**Deploy and configure infrastructure (25-30%)**

* Analyze resource utilization and consumption
* configure diagnostic settings on resources
* create baseline for resources
* create and rest 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
* Create and configure storage accounts
* configure network access to the storage account
* create and configure storage account
* generate shared access signature
* install and use Azure Storage Explorer
* manage access keys
* monitor activity log by using Azure Monitor logs
* implement Azure storage replication
* Create and configure a Virtual Machine (VM) for Windows and Linux
* configure high availability
* configure monitoring, networking, storage, and virtual machine size
* deploy and configure scale sets
* Automate deployment of Virtual Machines (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
* Implement solutions that use virtual machines (VM)
* provision VMs
* create Azure Resource Manager templates
* configure Azure Disk Encryption for VMs
* Create connectivity between virtual networks
* create and configure VNET peering
* create and configure VNET to VNET
* verify virtual network connectivity
* create virtual network gateway
* Implement and manage virtual networking
* configure private and public IP addresses, network routes, network interface, subnets, and virtual network
* Manage Azure Active Directory (AD)
* add custom domains
* configure Azure AD Identity Protection, Azure AD Join, and Enterprise State Roaming
* 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 and single sign-on
* manage Azure AD Connect
* manage password sync and writeback

**Implement workloads and security (20-25%)**

Migrate servers to Azure

* migrate by using Azure Site Recovery
* migrate using P2V
* configure storage
* create a backup vault
* prepare source and target environments
* backup and restore data
* deploy Azure Site Recovery agent
* prepare virtual network

Configure serverless computing

* manage a Logic App resource
* manage Azure Function app settings
* manage Event Grid
* manage Service Bus

Implement application load balancing

* configure application gateway and load balancing rules
* implement front end IP configurations
* manage application load balancing

Integrate on-premises network with Azure virtual network

* create and configure Azure VPN Gateway
* create and configure site to site VPN
* configure Express Route
* verify on-premises connectivity
* manage on-premises connectivity with Azure

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 policies
* assign RBAC roles

Implement Multi-Factor Authentication (MFA)

* enable MFA for an Azure tenant
* configure user accounts for MFA
* configure fraud alerts
* configure bypass options
* configure trusted IPs
* configure verification methods
* manage role-based access control (RBAC)
* implement RBAC policies
* assign RBAC Roles
* create a custom role
* configure access to Azure resources by assigning roles
* configure management access to Azure

**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 Docker file
* 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 and 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 (20-25%)**

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
* create, read, update, and delete data tables by using code

Configure a message-based integration architecture

* configure an app or service to send emails, Event Grid, and the Azure Relay Service
* create and configure Notification Hub, Event Hub, and Service Bus rules and patterns (schedule, operational/system metrics, code that addresses singleton application instances)
* implement code that addresses transient state

**AZ-301 Skills Measured:**

**Determine workload requirements (10-15%)**

Gather Information and Requirements

* identify compliance requirements, identity and access management infrastructure, and service-oriented architectures (e.g., integration patterns, service design, service discoverability)
* identify accessibility (e.g. Web Content Accessibility Guidelines), availability (e.g. Service Level Agreement), capacity planning and scalability, deploy-ability (e.g., repositories, failback, slot-based deployment), configurability, governance, maintainability (e.g. logging, debugging, troubleshooting, recovery, training), security (e.g. authentication, authorization, attacks), and sizing (e.g. support costs, optimization) requirements
* recommend changes during project execution (ongoing)
* evaluate products and services to align with solution
* create testing scenarios

Optimize Consumption Strategy

* optimize app service, compute, identity, network, and storage costs

Design an Auditing and Monitoring Strategy

* define logical groupings (tags) for resources to be monitored
* determine levels and storage locations for logs
* plan for integration with monitoring tools
* recommend appropriate monitoring tool(s) for a solution
* specify mechanism for event routing and escalation
* design auditing for compliance requirements
* design auditing policies and traceability requirements

**Design for identity and security (20-25%)**

Design Identity Management

* choose an identity management approach
* design an identity delegation strategy, identity repository (including directory, application, systems, etc.)
* design self-service identity management and user and persona provisioning
* define personas and roles
* recommend appropriate access control strategy (e.g., attribute-based, discretionary access, history-based, identity-based, mandatory, organization-based, role-based, rule-based, responsibility-based)

Design Authentication

* choose an authentication approach
* design a single-sign on approach
* design for IPSec, logon, multi-factor, network access, and remote authentication

Design Authorization

* choose an authorization approach
* define access permissions and privileges
* design secure delegated access (e.g., oAuth, OpenID, etc.)
* recommend when and how to use API Keys

Design for Risk Prevention for Identity

* design a risk assessment strategy (e.g., access reviews, RBAC policies, physical access)
* evaluate agreements involving services or products from vendors and contractors
* update solution design to address and mitigate changes to existing security policies, standards, guidelines and procedures

Design a Monitoring Strategy for Identity and Security

* design for alert notifications
* design an alert and metrics strategy
* recommend authentication monitors

**Design a data platform solution (15-20%)**

Design a Data Management Strategy

* choose between managed and unmanaged data store
* choose between relational and non-relational databases
* design data auditing and caching strategies
* identify data attributes (e.g., relevancy, structure, frequency, size, durability, etc.)
* recommend Database Transaction Unit (DTU) sizing
* design a data retention policy
* design for data availability, consistency, and durability
* design a data warehouse strategy

Design a Data Protection Strategy

* recommend geographic data storage
* design an encryption strategy for data at rest, for data in transmission, and for data in use
* design a scalability strategy for data
* design secure access to data
* design a data loss prevention (DLP) policy

Design and Document Data Flows

* identify data flow requirements
* create a data flow diagram
* design a data flow to meet business requirements
* design a data import and export strategy

Design a Monitoring Strategy for the Data Platform

* design for alert notifications
* design an alert and metrics strategy

**Design a business continuity strategy (15-20%)**

Design a Site Recovery Strategy

* design a recovery solution
* design a site recovery replication policy
* design for site recovery capacity and for storage replication
* design site failover and failback (planned/unplanned)
* design the site recovery network
* recommend recovery objectives (e.g., Azure, on-prem, hybrid, Recovery Time Objective (RTO), Recovery Level Objective (RLO), Recovery Point Objective (RPO))
* identify resources that require site recovery
* identify supported and unsupported workloads
* recommend a geographical distribution strategy

Design for High Availability

* design for application redundancy, autoscaling, data center and fault domain redundancy, and network redundancy
* identify resources that require high availability
* identify storage types for high availability

Design a Data Archiving Strategy

* recommend storage types and methodology for data archiving
* identify requirements for data archiving and business compliance requirements for data archiving
* identify SLA(s) for data archiving

**Design for deployment, migration, and integration (10-15%)**

Design Deployments

* design a compute, container, data platform, messaging solution, storage, and web app and service deployment strategy

Design Migrations

* recommend a migration strategy
* design data import/export strategies during migration
* determine the appropriate application migration, data transfer, and network connectivity method
* determine migration scope, including redundant, related, trivial, and outdated data
* determine application and data compatibility

Design an API Integration Strategy

* design an API gateway strategy
* determine policies for internal and external consumption of APIs
* recommend a hosting structure for API management

**Design an infrastructure strategy (15-20%)**

Design a Storage Strategy

* design a storage provisioning strategy
* design storage access strategy
* identify storage requirements
* recommend a storage solution and storage management tools

Design a Compute Strategy

* design compute provisioning and secure compute strategies
* determine appropriate compute technologies (e.g., virtual machines, functions, service fabric, container instances, etc.)
* design an Azure HPC environment
* identify compute requirements
* recommend management tools for compute

Design a Networking Strategy

* design network provisioning and network security strategies
* determine appropriate network connectivity technologies
* identify networking requirements
* recommend network management tools

Design a Monitoring Strategy for Infrastructure

* design for alert notifications
* design an alert and metrics strategy