# AZ-300/303 Comparison

# Microsoft Azure Architect Technologies

| **Current Skills Measured for AZ-300** | **Updated Skills Measured for AZ-303 List (ignore the numbering below)** |
|---|---|
| **2. Deploy and Configure Infrastructure**<br>**Analyze resource utilization and consumption**<br>• configure diagnostic settings on resources<br>• create baseline for resources<br>• create and test alerts<br>• analyze alerts across subscription<br>• analyze metrics across subscription<br>• create action groups<br>• monitor for unused resources<br>• monitor spend<br>• report on spend<br>• utilize Log Search query functions<br>• view Alerts in Azure Monitor logs<br>• visualize diagnostics data using Azure Monitor Workbooks<br>**Create and configure storage accounts**<br>• configure network access to the storage account<br>• create and configure storage account<br>• generate Shared access signature<br>• implement Azure AD authentication for storage<br>• install and use Azure Storage Explorer<br>• manage access keys<br>• monitor Activity log by using Azure Monitor logs<br>• implement Azure storage replication<br>• implement Azure storage account | **1. Implement and Monitor an Azure Infrastructure (50-55%)**<br>**1.1. Implement cloud infrastructure monitoring**<br>• monitor security<br>(Note: Log Analytics, Azure Security Center, Azure Sentinel)<br>• monitor performance<br>  • configure diagnostic settings on resources<br>  • create a performance baseline for resources<br>  • monitor for unused resources<br>  • monitor performance capacity<br>  • visualize diagnostics data using Azure Monitor<br>• monitor health and availability<br>  • monitor networking<br>  • monitor service health<br>• monitor cost<br>  • monitor spend<br>  • report on spend<br>• configure advanced logging<br>  • implement and configure Azure Monitor insights, including App Insights, Networks, Containers<br>  • configure a Log Analytics workspace<br>  • configure logging for workloads<br>• initiate automated responses by using Action Groups<br>• configure and manage advanced alerts |

| | |
|---|---|
| failover<br>**Create and configure a VM for Windows and Linux**<br>• configure High Availability<br>• configure Monitoring<br>• configure Networking<br>• configure Storage<br>• configure Virtual Machine Size<br>• implement dedicated hosts<br>• deploy and configure scale sets<br>**Automate deployment of VMs**<br>• modify Azure Resource Manager template<br>• configure Location of new VMs<br>• configure VHD template<br>• deploy from template<br>• save a deployment as an Azure Resource Manager template<br>• deploy Windows and Linux VMs<br>**Create connectivity between virtual networks**<br>• create and configure Vnet peering<br>• create and configure Vnet to Vnet connections<br>• verify virtual network connectivity<br>• create virtual network gateway<br>**Implement and manage virtual networking**<br>• configure private IP addressing<br>• configure public IP addresses<br>• create and configure network routes<br>• create and configure network interface<br>• create and configure subnets<br>• create and configure virtual network<br>• create and configure Network Security | • collect alerts and metrics across multiple subscriptions<br>• view Alerts in Azure Monitor logs<br>• NOT: create Log Analytics query<br>**1.2. Implement storage accounts**<br>• select storage account options based on a use case<br>• configure Azure Files and blob storage<br>• configure network access to the storage account<br>• implement Shared Access Signatures and access policies<br>• implement Azure AD authentication for storage<br>• manage access keys<br>• implement Azure storage replication<br>• implement Azure storage account failover<br>**1.3. Implement VMs for Windows and Linux**<br>• configure High Availability<br>• configure storage for VMs<br>• select virtual machine size<br>• implement Azure Dedicated Hosts<br>• deploy and configure scale sets<br>• configure Azure Disk Encryption<br>**1.4. Automate deployment and configuration of resources**<br>• save a deployment as an Azure Resource Manager template<br>• modify Azure Resource Manager template<br>• evaluate location of new resources<br>• configure a virtual disk template<br>• deploy from a template<br>• manage a template library<br>• create and execute an automation |

| | |
|---|---|
| Groups and Application Security Groups<br>**Manage Azure Active Directory**<br>• add custom domains<br>• configure Azure AD Identity Protection<br>• configure Azure AD Join<br>• configure self-service password reset<br>• implement conditional access policies<br>• manage multiple directories<br>• perform an access review<br>**Implement and manage hybrid identities**<br>• install and configure Azure AD Connect<br>• configure federation<br>• configure single sign-on<br>• manage and troubleshoot Azure AD Connect<br>• troubleshoot password sync and writeback<br>**Implement solutions that use virtual machines (VM)**<br>• provision VMs<br>• create Azure Resource Manager templates<br>• configure Azure Disk Encryption for VMs<br>• implement Azure Backup for VMs | runbook<br>**1.5. Implement virtual networking**<br>• implement VNet to VNet connections<br>• implement VNet peering<br>**1.6. Implement Azure Active Directory**<br>• add custom domains<br>• configure Azure AD Identity Protection<br>• implement self-service password reset<br>• implement Conditional Access including MFA<br>• configure user accounts for MFA<br>• configure fraud alerts<br>• configure bypass options<br>• configure Trusted IPs<br>• configure verification methods<br>• implement and manage guest accounts<br>• manage multiple directories<br>**1.7. Implement and manage hybrid identities**<br>• install and configure Azure AD Connect<br>• identity synchronization options<br>• configure and manage password sync and password writeback<br>• configure single sign-on<br>• use Azure AD Connect Health |
| **Implement Workloads and Security (25-30%)**<br>**Migrate servers to Azure**<br>• migrate servers using Azure Migrate<br>• *backup and restore data*<br>**Configure serverless computing** | **3. Implement Management and Security Solutions (25-30%)**<br>**3.1. Manage workloads in Azure**<br>• migrate workloads using Azure Migrate<br>  • assess infrastructure<br>  • select a migration method<br>  • prepare the on-premises for |

- create and manage objects
- manage a Logic App Resource
- manage Azure Function app settings
- manage Event Grid
- manage Service Bus

**Implement application load balancing**

- configure application gateway
- configure Azure Front Door service
- configure Azure Traffic Manager

**Integrate on premises network with Azure virtual network**

- create and configure Azure VPN Gateway
- create and configure site to site VPN
- configure ExpressRoute
- configure Virtual WAN
- verify on premises connectivity
- troubleshoot on premises connectivity with Azure

**Implement multi factor authentication (MFA)**

- configure user accounts for MFA
- configure fraud alerts
- configure bypass options
- configure Trusted IPs
- configure verification methods

**Manage role based access control (RBAC)**

- create a custom role
- configure access to Azure resources by assigning roles
- configure management access to Azure
- troubleshoot RBAC
- implement ~~RBAC~~ Azure Policies

    migration
    - recommend target infrastructure
- implement Azure Backup for VMs
- implement disaster recovery
- implement Azure Update Management

**3.2. Implement load balancing and network security**

- implement Azure Load Balancer
- implement an application gateway
- implement a Web Application Firewall
- implement Azure Firewall
- implement the Azure Front Door Service
- implement Azure Traffic Manager
- implement Network Security Groups and Application Security Groups
- implement Bastion

**3.3. Implement and manage Azure governance solutions**

- create and manage hierarchical structure that contains management groups, subscriptions and resource groups
- assign RBAC roles
- create a custom RBAC role
- configure access to Azure resources by assigning roles
- configure management access to Azure
- interpret effective permissions
- set up and perform an access review
- implement and configure an Azure Policy
- implement and configure an Azure Blueprint

**3.4. Manage security for applications**

- implement and configure KeyVault
- implement and configure Azure AD Managed Identities
- register and manage applications in

| | |
|---|---|
| • assign RBAC Roles | Azure AD |
| **Create and Deploy Apps (5-10%)**<br>**Create web apps by using PaaS**<br>• create an Azure app service Web App<br>• create documentation for the API<br>• create an App Service Web App for Containers<br>• create an App Service background task by using WebJobs<br>• enable diagnostics logging<br>**Design and develop apps that run in containers**<br>• configure diagnostic settings on resources<br>• create a container image by using a Dockerfile<br>• create an Azure Kubernetes Service<br>• publish an image to the Azure Container Registry<br>• implement an application that runs on an Azure Container Instance<br>• manage container settings by using code | **4. Implement Solutions for Apps (10-15%)**<br>**4.1. Implement an application infrastructure**<br>• create and configure Azure App Service<br>• create an App Service Web App for Containers<br>• create and configure an App Service plan<br>• configure an App Service<br>• configure networking for an App Service<br>• create and manage deployment slots<br>• implement Logic Apps<br>• implement Azure Functions<br>**4.2. Implement container-based applications**<br>• create a container image<br>• configure Azure Kubernetes Service<br>• publish and automate image deployment to the Azure Container Registry<br>• publish a solution on an Azure Container Instance<br>• NOT: Service Fabric |
| **Implement Authentication and Secure Data (5-10%)**<br>**Implement authentication**<br>• implement authentication by using certificates, forms-based authentication, tokens, or Windows-integrated authentication<br>• implement multi-factor authentication by using Azure AD<br>• implement OAuth2 authentication<br>• implement Managed Identities for Azure | [no mapping] |

| | |
|---|---|
| resources Service Principal authentication<br>**Implement secure data solutions**<br>• encrypt and decrypt data at rest and in transit<br>• encrypt data with Always Encrypted<br>• implement Azure Confidential Compute<br>• implement SSL/TLS communications<br>• create, read, update, and delete keys, secrets, and certificates by using the KeyVault API | |
| **6. Develop for the Cloud and for Azure Storage (15-20%)**<br>**Configure a message-based integration architecture**<br>• configure an app or service to send emails<br>• configure Event Grid<br>• configure the Azure Relay service<br>• create and configure a Notification Hub<br>• create and configure an Event Hub<br>• create and configure a Service Bus<br>**Develop for autoscaling**<br>• implement autoscaling rules and patterns (schedule, operational/system metrics<br>• implement code that addresses singleton application instances<br>• implement code that addresses transient state<br>**Develop solutions that use Cosmos DB storage**<br>• create, read, update, and delete data by using appropriate APIs<br>• implement partitioning schemes | **5. Implement and Manage Data Platforms (10-15%)**<br>**5.1. Implement NoSQL databases**<br>• configure storage account tables<br>• select appropriate CosmosDB APIs<br>• set up replicas in CosmosDB<br>**5.2. Implement Azure SQL databases**<br>• configure Azure SQL database settings<br>• implement Azure SQL Database managed instances<br>• configure HA for an Azure SQL database<br>• publish an Azure SQL database |

| | |
|---|---|
| • set the appropriate consistency level for operations<br>**Develop solutions that use a relational database**<br>• provision and configure relational databases<br>• configure elastic pools for Azure SQL Database<br>• implement Azure SQL Database managed instances<br>• create, read, update, and delete data tables by using code | |