AZ-900: AZURE FUNDAMENTALS

INSTRUCTOR: Mohammed Arif

Table of Contents

SECTION 1: Intro to Course

The exam covers the topics on the following page:

- https://www.microsoft.com/en-us/learning/exam-az-900.aspx

Passing the exam gets you the "Microsoft Certified Azure Fundamentals" badge. The certification has no expiry date. Good for "life".

Optional exam. Not a prerequisite to any of the other Microsoft Exams. But it's a good way to get a solid understanding of Azure before jumping in to the future exams.

Currently $99 USD. Available in English, Japanese, Chinese (Simplified), Korean, Spanish, German, and French

The exam covers:

- Describe cloud concepts (20-25%)
- Describe core Azure services (15-20%)
- Describe core solutions and management tools on Azure (10-15%)
- Describe general security and network security features (10-15%)
- Describe identity, governance, privacy, and compliance features (20-25%)
- Describe Azure cost management and Service Level Agreements (10-15%)

Who's the Exam For?

- Candidates with non-technical backgrounds, such as those involved in selling or purchasing cloud based solutions and services or who have some involvement with cloud based solutions and services, and
- Candidates with a technical background who have a need to validate their foundational level knowledge around cloud services.

SECTION 2: Cloud Concepts (20-25%)

Benefits of Cloud Computing

Cloud computing is:

- The ability to rent computing services of all types (compute, storage, networking, database, machine learning, etc.)
- Available for use in only a few minutes
- Only pay for what you use
- No contract or long-term commitment

This ability unlocks so much value in the ability of businesses (like mine and yours) to deliver our products and services to the end users.

Cloud computing provides:

- Reduced up-front investment required
- Ongoing, monthly cost savings to the business (you)
- Vast catalog of computing services that you are able to use to serve your customers that wouldn't otherwise be available to you
- With increased performance, availability and security to the end user

Benefits of Cloud Services

Availability - what percentage of time does a system respond properly to requests, expressed as a percentage over time

I.e. 99.99% availability implies up to 4 minutes per month of acceptable downtime

High Availability - a system specifically designed to be resilient when some component of the system fails

Scalability - the ability of a system to grow it's capacity "easily" when a system reaches its maximum capacity

Elasticity - the ability of a system to automatically grow when maximum capacity is reached, and automatically shrink to minimize waste

Agility - the ability to respond to change "rapidly" based on changes to market or environment

Disaster Recovery - the ability to recover from a big failure within an acceptable period of time, with an acceptable amount of data lost

Microsoft (and Google and AWS) can buy and run a server cheaper that you could ever possibly do yourself.

Capital Expenditure (CapEx) - a (usually large) amount of money invested in an asset (building, computers, equipment) spent up front, and it returns back profits slowly over time; major cash drain or loan required; cannot be deducted from your taxes in one year, depreciated over several years

Operating Expenditure (OpEx) - an amount of money spent "every month" as an operating expense; hopefully you earn more money in revenue from it than you spend; can be deducted from your taxes immediately; many accountants prefer OpEx over CapEx for the tax and cash flow benefits

Consumption-Based Model - paying for something based on how much you used, as opposed to paying for something no matter if you use it or not.

I.e. A monthly gym membership is a fixed-price model, you pay the same every month. But if you only paid when you actually went to the gym (like an entry fee), that would be a consumption model

Most cloud services charge only when you use the thing, not a fixed-price per month.

Categories of Cloud Services

Infrastructure-as-a-Service (IaaS) - this is the computing paradigm where Azure provides you the virtual hardware (Virtual machine, load balancer, virtual network), and you can have complete control over that. It replicates the exact function of equipment that you'd have in your own data center (like a server, firewall, router, etc)

IaaS Examples: Virtual machine, load balancer, application gateway, virtual network

Platform-as-a-Service (PaaS) - you lose some control over the hardware; generally, you upload your code and just configure the environment in Azure to run it

PaaS Examples: App Services, Web Apps, SQL Database

Serverless Compute – Removes both the need to manage the infrastructure and the need to configure the environment that runs your code.

PaaS Examples: Azure Functions, Kubernetes, Application Environments

Software-as-a-Service (SaaS) - you lose even more control over the hardware and the software; generally, Azure provides you an application that they developed, and you just configure it to your usage. You are a tenant using their software.

SaaS Examples: Azure Portal, Outlook 365, Windows Virtual Desktop, Azure DevOps

Azure Cloud Service Model - Comparing your responsibilities vs Azure across the three paradigms.

Source: https://docs.microsoft.com/en-us/azure/security/fundamentals/media/shared-responsibility/shared-responsibility.png

Types of Cloud Computing

Public Cloud - Cloud services provided over the public Internet to anyone who wants to sign up for them. Azure owns the hardware, and you rent it from them.

Private Cloud - Cloud services offered only to select users. This is sometimes called an "internal cloud". Looks and acts like a cloud computing, but uses resources and servers available only to your company/organization. You own the hardware or have exclusive use of it.

Hybrid Cloud - A mixture between your own private networks and servers, and using the public cloud for some things. Typically used to take advantage of the unlimited, inexpensive growth benefits of the public cloud.

For Further Reading:

Azure Official definitions - https://azure.microsoft.com/en-ca/overview/cloud-computing-dictionary/

What is IaaS - https://azure.microsoft.com/en-ca/overview/what-is-iaas/

What is PaaS - https://azure.microsoft.com/en-ca/overview/what-is-paas/

What is SaaS - https://azure.microsoft.com/en-ca/overview/what-is-saas/

What is a Public cloud - https://azure.microsoft.com/en-ca/overview/what-is-a-public-cloud/

What is a Private cloud - https://azure.microsoft.com/en-ca/overview/what-is-a-private-cloud/

What is a Hybrid cloud - https://azure.microsoft.com/en-ca/overview/what-is-hybrid-cloud-computing/

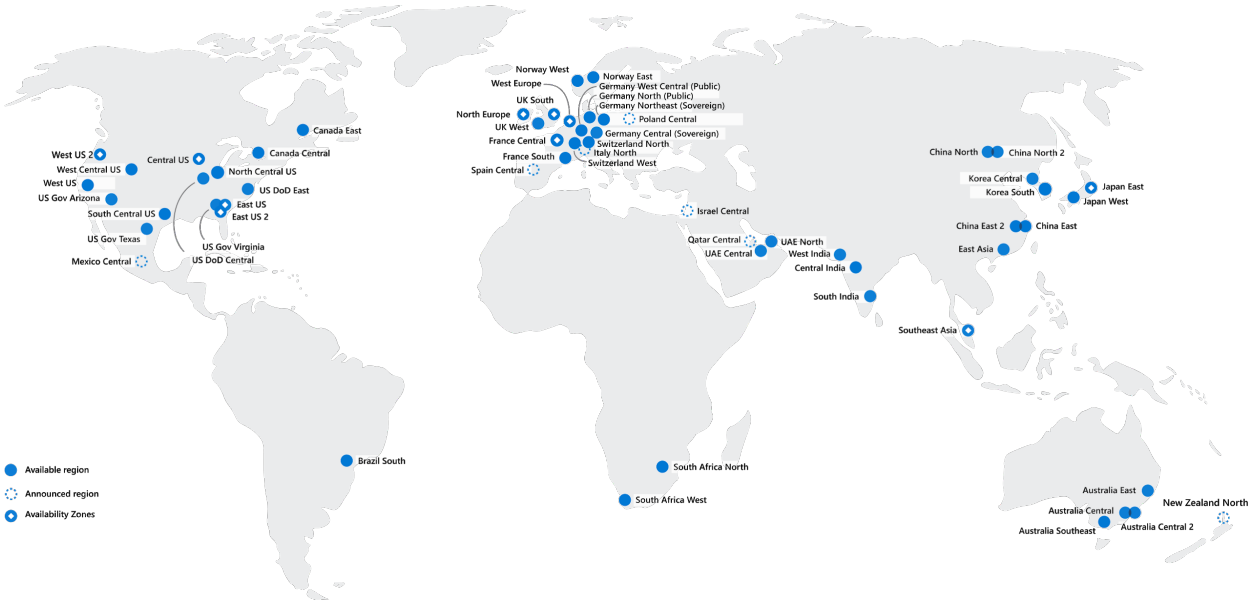
What is a Serverless Computing - https://azure.microsoft.com/en-us/overview/serverless-computing/

SECTION 3: Core Azure Services (15-20%)

Azure Architectural Components

Azure Datacenter - a group of interconnected buildings in the same location that contain all the servers, power, wiring and internet connectivity to run Azure services

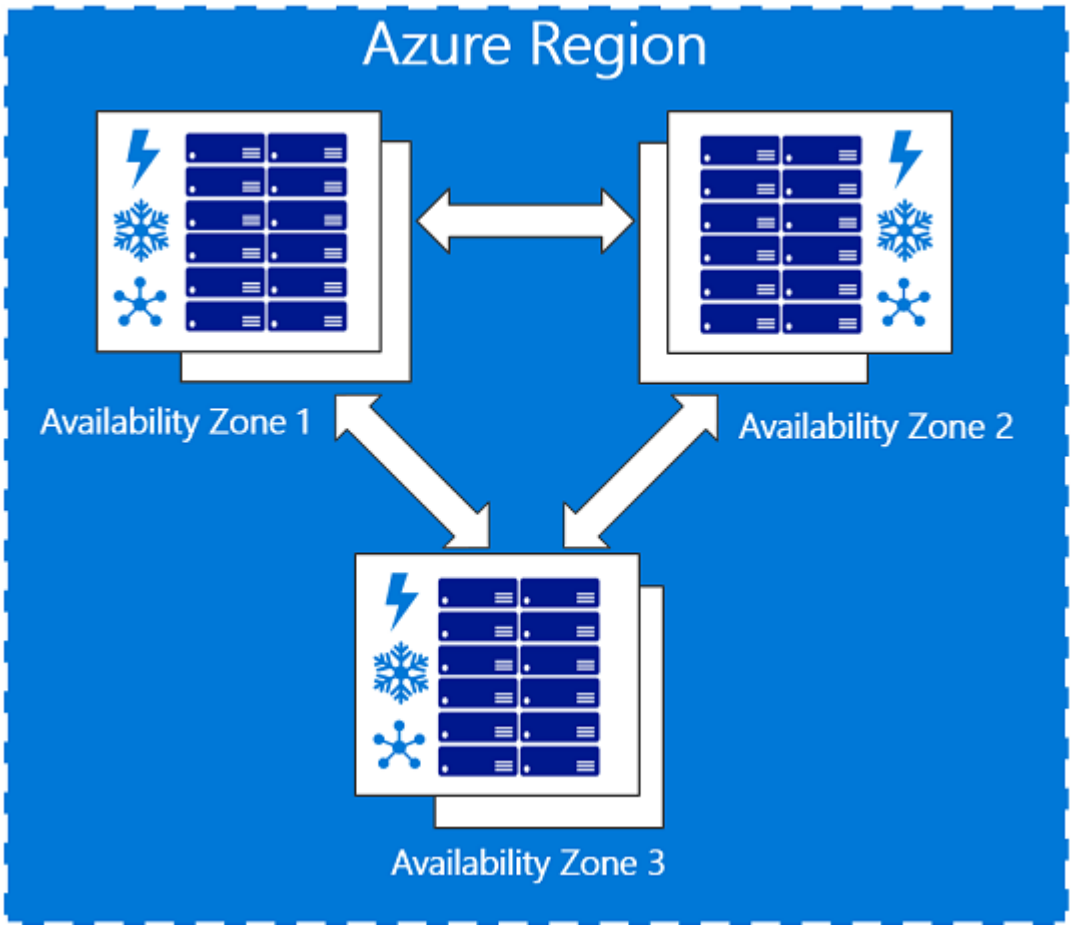
Regions - a set of related, interconnected datacenters which are no more than a few miles apart; you must select a region when creating most Azure services; there are currently 60+ active or planned worldwide; the most of any cloud computing provider; you will not have access to all 54 because some of them are restricted



Source: https://azure.microsoft.com/en-ca/global-infrastructure/geographies/#overview

Region Pairs - Each region is "paired" with one other region, which provides the highest-speed, lowest-latency connection between them; Azure treats them as a pair, trying to minimize the chance of them both going down at the same time. Good as a place to store backups and have redundant servers running.

Availability Zones - Unique physical locations within an Azure region, made up of one or more datacenters; there is a minimum of three zones in each region; you can manually place your resources in an availability zone for highest availability



Source: https://docs.microsoft.com/en-us/azure/availability-zones/az-overview

Resource Groups - a folder structure in Azure in which you organize resources like databases, virtual machines, virtual networks, or almost any resource

Azure Resource Manager (ARM) - this is the common resource deployment model that underlies all resource creation or modification; no matter whether you use the portal, PowerShell or the SDK, the Azure Resource Manager takes those commands and executes them

Azure Subscriptions

Subscriptions - a billing unit within Azure; all resources under a subscription get billed to a single owner

Multiple Subscriptions - possible to create multiple subscriptions to separate out billing

Management Groups - a hierarchy of subscriptions; can have many subscriptions, and group them, and put those groups into other groups

Core Azure Products

Compute Services - a category of services in Azure that provides CPU cycles for rent

Virtual Machines - looks, acts, feels, tastes like a real server in front of you; except it's running inside Azure's data center in a virtualized environment; Azure supports Windows and Linux virtual machines, with dozens of varieties of each; IaaS

Hypervisor - a layer that runs on top of the physical server Operating System that allows multiple guest operating systems (virtual machines) to run in an isolated manner on top

App Services - allows you to upload your code and configuration into Azure, and Azure will run the application as you specify; lots of integrations with Visual Studio, and other features and benefits provided on this platform; PaaS

Azure Container Instances (ACI) - the quickest way to create a container on Azure. You can deploy an image to Azure in about a minute. It can be used in production, but is not easily scalable.

Azure Kubernetes Services (AKS) - Kubernetes containers in Azure. Runs on Virtual Machine Scale Sets. Has auto-scaling, but also requires more overhead to run.

Windows Virtual Desktop (WVD) - A hosted version of Windows, in the cloud. Users can log into Windows from any device, and see their installed programs and files.

Networking Services - a category of services in Azure that provides network connectivity, performance, and monitoring services for inter-server and Internet communication

Virtual Network - a representation of a real network; all virtual machines must be connected to a virtual network subnet, and this allows them to talk to each other and to the Internet as long as it follows the rules of the network that you define

Virtual Network Peering- allows you to connect two or more virtual networks in Azure

ExpressRoute- through a connectivity provider, the ability to extend your Microsoft cloud networks to on-premises networks over a private connection

VPN Gateway - a device that allows encrypted private communication between a single computer or a network of servers, and an Azure network; IaaS

Storage Services - a category of services in Azure that provides cheap, infinite file storage

Azure Storage - a cheap place to store files, along with basic table and queue features; pay per Gigabyte; IaaS

Managed Disk - slightly more expensive, but this will allow Azure to provide some additional features that reduce the burden of managing your own storage account; pay per month for a provided GB limit; IaaS

Backup and Recovery Storage - as you'd expect, this is a specialized storage account that will manage your backups from virtual machines and perform recoveries

Database Services - a category of services in Azure that provides fast, structured and unstructured data storage

Containers – are the preferred way to deploy and manage cloud applications, where code is isolated and packaged into running instances of images (snapshots). Many instances of images can be deployed, configured, replicated with ease thereby solving the problem of complicated deployments. For instance, code compiled into an image can be deployed identically where ever needed, and with Azure Container Instances management of virtual machines is not needed.

Blob Storage – is Microsoft's object storage solution for Azure cloud

Disk Storage – block storage for Azure virtual machines

File Storage (Azure Files) – a managed cloud file share accessible by SMB and NFS protocol

Storage Tiers – optimized frequency access tiers for storage indicated as hot, cool, or archive

Cosmos DB - extremely low latency (fast) storage designed for smaller pieces of data quickly; PaaS

Azure SQL Database - a managed database solution that is compatible with SQL Server; DBaaS/PaaS

Azure SQL Database for MySQL - Managed MySQL database in Azure

Azure SQL Database for PostgreSQL - Managed PostgreSQL database in Azure

SQL Managed Instance – a scalable cloud database platform as a service utilizing SQL server database engine

Azure SQL Data Warehouse - designed for analyzing and reporting on huge data sources; not for inserts or updates; just reports

Azure Marketplace - a place for Microsoft and third-parties to offer their own solutions that are compatible with Azure; you'll find lots of vendors you'll recognize like Cisco, Citrix, Barracuda Networks, Oracle, etc.

SECTION 4: Core Solutions and Management Tools (10-15%)

Core Azure Solutions

Internet of Things (IoT) - thousands or millions of devices around the world that collect data and send them back to the cloud for processing

IoT Central – the application platform that helps reduce the complexity of enterprise grade IoT solutions

IoT Hub – a managed and cloud hosted service for bi-directional communication between IoT application and devices

Azure Sphere – a secured, connected, crossover microcontroller unit used as a high-level application platform for internet-connected devices

Azure Synapse Analytics – an analytics service that joins enterprise data warehousing and Big Data analytics

HDInsight - the Azure equivalent of the open source Apache Hadoop tools

Azure Databricks - A central dashboard for managing big data in Azure, where data analysts, data scientists and data developers can work together to derive business intelligence from data.

Artificial Intelligence (AI) - machine learning APIs offered in Azure that can analyze voice, text, images, videos, natural language processing, and do various intelligent actions based on that; can do chatbots, real time transcription, translation, etc.

Serverless Computing - a set of Azure services that allow you to use execute code in the cloud but don't require (or even allow) you to manage the underlying server or have

any control over its performance; functions, logic apps, and app grid are examples of serverless computing in Azure

Azure Functions - small pieces of code that are designed to perform some task quickly; these are like connector code designed to do small things; serverless model

Azure DevOps - A set of tools to help companies manage development from development to deployment. Includes project management tools such as Boards and deployment tools such as Pipelines.

GitHub - provides hosting for software development, distributed version control using Git, and source code management (SCM) functionality

GitHub Actions – used to help automate software development workflows from within GitHub

Azure DevTest Labs - enables developers on teams to efficiently self-manage virtual machines (VMs) and PaaS resources without waiting for approvals.

Azure Management Tools

Command Line Interface (CLI) - a command line tool that allows you to manage your Azure subscription and resources using scripts or commands

PowerShell - another type of command line tool

Azure Portal - the website located at http://portal.azure.com that we use to manage your Azure subscription and resources using a friendly user interface

Cloud Shell - allows access to the CLI and PowerShell consoles in the Azure Portal

Azure Advisor - a tool that will analyze your use of Azure and make you specific recommendations based on your usage across availability, security, performance and cost categories

Azure Mobile App – native mobile application of the Azure portal

Azure Resource Manager (ARM) - a deployment management service for your Azure resources

Azure Monitor - a centralized dashboard that collects all the logs, metrics and events from your resources

Azure Service Health - a customizable dashboard tool that allows you to track the health of your Azure services in regions where they are used

For Further Reading:

Azure PowerShell - https://docs.microsoft.com/en-us/powershell/azure/?view=azps-5.1.0

Azure CLI - https://docs.microsoft.com/en-us/cli/azure/install-azure-cli

Azure Cloud Shell - https://docs.microsoft.com/en-us/azure/cloud-shell/overview

Azure Portal - https://docs.microsoft.com/en-us/azure/azure-portal/

SECTION 5: General Security and Network Security (10-15%)

Security features

Azure Security Center – provides advanced threat protection and is a unified security management system

Key Vault – Azure's management solution for secrets, keys, and certificates

Azure Sentinel – a security information event management and security orchestration automated response solution

Azure Dedicated Hosts – a service that provides physical servers for use by indicated virtual machine(s) as isolated machines not shared between Azure customers

Network Security

Azure Firewall - a managed service inside Azure that protects your virtual networks from unauthorized traffic

Distributed Denial of Service attacks (DDoS) -a type of attack that originates from the Internet that attempts to overwhelm a network with millions of packets of bad traffic that aims to prevent legitimate traffic from getting through

Azure DDoS Protection - basic level of protection is included free; there is a standard level that you can upgrade to (pay for) that will add logging, alerting and telemetry for you to see these attacks happening

Network Security Group (NSG) - a fairly basic set of rules that you can apply to both inbound traffic and outbound traffic that lets you specify what sources, destinations and ports are allowed to travel through from outside the virtual network to inside the virtual network

Application Security Group (ASG) - A way of grouping related resources together to simplify the way NSG rules are created. All front end VMs can be in one ASG, while the mid-tier is in another. And then you can refer to them in the NSG rule by their ASG name.

User Defined Routes (UDR) - A way of forcing traffic travelling over a virtual network over a specific path. This is usually used in conjunction with Firewall devices, or ExpressRoute.

Best practices for security:

- All virtual networks should use an NSG
- Similar to locking the doors to your house, a basic level of security but not the ultimate
- Enhanced DDoS protection, should be used if you are likely to be a target
- Application Gateway with WAF is generally a good idea for production systems
- Security through layers is also a good idea because if one layer is breached, there are backups

SECTION 6: Identity, Governance, Privacy, Compliance (20-25%)

Azure Identity Services

Authentication - you provide something that proves who you are, like userid and password; multi-factor authentication (sms or app) falls into this category

Authorization - once we know who you are, what permissions do they have

Admin/Root Access - should be reserved for the very few trusted people

Azure Active Directory (Azure AD) - Microsoft's preferred Identity as a Service solution

Azure AD revolves around users, groups, and applications and managing the permissions between those objects

Single-Sign On - the ability to use the same user id and password to log into every application that your company has; enabled by Azure AD

AD Connect - software that can synchronize your on premises Active Directory with Azure Ad

Multi-Factor Authentication (MFA) - the concept of having something additional to a "password" that is required to log in; passwords are findable or guessable; but having your mobile phone on you to receive a phone call, text or run an app to get a code is harder for an unknown hacker to get

Azure Governance Features

Governance - the policies and procedures of your company that protect your account and your data

Azure Policy - implement standards for your organization across Azure

Rules can be enforced by blocking the action or just reporting the action

Built-In Policies Examples:

- Require SQL Server 12.0
- Allowed Storage Account SKUs
- Allowed Regions for resources to be created in
- Allowed Virtual Machine SKUs
- Require resources have tags
- And others

Custom Policies - you can create your own policies if the built-in ones don't meet your needs

Role Based Access Control (RBAC) - assigning permissions by role instead of to individuals one by one

Locks - allows you to "lock" resources to prevent them from being changed without removing the lock; an easy way to stop someone from accidentally stopping or deleting an important resource

Locks Access Control - you can limit who has the ability to delete locks

Azure Advisor - mentioned earlier, but it has a security section that makes recommendations based on your specific account

Azure Blueprints - a way of defining templates for subscriptions, so that new subscriptions already come with a default set of users and policies. Instead of having to set a Subscription up before using and possibly missing a security policy.

Privacy and Compliance Resources

Security Layers (available to use in cloud computing):

- Data - i.e. virtual network endpoint, limit SQL Server user rights
- Application - i.e. run API management in front of APIs
- Compute - i.e. Limit remote desktop access, limit ssh, run Windows update
- Network - i.e. Set up an NSG, use subnets, deny traffic by default
- Perimeter - i.e. DDoS protection, firewalls
- Identity & access - i.e. Azure AD
- Physical - i.e. Door locks, fingerprint readers, and key cards

Azure Security Center - unified security management and threat protection; a security dashboard inside Azure Portal

Azure Information Protection (AIP) - a way to classify emails and documents; like a DRM for documents; secret, top secret, public, etc.; enforced by Outlook 365

Azure Advanced Threat Protection (ATP) - monitor Azure AD and detect when users are behaving differently than they normally do; requires additional login requirements like MFA or even locks them out when they do

Compliance - meeting the terms of industry or government standards

General Data Protection Regulation (GDPR) - a law that covers how you collect, store, protect and report data of EU citizens

ISO - Azure is in compliance with a number of ISO standards

NIST Cybersecurity Framework (CSF) - requires an audit to see that you're following security and privacy best practices

Microsoft Privacy Statement - http://privacy.microsoft.com

Microsoft Trust Center - https://www.microsoft.com/en-us/trust-center/product-overview

Service Trust Portal - http://servicetrust.microsoft.com/

Compliance Manager - a tool that helps you manage your own regulatory compliance

Azure Government Services - http://portal.azure.us/ specific for US government agencies; a private cloud

Department of Defense (DoD) - another private isolated cloud for the US military

Private cloud accounts have different endpoint URLs for services than the public cloud

For Further Reading:

Azure Privacy and Compliance Resources - https://azure.microsoft.com/en-us/blog/trusted-cloud-security-privacy-compliance-resiliency-and-ip/

SECTION 7: Cost Management and SLA (10-15%)

Planning and Management of Costs

Factors Affecting Your Bill:

- Understand by which metric each service you use is charged
    - Pay per usage, consumption model - Gigabytes used, or # of executions
    - Pay per time - pay per minute or per hour regardless if you use it
- Look at other models for application design that can save money
    - Web apps, functions, etc.
- Understand how traffic from inside Azure to the Internet is charged, and data transfers between regions
- Understand that Azure has dev/test options for licensing for some software

Pricing Calculator - https://azure.microsoft.com/en-ca/pricing/calculator/

Spend 20 minutes playing around with this before taking the exam.

Total Cost of Ownership (TCO) - the all-in price of running a server that includes the cost of the hardware, software, human labor for installation and maintenance, electricity, cooling, backups, real estate, internet connectivity, etc

TCO Calculator - https://azure.microsoft.com/en-ca/pricing/tco/calculator/

Best Practices for Reducing Costs in Azure:

- Use Azure Advisor cost tab for recommendations
- Auto shutdown of Dev/QA resources
- Utilize storage lifecycle - hot, cool, archive storage tiers
- Utilize reserved instances (1 or 3 year contract) if you're likely to use a VM for that long
- Configure alerts when billing exceeds an expected level

- Use Azure Policy to prevent excessive spending like restricting VM SKUs
- Implement automatic scaling to reduce costs
- Downsize resources like managed storage accounts that are a lot bigger than you actually need
- Use tags to more easily identify named owners/projects of running resources in Azure

Azure Cost Management - a tool to analyze historical spending in the cloud

Azure SLAs

Service Level Agreements (SLA) - a financial guarantee that they will deliver the services as promised

Microsoft will refund 10% or 25% of your bill if their uptime guarantee doesn't meet the published standard

Azure Updates - https://azure.microsoft.com/en-ca/updates/

For Further Reading:

Azure Service Level Agreements - https://azure.microsoft.com/en-us/support/legal/sla/