Microsoft Certified Azure Fundamentals – Skills Measured

This document contains the skills measured on the exams associated with this certification. It does not include any upcoming or recent changes that have been made to those skills. For more information about upcoming or recent changes, see the associated exam details page(s).

Exam AZ-900: Microsoft Azure Fundamentals

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).

Describe Cloud Concepts (15-20%)

Describe the benefits and considerations of using cloud services

- describe terms such as High Availability, Scalability, Elasticity, Agility, Fault Tolerance, and Disaster Recovery
- describe the principles of economies of scale
- describe the differences between Capital Expenditure (CapEx) and Operational Expenditure (OpEx)
- describe the consumption-based model

Describe the differences between Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS)

- describe Infrastructure-as-a-Service (IaaS),
- describe Platform-as-a-Service (PaaS)
- describe Software-as-a-Service (SaaS)
- compare and contrast the three different service types

Describe the differences between Public, Private and Hybrid cloud models

- describe Public cloud
- describe Private cloud
- describe Hybrid cloud
- compare and contrast the three different cloud models

Describe Core Azure Services (30-35%)

Describe the core Azure architectural components

- describe Regions
- describe Availability Zones
- describe Resource Groups
- describe Azure Resource Manager
- describe the benefits and usage of core Azure architectural components

Describe some of the core products available in Azure

- describe products available for Compute such as Virtual Machines, Virtual Machine Scale Sets, App Services, Azure Container Instances (ACI) and Azure Kubernetes Service (AKS)
- describe products available for Networking such as Virtual Network, Load Balancer, VPN Gateway, Application Gateway and Content Delivery Network
- describe products available for Storage such as Blob Storage, Disk Storage, File Storage, and Archive Storage
- describe products available for Databases such as Cosmos DB, Azure SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, Azure Database Migration service
- describe the Azure Marketplace and its usage scenarios

Describe some of the solutions available on Azure

- describe Internet of Things (IoT) and products that are available for IoT on Azure such as IoT Hub and IoT Central
- describe Big Data and Analytics and products that are available for Big Data and Analytics such as Azure Synapse Analytics, HDInsight, and Azure Databricks
- describe Artificial Intelligence (AI) and products that are available for AI such as Azure Machine Learning Service and Studio
- describe Serverless computing and Azure products that are available for serverless computing such as Azure Functions, Logic Apps, and Event Grid
- describe DevOps solutions available on Azure such as Azure DevOps and Azure DevTest Labs
- describe the benefits and outcomes of using Azure solutions

Describe Azure management tools

- describe Azure tools such as Azure Portal, Azure PowerShell, Azure CLI and Cloud Shell
- describe Azure Advisor

Describe Security, Privacy, Compliance, and Trust (25-30%)

Describe securing network connectivity in Azure

- describe Network Security Groups (NSG)
- describe Application Security Groups (ASG)
- describe User Defined Rules (UDR)
- describe Azure Firewall
- describe Azure DDoS Protection
- choose an appropriate Azure security solution

Describe core Azure Identity services

- describe the difference between authentication and authorization
- describe Azure Active Directory
- describe Azure Multi-Factor Authentication

Describe security tools and features of Azure

- describe Azure Security Center
- describe Azure Security Center usage scenarios
- describe Key Vault
- describe Azure Information Protection (AIP)
- describe Azure Advanced Threat Protection (ATP)

Describe Azure governance methodologies

- describe policies and initiatives with Azure Policy
- describe Role-Based Access Control (RBAC)
- describe Locks
- describe Azure Advisor security assistance
- describe Azure Blueprints

Describe monitoring and reporting options in Azure

- describe Azure Monitor
- describe Azure Service Health
- describe the use cases and benefits of Azure Monitor and Azure Service Health

Describe privacy, compliance and data protection standards in Azure

- describe industry compliance terms such as GDPR, ISO and NIST
- describe the Microsoft Privacy Statement
- describe the Trust center
- describe the Service Trust Portal
- describe Compliance Manager

- determine if Azure is compliant for a business need
- describe Azure Government cloud services
- describe Azure China cloud services

Describe Azure Pricing, Service Level Agreements, and Lifecycles (20-25%)

Describe Azure subscriptions

- describe an Azure Subscription
- describe the uses and options with Azure subscriptions such access control and offer types
- describe subscription management using Management groups

Describe planning and management of costs

- describe options for purchasing Azure products and services
- describe options around Azure Free account
- describe the factors affecting costs such as resource types, services, locations, ingress and egress traffic
- describe Zones for billing purposes
- describe the Pricing calculator
- describe the Total Cost of Ownership (TCO) calculator
- describe best practices for minimizing Azure costs such as performing cost analysis, creating spending limits and quotas, using tags to identify cost owners, using Azure reservations and using Azure Advisor recommendations
- describe Azure Cost Management

Describe Azure Service Level Agreements (SLAs)

- describe a Service Level Agreement (SLA)
- describe Composite SLAs
- describe how to determine an appropriate SLA for an application

Describe service lifecycle in Azure

- describe Public and Private Preview features
- describe the term General Availability (GA)
- describe how to monitor feature updates and product changes

Microsoft Certified: Azure Administrator Associate – 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).

Manage Azure identities and governance

Manage Azure AD objects

- create users and groups
- manage user and group properties
- manage device settings
- perform bulk user updates
- manage guest accounts
- configure Azure AD Join
- configure self-service password reset
- NOT: Azure AD Connect; PIM

Manage role-based access control (RBAC)

- create a custom role
- provide access to Azure resources by assigning roles
    - subscriptions
    - resource groups
    - resources (VM, disk, etc.)
- interpret access assignments
- manage multiple directories

Manage subscriptions and governance

- configure Azure policies
- configure resource locks
- apply tags
- create and manage resource groups
    - move resources
    - remove RGs
- manage subscriptions

- configure Cost Management
- configure management groups

Implement and manage storage

Manage storage accounts

- configure network access to storage accounts
- create and configure storage accounts
- generate shared access signature
- manage access keys
- implement Azure storage replication
- configure Azure AD Authentication for a storage account

Manage data in Azure Storage

- export from Azure job
- import into Azure job
- install and use Azure Storage Explorer
- copy data by using AZCopy

Configure Azure files and Azure blob storage

- create an Azure file share
- create and configure Azure File Sync service
- configure Azure blob storage
- configure storage tiers for Azure blobs

Deploy and manage Azure compute resources

Configure VMs for high availability and scalability

- configure high availability
- deploy and configure scale sets

Automate deployment and configuration of VMs

- modify Azure Resource Manager (ARM) template
- configure VHD template
- deploy from template
- save a deployment as an ARM template
- automate configuration management by using custom script extensions

Create and configure VMs

- configure Azure Disk Encryption
- move VMs from one resource group to another
- manage VM sizes
- add data discs
- configure networking
- redeploy VMs

Create and configure containers

- create and configure Azure Kubernetes Service (AKS)
- create and configure Azure Container Instances (ACI)
- NOT: selecting an container solution architecture or product; container registry settings

Create and configure Web Apps

- create and configure App Service
- create and configure App Service Plans
- NOT: Azure Functions; Logic Apps; Event Grid

Configure and manage virtual networking

Implement and manage virtual networking

- create and configure VNET peering
- configure private and public IP addresses, network routes, network interface, subnets, and virtual network

Configure name resolution

- configure Azure DNS
- configure custom DNS settings
- configure a private or public DNS zone

Secure access to virtual networks

- create security rules
- associate an NSG to a subnet or network interface
- evaluate effective security rules
- deploy and configure Azure Firewall
- deploy and configure Azure Bastion Service
- NOT: Implement Application Security Groups; DDoS

Configure load balancing

- configure Application Gateway
- configure an internal load balancer
- configure load balancing rules
- configure a public load balancer
- troubleshoot load balancing
- NOT: Traffic Manager and FrontDoor and PrivateLink

Monitor and troubleshoot virtual networking

- monitor on-premises connectivity
- use Network Performance Monitor
- use Network Watcher
- troubleshoot external networking
- troubleshoot virtual network connectivity

Integrate an on-premises network with an Azure virtual network

- create and configure Azure VPN Gateway
- create and configure VPNs
- configure ExpressRoute
- configure Azure Virtual WAN

Monitor and back up Azure resources

Monitor resources by using Azure Monitor

- configure and interpret metrics
    - analyze metrics across subscriptions
- configure Log Analytics
    - implement a Log Analytics workspace
    - configure diagnostic settings
- query and analyze logs
    - create a query
    - save a query to the dashboard
    - interpret graphs
- set up alerts and actions
    - create and test alerts
    - create action groups
    - view alerts in Azure Monitor
    - analyze alerts across subscriptions
- configure Application Insights
- NOT: Network monitoring

Implement backup and recovery

- configure and review backup reports
- perform backup and restore operations by using Azure Backup Service
- create a Recovery Services Vault
    - use soft delete to recover Azure VMs
- create and configure backup policy
- perform site-to-site recovery by using Azure Site Recovery
- NOT: SQL or HANA

Microsoft Certified: Azure Security Engineer Associate – Skills Measured

This document contains the skills measured on the exams associated with this certification. It does not include any upcoming or recent changes that have been made to those skills. For more information about upcoming or recent changes, see the associated exam details page(s).

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).

Exam AZ-500: Microsoft Azure Security Technologies

Manage identity and access (30-35%)

Manage Azure Active Directory identities

- configure security for service principals
- manage Azure AD directory groups
- manage Azure AD users
- configure password writeback
- configure authentication methods including password hash and Pass Through Authentication (PTA), OAuth, and passwordless
- transfer Azure subscriptions between Azure AD tenants

Configure secure access by using Azure AD

- monitor privileged access for Azure AD Privileged Identity Management (PIM)
- configure Access Reviews
- activate and configure PIM
- implement Conditional Access policies including Multi-Factor Authentication (MFA)
- configure Azure AD identity protection

Manage application access

- create App Registration
- configure App Registration permission scopes
- manage App Registration permission consent
- manage API access to Azure subscriptions and resources

Manage access control

- configure subscription and resource permissions
- configure resource group permissions
- configure custom RBAC roles
- identify the appropriate role
- apply principle of least privilege
- interpret permissions
- check access

Implement platform protection (15-20%)

Implement advanced network security

- secure the connectivity of virtual networks (VPN authentication, Express Route encryption)
- configure Network Security Groups (NSGs) and Application Security Groups (ASGs)
- create and configure Azure Firewall
- configure Azure Front Door service as an Application Gateway
- configure a Web Application Firewall (WAF) on Azure Application Gateway
- configure Azure Bastion
- configure a firewall on a storage account, Azure SQL, KeyVault, or App Service
- implement Service Endpoints
- implement DDoS protection

Configure advanced security for compute

- configure endpoint protection
- configure and monitor system updates for VMs
- configure authentication for Azure Container Registry
- configure security for different types of containers
- implement vulnerability management
- configure isolation for AKS
- configure security for container registry
- implement Azure Disk Encryption
- configure authentication and security for Azure App Service
- configure SSL/TLS certs
- configure authentication for Azure Kubernetes Service
- configure automatic updates

Manage security operations (25-30%)

Monitor security by using Azure Monitor

- create and customize alerts
- monitor security logs by using Azure Monitor
- configure diagnostic logging and log retention

Monitor security by using Azure Security Center

- evaluate vulnerability scans from Azure Security Center
- configure Just in Time VM access by using Azure Security Center
- configure centralized policy management by using Azure Security Center
- configure compliance policies and evaluate for compliance by using Azure Security Center

Monitor security by using Azure Sentinel

- create and customize alerts
- configure data sources to Azure Sentinel
- evaluate results from Azure Sentinel
- configure workflow automation by using Azure Sentinel

Configure security policies

- configure security settings by using Azure Policy
- configure security settings by using Azure Blueprint
- configure a playbook by using Azure Sentinel

Secure data and applications (20-25%)

Configure security for storage

- configure access control for storage accounts
- configure key management for storage accounts
- configure Azure AD authentication for Azure Storage
- configure Azure AD Domain Services authentication for Azure Files
- create and manage Shared Access Signatures (SAS)
- create a shared access policy for a blob or blob container
- configure Storage Service Encryption

Configure security for databases

- enable database authentication
- enable database auditing
- configure Azure SQL Database Advanced Threat Protection
- implement database encryption

- implement Azure SQL Database Always Encrypted

Configure and manage Key Vault

- manage access to Key Vault
- manage permissions to secrets, certificates, and keys
- configure RBAC usage in Azure Key Vault
- manage certificates
- manage secrets
- configure key rotation
- backup and restore of Key Vault items