

Implementing Microsoft Azure Infrastructure Solutions

Module I - Create and Manage Azure Resource Manager Virtual Machines

Deploy workloads on Azure Resource Manager (ARM) virtual machines (VMs)

- Identify workloads that can and cannot be deployed run workloads that use Microsoft or Linux operating systems;
- Create VMs; connect to a Windows/Linux VM;
- Deploy workloads; deploy Bring Your Own License (BYOL) images

Perform configuration management

- Automate configuration management by using PowerShell Desired State Configuration (DSC) and VM Agent (custom script extensions);
- Enable remote debugging

Design and implement VM storage

- Configure disk caching & plan storage capacity.
- Configure operating system disk redundancy.
- Configure shared storage using Azure File service & Azure File Share snapshots.
- Configure geo-replication. Encrypt disk.
- Implement ARM VMs with Standard and Premium Storage.
- Configure Blob-Level Tiering (Hot, Cool, Archive). Manage storage encryption keys

Monitor ARM VMs

- Configure ARM VM monitoring; configure alerts.
- Configure diagnostic and monitoring storage location

Manage ARM VM availability

- Configure multiple ARM VMs in an availability set for redundancy.
- Configure each application tier into separate availability sets.
- Combine the Load Balancer with availability sets.
- Configure fault domains and update domains.
- Leverage Availability Zones

Scale ARM VMs

- Scale up and scale down VM sizes.
- Deploy ARM VM Scale Sets (VMSS).
- Configure ARM VMSS auto-scale.

Lab 1

- Create ARM VM & scale Set.
- Create availability set and associate with VM.

Module II - Design and Implement a Storage Strategy

Implement Azure Storage blobs and Azure Files

- Identify appropriate blob type for specific storage requirements.
- Read data, change data ,set metadata on a container.
- Store data using block and page blobs & stream data using blob
- Access blobs securely & implement async blob copy.
- Configure Content Delivery Network (CDN).
- Design blob hierarchies; configure custom domains.
- Scale blob storage; manage SMB file storage; implement Azure StorSimple

Manage access

- Create and manage shared access signatures.
- Use stored access policies & regenerate keys.
- Encrypt keys by using Azure Key Vault integration

Configure diagnostics, monitoring and analytics

- Set retention policies and logging levels; access, add, and remove logs; analyze logs

Implement storage encryption

- Encrypt data as written to Azure Storage by using Azure Storage Service Encryption (SSE).
- Implement encrypted and role-based security for data managed by Azure Data Lake Store.

Lab 2

- Created Azure Storage account.
- Install and browse storage account using Storage Explorer.
- Upload file to Azure Blob Storage using command line & Storage explorer.
- Created and mount Azure File share in windows & Linux Servers.
- Access a storage account with Share access signature.

Module III - Implement Virtual Networks

Configure virtual networks

- Deploy a VM into a virtual network.
- Configure external and internal load balancing.
- Implement Application Gateway & design subnets.
- Configure static, public, and private IP addresses.
- Set up Network Security Groups (NSGs), DNS at the virtual network level, HTTP and TCP health probes, public IPs, User Defined Routes (UDRs), firewall rules, and direct server return.
- Connect VNets by virtual network peering.

Design and implement multi-site or hybrid network connectivity

- Choose the appropriate solution between Azure ExpressRoute, site-to-site, and point-to-site.
- Choose the appropriate gateway.
- Identify supported devices and software VPN solutions.
- Identify networking prerequisites, configure virtual networks and multi-site virtual networks.
- Implement virtual network peering and service chaining.
- Implement hybrid connections to access on-premises data sources, leverage S2S VPNs to connect to on-premises infrastructure.
- Monitor ExpressRoute.

Configure ARM VM networking

- Configure static IP addresses, Network Security Groups (NSGs), DNS, User Defined Routes (UDRs), external and internal load balancing with HTTP and TCP health probes, public IPs, firewall rules, and direct server return.
- Design and implement Application Gateway.
- Configure Accelerated Networking.
- Configure virtual network service endpoints.

Design and implement a connection strategy

- Implement Hybrid Connections to access data sources on-premises; leverage S2S VPN to connect to an on-premises infrastructure

Lab 3

- Create VNet and Subnets.
- Configured VNet Peering between the virtual networks.
- Configure Site to Site VPN between different azure region using Azure VPN Gateway.
- Configure Point to Site VPNN to access the Azure resources from public client machine.

Module IV - Design and Deploy ARM Templates

Implement ARM templates

- Author ARM templates.
- Create ARM templates to deploy multiple ARM Resource Providers resources of different types with count loops and Marketplace items.
- Deploy templates with PowerShell, Azure CLI, Azure Portal and REST API

Control access

- Leverage service principals with ARM authentication.
- Use Azure Active Directory Authentication with ARM.
- Set management policies.
- Configure lock policies.
- lock resources.

Design role-based access control (RBAC)

- Secure resource scopes such as the ability to create VMs and Azure Web Apps.
- Implement Azure RBAC standard roles.

- Design Azure RBAC custom roles.

Lab 4

- Deploy Azure ARM resources using ARM template.
- Create and modify the resource using the visual studio ARM templates.
- Implement the RBAC and control the users access.

Module V - Manage Azure Security and Recovery Services

Manage data protection and security compliance

- Create and import encryption keys with Key Vault.
- Automate tasks for SSL/TLS certificates.
- Prevent and respond to security threats with Azure Security Center.
- Configure single sign-on with SaaS applications using federation and password based authentication.
- Add users and groups to applications.
- Revoke access to SaaS applications.
- Configure access.
- Configure federation with public consumer identity providers such as Facebook and Google.

Implement recovery services

- Create a backup vault.
- Deploy a backup agent; backup and restore data, use snapshots and Geo-replication for recovery.
- Implement DR as service.
- Deploy Azure Site Recovery (ASR) agent, configure ASR; configure ASR one-click failover

Lab 5

- Azure Security center configuration and manage policies.
- Created ASR Vault and configured Backup for VM.
- Restore VM or files using ASR Vault

Module VI - Manage Azure Operations

Enhance cloud management with automation

- Implement PowerShell runbooks.
- Integrate Azure Automation with Web Apps.
- Create and manage PowerShell Desired State Configurations (DSC).
- Import DSC resources; generate DSC node configurations; monitor and automatically update machine configurations with Azure Automation DSC.
- Implement serverless computing, including Azure Functions, Event Grid, and Service Bus

Collect and analyze data generated by resources in cloud and on-premises environments

- Collect and search across data sources from multiple systems.
- Build custom visualisations.
- Visualize Azure resources across multiple subscriptions.

- Transform Azure activity data and managed resource data into an insight with flexible search queries; monitor system updates and malware status.
- Track server configuration changes by using Azure Log Analytics.
- Configure the IT Service Management Connector (ITSMC).

Lab 6

- Create Azure Automation Account & run the custom PowerShell script through the account.
- Create Azure Log Analytics to explore the “Azure Migrate”.
- PowerShell DSC implementation.

Module VII - Manage Azure Identities

Monitor on-premises identity infrastructure and synchronization services with Azure AD Connect Health

- Monitor AD FS proxy and web application proxy servers.
- Setup email notifications for critical alerts.
- Generate utilization report.
- Monitor Sync Engine.
- Monitor domain controllers & monitor replication

Manage domains with Azure Active Directory Domain Services

- Join Azure virtual machines to a domain, securely administer domain-joined virtual machines by using Group Policy.
- Migrate on-premises apps to Azure.
- Handle traditional directory-aware apps along with SaaS apps

Integrate with Azure Active Directory (Azure AD)

- Implement Azure AD Connect and single sign-on with on-premises Windows Server 2016.
- Add custom domains.
- Monitor Azure AD.
- Configure MFA.
- Configure Windows 10 with Azure AD join.
- Implement Enterprise State Roaming, implement Azure AD integration in web and desktop applications.
- leverage Microsoft Graph API.
- Implement Azure Managed Service Identity; implement Privileged Identity Management, implement Azure AD Identity Management, enable self-service password reset.

Lab 7

- Create & Manage users in Azure Active Directory.
- Install Azure AD connect on on-premise Active directory.
- Integrate on-Premise AD to Azure AD.
- Manage Azure AD users and Roles.