AZ-101
Microsoft Azure Integration and Security

Exam Design

Audience Profile

Candidates for this exam are Azure Administrators who manage cloud services that span storage, security, networking, and compute cloud capabilities. Candidates have a deep understanding of each service across the full IT lifecycle, and take requests for infrastructure services, applications, and environments. They make recommendations on services to use for optimal performance and scale, as well as provision, size, monitor, and adjust resources as appropriate.

Candidates for this exam should have proficiency in using PowerShell, the Command Line Interface, Azure Portal, ARM templates, operating systems, virtualization, cloud infrastructure, storage structures, and networking.

Skills measured

Note: This document shows tracked changes that are effective as of December 21, 2018.

Evaluate and perform server migration to Azure (15-20%)

Evaluate migration scenarios by using Azure Migrate
May include but is not limited to: Discover and assess environment, identify workloads that can and cannot be deployed, identify ports to open, identify changes to network, identify if target environment is supported, setup domain accounts and credentials

Migrate servers to Azure
May include but is not limited to: Migrate by using Azure Site Recovery (ASR), migate using P2V, configure storage, create a recovery services vault, prepare source and target environments, backup and restore data, deploy Azure Site Recovery (ASR) agent, prepare virtual network

Implement and manage application services (20-25%)

Configure serverless computing
May include but is not limited to: Create and manage objects, manage an Logic App Resource, manage Azure Function app settings, manage Event Grid, manage Service Bus

Manage App Service Plan
May include but is not limited to: configure application for scaling, enable monitoring and diagnostics, configure App Service Plans

Manage App services
May include but is not limited to: Assign SSL Certificates, configure application settings, configure deployment slots, configure CDN integration, manage App service protection, manage roles for an App service, create and manage App Service Environment

Implement advanced virtual networking (30-35%)

Implement application load balancing
May include but is not limited to: Configure application gateway, configure load balancing rules, implement front end IP configurations, troubleshoot load balancing

Implement Azure load balancer
May include but is not limited to: Configure internal load balancer, configure load balancing rules, configure public load balancer, troubleshoot load balancing

Monitor and troubleshoot networking
May include but is not limited to: Monitor on-premises connectivity, use Network resource monitoring, use Network Watcher, troubleshoot external networking, troubleshoot virtual network connectivity

Integrate on premises network with Azure virtual network
May include but is not limited to: Create and configure Azure VPN Gateway, create and configure site to site VPN, configure Express Route, verify on premises connectivity, troubleshoot on premises connectivity with Azure

Secure identities (25-30%)

Implement multi-factor authentication (MFA)
May include but is not limited to: ~~Enable MFA for an Azure AD tenant~~ Configure user accounts for MFA, <u>E</u>enable MFA by using bulk update, configure fraud alerts, configure bypass options, configure Trusted IPs, configure verification methods

Manage role based access control (RBAC)
May include but is not limited to: 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 Azure AD Privileged Identity Management
May include but is not limited to: Activate a PIM role, configure Just-in-time access, configure permanent access, configure PIM management access, configure time-bound access, create a Delegated Approver account, enable PIM, process pending approval requests