Backup Policies

Objective: Implement and manage Azure Backup Policies for efficient data protection.

Tasks:

- Backup Policy Creation:
- Create custom Azure Backup Policies for different resource types.
- Configure backup frequency, retention, and storage settings.
- Policy Application:
- Apply backup policies to relevant resources (e.g., virtual machines, Azure Files).
- Ensure that backup policies align with data protection requirements.
- Backup Policy Versioning:
- Explore and implement backup policy versioning.
- Test the impact of policy changes on existing backups.
- Policy Monitoring and Reporting:
- Monitor backup policy compliance.
- Set up reporting and alerts for backup policy events.

Module 9.4 Advanced Data Protection Scenarios

Objective: Implement advanced data protection scenarios for complex environments.

Tasks:

- Long-term Retention:
- Configure long-term retention settings for critical data.
- Implement Azure Backup Vault for archiving.
- Application-Aware Backups:
- Implement application-aware backups for applications like Microsoft Exchange or SharePoint.
- Ensure consistent backups without impacting application functionality.
- Backup and Restore Automation:
- Use Azure PowerShell or Azure CLI to automate backup and restore processes.
- Implement scripts for regular backup tasks.

- Backup Monitoring and Alerts:
- Implement monitoring for backup job status.
- Configure alerts for backup failures or delays.

Module 9.5 Data Protection Governance and Compliance

Objective: Establish data protection governance and ensure compliance.

Tasks:

- Backup Policy Compliance:
- Implement Azure Policy for enforcing backup policies.
- Ensure that all relevant resources comply with backup requirements.
- Data Classification for Backups:
- Implement Azure Information Protection for classifying sensitive data.
- Apply data classification policies to backup processes.
- Backup Security and Access Control:
- Configure secure access controls for Azure Backup.
- Monitor and enforce security policies related to backup storage.
- Incident Response for Data Loss:
- Set up incident response plans for data loss scenarios.
- Implement Azure Automation Runbooks for automatic recovery in case of data loss.

Module 10: Automation and Scripting

- Introduction to Azure Automation
- Azure PowerShell and Azure CLI
- Azure Resource Manager (ARM) Templates

Hands-On:

Module 10.1 Introduction to Azure Automation

Objective: Explore the basics of Azure Automation and its capabilities.

Tasks:

- Azure Automation Account Creation:
- Create an Azure Automation account.
- Configure the necessary settings and modules.
- Runbook Creation:
- Develop a basic PowerShell runbook within the Azure Automation account.
- Test the runbook execution and understand the output.

- Scheduling Automation Jobs:
- Schedule the runbook to execute at specific intervals.
- Monitor and review the job status and logs.
- Hybrid Runbook Workers:
- Set up a hybrid runbook worker to run scripts on on-premises servers.
- Test the execution of runbooks on the hybrid worker.

Module 10.2 Azure PowerShell and Azure CLI

Objective: Practice scripting and automation using Azure PowerShell and Azure CLI.

Tasks:

- Azure PowerShell Scripting:
- Write a PowerShell script to create an Azure resource (e.g., virtual machine, storage account).
- Understand how to authenticate using Azure PowerShell.
- Azure CLI Scripting:
- Write an Azure CLI script to perform a specific task (e.g., creating a network security group, deploying a web app).
- Understand how to authenticate using Azure CLI.
- Combining PowerShell and Azure CLI:
- Develop a script that combines both Azure PowerShell and Azure CLI commands.
- Execute the script to perform a comprehensive automation task.
- Error Handling and Logging:
- Implement error handling mechanisms in scripts.
- Configure logging for better troubleshooting.

Module 10.3 Azure Resource Manager (ARM) Templates

Objective: Learn and utilize Azure Resource Manager (ARM) Templates for infrastructure as code.

Tasks:

- Simple ARM Template Creation:
- Create a basic ARM template to deploy a single Azure resource (e.g., virtual machine, storage account).
- Understand the structure of an ARM template.
- Parameterization:
- Parameterize the ARM template to make it more reusable.
- Test the template with different parameter values.
- Linked Templates:
- Create a master ARM template that links to multiple sub-templates.

- Deploy a complex infrastructure using linked templates.
- Deployments and Rollbacks:
- Understand how to deploy an ARM template using Azure PowerShell or Azure CLI.
- Implement a rollback mechanism in case of deployment failures.

Module 10.4 Advanced Automation Scenarios

Objective: Implement advanced automation scenarios using a combination of Azure Automation, PowerShell, Azure CLI, and ARM templates.

Tasks:

- Dynamic Resource Provisioning:
- Develop a script or template that dynamically provisions resources based on user input or external factors.
- Scaling Automation:
- Implement a solution that automatically scales resources based on predefined conditions (e.g., CPU usage, incoming traffic).
- Environment Provisioning:
- Create a script or template that provisions an entire development or testing environment with multiple interconnected resources.
- Custom Logging and Reporting:
- Enhance scripts and templates with custom logging and reporting features.
- Generate reports on automation job outcomes and resource configurations.

Module 10.5 Automation Governance and Compliance

Objective: Establish governance and compliance practices for automation scripts and templates.

Tasks:

- Policy Enforcement:
- Implement Azure Policy to enforce standards and compliance rules for automation scripts and templates.
- Ensure that scripts adhere to organizational policies.
- Version Control Integration:
- Integrate automation scripts and templates with a version control system (e.g., GitHub, Azure DevOps).
- Manage versioning and track changes.

- Security Best Practices:
- Apply security best practices to automation scripts and templates.
- Ensure that sensitive information is handled securely.
- Continuous Integration/Continuous Deployment (CI/CD):
- Implement a CI/CD pipeline for automation scripts and templates.
- Automate the testing and deployment of scripts in a controlled manner

Module 11: Security and Compliance

- Azure Security Center
- Azure Policy
- Azure Key Vault

Hands-On:

Module 11.1 Azure Security Center Implementation Objective:

Strengthen security posture and monitor security across Azure resources.Tasks:

- Security Center Setup:
- Set up Azure Security Center for the Azure subscription.
- Configure basic security policies.
- Policy Compliance Assessment:
- Assess the compliance of resources using Security Center.
- Address and remediate identified security vulnerabilities.
- Threat Detection Configuration:
- Configure threat detection policies for virtual machines and other resources.
- Investigate and respond to identified threats.
- Just-In-Time Access Control:
- Implement Just-In-Time (JIT) access control for virtual machines.
- Test and validate the impact of JIT policies on access.

Module 11.2 Azure Policy Enforcement

Objective: Establish and enforce governance standards using Azure Policy.

Tasks:

- Policy Definition Creation:
- Create custom Azure Policy definitions based on organizational standards.
- Include policies related to resource naming conventions, tagging, and security.
- Policy Assignment:
- Assign policies to specific resource groups or the entire subscription.
- Verify policy enforcement and compliance.
- Policy Exemptions:
- Explore and implement policy exemptions for specific resources.
- Document and justify the need for exemptions.
- Monitoring and Reporting:
- Monitor policy compliance and violations using Azure Policy.
- Set up reporting and alerts for policy-related events.

Module 11.3 Azure Key Vault Implementation

Objective: Centralize and manage secrets, keys, and certificates securely.

Tasks:

- Key Vault Creation:
- Create an Azure Key Vault to store secrets, keys, and certificates.
- Configure access policies to define who can manage keys.
- Secrets and Keys Management:
- Add secrets and keys to the Key Vault.
- Explore versioning and rotation capabilities.
- Certificate Management:
- Import or generate certificates in the Key Vault.
- Configure automated certificate renewal if applicable.
- Integration with Azure Resources:
- Integrate Azure virtual machines, web apps, or other services with Key Vault.
- Securely retrieve secrets, keys, or certificates from Key Vault in applications.

Module 12: Exam Preparation and Practice

- Overview of the Microsoft Azure Administrator Exam
- Practice Tests and Mock Exams
- Exam Tips and Strategies

Prerequisites:

- Basic understanding of networking concepts
- Familiarity with virtualization and cloud computing basics
- Fundamental knowledge of operating systems (Windows/Linux)

Target Audience:

- IT professionals interested in becoming Azure administrators
- System administrators and network administrators
- Individuals preparing for the Microsoft Azure Administrator Associate Certification exam (Exam AZ-104)