Exam AZ-300: Microsoft Azure Architect Technologies – Skills Measured

A NEW VERSION OF THIS EXAM, AZ-303, IS AVAILABLE. The objective domain for AZ-304 is appended below along with a comparison table showing the side by side changes from AZ-300 to AZ-303.

The English version of this exam retired on September 30, 2020. Localized language versions retired on October 30, 2020.

Audience Profile

Candidates for this exam should have subject matter expertise in designing and implementing solutions that run on Microsoft Azure, including aspects like compute, network, storage, and security.

Responsibilities for an Azure Solution Architect include advising stakeholders and translating business requirements into secure, scalable, and reliable cloud solutions.

An Azure Solution Architect partners with cloud administrators, cloud DBAs, and clients to implement solutions.

A candidate for this exam should have advanced experience and knowledge across various aspects of IT operations, including networking, virtualization, identity, security, business continuity, disaster recovery, data management, budgeting, and governance–this role should manage how decisions in each area affect an overall solution. In addition, this role should be proficient in at least one of these Azure knowledge domains: administration, development, or DevOps.

Skills Measured

NOTE: The bullets that appear below each of the skills measured are intended to illustrate how we are assessing that skill. This list is NOT definitive or exhaustive.

NOTE: In most cases, exams do NOT cover preview features, and some features will only be added to an exam when they are GA (General Availability).

Deploy and configure infrastructure (40-45%)

Analyze resource utilization and consumption

- configure diagnostic settings on resources
- create baseline for resources

- create and test alerts
- analyze alerts across subscription
- analyze metrics across subscription
- create action groups
- monitor for unused resources
- monitor spend
- report on spend
- utilize Log Search query functions
- view Alerts in Azure Monitor logs
- visualize diagnostics data using Azure Monitor Workbooks

Create and configure storage accounts

- configure network access to the storage account
- create and configure storage account
- generate Shared access signature
- implement Azure AD authentication for storage
- install and use Azure Storage Explorer
- manage access keys
- monitor Activity log by using Azure Monitor logs
- implement Azure storage replication
- implement Azure storage account failover

Create and configure a VM for Windows and Linux

- configure High Availability
- configure Monitoring
- configure Networking
- configure Storage
- configure Virtual Machine Size
- implement dedicated hosts
- deploy and configure scale sets

Automate deployment of VMs

- modify Azure Resource Manager template
- configure Location of new VMs
- configure VHD template
- deploy from template
- save a deployment as an Azure Resource Manager template
- deploy Windows and Linux VMs

Create connectivity between virtual networks

- create and configure Vnet peering

- create and configure Vnet to Vnet connections
- verify virtual network connectivity
- create virtual network gateway

Implement and manage virtual networking

- configure private IP addressing
- configure public IP addresses
- create and configure network routes
- create and configure network interface
- create and configure subnets
- create and configure virtual network
- create and configure Network Security Groups and Application Security Groups.

Manage Azure Active Directory

- add custom domains
- configure Azure AD Identity Protection
- configure Azure AD Join
- configure self-service password reset
- implement conditional access policies
- manage multiple directories
- perform an access review

Implement and manage hybrid identities

- install and configure Azure AD Connect
- configure federation
- configure single sign-on
- manage and troubleshoot Azure AD Connect
- troubleshoot password sync and writeback

Implement solutions that use virtual machines (VM)

- provision VMs
- create Azure Resource Manager templates
- configure Azure Disk Encryption for VMs
- implement Azure Backup for VMs

Implement workloads and security (25-30%)

Migrate servers to Azure

- migrate servers using Azure Migrate

Configure serverless computing

- 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

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

Manage role-based access control

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

Create and deploy apps (5-10%)

Create web apps by using PaaS

- create an Azure app service Web App
- create documentation for the API

- create an App Service Web App for Containers
- create an App Service background task by using WebJobs
- enable diagnostics logging

Design and develop apps that run in containers

- configure diagnostic settings on resources
- create a container image by using a Dockerfile
- create an Azure Kubernetes Service
- publish an image to the Azure Container Registry
- implement an application that runs on an Azure Container Instance
- manage container settings by using code

Implement authentication and secure data (5-10%)

Implement authentication

- implement authentication by using certificates, forms-based authentication, tokens, or Windows-integrated authentication
- implement multi-factor authentication by using Azure AD
- implement OAuth2 authentication
- implement Managed Identities for Azure resources Service Principal authentication

Implement secure data solutions

- encrypt and decrypt data at rest and in transit
- encrypt data with Always Encrypted
- implement Azure Confidential Compute
- implement SSL/TLS communications
- create, read, update, and delete keys, secrets, and certificates by using the KeyVault API

Develop for the cloud and for azure storage (15-20%)

Configure a message-based integration architecture

- configure an app or service to send emails
- configure Event Grid
- configure the Azure Relay service
- create and configure a Notification Hub
- create and configure an Event Hub
- create and configure a Service Bus

Develop for autoscaling

- implement autoscaling rules and patterns (schedule, operational/system metrics

- implement code that addresses singleton application instances
- implement code that addresses transient state

Develop solutions that use Cosmos DB storage

- create, read, update, and delete data by using appropriate APIs
- implement partitioning schemes
- set the appropriate consistency level for operations

Develop solutions that use a relational database

- provision and configure relational databases
- configure elastic pools for Azure SQL Database
- implement Azure SQL Database managed instances
- create, read, update, and delete data tables by using code

AZ-303 Microsoft Azure Architect Technologies

Audience Profile

Candidates for this exam should have subject matter expertise in designing and implementing solutions that run on Microsoft Azure, including aspects like compute, network, storage, and security.

Responsibilities for an Azure Solution Architect include advising stakeholders and translating business requirements into secure, scalable, and reliable cloud solutions.

An Azure Solution Architect partners with cloud administrators, cloud DBAs, and clients to implement solutions.

A candidate for this exam should have advanced experience and knowledge across various aspects of IT operations, including networking, virtualization, identity, security, business continuity, disaster recovery, data management, budgeting, and governance–this role should manage how decisions in each area affect an overall solution. In addition, this role should be proficient in at least one of these Azure knowledge domains: administration, development, or DevOps.

Skills Measured

NOTE: The bullets that appear below each of the skills measured are intended to illustrate how we are assessing that skill. This list is not definitive or exhaustive.

NOTE: Unless otherwise noted in the skills measured or in the exam description, exams do not cover preview features. In most cases, features will only be added to exams when they are GA (general availability).

Implement and monitor an azure infrastructure (50-55%)

Implement cloud infrastructure monitoring

- monitor security
- monitor performance
    - configure diagnostic settings on resources
    - create a performance baseline for resources
    - monitor for unused resources
    - monitor performance capacity
    - visualize diagnostics data using Azure Monitor
- monitor health and availability
    - monitor networking
    - monitor service health
- monitor cost
    - monitor spend
    - report on spend
- configure advanced logging
    - implement and configure Azure Monitor insights, including App Insights, Networks, Containers
    - configure a Log Analytics workspace
- configure logging for workloads
- initiate automated responses by using Action Groups
- configure and manage advanced alerts
    - collect alerts and metrics across multiple subscriptions
    - view Alerts in Azure Monitor logs
    - NOT: create Log Analytics query

Implement storage accounts

- select storage account options based on a use case
- configure Azure Files and blob storage
- configure network access to the storage account
- implement Shared Access Signatures and access policies
- implement Azure AD authentication for storage

- manage access keys
- implement Azure storage replication
- implement Azure storage account failover

Implement VMs for Windows and Linux

- configure High Availability
- configure storage for VMs
- select virtual machine size
- implement Azure Dedicated Hosts
- deploy and configure scale sets
- configure Azure Disk Encryption

Automate deployment and configuration of resources

- save a deployment as an Azure Resource Manager template
- modify Azure Resource Manager template
- evaluate location of new resources
- configure a virtual disk template
- deploy from a template
- manage a template library
- create and execute an automation runbook

Implement virtual networking

- implement VNet to VNet connections
- implement VNet peering

Implement Azure Active Directory

- add custom domains
- configure Azure AD Identity Protection
- implement self-service password reset
- implement Conditional Access including MFA
- configure user accounts for MFA
- configure fraud alerts
- configure bypass options
- configure Trusted IPs
- configure verification methods
- implement and manage guest accounts
- manage multiple directories

Implement and manage hybrid identities

- install and configure Azure AD Connect
- identity synchronization options
- configure and manage password sync and password writeback
- configure single sign-on
- use Azure AD Connect Health

Implement management and security solutions (25-30%)

Manage workloads in Azure

- migrate workloads using Azure Migrate
  - assess infrastructure
  - select a migration method
  - prepare the on-premises for migration
  - recommend target infrastructure
- implement Azure Backup for VMs
- implement disaster recovery
- implement Azure Update Management

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

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

Manage security for applications

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

Implement solutions for apps (10-15%)

Implement an application infrastructure

- create and configure Azure App Service
- create an App Service Web App for Containers
- create and configure an App Service plan
- configure an App Service
- configure networking for an App Service
- create and manage deployment slots
- implement Logic Apps
- implement Azure Functions

Implement container-based applications

- create a container image
- configure Azure Kubernetes Service
- publish and automate image deployment to the Azure Container Registry
- publish a solution on an Azure Container Instance
- NOT: Service Fabric

Implement and manage data platforms (10-15%)

Implement NoSQL databases

- configure storage account tables
- select appropriate CosmosDB APIs
- set up replicas in CosmosDB

Implement Azure SQL databases

- configure Azure SQL database settings

- implement Azure SQL Database managed instances
- configure HA for an Azure SQL database
- publish an Azure SQL database

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
 	
Analyze resource utilization and consumption
• aonfigure diagnostic settings on resources
• create baseline for resources
• create and test alerts
• analyze alerts across subscription
• analyze metrics across subscription
• create action groups
• monitor for unused resources
• monitor spend
• report on spend
• utilize Log Search query functions
• view Alerts in Azure Monitor logs
• visualize diagnostics data using Azure Monitor Workbooks
 	
Create and configure storage accounts
• configure network access to the storage account
• create and configure storage
	1. Implement and Monitor an Azure Infrastructure (50-55%)
	1.1. implement cloud infrastructure monitoring
	• monitor security (Note: Log Analytics, Azure Security Center, Azure Sentinel)
	• monitor performance
	  ○ configure diagnostic settings on resources
	  ○ create a performance baseline for resources
	  ○ monitor for unused resources
	  ○ monitor performance capacity
	  ○ visualize diagnostics data using Azure Monitor
	• monitor health and availability
	  ○ monitor networking
	  ○ monitor service health
	• monitor cost
	  ○ monitor spend
	  ○ report on spend
	• configure advanced logging
	  ○ implement and configure Azure Monitor insights, including App Insights, Networks, Containers

account • generate Shared access signature • implement Azure AD authentication for storage • install and use Azure Storage Explorer • manage access keys • monitor Activity log by using Azure Monitor logs • implement Azure storage replication • implement Azure storage account failover **Create and configure a VM for Windows and Linux** • configure High Availability • configure Monitoring • configure Networking • configure Storage • configure Virtual Machine Size • implement dedicated hosts • deploy and configure scale sets **Automate deployment of VMs** • modify Azure Resource Manager template • configure Location of new VMs • configure VHD template • deploy from template • save a deployment as an Azure Resource Manager template • deploy Windows and Linux VMs **Create connectivity between virtual networks** • create and configure Vnet	○ configure a Log Analytics workspace ○ configure logging for workloads • initiate automated responses by using Action Groups • configure and manage advanced alerts ○ collect alerts and metrics across multiple subscriptions ○ view Alerts in Azure Monitor logs • NOT: create Log Analytics query **1.2. implement storage accounts** • select storage account options based on a use case • configure Azure Files and blob storage • configure network access to the storage account • implement Shared Access Signatures and access policies • implement Azure AD authentication for storage • manage access keys • implement Azure storage replication • implement Azure storage account failover **1.3. implement VMs for Windows and Linux** • configure High Availability • configure storage for VMs • select virtual machine size • implement Azure Dedicated Hosts • deploy and configure scale sets • configure Azure Disk Encryption **1.4. automate deployment and configuration of resources**

peering
- create and configure Vnet to Vnet connections
- verify virtual network connectivity
- create virtual network gateway

Implement and manage virtual networking
- configure private IP addressing
- configure public IP addresses
- create and configure network routes
- create and configure network interface
- create and configure subnets
- create and configure virtual network
- create and configure Network Security Groups and Application Security Groups.

Manage Azure Active Directory
- add custom domains
- configure Azure AD Identity Protection
- configure Azure AD Join
- configure self-service password reset
- implement conditional access policies
- manage multiple directories
- perform an access review

Implement and manage hybrid identities
- install and configure Azure AD connect
- configure federation
- configure single sign-on
- save a deployment as an Azure Resource Manager template
- modify Azure Resource Manager template
- evaluate location of new resources
- configure a virtual disk template
- deploy from a template
- manage a template library
- create and execute an automation runbook

1.5. Implement virtual networking
- implement VNet to VNet connections
- implement VNet peering

1.6. Implement Azure Active Directory
- add custom domains
- configure Azure AD Identity Protection
- implement self-service password reset
- implement Conditional Access including MFA
- configure user accounts for MFA
- configure fraud alerts
- configure bypass options
- configure Trusted IPs
- configure verification methods
- implement and manage guest accounts
- Manage multiple directories

1.7. Implement and manage hybrid identities
- install and configure Azure AD Connect
- identity synchronization options
- configure and manage password sync and password writeback

• manage and troubleshoot Azure AD Connect • troubleshoot password sync and writeback **Implement solutions that use virtual machines (VM)** • provision VMs • create Azure Resource Manager templates • configure Azure Disk Encryption for VMs • implement Azure Backup for VMs	• configure single sign-on • use Azure AD Connect Health

Implement Workloads and Security (25-30%)
Migrate servers to Azure
• migrate servers using Azure Migrate
• *Backup and restore data*
 	
Configure serverless computing
• 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
	3. Implement Management and Security Solutions (25-30%)
	3.1. Manage workloads in Azure
	• migrate workloads using Azure migrate
	  ○ assess infrastructure
	  ○ select a migration method
	  ○ prepare the on-premises for 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

• 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 • assign RBAC Roles	• 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 Azure AD
Create and Deploy Apps (5-10%) **Create web apps by using PaaS** • create an Azure app service Web App • create documentation for the API • create an App Service Web App for Containers	**4. Implement Solutions for Apps (10-15%)** **4.1. Implement an application infrastructure** • create and configure Azure App Service • create an App Service Web App

• create an App Service background task by using WebJobs • enable diagnostics logging **Design and develop apps that run in containers** • configure diagnostic settings on resources • create a container image by using a Dockerfile • create an Azure Kubernetes Service • publish an image to the Azure Container Registry • implement an application that runs on an Azure Container Instance • manage container settings by using code	for Containers • create and configure an App Service plan • configure an App Service • configure networking for an App Service • create and manage deployment slots • implement Logic Apps • implement Azure Functions **4.2. Implement container-based applications** • create a container image • configure Azure Kubernetes Service • publish and automate image deployment to the Azure container Registry • publish a solution on an Azure Container Instance • NOT: Service Fabric
Implement Authentication and Secure Data (5-10%) **Implement authentication** • implement authentication by using certificates, forms-based authentication, tokens, or Windows-integrated authentication • implement multi-factor authentication by using Azure AD • implement OAuth2 authentication • implement Managed Identities for Azure resources Service Principal authentication **Implement secure data solutions** • encrypt and decrypt data at rest and in transit • encrypt data with Always Encrypted	[no mapping]

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

relational database • provision and configure relational databases • configure elastic pools for Azure SQL Database • implement Azure SQL Database managed instances • create, read, update, and delete data tables by using code	