JON BONSO AND GEROME PAGATPATAN

AZURE CERTIFIED

AZ-900 Microsoft Azure Fundamentals

Tutorials Dojo Study Guide

TABLE OF CONTENTS

INTRODUCTION

With the rapid advancement of technology, enterprises are adopting newer technologies that will help their businesses transform and grow. Microsoft Azure is one of the emerging technologies that you can leverage in this age since a lot of companies are shifting their existing infrastructures in the cloud. Unlike the traditional setup, cloud computing allows you to obtain resources on-demand with just one click on their platform, including the servers, storage, databases, networking, analytics, artificial intelligence, and a lot more.

Microsoft Azure offers a range of cloud services, depending on your business needs. These services are continuously upgrading, and new features are being added every year to deliver customer satisfaction. Since Azure's resources and services are too vast, the **Microsoft Azure Certification** program offers different certification paths that will help aspiring candidates and IT professionals validate their skills and knowledge to maximize the solutions created in the cloud.

Microsoft Azure is the second biggest cloud service provider in the market next to AWS, and a lot of companies are now adopting a **multicloud** strategy, which makes it all the more beneficial for IT professionals like you to expand your skill set and learn multiple cloud technologies. Learning is a lot more fun if you merge it with various cloud services. It will be an exciting and enjoyable journey for you, and the first step is to become **AZ-900 Microsoft Azure Fundamentals** certified. This eBook will help familiarize yourself with the basic cloud concepts as well as the core services of Microsoft Azure, which are the building blocks that will help you pass the exam and make a successful career shift to cloud computing.

Note: We took extra care to come up with these study guides and cheat sheets, however, this is meant to be just a supplementary resource when preparing for the exam. We highly recommend working on **hands-on sessions** and **practice exams** to further expand your knowledge and improve your test taking skills.

AZ-900 MICROSOFT AZURE FUNDAMENTALS EXAM OVERVIEW

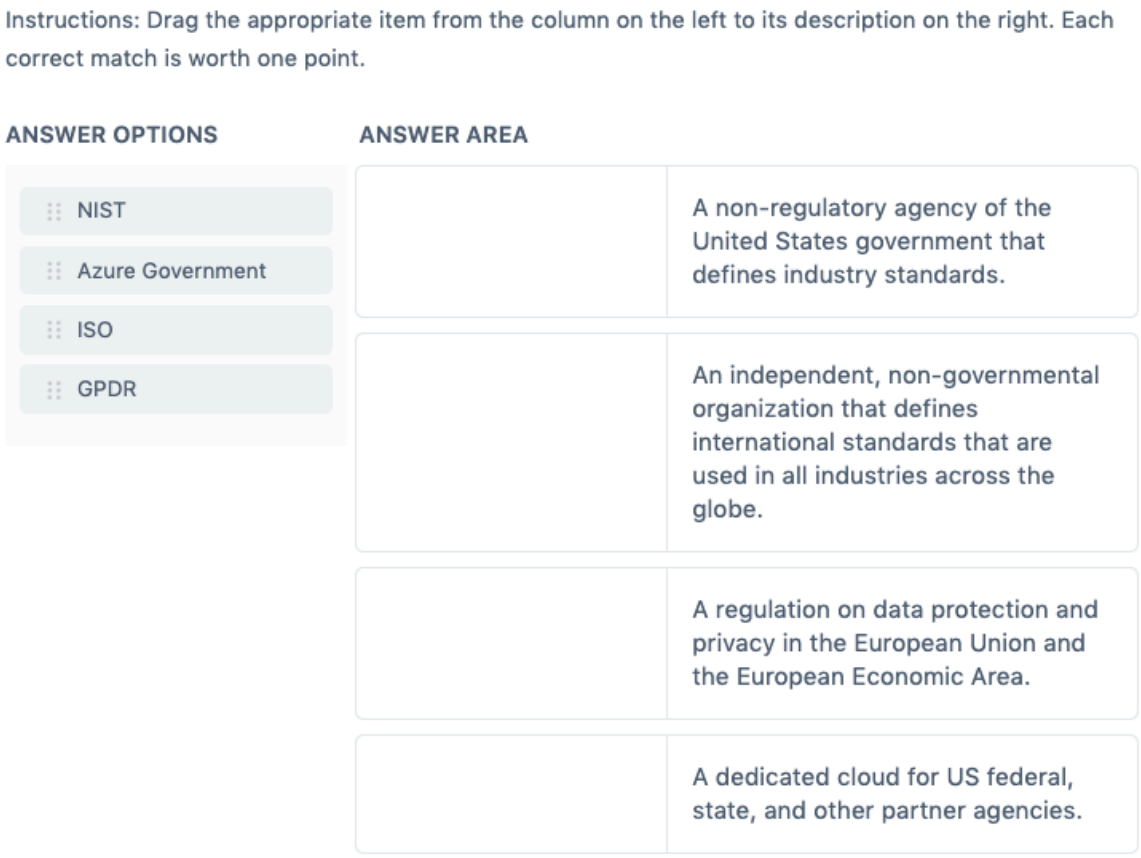
The Microsoft Azure Certification Program validates the technical skills and knowledge for building secure and reliable cloud-based applications using the Azure platform. By successfully passing the Microsoft Azure exam, individuals can prove their expertise to their current and future employers. The AZ-900 Microsoft Azure Fundamentals exam is currently the most basic certificate that you can get and is also known to be the easiest among all of the Azure certification exams.

Exam Details

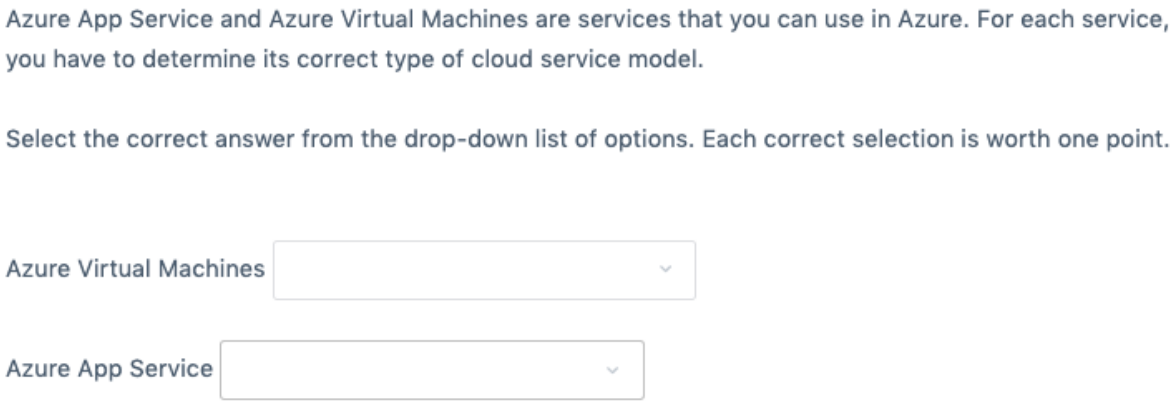
The AZ-900 Microsoft Azure Fundamentals examination is intended for candidates who have the knowledge and skills necessary to effectively demonstrate an overall understanding of the Azure Cloud, independent of specific technical roles addressed by other Microsoft certifications (for example, Administrator Associate and Developer Associate). The exam is composed of different types of questions.

For multiple-choice type of questions, you will have to choose one correct response out of four options.

For Drag and Drop questions, match the items by dragging them to their correct descriptions.



For Dropdown type of questions, select the correct answer from the drop-down list of options.



For Hotspot type of questions such as multiple Yes/No, evaluate whether the presented statements relating to a certain topic are correct/incorrect.

For each of the following items, choose **Yes** if the statement is true or choose **No** if the statement is false. Take note that each correct item is worth one point.

Questions	Yes	No
Azure virtual machines are billed on a per-hour basis.	○	○
When you delete a virtual machine in Azure, by default, any disks that are attached to the VM are deleted.	○	○
Disks attached to stopped virtual machines do not incur costs.	○	○

You can take the exam via online proctoring or from a testing center close to you.

Exam Code:	AZ-900
Prerequisites:	None
No. of Questions:	30-40
Score Range:	100-1000
Cost:	99 USD
Passing Score:	700
Time Limit:	90 minutes

Exam Domains

The AZ-900 Microsoft Azure Fundamentals exam has three areas to assess your skills, each with a corresponding weight and topic coverage. The skills measured are: Cloud Concepts (25-30%), Azure Architecture and Services (35–40%), and Azure Management and Governance (30–35%).

Cloud Concepts

- Describe cloud computing
- Describe the benefits of using cloud services
- Describe cloud service types

Azure Architecture and Services

- Describe the core architectural components of Azure
- Describe Azure compute and networking services
- Describe Azure storage services
- Describe Azure identity, access, and security

Azure Management and Governance

- Describe cost management in Azure
- Describe features and tools in Azure for governance and compliance
- Describe features and tools for managing and deploying Azure resources
- Describe monitoring tools in Azure

Exam Scoring System

You can get a score from 100 to 1,000 with a minimum passing score of 700 when you take the AZ-900 Microsoft Azure Fundamentals exam. Microsoft uses a scaled scoring model to associate scores across multiple exam types that may have different levels of difficulty. Your complete score report will be sent to you by email 1 - 5 business days after your exam. However, as soon as you finish your exam, you'll immediately see a pass or fail notification on the testing screen.
For individuals who unfortunately do not pass their exams, you must wait 24 hours before you are allowed to retake the exam. There is no hard limit on the number of attempts you can retake an exam.

Once you receive your score report via email, the result should also be saved in your Microsoft Certification account. The score report contains a table of your performance in each domain and it will indicate whether you have met the level of competency required for these. Take note that you do not need to achieve competency in all areas for you to pass the exam. In the first part of the report, there will be a performance summary by exam section that highlights your strengths and weaknesses, which can help you determine the areas you need to improve on.

Exam Benefit

If you successfully pass any Microsoft Certification exam, you will receive a **Certified Digital Badge**. You can showcase your achievements to your colleagues and employers by adding these digital badges to your email signatures, Linkedin profile, or on your social media accounts. To view your badges, simply go to the "Dashboard" section of your Acclaim Account.

You can visit the official Microsoft Certification FAQ page to view the frequently asked questions about getting certified and other information about the Microsoft Certification:
https://docs.microsoft.com/en-us/learn/certifications/certification-exam-policies.

AZ-900 MICROSOFT AZURE FUNDAMENTALS EXAM STUDY GUIDE

The AZ-900 Microsoft Azure Fundamentals certification exam is intended for individuals who want to have a foundational knowledge when venturing into the Cloud. Although the AZ-900 test is the easiest to achieve among all the Azure certification exams, you still need to learn and properly understand the concepts on cloud computing, and know the basics on the Azure services.

In the Microsoft Azure Fundamentals Exam (or AZ-900 for short), questions will test your ability to:

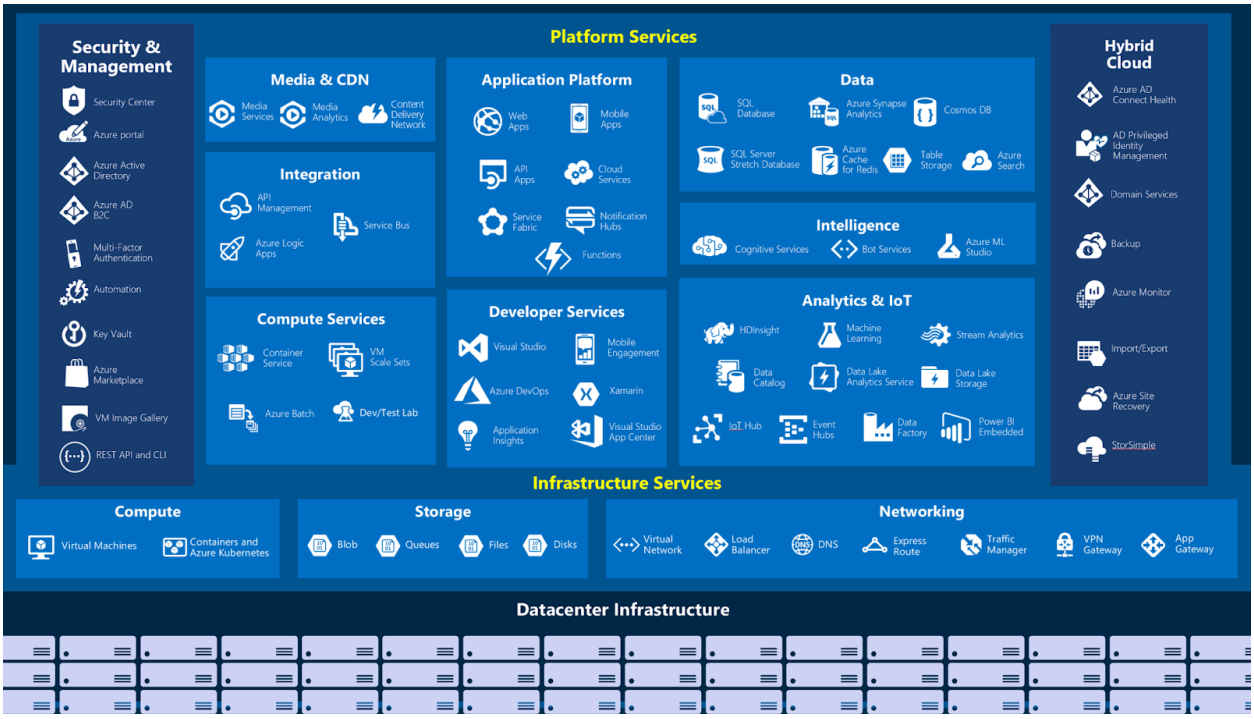
- Describe Cloud Concepts
- Describe Core Azure Services
- Describe Core Solutions and Management Tools on Azure
- Describe General Security and Network Security Features
- Describe Identity, Governance, Privacy, and Compliance Features
- Describe Azure Cost Management and Service Level Agreements

Given the scope of the exam above, you should also be familiar with the concepts of compute, storage, networking, application support, and application development. This guide aims to help you pass your exam on your first try.

Study Materials

The primary study materials that you can use for your review are: Azure Fundamentals Learning Path, Azure Documentation, Tutorials Dojo's Azure Cheat Sheets, and our AZ-900 Practice Exams.

Having an Azure account will help you better understand the concepts written within the documentations, since the exam itself contains different types of questions (multiple-choice, drag and drop, hotspot, and dropdown) to test your knowledge on these services.



Additional details regarding your AZ-900 exam can be found in this Azure Exam Skills Outline.

To learn more about each of the AZ-900 exam domains, you can take these free training materials from the Microsoft site:

1. Explore Microsoft Azure cloud concepts - learn and understand the fundamentals of the Azure platform.
2. Distinguish Microsoft Azure Core Services - explore the core products and solutions in Azure.
3. Understand the various management tools from Microsoft Azure - learn how to choose the appropriate tools and services to address different kinds of business challenges.
4. Securing your data in the cloud - know the security best practices to ensure your resources in the cloud are safe and secured.
5. Examine Microsoft Azure identity, privacy, compliance, and trust - study the basics of how you can secure access to your applications, the difference between authentication and authorization, and various security tools to protect your account.
6. Review Microsoft Azure pricing, service level agreements, and lifecycles - explore the factors that affect your cost when using Azure services.

Azure Services to Focus On

Azure offers extensive documentation and various learning paths for all of their services. Knowing the basic concepts and Azure services will help you easily pass the AZ-900 exam, which can pave the way toward a

rewarding career in cloud computing. I suggest that you read Tutorials Dojo's Azure Cheat Sheets, which provide bullet-point summaries of the most important concepts about the different Azure services.

Concepts that you need to focus on:

1. Cloud Concepts - You should be able to understand the various concepts in cloud computing, such as benefits, economies of scale, deployment models, and types of cloud services.
2. Compute - Study the different types of compute services, and their use cases.
3. Storage - Azure offers many types of storage services, depending on your needs. Understand what these types are and how they differ from each other.
4. Network - This is the fundamental building block in launching your resources. Study the different types of networking services and the features each of them supports.
5. Security - Understand how you can secure your account in Azure. You also need to know the various security services that you can use in different scenarios.

Aside from these, you should know the differences between Azure Portal, CLI, Powershell, and Cloud Shell. It's also important to familiarize yourself with the portal's interface since there are questions that show an image of the portal and ask you to select the answer that matches the image.

Validate Your Knowledge

After going through the training and reading materials we gave above, we recommend taking a practice exam first before booking your AZ-900 exam. Tutorials Dojo offers a top-notch set of **AZ-900 Microsoft Azure Fundamentals practice tests**. Combined with our cheat sheets and this study guide, we're confident that these will help you pass the exam.

Sample Practice Test Questions

Question 1

A company is planning to deploy its suite of enterprise applications to Microsoft Azure, where each application has several dependencies and subcomponents. The company must also control and manage the patching activities of the underlying operating system of the servers.

What type of cloud deployment solution should you recommend?

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)
4. Functions as a service (FaaS)

Correct Answer: 1

Infrastructure as a service (IaaS) is an instant computing infrastructure, provisioned, and managed over the internet. It's one of the types of cloud services, along with software as a service (SaaS), platform as a service (PaaS), and serverless.

IaaS quickly scales up and down with demand, letting you pay only for what you use. It helps you avoid the expense and complexity of buying and managing your own physical servers and other datacenter

infrastructure. Each resource is offered as a separate service component, and you only need to rent a particular one for as long as you need it.

A cloud computing service provider, such as Azure, manages the infrastructure, while you purchase, install, configure, and manage your own software — operating systems, middleware, and applications.

You can also use the Azure Virtual Machines, which is an Infrastructure as a Service (IaaS), to host the suite of enterprise applications and manage the patching activities of the underlying operating system of the servers.

Therefore, the correct answer is: ***Infrastructure as a Service (IaaS).***

Platform as a Service (PaaS) is incorrect because this is a type of cloud service that allows you to focus on developing your applications and services by letting the cloud service provider handle the administrative tasks of the underlying application infrastructure. It doesn't allow the customers to control and manage the patching activities of the underlying operating system of the servers.

Software as a Service (SaaS) is incorrect because this cloud service type just allows customers to connect to and use its cloud-based apps over the Internet, and not deploy their custom applications. Just like PaaS, it doesn't allow the customers to control and manage the patching activities of the underlying operating system of the servers that you use.

Function as a Service (FaaS) is incorrect because this is simply an event-driven serverless compute platform. The underlying servers are abstracted and not accessible to the end-user.

References:
https://azure.microsoft.com/en-au/overview/what-is-iaas
https://azure.microsoft.com/en-au/overview/what-is-azure/iaas/#overview
https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/5-types-of-cloud-services
ht
tps://docs.microsoft.com/en-us/azure/security/fundamentals/paas-deployments

Question 2
Which of the following is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization?

1. Microsoft Entra Connect Health
2. Azure Advanced Threat Protection (ATP)
3. Azure Information Protection
4. Azure Service Health

Correct Answer: 2

Azure Advanced Threat Protection (ATP) is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Azure ATP enables SecOp analysts and security professionals struggling to detect advanced attacks in hybrid environments to:

- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage

Azure ATP monitors and analyzes user activities and information across your network, such as permissions and group membership, creating a behavioral baseline for each user. Azure ATP then identifies anomalies with adaptive built-in intelligence, giving you insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats facing your organization. Azure ATP's proprietary sensors monitor organizational domain controllers, providing a comprehensive view for all user activities from every device.

Azure ATP provides you invaluable insights on identity configurations and suggested security best-practices. Through security reports and user profile analytics, Azure ATP helps dramatically reduce your organizational attack surface, making it harder to compromise user credentials and advance an attack. Azure ATP's visual Lateral Movement Paths help you quickly understand exactly how an attacker can move laterally inside your organization to compromise sensitive accounts and assists in preventing those risks in advance. Azure ATP security reports help you identify users and devices that authenticate using clear-text passwords and provide additional insights to improve your organizational security posture and policies.

Hence, the correct answer is: ***Azure Advanced Threat Protection (ATP).***

Microsoft Entra Connect Health is incorrect because this is simply a Microsoft tool designed to meet and accomplish your hybrid identity goals, such as password hash synchronization, pass-through authentication, federation integration, synchronization, and health monitoring. It doesn't leverage on your on-premises Active Directory signals either.

Azure Information Protection is incorrect because this is just a service that is primarily used to helps organizations label and classify their sensitive documents and emails.

Azure Service Health is incorrect because this service only provides personalized guidance and support when issues in Azure services affect your resources. This is not a cloud-based security solution that leverages your

on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/what-is-atp
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-architecture

Check out our **AZ-900 Microsoft Azure Fundamentals Practice Exams** for more practice test questions with detailed explanations.

You should get some rest before the day of your exam and review any notes that you have written down. Since the AZ-900 exam is not composed of scenario-based questions and case studies, the exam itself should be straightforward.

AZURE CHEAT SHEETS

AZURE OVERVIEW

Azure Cloud Concepts

- Terminologies of the cloud: **High Availability, Fault Tolerance, Disaster Recovery, Scalability, Elasticity,** and **Agility**

High Availability

- If hardware fails, you can get a new, exact copy of it in very little time
- Use clusters (a group of virtual machines) to ensure high availability

Fault Tolerance

- Fault tolerance is part of the resilience of cloud computing
- **Zero Down-Time** - if one component fails, a backup component takes its place

Disaster Recovery

- Plan to recover critical business systems:
  - **Recovery Time Objective (RTO)** is the time it takes after a disruption to restore business process to its service level
  - **Recovery Point Objective (RPO)** is the acceptable amount of data loss measured in time before the disaster occurs
- Services for backup and disaster recovery:
  - **Azure Backup** - simplify data protection while saving costs
  - **Azure Site Recovery** - keep your business running with disaster recovery service
  - **Azure Archive Storage** - store rarely used data in the cloud

Scalability

- You may increase or decrease the resources and services used at any given time, depending on the demand or workload.
  - **Vertical Scaling** - adding resources to increase the power of an existing server
  - **Horizontal Scaling** - adding more servers that function together as one unit
- Use **scale sets** for critical scenarios.

Elasticity

- Quickly expand or decrease computing resources
- Automatically provisions more computing resources to handle the increased traffic. Once the traffic begins to normalize, the cloud automatically de-allocates the extra resources automatically to reduce costs

Agility

- The ability to design, test, and launch software applications quickly that stimulate business growth.
- Cloud agility enables companies to concentrate on other concerns such as security, monitoring, and analysis, instead of provisioning and maintaining the resources.

Sources:
https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/3-benefits-of-cloud-computing
https://docs.microsoft.com/en-us/azure/virtual-machines/workloads/sap/sap-high-availability-architecture-scenarios
https://azure.microsoft.com/en-us/solutions/backup-and-disaster-recovery/

Azure CapEx vs OpEx

Capital Expenditure (CapEx)

- Upfront cost on physical infrastructure
- You need to plan your expenses at the start of a project or budget period.
- CapEx computing costs:
    - **Server costs** - server clustering, redundant power supplies, and uninterruptible power supplies
    - **Storage costs** - centralized storage and fault-tolerant storage for critical applications.
    - **Network costs** - cabling, switches, access points, routers, wide area networks, and Internet connections.
    - **Backup and archive costs** - backup maintenance and consumables like tapes.
    - **Organization continuity and disaster recovery costs** - recover from a disaster and continue operating using backup generators.
    - **Datacenter infrastructure costs** - costs for construction and building equipment.
    - **Technical personnel** - technical expertise and workforce to install, deploy, and manage the systems in the data center and at the DR site.

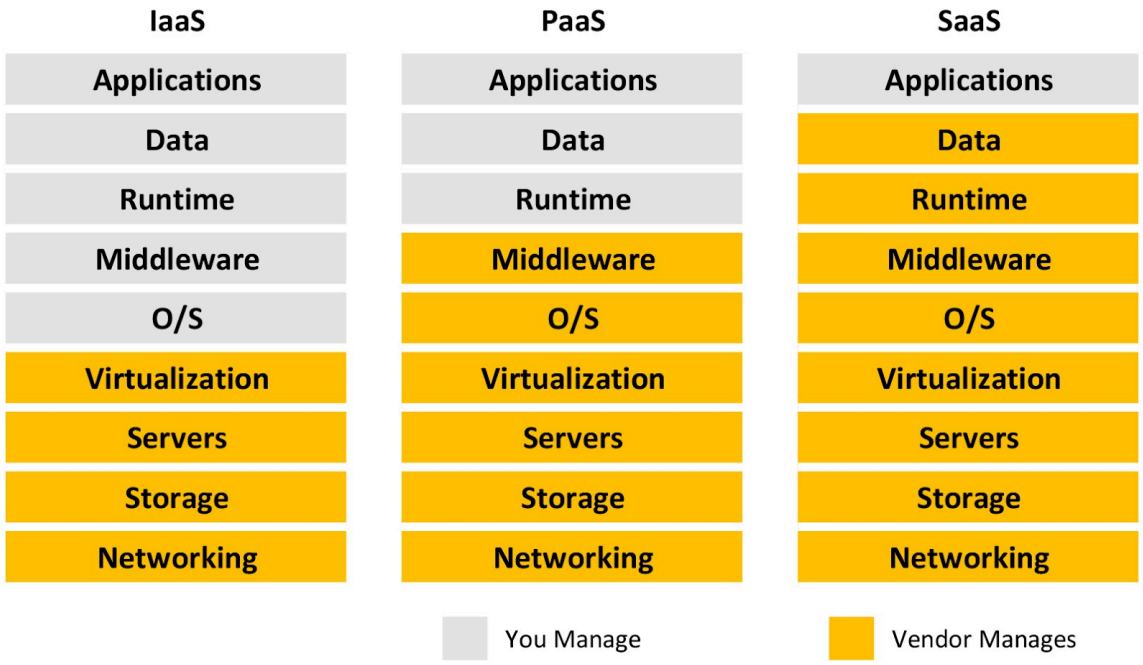
Operational Expenditure (OpEx)

- No upfront cost but you pay for the service/product as you use it
- OpEx is particularly appealing if the demand fluctuates or is unknown
- OpEX computing costs:
    - **Leasing software and customized features** - responsibility to de-provision the resources when they aren't in use so that you can minimize costs.
    - **Scaling charges based on usage/demand instead of fixed hardware or capacity** - plan for backup traffic and disaster recovery traffic to determine the bandwidth needed.
    - **Billing at the user or organization level** - when using a dedicated cloud service, you could pay based on server hardware and usage.

Sources:
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/business-outcomes/fiscal-outcomes
https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/3c-capex-vs-opex

Azure Cloud Service Models

- The three cloud computing service models are **IaaS, PaaS,** and **SaaS**.
- You can also use **serverless computing** to eliminate the need to manage infrastructure.
- The **shared responsibility model** determines the security tasks that are handled by the cloud provider and handled by the customer.
    - Azure is responsible for protecting the infrastructure such as hosts, network, and data center.
    - The customer is responsible for protecting their data, endpoints, account, and access management.
- IaaS, PaaS, and SaaS have different levels of managed services:



Infrastructure as a service (IaaS)

- Most user management
- You are responsible for managing the **operating systems, data,** and **applications.**
- IaaS helps you to extend resources rapidly to meet the spikes required for your application.
- Used in the following scenarios:
    - **Migrating workloads** - move existing applications to the cloud.
    - **Test and development** - quickly set up and dismantle test and development environments. IaaS makes scaling development and testing environments, fast and economical.
    - **Storage, backup, and recovery** - simplify the planning and management of backup and recovery systems.
    - **Website hosting** - less expensive than traditional web hosting.

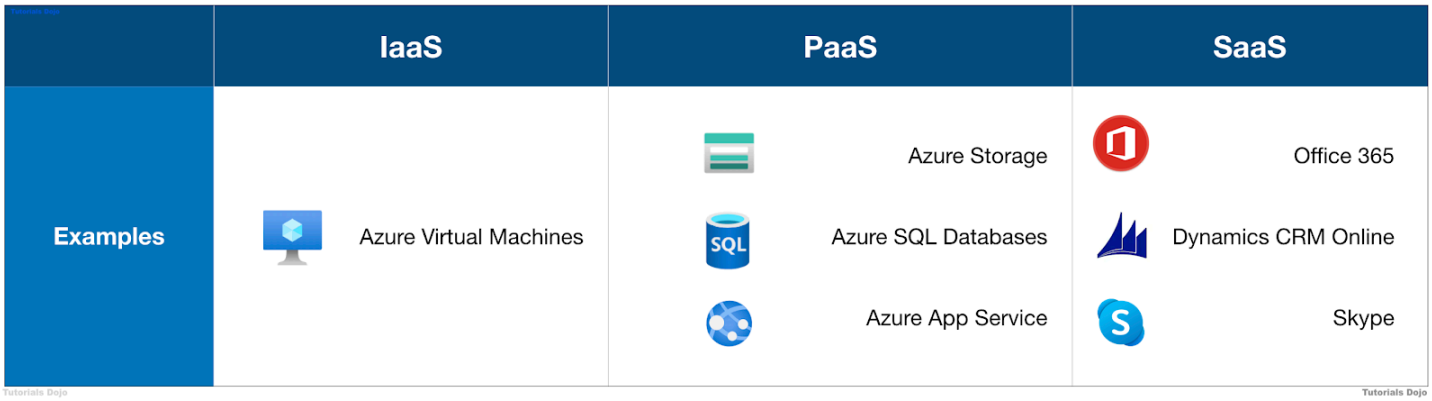
- **High-performance computing (HPC)** - clusters of computers that help solve complex problems involving millions of variables or calculations.
- **Big data analysis** - for massive data sets that require a huge amount of processing power.

Platform as a service (PaaS)

- Less user management
- The operating systems are managed by the cloud provider, while the user is responsible for the applications and data they run and store.
- PaaS offers all the functionality you need to support the entire lifecycle of web applications: **building, testing the application**, **deploying the source code**, **managing**, and **updating** within the same integrated environment.
- Used in the following scenarios:
  - **Development framework** - a framework for creating or customizing cloud-based applications.
  - **Analytics or business intelligence** - find insights and patterns, and predict outcomes to improve business decisions.

Software as a service (SaaS)

- Requires the least amount of management.
- Allows organizations to focus on the business aspect rather than managing the infrastructure, security, and application.



	IaaS	PaaS	SaaS
Costs	No upfront costs. Users pay only for what they consume.	No upfront costs. Users pay only for what they consume.	No upfront costs. Users pay a subscription, typically on a monthly or annual basis.
User Responsibility	Purchase, installation, configuration, and management of their own software, operating systems, middleware, and applications.	Custom development of their own applications. Allows the user to focus on the application or workload they want to run. Not responsible for managing the underlying server or infrastructure.	Users just use the application software Not responsible for any maintenance or management of the underlying software.
Cloud Provider Responsibility	Ensures that the underlying cloud infrastructure *(such as virtual machines, virtualization, storage, and networking)* is available for the user.	Operating system management, network, and service configuration. Typically responsible for everything apart from the application that a user wants to run. Provide the user a complete managed platform on which to run the application.	Provision, management, and maintenance of the application software.
Examples	Azure Virtual Machines	Azure Storage Azure SQL Databases Azure App Service	Office 365, Skype, and Dynamics CRM Online

Serverless Computing

- Function as a Service (FaaS)
- You simply deploy the code with a serverless platform, and it runs at high availability.
- Dynamically scales up and down to meet the demands of each workload within seconds.
- A **pay-per-execution model** that charges sub-second billing only for the time and resources required to execute the code.

AZ-900 Exam Notes:

It's important that you understand security in the cloud. Microsoft Azure provides a shared responsibility model that will help you understand the responsibilities of the cloud provider and the customer. The responsibilities vary depending on the cloud service model.

Sources:

https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/5-types-of-cloud-services
https://azure.microsoft.com/en-us/overview/what-is-iaas/
https://azure.microsoft.com/en-us/overview/what-is-paas/
https://azure.microsoft.com/en-us/overview/what-is-saas/

Azure Cloud Architecture Models

- Cloud computing is the delivery of services over the Internet that helps you reduce your operating costs, run your infrastructure efficiently, and scale as business requirements change.
    - Benefits of cloud computing:
        - Cost - eliminates capital expense.
        - Global scale - ability to scale elastically.
        - Performance - computing hardware is always upgraded to the latest generation.
        - Security - data stored in the cloud has a broad set of policies, technologies, and controls.
        - Speed - computing resources can be provisioned in minutes.
        - Productivity - enables the customer to focus on business requirements instead of setting up on-site datacenters.
        - Reliability - availability of your resources at all times.
- Three deployment methods of cloud computing: **Public vs Private vs Hybrid.**
- The model you choose for cloud deployment depends on your budget, security, scalability, and maintenance needs.

Public Cloud

- Focus on maintaining your applications without having to worry about purchasing, managing, or maintaining the hardware on which it runs.
- You can use multiple public cloud providers of varying scale.

Advantages	Disadvantages
High scalability/agility	Specific security requirements
Pay-as-you-go pricing	Government policies, industry standards, or legal requirements
You are not responsible for the updates and maintenance of the hardware.	You don't own the hardware or services and you also can't manage them as you may want to.
The required technical knowledge is minimal.	Maintaining a legacy application might be hard to meet

Private Cloud

- A dedicated on-premises datacenter configured to be a cloud environment that provides users in your organization with self-service access to compute resources.
- The headache of maintaining your hardware and software services are all in your hands.
- You can use a private cloud when an organization has data that cannot be put in the public cloud, perhaps for legal reasons.

Advantages	Disadvantages
Any scenario or legacy application configuration is supported.	CapEx involved - principal cost is the procurement of the equipment.
You have control (and responsibility) over security	To scale, you must buy, install, and set up new hardware
Compliance, or security requirements in your organization	Private clouds require IT skills and expertise

Hybrid Cloud

- Enables you to move data and applications between **private** and **public** clouds.
- When there is a spike in demand in your private cloud, you can "burst through" to the public cloud for additional computing resources.

Advantages	Disadvantages
Maintain a private infrastructure for sensitive assets.	More expensive than selecting one deployment model since it involves some CapEx cost upfront
Take advantage of the resources in the public cloud when needed.	It can be more complicated to set up and manage
With the ability to scale to the public cloud, you pay for extra computing power only when needed.	
Allows you to use your own equipment to meet the security and compliance requirements in your organization.	

Sources:
https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/
https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/4-cloud-deployment-models

Azure Global Infrastructure

Regions

- Each region has more than one data center, which is a physical location.
- A group of data centers deployed in a latency-defined perimeter and connected through a dedicated regional low latency network.
- Criteria in choosing a Region:
    - **Location** - a region closest to your users minimizes the latency
    - **Features** - some features **are not available** in all regions
    - **Price** - the price of services vary from region to region
- Each Region is paired within the same geographic area
- If the primary region has an outage, you can **failover** to the secondary region
- You can use paired regions for **replication**
- Regions that are unique when it comes to compliance:
    - **Azure Government Cloud** - only US federal, state, local, and tribal governments and their partners have access to this dedicated instance
    - **China Region** - data center is physically located within China and has no connection outside of China, including other Azure regions.

Availability Zones

- Each availability zone is a physical location within a region
- A zone is composed of one or more data centers with independent power, cooling, and networking facilities.
- Azure services that support Availability Zones fall into two categories:
    - **Zonal services** - a resource is pinned to a specific zone
    - **Zone-redundant services** - replicates automatically across zones
- The data moving in and out of Azure data centers, as well as data moving between Azure data centers, is called **bandwidth**.
    - Data transfer to Azure is always free.
    - Data transfer between Availability Zones is not free.
    - Data transfer within the same Availability Zone is free.
    - Data transfer between Azure regions and to other continents is not free.

AZ-900 Exam Notes:

Take note that each availability zone is isolated or physically separated. To protect your services from single points of failure, you must replicate your applications and data in more than one Availability Zone.

Azure Site Recovery

- Azure's disaster recovery as a service (DRaaS)
- You can minimize recovery issues by sequencing the order of multi-tier applications that run on several virtual machines.
- Keep applications available from on-premises to Azure or Azure to another Azure region during outages with automatic recovery.

Sources:

https://docs.microsoft.com/en-us/learn/modules/explore-azure-infrastructure/
https://docs.microsoft.com/en-us/azure/availability-zones/az-overview
https://azure.microsoft.com/en-us/global-infrastructure/government/
https://docs.microsoft.com/en-us/azure/china/overview-operations
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview
https://azure.microsoft.com/en-us/services/site-recovery/

Azure User Tools

- Manage your Azure resources through; **Portal, CLI, Powershell,** and **Cloudshell.**

Azure Portal

- Create, manage, and monitor all resources in one console, from simple web applications to complex cloud applications.
- Portal Features:
    - **Personalize** - create your own dashboards, layouts, workflows, and colors
    - **Access Control** - fine-grained access control to all your resources
    - **Cost Management** - keep track of current and projected costs
    - **Multi-Platform** - available through web and mobile devices
    - **Marketplace** - an online store that consists of thousands of built-in product offerings such as:
        - Virtual machine images
        - Managed applications
        - Software-as-a-service solutions
        - Consulting and managed services

AZ-900 Exam Notes:

We recommend that you explore the Azure Portal. Defining each service in the cheat sheets alone won't help you understand how to use the portal to configure your services. By simulating it yourself, you'll be able to remember and understand the different configurations in the portal.

Azure CLI

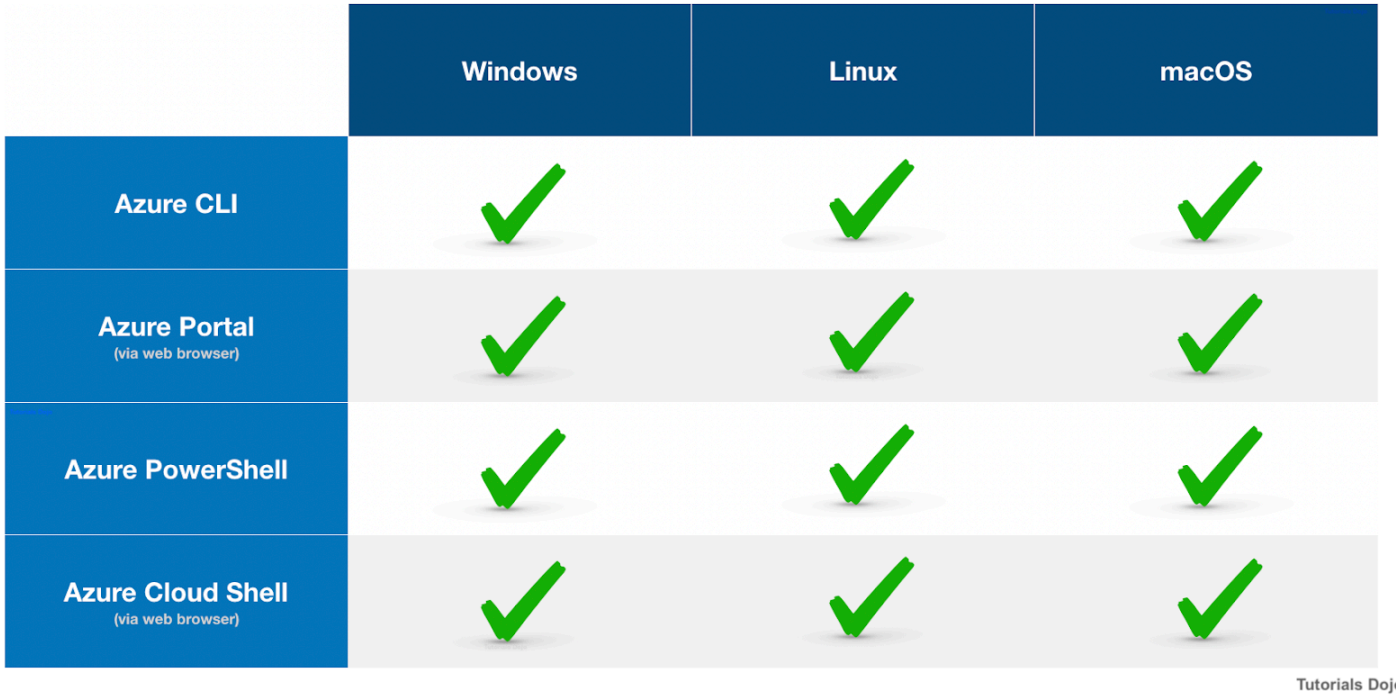
- Command Line Interface (CLI) works on Windows, Mac, and Linux
- You can create and manage Azure resources with a set of commands
- It's built to get you to work with Azure quickly, with a focus on **automation**.

Azure Powershell

- Fully supported by Azure with modules and **cmdlets**
    - **cmdlet** is a lightweight command, which is used in PowerShell.
- PowerShell provides powerful features for automation
- PowerShell also uses **Azure Resource Manager** to manipulate Azure resources

Azure Cloud Shell

- An interactive, **browser-accessible shell** for managing Azure resources.
- You can choose between **Bash** or **PowerShell**
- Shell access from anywhere using the web or mobile app
- Cloud Shell attaches **Azure Files** share to persist your data
- It also offers an integrated **file editor** built on the open-source Monaco Editor



Azure Mobile App

- You can monitor the status and health of your Azure resources
- Monitor your metrics and alerts and take the necessary actions to fix common issues.
- You can run commands via Azure CLI or PowerShell to manage your Azure resources.

Sources:

https://azure.microsoft.com/en-us/features/azure-portal/
https://docs.microsoft.com/en-us/cli/azure/
https://docs.microsoft.com/en-us/powershell/azure/
https://docs.microsoft.com/en-us/azure/cloud-shell/overview

AZURE PRICING

- Azure offers pay-as-you-go and reserved instances for pricing.
- Azure Pricing Factors:
    - Resource size and resource type.
    - Different Azure locations have different prices for services.
    - The bandwidth of your services.
    - Any data transfer between two different billing zones is charged.
        - **Ingress (data in)** = free
        - **Egress (data out)** = charged based on data going out of Azure datacenters.
- Factors that can reduce costs:
    - By purchasing a **reserved instance** (one-year or three-year terms), you can significantly reduce costs up to 72 percent compared to pay-as-you-go pricing.
    - A **reserved capacity** is a commitment for a period of one or three years for SQL Database and SQL Managed Instance.
    - **Hybrid Benefit** allows you to use your on-premises Software Assurance-enabled Windows Server and SQL Server licenses on Azure.
    - If you purchase an unused compute capacity, you can get deep discounts up to 90 percent compared to pay-as-you-go pricing. A **spot virtual machine** is for workloads that can tolerate interruptions.
- All resources belong to a **subscription**.
    - An Azure account can have multiple subscriptions.
    - Organize your resources and subscriptions using **Azure management groups**.
- **Azure Cost Management** gives you a detailed view of current and projected costs.
- For new accounts, the **Azure Free Tier** is available.
    - Free Tier offers limited usage of Azure products at no charge for 12 months.
    - You also get $200 credit that you can spend during the first 30 days.
    - More details at https://azure.microsoft.com/en-us/free/

AZ-900 Exam Notes:

In the first 30 days of an Azure free account, all the resources that you use are deducted from the $200 credit. After 30 days, you'll have to upgrade to a pay as you go subscription so you can continue to get access to all the free products in the free account.

- Estimate your expected monthly costs using **Azure Pricing Calculator.**
- **Total Cost of Ownership (TCO) Calculator**
    - Estimate total savings over a period of time by using Azure.
    - Compares costs and savings against on-premises and co-location environments.

- Azure Support Plans:
  - **Basic** - included for all Azure customers.
  - **Developer** - recommended for non-production environments. Limited access to technical support during business hours by email only.
  - **Standard** - appropriate for production workload environments. Has 24/7 access to Azure's technical support engineers by phone or email.
  - **Professional Direct** - suitable for business-critical workloads. Has 24/7 access to Azure's technical support engineers by phone or email. Provides access to Operations Support, ProDirect delivery managers, and Support APIs.

	BASIC	DEVELOPER	STANDARD	PROFESSIONAL DIRECT
Scope	Included for all Azure customers	Trial and non-production environments	Production workload environments	Business-critical dependence
Billing and subscription management support	✓	✓	✓	✓
24/7 self-help resources, including Microsoft Learn, Azure portal how-to videos, documentation, and community support	✓	✓	✓	✓
Ability to submit as many support tickets as you need	✓	✓	✓	✓
Azure Advisor—your free, personalized guide to Azure best practices	✓	✓	✓	✓
Azure health status and notifications	✓	✓	✓	✓
Third-party software support with interoperability and configuration guidance and troubleshooting		✓	✓	✓
24/7 access to technical support by email and phone		Available during business hours by email only.	✓	✓
Case severity and response time		Minimal business impact (Sev C): Within eight business hours[1]	Minimal business impact (Sev C): Within eight business hours[1] Moderate business impact (Sev B): Within four hours Critical business impact (Sev A): Within one hour	Minimal business impact (Sev C): Within four business hours[1] Moderate business impact (Sev B): Within two hours Critical business impact (Sev A): Within one hour
Architecture Support		General guidance	General guidance	Guidance from a pool of ProDirect delivery managers
				A single view to managing your active support tickets
Operations Support				Service reviews and advisory consultation from a pool of ProDirect delivery managers
Training				Webinars led by Azure engineers
Proactive Guidance				From a pool of ProDirect delivery managers

[1] For most countries and regions, business hours are from 9:00 AM to 5:00 PM (local time) Monday through Friday, excluding holidays. For North America, business hours are from 6:00 AM to 6:00 PM (Pacific time), Monday through Friday, excluding holidays. In Japan, business hours are from 9:00 AM to 5:30 PM, Monday through Friday, excluding holidays.

Tutorials Dojo

Service Level Agreement (SLA)

- It is the commitment of Microsoft for the uptime and connectivity of a service.
- You could obtain a service credit if the service level agreement is not met by Microsoft.
- Composite SLAs include several resources (*with different availability levels*) to support an application.
- SLAs for multi-region deployments distribute the application in more than one region for high availability and use Azure Traffic Manager for failover if one region fails.

AZ-900 Exam Notes:

Take note that Azure offers different SLAs for each service. To compute the total composite SLA of an application, you would have to multiply the SLA of each service.
For example,

- App Service web apps (SLA) = 99.95%
- SQL Database (SLA) = 99.99%

The composite SLA is 99.95% × 99.99% = 99.94%. We could see that the SLA is lower than the individual SLAs since multiple services have more potential failure points.

During your examination, you could use the calculator button if you need to compute for the composite SLA.

Service Lifecycle

- **Private Preview** is only available to a few customers for early access to new technologies and features.
- **Public Preview** makes the service in the public phase and can be used by any customers to evaluate the new features but SLA does not apply.
- **General Availability** is the release of service to the general public and is fully supported by SLAs.
- Azure updates allow you to get the latest updates on any Azure products and features.

	Private Preview	Public Preview	General Availability
Access	Subset of Azure customers *(By Invitation)*	All Azure customers	All Azure customers
Subject to Service Level Agreement (SLA)	**No**	**No**	**Yes**
Covered by Microsoft Customer Support Services	**No**	**Yes**	**Yes**

Tutorials Dojo

Sources:
https://azure.microsoft.com/en-us/pricing/
https://docs.microsoft.com/en-us/azure/cost-management-billing/cost-management-billing-overview
https://docs.microsoft.com/en-us/azure/architecture/framework/resiliency/business-metrics
https://azure.microsoft.com/en-us/support/legal/preview-supplemental-terms/

COMPUTE

Azure Virtual Machines

- Linux-based and Windows-based virtual machines.

Features

- Server environments are called **virtual machines**.
- A package OS and additional installations in a reusable template are called **VM Images**.
- Supports various configurations of CPU, memory, storage, and networking capacity for your virtual machines, known as **virtual machine series**.
    - A, Bs, D, and DC-Series for general purpose
    - F-Series for compute optimized
    - E and M-Series for memory optimized
    - Ls-Series for storage optimized
    - G-series for memory and storage optimized
    - H-series for high-performance computing
    - N-series for GPU optimized
- Contain the virtual machines using a **resource group**.
- Secure login information for your virtual machines using **key pairs.**
- Persistent storage volumes for your data using **Azure Disk.**
- Multiple physical locations for deploying your resources, such as virtual machines and Azure disk, known as **Regions** and **Availability Zones**.
- You can replicate your data in Availability Zones or Availability Sets.
- Azure VMs have one operating system disk and a temporary disk for short-term storage.
- Metadata, known as **tags**, that you can create and assign to your VM resources.
- Virtual networks that you can create are logically isolated from the rest of the Azure environment and can optionally connect to your own network, known as **Azure Virtual Network** or **VNet**.
- Add a script that will be run into the virtual machine while it is being provisioned called **custom data**.
- A firewall allows you to specify the protocols, ports, and source IP ranges that can reach your virtual machines using **network security groups**.

VM Status

- **Start** - run your virtual machines. You are continuously billed while your VM is running.
- **Restart** - some updates do require a reboot. In these cases, the VMs will be shut down while Azure patches the infrastructure, and then the VMs are restarted.
- **Stop** - it is just a normal shutdown. If the VM is in a deallocated status, you will continue to be charged for the storage needed for the operating system disk.
- You can also directly delete the virtual machines/resources. Deleting the selected virtual machines is irreversible.

VM STATE	BILLED	DETAILS
Starting	Yes	The initial starting state of virtual machines as they're going through the boot cycle. This period is billed as the virtual machines are running.
Running (Started)	Yes	The running state of the virtual machine.
Stopped	Yes	You are billed for allocated cores, but not software licences.
Deleted (Deallocated)	No	Cores are no longer allocated to the virtual machine, and are no longer billed.

Tutorials Dojo

Disks

- Select an OS disk type using Standard HDD, Standard SSD, and Premium SSD.
- Every virtual machine has one attached operating system disk.
- The OS disk has a maximum capacity of 4,095 GiB.
- Every VM contains a temporary disk that provides short-term storage only for page or swap files.
- Data on the temporary disk may be lost during a maintenance event or when you redeploy a VM.
- You can enable ultra disk compatibility for high throughput, high IOPS, and consistent low latency disk storage.
- A VM with an enabled Ultra Disk capability will result in a reservation charge even without attaching an Ultra Disk.
- An Availability zone supports managed disks.
- You get lower read/write latency to the OS disk with Ephemeral OS disk, and faster reimage of VM. You incur no storage cost with ephemeral OS disks.

Dedicated Host

- Provide physical servers that can host multiple virtual machines.
- Allows you to achieve compliance and regulatory requirements that require you to be the only customer to use the physical server that will host your virtual machines.
- You have control of the scheduled maintenance events of Azure, wherein you can opt-in to maintenance windows.
- Bring your existing Windows licenses with Software Assurance to reduce costs.

- A **Host group** consists of one or more dedicated hosts.
- When you create a **host**, it will automatically be mapped to a physical server and is created within a host group. A host can consist of multiple virtual machines.

Pricing

- Pay as you go - pay for the instances that you use by the second, with no long-term commitments or upfront payments.
- Reserved - make a low, one-time up-front payment for an instance, reserve it for a one-or three-year term.
- Spot - request unused compute capacity, which can lower your costs significantly. Spot pricing gives you up to 90 percent compared to pay as you go prices.

Backup and Recovery

- A snapshot is a full copy of a virtual machine's OS or data disk. Snapshots are useful for backup, disaster recovery, and troubleshooting.
- With the **enabled backup** option, your VM will be backed up to Recovery Services vault with default backup policy, or your custom backup policy and will be charged as per backup pricing.
- **Azure Site Recovery** allows organizations to meet their business continuity and disaster recovery (BCDR) requirements by having your virtual machines' data replicated to a secondary region and failover in the event of a downtime.
- You can set up disaster recovery of Azure VMs from a primary region to a secondary region using **Azure Site Recovery**.

Scale Sets

- Create and manage a group of load-balanced VMs to provide high availability to your applications.
- Automatically scale your application as demand changes.
- Support up to 1,000 VM instances. But if you create and upload your own custom VM images, the limit is 600.
- Use **Azure Monitor** to automate the collection of information from the VMs in your scale set.
- No additional cost to scale sets. You only pay for the underlying computing services, such as virtual machines, load balancers, or managed disk storage.

Scenario	Manual group of VMs	Virtual Machine Scale Set
Add additional VM instances	To create, configure, and ensure compliance with the manual process.	Create automatically from a central configuration.
Traffic balancing and distribution	Manual process in creating and configuring the Load Balancer or	Automatically create and integrate the Load Balancer or Application Gateway.

	Application Gateway.	
High availability and redundancy	Create Availability Set or distribute and track virtual machines across Availability Zones manually.	Distribute virtual machines across Availability Zones or Availability Sets automatically.
Scaling of VMs	Manual monitoring and Azure Automation.	Autoscale based on metrics, Application Insights, or by schedule.

Scenario	Manual group of VMs	Virtual Machine Scale Set
Add additional VM instances	Manual process to create, configure, and ensure compliance	Automatically create from central configuration
Traffic balancing and distribution	Manual process to create and configure Azure load balancer or Application Gateway	Can automatically create and integrate with Azure load balancer or Application Gateway
High availability and redundancy	Manually create Availability Set or distribute and track VMs across Availability Zones	Automatic distribution of VM instances across Availability Zones or Availability Sets
Scaling of VMs	Manual monitoring and Azure Automation	Autoscale based on host metrics, in-guest metrics, Application Insights, or schedule

Tutorials Dojo

	Scale Set	Availability Set
Description	A group of load balanced VMs that can automatically increase or decrease in response to demand or a defined schedule.	A logical grouping of VMs within a datacenter
Virtual Machine Distribution	VMs are automatically distributed across fault domains (FD), update domains (UD) and Availability Zones	VMs are automatically distributed across fault domains (FD) and update domains (UD).
Fault tolerant if a single data center fails	**Yes**	**No**
Fault tolerant if the primary Azure region fails	**No**	**No**

Tutorials Dojo

Monitoring

- **Azure Resource Health** helps you diagnose problems that affect your resources.
- Capture serial console output and screenshots of the virtual machine with **boot diagnostics**.
- Enable OS guest diagnostics to get the metrics every minute
- Automatically shutdown virtual machines for cost-efficiency with **enable the auto-shutdown** option.

Network

- You can provision a virtual machine that has a static public IP address.
- Enable accelerated networking for low latency and high throughput on the network interface.
- Distribute traffic among virtual machines using Load Balancer.

Security

- By default, access to the VM is restricted to sources in the same virtual network.
- You can control ports, inbound and outbound connectivity with security group rules.
- With system assigned managed identity, all necessary permissions can be granted via Azure role-based access control.
- Encrypt your data at rest with a platform-managed key or customer-managed key.
- By default, encryption at-rest uses a platform-managed key.
- Encrypt the OS and Data disks with Azure Disk Encryption.
- The temporary disk is not encrypted by server-side encryption unless you enable encryption at the host.

Sources:

https://docs.microsoft.com/en-us/learn/paths/azure-fundamentals/
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/overview/
https://azure.microsoft.com/en-us/pricing/details/virtual-machines/series//
https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/overview

Azure App Service

- A fully managed platform (PaaS) for building, deploying, and scaling your web apps.
- Different types of App Services: **Web Apps, Web Apps for Containers,** and **API Apps**
- Automatically patches and maintains the OS and language frameworks.
- App Service can scale up or out manually or automatically.
- App Service supports the following languages:
    - .NET
    - .NET Core
    - Java
    - Ruby
    - Node.js
    - PHP
    - Python
- An **App Service plan** is a collection of compute resources needed for a web app to run.
- Each App Service plan consists of a **region, number & size of virtual machines** and **pricing tier**.
- App Service plan pricing tier:
    - **Shared Compute** - **Free** and **Shared** are the two base tiers. These tiers allocate CPU quotas to every app running on the shared resources, but the resources cannot scale-out.
    - **Dedicated Compute** - It is composed of **Basic, Standard, Premium,** and **PremiumV2** tiers. As the tier gets higher, you will have more VMs to scale-out.
    - **Isolated** - A dedicated virtual machine that provides maximum scale-out capabilities.

AZ-900 Exam Notes:

When do we use Azure App Service vs other compute options?
The advantage of using the Azure App Service is that it's PaaS. This means that you just need to define your environment settings and Azure will handle the integration and provisioning of servers for you. After that, you can simply upload your application and you'll already have a fully working environment. Managing App Service is very easy since you don't need to understand how different services work together before you can launch your application.

App Services Types:

- **Web Apps**
    - Website and online applications hosted on Azure's managed platform.
    - Build and deploy mission-critical web applications that scale with your business.
    - It supports auto-scaling and load balancing for resilience and high availability.
- **Web Apps for Containers**
    - Deploy and run containerized applications in Azure.

    - All dependencies are shipped inside the container.
- **API Apps**
    - Expose and connect your backend data.
    - Connect other applications programmatically.

Deployment

- Deployment components in App Service:
    - Deployment Source - it is where the application code is stored.
    - Build Pipeline - reads your code and takes the application in a running state.
    - Deployment Mechanism - enables you to put your application in the /wwwroot directory. It also supports Kudu endpoints, FTP, and WebDeploy.
- **Deployment Center** lets you choose the location of your code, as well as build and deploy to the cloud. It also has built-in continuous delivery for containers.
- Swap app content and configurations elements with **deployment slots**.
- App Service supports the continuous deployment of code and containers.
- You can use **local cache** and deployment slots to prevent downtime.
- App Service **diagnostics** will help you in troubleshooting your application.

Security

- App Service protocols: HTTPS, TLS 1.1/1.2 and FTPS
- The default domain name is using HTTPs. You can also secure your custom domain using an SSL/TLS certificate.
- **Service endpoints** allow you to restrict access from a virtual network.
- The first IP restriction rule has an explicit **Deny all** rule with a priority of 2147483647.
- Service-to-service authentication:
    - Service Identity - you can use the identity of the app to access the remote resource.
    - On-behalf-of (OBO) - allows you to access a remote service using a delegated sign-in.

VNet Integration

- It allows your app to access resources in your virtual network.
    - Regional VNet Integration
        - You need to have a dedicated subnet to the services that you integrate with.
        - Block outbound traffic using network security groups.
        - Route table allows you to send outbound traffic.
    - Gateway-required VNet Integration
        - Allows access to resources in the target virtual network.
        - **Sync network** allows you to sync certificates and network information.
        - You can also **add routes** for outbound traffic.

Hybrid Connections

- Uses host:port combination.
- It provides network access to your application using a TCP endpoint.
- Supports access to multi-networks from a single app.
- Host your hybrid connection endpoint using a relay agent or **Hybrid Connection Manager (HCM)**.
- You can run multiple HCMs on a separate machine to achieve high availability.

Pricing

- You are charged on a per-second basis in the App Service plan.
- You are charged for the applications while they are in a stopped state.
- You are charged for data egress when using VNet Integration.
- You are charged for each listener in a Hybrid Connection.

Sources:
https://azure.microsoft.com/en-us/services/app-service/
https://docs.microsoft.com/en-us/azure/app-service/overview

Azure Container Instances (ACI)

- Run containers without managing servers.
- For event-driven applications, quickly deploy from your container development pipelines, run data processing, and build jobs.
- Azure Container Instances is a regional service.

Features

- Containers have less overhead than VMs and can be deployed consistently.
- All the dependencies for an application are included in the container image.
- Applications running in containers can be deployed easily to multiple operating systems and hardware platforms.
- Select an image source using **Quickstart images, Azure Container Registry,** and **Docker Hub.**
- Create a container image only when you need it and process data on-demand.
- You can choose to **always** restart the container regardless of how it stopped, to only restart if it **failed,** to exit successfully, or to **never** restart.
- Enables you to set a command to be executed first when running the container.
- Resources can be tagged with values that you define, to help you organize and identify them.
- By default, Azure Container Instances are stateless.
- You can't deploy an image from an on-premises registry to ACI.

Storage

- You can mount Azure Files shares in your ACI for persistent storage.
- To mount an Azure file share as a volume in Azure Container Instances, you need: Storage account name, Share name, and Storage account key.

Networking

- Choose between three networking options: Public, Private, and None.
- Private IP is not yet available for Windows Containers.
- None IP containers (logs) can still be accessed using the CLI.
- DNS name label: <*tutorialsdojo*>.<*region*>.azurecontainer.io

Security

- Deploy Azure WAF in front of critical web applications hosted in ACI for additional inspection of incoming traffic.
- Use Azure Key Vault to safeguard encryption keys and secrets for containerized applications.

Pricing

- You pay based on what you need and get billed by the second.
- The assigned public IP addresses to your container group are billed.
- You are billed for each GB and vCPU your container group consumes.

Sources:
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-overview
https://azure.microsoft.com/en-us/services/container-instances/#overview

Azure Kubernetes Service (AKS)

- An open-source tool for orchestrating and managing many container images and applications.
- Lets you deploy a managed Kubernetes cluster in Azure.

Features

- Uses clusters and pods to scale and deploy applications.
- Kubernetes can deploy more images of containers as needed.
- It supports horizontal scaling, self-healing, load balancing, and secret management.
- Automatic monitoring of application load to determine when to scale the number of containers used.
- Allows you to replicate container architectures.
- Use Kubernetes with supported Azure regions and on-premises installations using **Azure Stack.**
- The images used by AKS come from Azure Container Registry.
- Use **Azure Advisor** to optimize your Kubernetes deployments with real-time, personalized recommendations.

Components

- A **control plane** is a managed Azure resource. It is where the components run, including API server and cluster database (etcd).
    - kube-apiserver - allows communication for management tools (kubectl).
    - etcd - a key-value store within Kubernetes.
    - kube-scheduler - defines what nodes should run in the workload.
    - kube-controller-manager - it oversees the smaller controllers that handle node operations and replication of pods.
- Kubernetes runs an application in your instance using **pods**.
- A **node** is made up of several pods, and **node pools** are a group of nodes with the same configuration.
- Use a **node selector** to control where a pod should be placed.
- You can run at least 2 nodes in the default node pool to ensure your cluster operates reliably.
- Multi-container pods are placed on the same node and allow containers to share the related resources.
- You can specify maximum resource limits that prevent a given pod from consuming too much compute resources from the underlying node.
- A **deployment** determines the number of replicas (pods) to be created, but you must define a manifest file in YAML format first.
- With **StatefulSets**, you can maintain the application's state within a single pod life cycle.
- The resources are logically grouped into a **namespace**, and a user may only interact with resources within their assigned namespaces.

Storage

- Persistent volumes are provided by Azure disk and file storage.
- Create a Kubernetes DataDisk resource using Azure Disk.
- Mount an SMB 3.0 share backed by an Azure Storage account to pods with Azure Files.
- Volumes that are defined and created as part of the pod lifecycle only exist until the pod is deleted.
- AKS has four initial storage classes:
    - default - uses Azure StandardSSD storage to create a Managed Disk.
    - managed-premium - uses Azure Premium storage to create Managed Disk.
    - azurefile - uses Azure Standard storage to create an Azure File Share.
    - azurefile-premium - uses Azure Premium storage to create an Azure File Share.
- If no StorageClass is specified for a persistent volume, the default StorageClass is used.

Security

- With Kubernetes RBAC, you can create roles to define permissions and then assign those roles to users with role bindings.
- You can limit network traffic between pods in your cluster with Kubernetes network policies.
- Dynamic rules enforcement across multiple clusters with Azure Policy.
- Microsoft Entra-integrated AKS clusters can grant users or groups access to Kubernetes resources within a namespace or across the cluster.
- Secure communication paths between namespaces and nodes with Azure Private Link.

Pricing

- You only pay for virtual machines, associated storage, and networking resources.
- There is no charge for cluster management.

Versions

- Uses semantic versioning: [major].[minor].[patch]
- A user has 30 days from the version removal to upgrade into a supported patch and continue receiving support.
- Azure updates the cluster automatically if it has been out of support for more than 3 minor versions.
- Downgrading a version is not supported.

Sources:
https://docs.microsoft.com/en-us/azure/aks/intro-kubernetes
https://azure.microsoft.com/en-us/services/kubernetes-service/

Azure Container Registry (ACR)

- A service to manage your container images and related artifacts.
- ACR is a regional service.

Features

- Keep track of current valid container images.
- Registries (SKUs) are available in three tiers: Basic, Standard, and Premium.
- You can use the geo-replication feature of Premium registries for advanced replication and container image distribution scenarios.
- Streamline building, testing, pushing, and deploying images to Azure with **Azure Container Registry Tasks**.
- ACR Tasks supports **quick task**, **automatically triggered tasks**, and **multi-step task**
- Tag your containers using stable and unique tags.

Concepts

- **Registry**
  - A registry is a collection of repositories to store and distribute container images.
  - You must be authenticated before you can pull and push images.
- **Artifact**
  - The address of an artifact contains loginUrl, repository and tag
    - [loginUrl]/[repository:][tag]
- **Repository**
  - A repository is a group of similar container images and other artifacts.
  - Identify similar repositories and artifacts with namespaces.
- **Image**
  - Images are used in ACR tasks.
  - A container image consists of tags, layers, and a manifest.
  - Orphaned images are generated by repeated pushing of modified images with identical tags.

Best Practices

- If you place your registry near your container hosts, it will help reduce both latency and costs.
- When you are deploying containers to multiple regions, you can use the geo-replication feature.
- ACR supports nested namespaces that allow you to share a single registry across multiple groups.
- There are two main situations when authenticating with an ACR:
  - Individual identity - allows you to pull or push images from the development machine.
  - Service/Headless identity - enables you to build and deploy pipelines where the user is not directly involved.
- ACR allows you to delete images by tag, by manifest digest, and by repository.

Tasks

- **Quick Task**
  - Verify your automated build definitions and catch potential problems prior to committing your code.
  - Build and push a single container image to a container registry on-demand, in Azure, without needing a local Docker Engine installation.
- **Trigger Task**
  - You can create an image using one or more triggers on:
    - Source code update
    - Base image update
    - Schedule
- **Multi-step Task**
  - Multi-container-based workflows
  - With multi-step tasks in ACR Tasks, you have more granular control over image building, testing, and OS and framework patching workflows.
- Deleted registry resources such as repositories, images, and tags cannot be recovered after deletion.

Tagging

- Use stable tags to maintain base images for your container builds.
- If the updated image has a stable tag, the previously tagged image is untagged, resulting in an orphaned image.
- You can use unique tags for deployments, particularly in an environment where multiple nodes can scale.

Network

- You can connect to your ACR via public and private endpoints.
- A private endpoint connection is only available for Premium SKU.

Security

- Encrypts the registry content at rest with service-managed keys or customer-managed keys.
- Customer-Managed Key is only available for Premium SKU.
- You can enable a customer-managed key only when you create a registry.
- Authenticate through **Microsoft Entra ID** user, service principal, admin login, or through Azure managed identity.

Pricing

- You are charged (GiB/day) for the image storage.
- Users will be charged for the preceding SKU price until the point of change and will be charged for the new SKU price after the change has been made.
- Standard networking fees apply to network egress.
- If you replicate a registry to your desired regions, you are charged with premium registry fees for each region.

Sources:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-intro
https://azure.microsoft.com/en-us/services/container-registry/

Azure Batch

- A service that runs large-scale parallel and high-performance computing (HPC) batch jobs in Azure.
- Allows you to run jobs in a group of Linux or Windows virtual machines.

Components

- A **task** represents a unit of computation and a **job** is a collection of tasks.
- **Job priority** values range from the lowest priority to the highest priority.
- To specify certain limits for your jobs, you can use **job constraints**:
    - Maximum wallclock time - tasks are terminated if the job runs longer than the specified time.
    - Maximum number of task retries - if the task fails, it will be requeued to run again.
- A **job manager task** contains the information needed to create the tasks required for the job.
- **Scheduled jobs** allow you to create recurring jobs.
- Simultaneously run on more than one compute node with a **multi-instance task**.
- With **task dependencies**, the task depends on the completion of other tasks before its execution.

Pricing

- No additional charge for using Azure Batch and you are only charged for the underlying resources consumed.

Sources:
https://docs.microsoft.com/en-us/azure/batch/batch-technical-overview
https://azure.microsoft.com/en-us/services/batch/

Azure CycleCloud

- Orchestrate and manage high-performance computing (HPC) environments on Azure.
- Enables you to provision infrastructure for HPC systems, deploy familiar HPC schedulers, and scale the infrastructure automatically to run jobs efficiently at any scale.

Features

- **Scheduler Agnostic** - use standard HPC schedulers or extend CycleCloud autoscaling plugins to work with your own scheduler.
- **Manage Compute Resources** - manage VMs and scale sets to provide a set of compute resources to meet your workload requirements.
- **Autoscale Resources** - adjust cluster size and components automatically based on workload, availability, and time requirements.
- **Monitor and Analyze** - collect node-level metrics and analyze the performance data using a visualization tool.
- **Template Clusters** - enables you to share your cluster topologies.
- **CycleCloud agent (called Jetpack)** - Installed by Azure CycleCloud on each virtual machine to provide the following functions:
    - Node Configuration
    - Distributed Synchronization
    - Health Check

Sources:
https://docs.microsoft.com/en-us/azure/cyclecloud/overview?view=cyclecloud-7
https://azure.microsoft.com/en-us/features/azure-cyclecloud/

Azure Service Fabric

- A distributed systems platform that helps package, deploy, and manage scalable and reliable microservices and containers.
- Build microservices and container-based applications using the programming language of your choice, including .NET Core 2.0, C #, and Java. It supports two types of microservices:
    - **Stateless** - It does not maintain a mutable state outside a request and its response from the service such as protocol gateways and web proxies.
    - **Stateful** - It maintains a mutable, authoritative state beyond the request and its response.
- Enables low-touch workflows to provision, deploy, patch, and monitor applications with Service Fabric **application lifecycle management**.
- Supports the deployment of multiple application instances.
- A **service fabric cluster** is a set of virtual machines into which your microservices are deployed and managed.

Security

- Create or import a certificate using Azure Key Vault.
- Use Azure Firewall to complement your existing Network Security Group rules to control access to your cluster.

Pricing

- You are charged based on the number of vCPU and GBs of memory allocated to each VMs.
- You are charged based on the size, number of disks, and number of outbound data transfers.

Sources:
https://azure.microsoft.com/en-us/services/service-fabric/
https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-overview

Azure Virtual Desktop

- A fully managed desktop and app virtualization solution in the cloud.
- Supports Windows Desktop, Web, macOS, iOS, Android and Microsoft Store Client.
- Assign multiple users to a single VM using a client OS.

Concepts

- **Host pools** are a collection of identical virtual machines. The types of host pools are:
    - Personal
        - Automatic assignment - the service will automatically assign the user to an available host.
        - Direct Assignment - you can assign a user to a specific host.
    - Pooled
        - You can set the maximum number of users that have concurrent sessions on a single host
        - Breadth-first load balancing - evenly allocates your users across the host pool.
        - Depth-first load balancing - fully allocates users on a single virtual machine.
- A logical grouping of applications installed on a session host is called an **app group**.
    - RemoteApp - users can only access the RemoteApps you selected.
    - Desktop - users can fully access the desktop.
- A logical grouping of application groups is called **workspaces**.

Security

- Use Microsoft Entra ID for a consistent sign-on experience for your users.
- You can configure MFA and conditional access controls to determine access based on your identity, device, and location.
- Supports different types of authentication.
    - Session host authentication
    - Hybrid identity
    - Single sign-on (SSO)
- Use Azure RBAC to assign multiple roles to your users: Contributor, Reader, and Operator

Pricing

- You are charged on the following components:
  - Virtual machines and OS storage
  - Data disk and User profile storage
  - Networking

Sources:
https://docs.microsoft.com/en-us/azure/virtual-desktop/overview
https://azure.microsoft.com/en-us/services/virtual-desktop/

STORAGE

Azure Storage Overview

- An Azure storage account contains **blobs, files, queues, tables,** and **disks.**
- Types of Storage Accounts: **General-purpose (v2 and v1), BlockBlobStorage, FileStorage,** and **BlobStorage**
- All storage accounts are encrypted using Storage Service Encryption (SSE) for data at rest.
- Storage accounts endpoints:
    - **Blob storage:** https://*tutorialsdojo*.blob.core.windows.net
    - **Table storage:** https://*tutorialsdojo*.table.core.windows.net
    - **Queue storage**: https://*tutorialsdojo*.queue.core.windows.net
    - **Azure Files**: https://*tutorialsdojo*.file.core.windows.net
- Access tiers are: Hot, Cool, and Archive
    - Hot
        - Highest storage costs, but lowest access costs.
        - Store data that is accessed frequently.
        - By default, new storage accounts are created in the hot tier.
    - Cool
        - Lower storage costs, but higher access costs.
        - Store data that is infrequently accessed (at least 30 days).
        - You can use a cool access tier for short-term backup.
    - Archive
        - Lowest storage costs, but the highest retrieval costs.
        - Store data that is rarely accessed (at least 180 days).
        - Data needs to be stored for a long time.

	Premium performance	Hot tier	Cool tier	Archive tier
Availability	99.9%	99.9%	99%	Offline
Availability (RA-GRS reads)	N/A	99.99%	99.9%	Offline
Usage charges	Higher storage costs, lower access, and transaction cost	Higher storage costs, lower access, and transaction costs	Lower storage costs, higher access, and transaction costs	Lowest storage costs, highest access, and transaction costs
Minimum object size	N/A	N/A	N/A	N/A
Minimum storage duration	N/A	N/A	30 days[1]	180 days
Latency (Time to first byte)	Single-digit milliseconds	milliseconds	milliseconds	hours[2]

- Storage redundancy includes: Locally redundant storage (LRS), Zone-redundant storage (ZRS), Geo-redundant storage (GRS), Geo-zone-redundant storage (GZRS)
    - Locally redundant storage (LRS)
        - A low-cost redundancy strategy.
        - Your data is copied synchronously three times within the primary region.
    - Zone-redundant storage (ZRS)
        - Redundancy for high availability.
        - The data is copied synchronously across three Azure availability zones in the primary region.
    - Geo-redundant storage (GRS)
        - Cross-regional redundancy.
        - In the primary region, data is synchronously copied three times, and then asynchronously copied to the secondary region.
        - Enable read-only geo-redundant storage (RA-GRS) to access data in the secondary region.
    - Geo-zone-redundant storage (GZRS)
        - Redundancy for both high availability and maximum durability.
        - Data is copied synchronously across three Azure availability zones in the primary region, then copied asynchronously to the secondary region.
        - You can also enable RA-GZRS for read access data in the secondary region.

	Locally-Redundant Storage (LRS)	Zone Redundant Storage (ZRS)	Geo-redundant storage (GRS)
Replication	Replicates your data 3 times within a single physical location synchronously in the primary region.	Replicates your data across 3 Azure Availability Zones synchronously in the primary region	Replicates your data in your storage account to a secondary region
Redundancy	Low	Moderate	High
Cost	Provides the least expensive replication option	Costs more than LRS but provides higher availability	Costs more than ZRS but provides availability in the event of regional outages
Available if a node went down within a data center?	Yes	Yes	Yes
Available if the entire data center (zonal or non-zonal) went down?	No	Yes	Yes
Available on region-wide outage in the primary region?	No	No	Yes
Has read access to the secondary region if the primary region is unavailable?	No	No	Yes

Tutorials Dojo

- Moving of data into different storage account can be done automatically or manually.
- You can migrate data manually using:
    - AzCopy uses a command-line utility.
    - Data Movement Library is designed for high-performance, reliable, and easy data transfer operations similar to AzCopy.
    - REST API or client library lets you create a custom application to migrate your data.

Types of Storage Accounts

- **General-purpose v2 accounts**
    - Supports Data Lake Gen2, Blobs, Files Disks Queues Tables.
    - Delivers the lowest per-gigabyte capacity prices for Azure Storage.
- **General-purpose v1 accounts**
    - Supports Blobs, Files, Disks, Queues, Tables.
    - You can upgrade a general-purpose v1 account to a general-purpose v2 account with no downtime and without copying the data.
    - You can use general-purpose v1 accounts since the General-purpose v2 accounts and Blob storage accounts only support the Azure Resource Manager deployment model.

    - If you don't need a large capacity for transaction-intensive or significant geo-replication bandwidth, GPv1 is a suitable choice.
- **BlockBlobStorage accounts**
    - Provides low, consistent latency, and higher transaction rates.
    - Upgrading a Blob storage account to a general-purpose v2 account has no downtime and you don’t need to copy the data.
    - It doesn't support hot, cool, and archive access tiers
    - You can use BlockBlobStorage for storing unstructured object data as block blobs or append blobs.
- **FileStorage accounts**
    - Only supports file shares.
    - Offers IOPS bursting.

Storage Account Type	Supported Services	Supported Performance Tiers	Supported Access Tiers	Replication Options	Deployment Model	Encryption
General-purpose V2	Blob, File, Queue, Table, Disk, and Data Lake Gen2	Standard, Premium	Hot, Cool, Archive	LRS, GRS, RA-GRS, ZRS, GZRS (preview), RA-GZRS (preview)	Resource Manager	Encrypted
General-purpose V1	Blob, File, Queue, Table, and Disk	Standard, Premium	N/A	LRS, GRS, RA-GRS	Resource Manager, Classic	Encrypted
BlockBlob Storage	Blob (block blobs and append blobs only)	Premium	N/A	LRS, ZRS	Resource Manager	Encrypted
FileStorage	File only	Premium	N/A	LRS, ZRS	Resource Manager	Encrypted
BlobStorage	Blob (block blobs and append blobs only)	Standard	Hot, Cool, Archive	LRS, GRS, RA-GRS	Resource Manager	Encrypted

Security

- To grant access in your storage account, the request must include a valid **Authorization** header.
- If authentication of identity is successful, then **Microsoft Entra ID** returns a token to use in authorizing the request to Azure Storage Services.
- You can use shared key authorization to construct a connection string.
- Shared access signature allows you to have granular control on who can access your data.
- When you copy a file without the metadata for encryption, the blob content cannot be retrieved again.

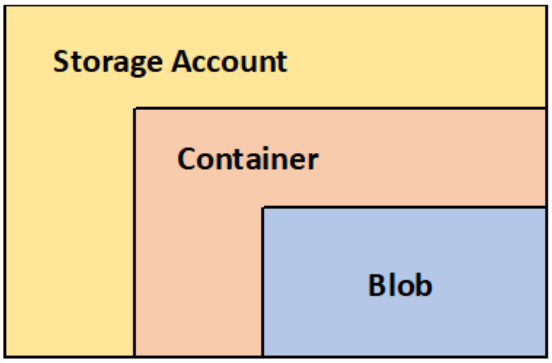
Pricing

- You are charged based on your Region, Account type, Access Tier, and Storage Capacity.
- The replication and reads/write operations also incur costs.
- If your data isn't running in the same region, you're charged for data egress.

Sources:
https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview?toc=/azure/storage/blobs/toc.json
https://docs.microsoft.com/en-us/azure/storage/common/storage-account-create?tabs=azure-portal

Azure Blob Storage

- **B**inary **L**arge **Ob**ject
- **Object storage** solution for the cloud.
- Stores all types of files: image, video, audio, log files backups, etc.



- **Storage Account**
  - Unique namespace in Azure for your data.
  - If your storage account name is *tutorialsdojo*, then the default endpoint for Blob storage is: *http://tutorialsdojo.blob.core.windows.net*
- **Container**
  - Organizes a set of blobs that are similar to a directory in a file system.

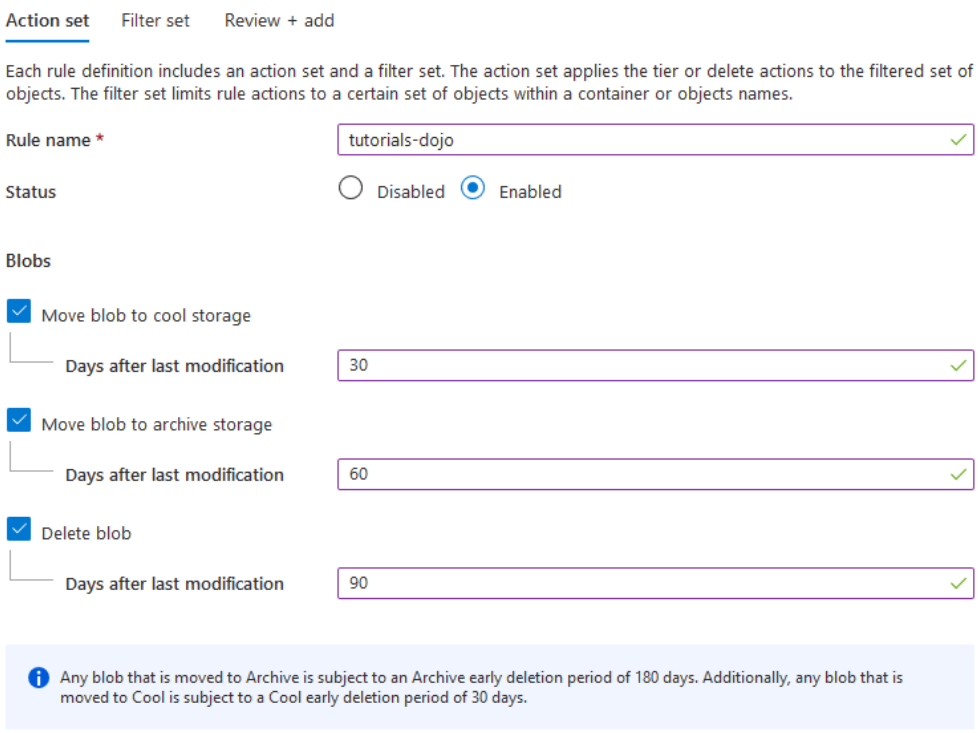
Blob Types

- **Block**
  - Store binary and text data up to 4.7 TB.
  - Preview larger block blobs up to 190.7 TiB.
- **Append**
  - Ideal for logging data from virtual machines.
- **Page**
  - Store random-access files up to 8 TB in size
  - Store virtual hard drive (VHD) files.

Supported Access Tiers

- **Hot**
  - Frequently accessed objects.
  - Most cost-effective, while storage costs are higher.
  - Default in new Storage Accounts.
- **Cool**
  - Infrequently accessed data.

  - More cost-effective, but higher access cost than hot tier.
  - Data remains for at least 30 days.
- **Archive**
  - Rarely accessed files.
  - Lowest cost for storing data but the highest access cost.
  - Data remains for at least 180 days.
- **Lifecycle Management Policy**
  - A *lifecycle configuration* has a set of rules that define actions that are applied to a group of objects.



  - Enables you to transition your data to the appropriate access tiers.
  - Delete blobs at the end of their lifecycles.

Features

- **Versioning**
  - Identified by a version ID.
  - Enable versioning and restore an earlier version of a blob to recover your data.
  - If you disable the versioning of the blob, it does not delete existing blobs, versions, or snapshots.
- **Snapshots**
  - A read-only version of a blob that was taken at a given point in time.
  - The snapshots persist until they are explicitly deleted.
- **Object Replication**
  - Copies block blobs asynchronously between a source Storage account and a destination account.
  - A source account can have up to two destination accounts. But there can be no more than two source accounts in the destination account.
- **Static Website**
  - Serve your static website directly from a storage container named *$web*.
  - CORS is not supported.
  - You can grant read-only access in your resources with a public access level.
  - Enable **Azure Content Delivery Network (CDN)** to cache content from a static website.
  - You can use Azure CDN to configure a custom domain endpoint.

Security

- Azure Storage is using 256-bit AES encryption.
- Customer-managed key
  - Using Azure Key Vault, you can encrypt and decrypt data in Blob storage and in Azure Files.
- Customer-provided key
  - A customer can include their own encryption key for granular control.

Key management parameter	Microsoft-managed keys	Customer-managed keys	Customer-provided keys
Encryption/decryption operations	Azure	Azure	Azure
Azure Storage services supported	All	Blob storage, Azure Files	Blob storage
Key storage	Microsoft key store	Azure Key Vault	Customer's own key store
Key rotation responsibility	Microsoft	Customer	Customer
Key control	Microsoft	Customer	Customer

Sources:
https://azure.microsoft.com/en-us/services/storage/blobs/
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-lifecycle-management-concepts?tabs=azure-portal

Azure Disk Storage

- **Block-level storage** volumes for Azure Virtual Machines.
- Disk Storage is a managed disk that is designed for 99.999% availability.
- You can create 50,000 VM disks for each region.

Features

- Different types of storage options: **Standard HDD, Standard SSD, Premium SSD,** and **Ultra Disk** volumes up to 64 TiB.
- The OS disk has a maximum capacity of 4,095 GiB.
- The maximum size of the data disk is 32,767 GiB.
- Managed disks are integrated with the **availability sets** to ensure that the VM disks are separated from each other in an availability set to prevent a single failure point.
- You can assign specific permissions for a managed disk to one or more users using **Azure RBAC**.
- You can use the temporary disk to store data such as page or swap files.
- Ephemeral OS disks are for stateless applications.
- Attach a managed disk to multiple VMs simultaneously using Azure shared disks.
- With snapshots, you can take a back up of your managed disks at any given point in time.

Disk Types

- **Standard HDD**
  - Low cost and suitable for backups.
  - **Write** latencies under **10ms**.
  - **Read** latencies under **20ms**.
- **Standard SSD**
  - Consistent performance at lower IOPS levels.
  - Higher reliability, scalability, and lower latency over HDD.
- **Premium SSD**
  - High-performance and low-latency disk for VMs.
  - Consistent IOPS, and throughput.
  - Offers **disk bursting** and can burst their IOPS per disk up to 3,500 and their bandwidth up to 170 Mbps.
  - Peak burst limit of 30 mins
- **Ultra Disk**
  - High throughput, IOPS, and consistent low latency disk storage.
  - Only supports un-cached reads and un-cached writes.
  - Doesn't support disk snapshots, VM images, availability sets, Azure Dedicated Hosts, or Azure disk encryption.
  - The integration with Azure Backup or Azure Site Recovery is not supported.

Detail	Standard HDD	Standard SSD	Premium SSD	Ultra Disk
Disk type	HDD	SSD	SSD	SSD
Scenario	Backup, non-critical, infrequent access	Web servers, and light applications of enterprise	Production and performance-sensitive workloads	IO-intensive workloads, top tier databases, and other transaction-heavy workloads
Max disk size	32,767 GiB	32,767 GiB	32,767 GiB	65,536 GiB
Max throughput	500 MB/s	750 MB/s	900 MB/s	2,000 MB/s
Max IOPS	2,000	6,000	20,000	160,000

Encryption

- **Server-Side Encryption (SSE)** is performed by the storage service.
- **Azure Disk Encryption (ADE)** can be enabled on the OS and data disks.
- Encrypted using 256-bit AES encryption.
- By default, managed disks use platform-managed encryption keys.
- Using Azure Key Vault, you can import your RSA keys or generate new RSA keys.
- For standard HDDs, standard SSDs, and premium SSDs: disabling or deleting the key will automatically shut down all the VMs with disks using that key.
- If you disable or delete a key, any virtual machines with **ultra disks** using the key won't automatically shut down.
- Once you enable end-to-end encryption, temp disks and ephemeral OS disks are encrypted with platform-managed keys.

Pricing

- Managed disk size is billed on the provisioned size.
- Snapshots are charged based on the size used.
- Outbound data transfers incur billing for bandwidth usage.
- You are charged for the number of transactions that you perform on a managed disk (the number of read and write data operations performed).

Sources:
https://azure.microsoft.com/en-us/services/storage/disks/
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/managed-disks-overview

Azure Files

- Offers fully managed cloud-based file storage that can be accessed through the industry-standard server message block (SMB) protocol.

Features

- Mount your Azure File share from Windows, Linux, or macOS.
- **Azure File Sync** enables you to access your data from SMB, REST, or even on-premises.
- Encrypt data at rest and in transit using SMB 3.0 and HTTPS.
- Lift and shift applications to the cloud, where the application data is moved to Azure Files, and the application continues to run on-premises.
- Store configuration files in a centralized location where they can be accessed from many application instances.
- Azure Files provides the capability of taking **share snapshots** of file shares.

Storage Tiers

- **Premium file shares (SSD)**
  - High performance & low latency, within single-digit milliseconds for most IO operations.
  - For IO-intensive workloads.
- **Standard file shares (HDD)**
  - Reliable performance for IO workloads which are less latency-sensitive.
- If you created either a premium or a standard file share, you cannot automatically convert it to the other tier.

Detail	Premium	Standard
Billing model	Provisioned Billing Model, pay for how much storage you provision rather than how much storage you actually ask for.	Pay-As-You-Go Model, the bill will increase if you use (read/write/mount) the Azure file share more.
Redundancy options	It is available for locally redundant (LRS) and zone redundant (ZRS) storage.	It is available for locally redundant, zone redundant, geo-redundant (GRS), and geo-zone redundant (GZRS) storage.
Maximum size of file share	Provisioned for up to 100 TiB.	5 TiB by default, 100 TiB for locally redundant or zone

		redundant storage accounts.
Regional availability	File shares are not available in each region, but zone redundant support is available in a smaller subset of regions.	Available in every Azure region.

Supported devices

- To use an Azure file share outside of the Azure region the OS must support SMB 3.0.
- To mount an Azure file sharing on Windows, you must have access to port 445.

Windows version	SMB version	Mountable in Azure VM	Mountable on-premises
Windows Server 2019	SMB 3.0	Yes	Yes
Windows 101	SMB 3.0	Yes	Yes
Windows Server semi-annual channel2	SMB 3.0	Yes	Yes
Windows Server 2016	SMB 3.0	Yes	Yes
Windows 8.1	SMB 3.0	Yes	Yes
Windows Server 2012 R2	SMB 3.0	Yes	Yes
Windows Server 2012	SMB 3.0	Yes	Yes
Windows 73	SMB 2.1	Yes	No
Windows Server 2008 R23	SMB 2.1	Yes	No

- Linux clients can also access the file storage through the SMB protocol.

Linux distribution	SMB 2.1 *(Mounts on VMs within same Azure region)*	SMB 3.0 *(Mounts from on-premises and cross-region)*
Ubuntu	14.04+	16.04+
Red Hat Enterprise Linux (RHEL)	7+	7.5+
CentOS	7+	7.5+
Debian	8+	10+
openSUSE	13.2+	42.3+
SUSE Linux Enterprise Server	12+	12 SP3+

Encryption

- By default, encrypted with Microsoft-managed keys and responsible for rotating them on a regular basis.
- Using Microsoft-managed keys, you can also choose to manage your own keys, which gives you control over the rotation process.
- With customer-managed keys, Azure file storage is authorized to access your keys to fulfill read and write requests from your clients.

Networking

- SMB uses port 445.
- Accessible from anywhere, via the public endpoint of the storage account.
- Azure file shares over an ExpressRoute or VPN connection:
    - Tunneling into a virtual network, even if port 445 is blocked.
    - Private endpoints give you a dedicated IP address from within the address space of the virtual network.
    - Allows you to configure DNS forwarding.

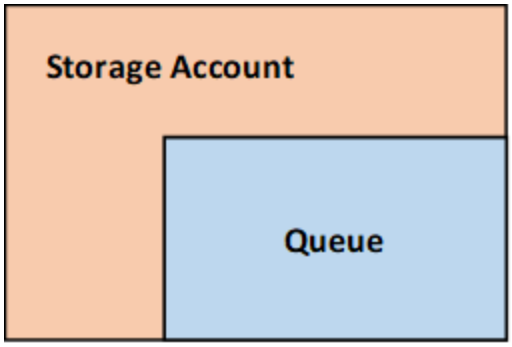
Azure File Sync

- Transform an on-premises (or cloud) Windows Server into a quick cache of your Azure file share.
- Only NTFS volumes are supported; ReFS, FAT, FAT32, and other file systems are not supported.
- The service supports interop with DFS Namespaces (DFS-N) and DFS Replication (DFS-R).

Sources:
https://azure.microsoft.com/en-us/services/storage/files/
https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction
https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows
https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-linux

Azure Queue Storage

- Durable queues for large-volume cloud services.
- Store large numbers of messages.
- Queue messages may have a size of up to 64 KB.



Features

- Asynchronous message queueing to communicate between components of the application.
- Built to be scalable and withstand the failure of individual components
- Monitor the length of the queue to add elasticity to your application, and hibernate or deploy additional nodes depending on customer demand.

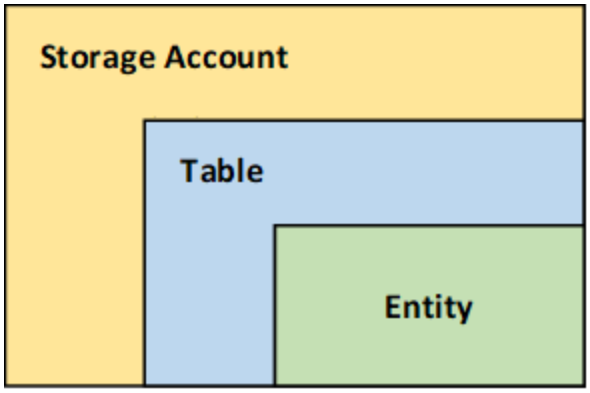
Pricing

- No upfront cost and termination fees.
- You only pay for what you use.

Sources:
https://azure.microsoft.com/en-us/services/storage/queues/
https://docs.microsoft.com/en-us/azure/storage/queues/storage-queues-introduction

Azure Table Storage

- A NoSQL key-value store for large semi-structured datasets.
- Supports flexible data schema.
- Performs OData-based queries.



Features

- Allows you to store and query huge sets of structured, non-relational data. And as demand grows, your tables will scale-out.
- Scale-up without having to manually shard your dataset.
- The data is replicated three times within a region using geo-redundant storage.
- An **entity** has a limit of 1MB in size.
- Store data sets that do not require complex joins, foreign keys, or stored procedures, and can be denormalized for fast access.
- Table storage is used to store flexible data sets such as user data for web applications, device information, or other types of metadata the service requires.
- You can store any number of entities in a table, up to the storage account's capacity limit.

Sources:
https://azure.microsoft.com/en-us/services/storage/tables/
https://docs.microsoft.com/en-us/azure/storage/tables/table-storage-overview

Azure Archive Storage

- Store rarely accessed data which are held for a period of 180 days.
- Snapshots are not applicable to archive storage.

Features

- It supports 2 rehydrate priorities: **High** and **Standard**
  - **Standard (Default)** - rehydration request may take up to 15 hours.
  - **High** - rehydration request may finish in under 1 hour for objects under 10 GB in size.
- Long-term backup, secondary backup, and archival datasets.
- Lowest storage costs but the highest data rehydrate and access costs.
- To read data in archive storage, you need to change the blob tier to hot or cold first.
- Compliance and archival data that must be preserved and are hardly ever accessed.
- Archive storage only supports block blobs.
- If a blob is in the archive tier, it can't be overwritten, unlike in hot or cool tier.
- Archive storage cannot be set as a default account access tier.
- Archive storage is initially available in selected regions.
- Blob index tags can be read, set, or modified while in the archive.
- You can only copy archive blobs within the same storage account.
- Encrypted data transfer to the cloud using HTTPS, and using 256-bit AES keys to automatically protect the data at rest.

Use Cases

- It is mainly used in long-term backup retention.
- If you need to minimize your cost, use Archive Storage to create a low cost, content archiving solution.
- Archive storage provides secure, globally compliant storage for sensitive data.
- You can also use Archive storage if you have a large amount of data that needs to be preserved.

Pricing

- Blobs are stored for at least 180 days in the archive tier. Deleting or rehydrating archived blobs before the minimum number of days will incur early deletion fees.
- Charges on data access increases as the tier gets cooler. For data in the cool and archive access tier, you're charged a per-gigabyte data access charge for reads.

Sources:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers?tabs=azure-portal
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-rehydration?tabs=azure-portal
https://azure.microsoft.com/en-us/services/storage/archive/

DATABASE

Azure Cosmos DB

- Globally distributed database that supports NoSQL.
- A fully-managed database service with **turnkey global distribution** and transparent **multi-master replication.**

Features

- Cosmos DB offers encryption at rest.
- It replicates every partition across all the regions.
- CosmosDB offers single-digit millisecond reads and writes in all regions.
- Supports automatic failover during a regional outage.
- Consistency Levels: **Strong, Bounded Staleness, Session, Consistent Prefix,** and **Eventual**
- You can set either standard (manual) or **autoscale** provisioned throughput on your databases and containers.
- Monitor both the provisioned autoscale max RU/s and the current throughput (RU/s) of the system with **Azure Monitor** metrics.

Consistency Levels

- **Strong -** reads are guaranteed to return the most recent committed version of an item.
- **Bounded Staleness** - is for low write latencies but requires a total global order guarantee.
- **Session -** reads are guaranteed to honor the consistent-prefix, monotonic reads, monotonic writes, read-your-writes, and write-follows-reads guarantees.
- **Consistent Prefix -** updates that are returned will contain some prefix of all the updates.
- **Eventual -** has no ordering guarantee for reads.

Security

- Encryption at rest is applied automatically.
- Uses AES-256 encryption in all regions.
- You can use the keys that are managed by Microsoft or customer-managed keys.
- Two types of keys to authenticate users:
    - Master Keys for administrative resources.
    - Resources Tokens for application resources.
- Detect suspicious activities which indicate unusual and potentially harmful attempts to access or exploit databases with **Advanced Threat Protection**.

Pricing

- Elastically scale the provisioned throughput and storage for your databases according to your needs and only pay for the throughput and storage needed.

- Cosmos DB throughput per second and request unit consumption varies by operation and JSON document.
- Additional backup copies will be billed as total GBs of data stored *(first two copies are free)*.
- You provision the number of RUs for your application on a per-second basis in increments of 100 RUs per second. You are billed on an hourly basis.
- With autoscale for containers, you pay per hour for the highest RU/s that the system scaled up to within the hour.

Sources:
https://docs.microsoft.com/en-us/azure/cosmos-db/introduction
https://azure.microsoft.com/en-us/free/cosmos-db/

Azure SQL

- A fully managed database built upon the SQL Server engine.
- SLA durability up to 99.995%.
- SQL Databases Resource type:
    - Single Database - offers serverless and hyperscale storage (up to 100TB).
    - Elastic Pool - a collection of databases with a shared set of resources.
    - Database Server - manage groups of single databases and elastic pools.
- **SQL Managed Instances** are for migrations "lift-and-shift" to the cloud.
    - The features of both SQL Server database engine and Azure SQL are available in SQL Managed Instance.
        - PaaS benefits - Azure will handle all infrastructure management.
        - Business continuity - the data are protected with automated backups.
        - Security and compliance - supports native VNet implementation, and it is exposed only through a private IP address.
        - Management operations - automatically deploy new instances, update instance properties, and delete instances that are no longer needed.
    - Automate the migration of existing SQL Server instances to SQL Managed Instance with Azure Data Migration Service.
    - Azure Hybrid Benefit for SQL Server allows you to exchange existing licenses to get discounted rates on SQL Managed Instance.
- **SQL Virtual Machines** are used for applications requiring OS-level access.
- Endpoint: <*server_name*>.database.windows.net
- vCore-based service tiers:
    - General Purpose is for common workloads.
    - Hyperscale is appropriate for online transaction processing (OLTP) and hybrid transactional analytical workloads (HTAP).
    - Business Critical is best for OLTP applications with high transaction rates and low IO latency.
- **Azure Hybrid Benefit for SQL Server** enables you to use your SQL Server licenses to pay a reduced rate on Azure SQL.
- **Azure Data Studio** is a modern cross-platform database tool with customizable code snippets, lightning-fast IntelliSense, useful peek definitions, and an integrated terminal to run other SQL tools.

Monitoring

- You can use **Intelligent Insights** to continuously monitor your Azure SQL usage and detect disruptive events that may lead to poor database performance.
- **Azure SQL Analytics** can be used to monitor your databases across multiple subscriptions. It can collect and visualize key performance metrics of your databases and enables you to create custom monitoring rules and alerts.

- **Automatic tuning i**n Azure SQL continuously monitors queries executed on your database, and automatically improves the performance using artificial intelligence.

Networking

- Private endpoint connections provide access to all databases in the server.
- Allow communications from all resources inside the Azure boundary with firewall rules.

Security

- You can use **Advanced Data Security (ADS)** for data classification, vulnerability assessment, and advanced threat protection.

Pricing

- The resources are billed hourly at a fixed rate based on the service tier and compute size you choose.
- You are billed for outgoing Internet traffic.

Sources:
https://docs.microsoft.com/en-us/azure/azure-sql/azure-sql-iaas-vs-paas-what-is-overview
https://azure.microsoft.com/en-us/services/sql-database/

Azure Database Migration Service (DMS)

- Accelerates the migration of your data to Azure.
- Enables seamless migrations from multiple database sources.
- To perform an online migration, you need to create an instance based on the **premium pricing tier**.

Features

- Migrates your database and server objects with minimal downtime.
- Supports Microsoft SQL Server, MySQL, PostgreSQL, MongoDB, and Oracle migration to Azure from on-premises and other cloud providers.
- You can use DMS for both operational database and data warehouse migrations.
- Automate the migration of data with **Azure PowerShell.**
- Use **Azure Migrate** to discover your on-premises data estate and assess migration readiness.
- You can create up to 2 DMS services per subscription.

Pricing

- Offline migrations of the DMS Standard tier are free to use.
- DMS premium tier is billed at an hourly rate based on the provisioned compute capacity.

Sources:
https://docs.microsoft.com/en-us/azure/dms/dms-overview
https://azure.microsoft.com/en-us/services/database-migration/

Azure Database for MySQL & PostgreSQL

- PaaS relational database services.
- Mitigate database downtime with high availability, redundancy, and resiliency capabilities.
- Enables you to scale vertically when needed.
- Receive alerts based on the metrics of your servers.
- Protect sensitive data at rest and in transit.
- Automated backups, up to 35 days.
- PostgreSQL deployment options: **Single Server** and **Hyperscale (Citus)**
- Single server pricing tiers: Basic, General Purpose, and Memory Optimized.
    - **Basic** - light compute and I/O performance workloads.
    - **General Purpose** - a balanced compute and memory with scalable I/O throughput workloads.
    - **Memory Optimized** - for high performance database workloads requiring in-memory performance.

PostgreSQL - Hyperscale (Citus)

- Sharding - scales horizontally across multiple machines.
- Supports query parallelization for faster responses on large datasets.
- Primarily used for multi-tenant applications, real-time operational analytics, and high throughput transactional workloads.

Source:
https://docs.microsoft.com/en-us/azure/mysql/overview
https://docs.microsoft.com/en-us/azure/postgresql/overview

NETWORKING AND CONTENT DELIVERY

Azure Virtual Network (VNet)

- You can create a virtual network in the cloud dedicated to your Azure account. It is the fundamental building block where you can launch Azure resources.
- Azure VNet is the networking layer of Azure VMs.
- A VNet spans all the Availability Zones in the region. After creating a VNet, you can add one or more subnets in each Availability Zone.

Key Concepts

- A **virtual network** (VNet) allows you to specify an IP address range for the VNet, add subnets, associate network security groups, and configure route tables.
- A **subnet** is a range of IP addresses in your VNet. You can launch Azure resources into a specified subnet. Use a **public subnet** for resources that need to connect to the Internet and a **private subnet** for resources that won't be connected to the Internet.
- To protect the Azure resources in each subnet, use **network security groups**.

VNet Use Case

- VNet with a single public subnet.
- VNet with public and private subnets (NAT).

Subnets

- When you create a VNet, you must specify a range of IPv4 addresses for the VNet in the form of a CIDR block (*example: 10.0.0.0/16*).
- A CIDR block must not overlap with any existing CIDR block that's associated with your VNet.
- You can add multiple subnets in each Availability Zone of your VNet's region.
- Types of subnets:
    - Public subnet
    - Private subnet
    - Gateway subnet
- The CIDR block size of an IPv4 address is between a /16 netmask (65,536 IP addresses) and /29 netmask (8 IP addresses).
- The 5 reserved addresses in each CIDR block is not available for you to use, and cannot be assigned to any virtual machines.
- You can delegate a subnet to be used by a dedicated service.

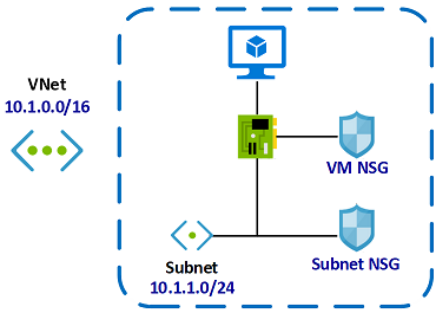
Security

- Network Security Groups - controls the inbound and outbound traffic of Azure resources.
- Application Security Group - allows you to define a VMs group network security policy.

- You can use **IP flow verify** of Azure Network Watcher to check which network security rule allows or denies the traffic.
- With VNet service endpoint policy, you can filter the egress VNet traffic to Azure Storage.

AZ-900 Exam Notes:

Understanding how to secure your virtual network is very important. Always remember that you can associate your network security group in the virtual network subnet and network interfaces.



VNet Components

- NAT Gateway
  - Allows your virtual network resources to have an outbound-only connection.
  - A NAT gateway resource can use up to 16 static IP addresses.
  - You can use multiple subnets in a NAT gateway.
- Route tables are used to determine where network traffic is directed.
  - A subnet can only be associated with one route table.
  - If multiple routes contain the same address prefix, the selection will be based on the following priority: User-defined route, BGP route, and System route.
- You can connect VNets to each other using **VNet peering**.
- If you need to connect privately to a service, you can use **Azure Private Endpoint** powered by Azure Private Link.

Pricing

- You are charged for the public IP address and reserved IP address inside your VNet.
- You are charged for the ingress and egress data of VNet Peering.
- You are charged for the NAT gateway resource hours and data processed (per GB).

Sources:

https://azure.microsoft.com/en-us/services/virtual-network/
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

Azure Load Balancer

- Distributes incoming network traffic across multiple targets.
- Allows you to route traffic based on source IP address and port to a destination IP address and port.

Features

- The load balancer supports TCP/UDP-based protocols.
- Scales automatically as traffic increases.
- The load-balancing decision is based on the following tuple connection:
    - Source IP address and port
    - Destination IP address and port
    - Protocol
- NAT allows you to control the inbound and outbound network traffic.
    - Inbound rules - traffic allowed to a specific virtual machine or instance in the backend pool.
    - Outbound rules - enable all resources to communicate to the Internet.
- Control the flow of traffic inside your private virtual network using an internal load balancer.
- You can use a **public load balancer** to allow outbound connections for your virtual machines.
- Azure Load Balancer supports IPv6.
- Load balancer tiers: **Basic** and **Standard**

Components

- A group of VMs or instances in a VM scale set serving the incoming request is called **backend pool**.
- Determine the health status of backend pool instances with **health probes**.
    - Health probe down behavior - if the probes in a backend pool fail, it will stop receiving traffic until it starts passing health probes again.
- Standard load balancer **availability zones**:
    - Zonal = single zone
    - Zone-redundant = multiple zones

Details	Basic Load Balancer	Standard Load Balancer
Backend pool size	Supports up to 300 instances.	Supports up to 1000 instances.
Backend pool endpoints	A single availability set for VMs or VM scale set.	A single virtual network for any VMs or VM scale sets.
Health probes	TCP, HTTP	TCP, HTTP, HTTPS
Health probe down behavior	TCP connections stay alive on an instance probe down. All TCP connections terminate when all probes are down.	TCP connections stay alive on an instance probe down and on all probes down.
Availability Zones	Not available	Zone-redundant and zonal frontends for inbound and outbound traffic.
Diagnostics	Azure Monitor logs	Azure Monitor multi-dimensional metrics
HA Ports	Not available	Available for Internal Load Balancer
Secure by default	Open by default. Network security group optional.	Closed to inbound flows unless allowed by a network security group. Please note that internal traffic from the VNet to the internal load balancer is allowed.
Outbound Rules	Not available	Declarative outbound NAT configuration
TCP Reset on Idle	Not available	Available on any rule
Multiple frontends	Inbound only	Inbound and outbound
Management Operations	60-90+ seconds typical	Most operations < 30 seconds
SLA	Not available	99.99%

Pricing

- You are charged based on the number of outbound rules.
- You are billed for the first five rules of load balancing.
- You are not charged for the NAT rules.

Sources:
https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview
https://azure.microsoft.com/en-us/services/load-balancer/

Azure VPN Gateway

- A secured hybrid cloud architecture.
- It is composed of gateway subnet, tunnel, and on-premises gateway.
- Protocols: Internet Protocol Security (IPsec) and Internet Key Exchange (IKE)
- VPN gateway connections: **VNet-to-VNet**, **Site-to-Site**, and **Point-to-Site**
- Create a secure connection from your on-premises network to an Azure virtual network with a site-to-site VPN.
- VNet-to-VNet connection automatically routes to the updated address space, if you updated the address space on the other VNet.
- If you need to establish a connection to your virtual network from a remote location, you can use a point-to-site (P2S) VPN.
- You can also have one VPN gateway with more than one on-premises network using a Multi-Site connection.

Details	Site-to-Site	Point-to-Site
Supported Services	Cloud Services and Virtual Machines	Cloud Services and Virtual Machines
Bandwidths	Typically < 1 Gbps aggregate	Based on the gateway SKU
Protocols	IPsec	Secure Sockets Tunneling Protocol (SSTP), OpenVPN and IPsec
Routing	We support PolicyBased (static routing) and RouteBased (dynamic routing VPN)	RouteBased (dynamic)
Connection resiliency	active-passive or active-active	active-passive
Use case	Dev / test / lab scenarios and small scale production workloads for cloud services and virtual machines	Prototyping, dev / test / lab scenarios for cloud services and virtual machines

Pricing

- You are billed hourly for the compute costs of the VNet gateway.
- You are charged for the egress data transfer from the virtual network gateway.
- You are only charged by the VPN Gateway when you transfer data between two different regions, except with Point-to-Site VPN.

Sources:
https://azure.microsoft.com/en-us/services/vpn-gateway/
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

Azure Application Gateway

- A web traffic load balancer.
- It allows you to distribute incoming traffic based on HTTP request properties such as URL and host headers.
- Application gateway has four tiers: **Standard**, **Standard V2**, **WAF**, and **WAF v2**
- You can use the same application gateway for up to 100+ websites with multi-site hosting.
- Set the minimum and maximum scale units based on your needs.
- Azure Application Gateway vs Azure Load Balancer
    - An application gateway operates at layer 7.
    - A load balancer functions at layer 4.
- You can use both public and private IP on the frontend.

Features

- Secure your data with end-to-end SSL.
- Route traffic based on URL path or host header-based.
- Protect your applications from common web vulnerabilities using WAF.
- Scales automatically based on your web application traffic load.
- With gateway-managed cookies, you can direct subsequent traffic from a user session to the same server.

Pricing

- You are charged per instance, per GB, and per gateway-hour.
- You are also charged with capacity units (*computed hourly or partial hourly*).

Sources:
https://docs.microsoft.com/en-us/azure/application-gateway/overview
https://azure.microsoft.com/en-us/services/application-gateway/

Azure Content Delivery Network (CDN)

- A distributed network of servers that delivers web content closer to users.
- CDNs store cache content on **edge servers** to minimize end-user latency.

Features

- Improves the performance of dynamic web pages using dynamic site acceleration.
- You can set two types of caching rules in Azure CDN:
    - Global caching rule - overrides any HTTP cache-directive headers.
    - Custom caching rule - you can set a rule to match specific paths and file extensions.
- Types of origin:
    - Storage
    - Storage Static website
    - Cloud service
    - Web App
    - Custom Origin
- Enable HTTPS to mitigate security threats on the content distribution network.
- Export basic usage metrics from your CDN by using diagnostic logs.
- With geo-filtering, you can set rules for different paths to allow or block content in selected countries/regions.
- CDN endpoint: <*tutorialsdojo*>.azureedge.net

How Caching Works

- Access the data quickly by storing the data in an origin server.
- If the file on the origin server has been updated, the cache must update its resource version.
- Azure CDN HTTP cache-directive headers:
    - Cache-Control - caching behavior of a browser.
    - Expires - a date based expiration time.
- Azure CDN HTTP cache validators:
    - ETag - a string that is unique to every file.
    - Last-Modified - the origin server compares the date with the last-modified resource header.
        - Status code 200 = Modified
        - Status code 304 = Not Modified
- Default caching behavior:
    - Honor origin - honor the HTTP response cache-directive headers, if they exist.
    - CDN cache duration - how long a resource is cached on the Azure CDN.

Pricing

- You are charged based on the number of rules.
- You are charged for outbound data transfers.

Limits

- The limit for the following resources is 25:
  - CDN profiles
  - CDN endpoints per profile
  - Custom domains per endpoint

Sources:
https://azure.microsoft.com/en-in/services/cdn/
https://docs.microsoft.com/en-us/azure/cdn/cdn-overview

Azure Traffic Manager

- A DNS-based traffic load balancer.
- Improves the responsiveness of your applications by sending the request to the closest endpoint.
- It offers a range of **traffic-routing methods** and **endpoint monitoring options**.

Features

- It is resilient to failure.
- You can obtain actionable insights about your users using a **traffic view.**
- Improve the availability of your applications by using traffic manager health checks.
- Offers automatic failover when an endpoint goes down.
- Traffic Manager endpoints: **Azure**, **External**, and **Nested**
- Combine multiple traffic-routing methods using **nested traffic manager profiles**.

Routing Methods

- Priority - allows you to set a primary endpoint for all traffic.
- Weighted - distribute traffic according to weights.
- Performance - routes users to the closest endpoint.
- Geographic - direct users to a specific endpoint.
- Multivalue - endpoints for IPv4/IPv6 addresses.
- Subnet - map a group of end-user IP address range to a specific endpoint.

Pricing

- You are charged based on the number of DNS queries received.
- You are also charged for each monitored endpoint.
- You can reduce your DNS query charges by configuring a larger TTL.
- You are charged for the number of data points used in the traffic view.

Sources:
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview
https://azure.microsoft.com/en-us/services/traffic-manager/

Azure DNS

- Enables you to host your DNS zone and manage your DNS records.
- DNS zone allows you to configure a private and public DNS zone.
- Alias recordsets:
    - A - maps the host to IPv4.
    - AAAA - maps the host to IPv6.
    - CNAME - create a record to point to another domain.
- A limit of 20 alias record sets per resource.
- Uses Anycast networking to route users to the closest name servers.
- You can monitor your DNS zone metrics using Azure Monitor.
    - QueryVolume - query traffic received.
    - RecordSetCount - the number of recordsets in your DNS.
    - RecordSetCapacityUtilization - percentage of utilization of your recordset capacity.
- **Azure Private DNS** allows you to use your custom domain name in your private VNet.
- Alias record allows you to point your naked domain or apex to a traffic manager or CDN endpoint.

Private DNS

- Allows you to manage and resolve domain names in a virtual network.
- Configure a split-horizon DNS to create zones with the same name.
- It also supports all types of DNS records types: A, AAAA, CNAME, MX, PTR, SOA, SRV, and TXT.
- A virtual network can be linked to only one private zone. But you can link multiple virtual networks to a single DNS zone.
- Private IP space in the linked virtual network allows reverse DNS.

Security

- To prevent accidental zone deletion, you can apply a 'CanNotDelete' lock.
- Create a custom role to ensure it doesn't have a zone delete permission.
- You can deploy a DNS firewall to mitigate DNS-related security issues.

Pricing

- Billed on the number of hosted DNS zones.
- You are charged based on the number of DNS queries received.

Sources:
https://azure.microsoft.com/en-us/services/dns/
https://docs.microsoft.com/en-us/azure/dns/dns-overview

Azure Front Door

- A service that uses Microsoft's global network to improve the availability and performance of your applications to your local and global users.
- It works at the HTTP/HTTPS layer and uses a **split TCP-based anycast protocol** to ensure your users connect to the nearest Front Door point of presence.
- Supports a range of **traffic-routing methods** and **backend health monitoring** options for various application needs and automatic failover models.
- With **URL-based routing**, it routes the traffic to backend pools based on URL paths of the request.
- You can configure more than one website on the same Front Door with **multiple-site hosting**.
- Use **cookie-based session affinity** to redirect the user session to the same application backend.
- Redirect traffic based on protocol, hostname, path, and query string with **URL redirect**.
- **URL rewrite** allows you to configure a Custom Forwarding Path that will copy any part of the incoming path that matches a wildcard path to the forwarded path.
- Front Door supports end-to-end IPv6 connectivity and HTTP/2 protocol.

Security

- If you need your domain name to be visible in your Front Door URL, you must have a custom domain. Front Door also supports managed certificates or custom TLS/SSL certificates.
- You can create custom rules to protect your HTTP/HTTPS workload from exploitation using Azure Web Application Firewall.

Pricing

- You are charged based on the following:
    - Inbound and outbound data transfers
    - The number of routing rules
- Front Door has a limit of 100 custom domains. You will be charged for additional domains.

Sources:
https://azure.microsoft.com/en-us/services/frontdoor/
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview

Azure ExpressRoute

- Enables you to establish a private connection between your on-premises data center or corporate network to your Azure cloud infrastructure.
- More secure, reliable, and faster than conventional VPN connections.
- Supports dynamic routing between your network and Microsoft via Border Gateway Protocol (BGP). The connection is redundant in every peering location for higher reliability.

Features

- ExpressRoute connections enable access to Microsoft Azure services and Microsoft Office 365 services from your on-premises network.
- Provides connectivity to all regions within a **geopolitical region**.
- To extend connectivity across geopolitical boundaries, you can enable **ExpressRoute Premium**.
- **ExpressRoute Global Reach** allows you to exchange data across your on-premises environments by connecting it to your ExpressRoute circuits.
- **ExpressRoute Direct** provides dual 100Gbps connectivity that supports Active/Active scale connectivity.
- Supported bandwidth options up to 10 Gbps.
- **ExpressRoute premium add-on** (*for ExpressRoute circuit*) provides the following capabilities:
    - Increased route limits from 4,000 routes to 10,000 routes for Azure public and private peering.
    - Global access to services across any other region.
    - Increase the number of VNet links (*from 10 to a larger limit*) on every ExpressRoute circuit.

Use Cases

- Transferring large data sets.
- Developing and using applications that use real-time data feeds.
- Building hybrid environments that satisfy regulatory requirements mandating the use of private connectivity.

Pricing

- Billing Models:
    - Unlimited data - all inbound and outbound data transfer is free.
    - Metered data - all inbound data transfer is free but outbound data transfer is billed per GB. The rate of data transfer varies by region.
- ExpressRoute billing begins when a service key is issued to the customer.
- If the service is active for the **entire month**, you will be billed for the monthly fee regardless of your usage. However, if you cancelled the service **during the month**, then you are charged for the hours used.

Sources:
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction
https://azure.microsoft.com/en-us/services/expressroute/

SECURITY

Microsoft Entra ID

- An identity and access management service that helps you access internal and external resources.
- Microsoft Entra ID licenses: **Free**, **P1**, **P2** and **Pay as you go**
    - Free - user and group management in your on-premises directory
    - P1 - allows access to both on-premises and cloud resources.
    - P2 - provides an additional feature called Microsoft Entra ID Identity Protection.
    - Pay as you go - offers a feature called Azure AD B2C.

Features

- You can use **Microsoft Entra Authentication** for a self-service password reset, MFA, custom banned password list, and smart lockout.
- Allows you to manage external identities using **Microsoft Entra B2B**.
- **Azure AD B2C** is a business-to-customer identity as a service that allows you to control how your users sign up, sign in, and manage their profiles when using your applications.
- You can manage the access in your cloud apps with **conditional access**.
- With **Microsoft Entra admin center**, it allows you to manage and configure device identities.
- If you need to manage domain services such as domain join, group policy, and authentication, you can use **Microsoft Entra Domain Services**.
- **Microsoft Entra ID Governance** ensures that only the authorized people have the right access to specific resources.
- Supports **hybrid identity** to access resources in the cloud or on-premises.
- Use **Microsoft Entra Connect** to accomplish your hybrid identity goals:
    - A sign-in method that uses password hash synchronization.
    - Pass-through authentication allows users to use the same password on-premises and in the cloud.
    - Enable federation integration to sign in to Microsoft Entra ID-based services without having to enter their passwords again.
    - Synchronization between your on-premises environment and Microsoft Entra ID.
    - Health Monitoring with Microsoft Entra Connect Health.

AZ-900 Exam Notes:

You can configure Microsoft Entra ID join during a Windows 10 first-run experience (*All Windows 10 devices except Windows 10 Home*). To verify whether a device is joined to your Microsoft Entra ID, you can take a look at the **Access work or school** dialog on your device.

Monitoring

- Monitor the security and usage patterns of your environment with **Microsoft Entra monitoring and health**.
- With **Microsoft Entra Connect Health**, you can view alerts, monitor performance and check usage analytics of your on-premises Active Directory and Microsoft Entra.

Security

- Detect potential vulnerabilities and resolve suspicious actions with **identity protection**.
- Microsoft Entra Privileged Identity Management (PIM) helps you control the access within your organization.
- You can use security defaults to enable MFA in your organization.
- Enabling **security defaults** protects you from common identity-related attacks.
- You use **block legacy authentication** if a user is using a legacy application.
- **Identity secure score** helps you verify your configurations if it's aligned with Microsoft's best practice for security.
- You can lockout intruders that try to guess your users' passwords or use brute-force methods in Microsoft Entra using **smart lockout**.
- Manage, control, and monitor access to significant resources in your organization with **Privileged Identity Management (PIM)**.

Sources:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis
https://azure.microsoft.com/en-us/services/active-directory/

Azure Firewall

- A service that uses a static public IP address to protect your VNet resources.
- Azure Firewall is PCI, SOC, ISO, ICSA Labs, and HITRUST compliant.

Features

- A stateful firewall service.
- You can enable **forced tunneling** to route Internet-bound traffic to an additional firewall or virtual network appliance.
- Limit outbound traffic to a given **FQDN** list, including wild cards.
    - Filter any TCP/UDP protocol outbound traffic.
    - To use FQDNs in your rules, you must enable DNS proxy.
- Deny the traffic of a malicious IP address with **threat intelligence-based filtering**.
    - It has the highest priority rules and will always be processed first.
    - Threat intelligence modes: Off, Alert only, Alert and deny
- With a DNS proxy, a firewall listens to port 53 and forwards the DNS requests to a DNS server.
- You can minimize the complexity of creating a security rule using a **service tag**.
- Associate up to 250 public IP addresses in your firewall.
- It supports SNAT and DNAT translation.
    - SNAT - Source NAT for outbound VNet traffic.
    - DNAT - Destination NAT for inbound network traffic.
- Azure Firewall diagnostic logs (JSON format):
    - Application rule log
    - Network rule log
- You can store all your logs in a storage account, event hubs, and Azure monitor logs.
- Azure Firewall metrics:
    - Application/Network rules hit count
    - Data processed
    - Throughput
    - Firewall health state
    - SNAT port utilization
- To manage multiple firewalls, you can use **Azure Firewall Manager**.
- Protect your VDI deployments using Azure firewall DNAT rules and threat Intelligence filtering.

Pricing

- You are charged for each firewall deployment
- You are charged for any data processed by your firewall

Sources:
https://azure.microsoft.com/en-us/services/azure-firewall/
https://docs.microsoft.com/en-us/azure/firewall/overview

Azure DDoS Protection

- Allows you to protect your Azure resources from denial of service (DoS) attacks.
- DDoS protection (layers 3 and 4) offers two service tiers: **Basic** and **Standard**.

Features

- **Basic**
  - Enabled by default (free).
  - It mitigates common network attacks.
  - Both basic and standard protects IPv4 and IPv6 public IP addresses.
- **Standard**
  - It has advanced capabilities to protect you against network attacks, such as logging, alerting, and telemetry.
  - Mitigates the following attacks:
    - Volumetric attacks - flood the network layer with attacks.
    - Protocol attacks - exploit a weakness in layers 3 and 4.
    - Resource layer attacks - a layer 7 attack that disrupts the transmission of data between hosts.
  - Enables you to configure alerts at the start and stop of an attack.
  - The metric data is retained for 30 days.
  - Provides autotuned mitigation policies (TCP/TCP SYN/UDP) for each public IP.

Feature	Basic	Standard
Active traffic monitoring & always-on detection	Yes	Yes
Automatic attack mitigations	Yes	Yes
Availability guarantee	Azure Region	Application
Mitigation policies	Tuned for Azure traffic region volume	Tuned for application traffic volume
Metrics & alerts	No	Real-time attack metrics and resource logs via Azure Monitor
Mitigation reports	No	Post attack mitigation reports

Mitigation flow logs	No	NRT log stream for SIEM integration
Mitigation policy customization	No	Engage DDoS Experts

Pricing

- Basic DDoS Protection provides protection at no additional charge.
- Standard DDoS Protection is a paid service. You are charged for the processed data every month (per GB).

Sources:
https://azure.microsoft.com/en-us/services/ddos-protection/
https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview
https://docs.microsoft.com/en-us/azure/security/fundamentals/ddos-best-practices

Microsoft Defender for Cloud

- Manages all the security features of Azure.
- Detect vulnerabilities, restrict your exposure to threats, and quickly detect and respond to attacks.
- **Secure Score** allows you to get continuous assessment and security recommendations.
- It helps you to detect unusual activities and prevent threats in your PaaS workloads.
- Protect your virtual machines with configuration and vulnerability management, workload hardening, and server EDR.
- It also supports advanced monitoring to track and manage compliance & governance.
- Allows you to protect your resources using free or standard tiers.

Concepts

- Defender for Cloud displays the overall **secure score** of your account. The higher the score, the lower the identified risk level.
- **Recommendations** help you remediate potential security vulnerabilities in your Azure resources.
- **Security controls** help you implement a set of security recommendations. After you remediate all of the recommendations, it will reflect in your overall security score.
- To help in complying with the security requirement of your organization, you can define a **security policy** in your workloads.
- You can quickly investigate the problem and make recommendations on how to remediate an attack using **security alerts**.
- Microsoft Defender for Cloud just-in-time **(JIT)** enables you to lock down inbound traffic to your Azure virtual machines.

Pricing

- With Standard Tier, you are charged
    - Per hour for VMs, app services, SQL database
    - Per transactions for storage and IoT messages
    - Per month for IoT devices
    - Per image for ACR
    - Per vCore/hour for AKS

Sources:
https://azure.microsoft.com/en-us/services/defender-for-cloud/
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

Azure Key Vault

- A service that allows you to store tokens, passwords, certificates, and other secrets.
- You can also create and manage the keys used to encrypt your data.

Features

- **Soft delete** allows a deleted key vault and its objects to be retrieved during the retention time you designate.
- The retention period of a deleted vault is between 7 to 90 days.
- With soft-delete and **purge protection** enabled, it will not purge a vault or object in the deleted state until the retention period has expired.
- You may connect to a key vault via
    - A public endpoint in all networks
    - A public endpoint in selected networks
    - A private endpoint
- Share access to your applications and resources without revealing your credentials.

Concepts

- A **tenant** is a representation of an organization.
    - Microsoft Entra ID allows you to publish multi-tenant applications.
    - Azure Active Directory (B2C) tenant represents a collection of identities.
- A **vault owner** enables you to create a key vault and set up an auditing log of who has access to secrets and keys.
- A **vault consumer** can only perform actions on the assets inside the key vault if the vault owner grants the consumer access.
- A manageable item in Azure is called **resource**, and **resource groups** are containers that hold related resources.
- **Service principal** gives you control over which resources can be accessed. At the same time, a **managed identity** eliminates the need for you to create and manage service principals directly since it provides Azure services with an automatically managed identity in Microsoft Entra.
- You can identify an Microsoft Entra instance within your Azure subscription using a **tenant ID**.

Pricing

- You are charged if the key has been used at least once in the last 30 days (*based on the key's creation date*).
- You are charged for each historical version of a key.

Sources:
https://docs.microsoft.com/en-us/azure/key-vault/general/overview
https://azure.microsoft.com/en-us/services/key-vault/

Azure Information Protection (AIP)

- You can protect your documents and emails by applying labels.
- Labels can be applied:
    - Automatically - administrators
    - Manually - users
    - By combination - recommendations
- Allows you to track your shared data and revoke access if needed.
- Configure policies based on the sensitivity of your data.
- Sharing data with others will be safe, and you are in control of who can edit, view, and print.
- Labeling content includes:
    - Classification
    - Visual Markings
    - Metadata
- You can use default labels or custom labels.
- The default classification labels are:
    - Personal
    - General
    - Confidential
    - Highly Confidential

Sources:
https://azure.microsoft.com/en-us/services/information-protection/
https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

Microsoft Defender for Identity

- Enables you to identify, detect, and investigate advanced threats in your organization.
- Allows you to monitor user activities and information.
- Identify and investigate advanced threats throughout the entire cyber-attack kill chain:
    - **Reconnaissance** - identify attempts by attackers to gain information.
    - **Compromised credentials** - any attempts that compromise user credentials shall be detected.
    - **Lateral movements** - attacks to gain access to sensitive accounts.
    - **Domain dominance** - the attacker has the credentials to access your domain controller.
    - **Exfiltration** - unauthorized data transfer.

Sources:
https://www.microsoft.com/en-ww/security/business/threat-protection/identity-defender
https://docs.microsoft.com/en-us/defender-for-identity/what-is

Microsoft Sentinel

- A cloud-native SIEM and SOAR solution.
- It offers a birds-eye view across your enterprise.
- Sentinel is an intelligent security analytics and threat intelligence service that provides alert detection, threat visibility, proactive hunting, and threat response.
- Data connection methods in Sentinel: Service to service integration, External solutions via API, and External solutions via an agent.
- Microsoft Sentinel roles: Reader, Responder, and Contributor.

Threat Management

- Sentinel provides the following features: Collect, Detect, Investigate, and Respond.
- Quickly gain insights across your data with Azure Sentinel **Workbooks**.
- Investigate and resolve possible threats with **incidents** (*groups of related alerts*).
- You can automate tasks and simplify security orchestration using **playbooks**.
- Sentinel provides **deep investigation** tools to find the root cause of a potential security threat.
- **Hunting** allows you to find issues in your data.

Pricing

- Data retention is charged after 90 days.
- You are charged for the ingested data (per GB).

Sources:
https://docs.microsoft.com/en-us/azure/sentinel/overview
https://azure.microsoft.com/en-in/services/microsoft-sentinel/

Microsoft Compliance Offerings

- **Microsoft Trust Center** provides access to security, privacy, and compliance information.
    - Security - provides information about identity & access management, threat & information protection, and cloud security.
    - Privacy - provides information on how you can secure your data at rest and in transit.
    - Compliance - provides information about industry-specific requirements, audit reports, and shared responsibility.
- **Microsoft Privacy Statement** explains how Microsoft collects personal data, how they use it, and the reasons why they need to share personal data.
- The terms and conditions when you purchase licenses for products and online services through Microsoft Volume Licensing programs are documented in **Online Services Terms (OST)**.
- The **Data Protection Amendment (DPA)** sets the responsibilities of the customer and Microsoft with respect to the collection and protection of Customer Data and Personal Data in accordance with Azure.

National Institute of Standards and Technology (NIST)

- NIST maintains measurement standards and guidance to help organizations assess risk.
- NIST releases a Framework for Improving Critical Infrastructure Cybersecurity (FICIC) to strengthen the cybersecurity of federal networks and critical infrastructures.
- The NIST Cybersecurity Framework (CSF) consists of standards, guidelines, and best practices to manage cybersecurity-related risks.
- Quickly build NIST CSF solutions on Azure using the Azure Security and Compliance NIST CSF Blueprint.

General Data Protection Regulation (GDPR)

- GPDR establishes new rules for organizations that offer goods and services to citizens in the European Union.
- It also collects and analyzes data of EU residents. The GDPR applies no matter where your company is located.
- GDPR grants individuals certain rights to manage the personal data gathered by an organization through a Data Subject Request (DSR).
- GDPR requires an organization to provide timely information on DSRs, data breaches, and to conduct data protection impact assessments (DPIAs).

International Organization for Standardization (ISO)

- ISO provides international standards to safeguard consumers and end-users of products and services.
- The International Electrotechnical Commission (IEC) is an organization that prepares and publishes international standards for electrical, electronic, and related technologies.
- ISO/IEC 27001 is an information security management standard designed to bring information security under explicit management control.

- If a company has been granted with an ISO certification, it means that it has established standards and general principles in the initiation, implementation, maintenance, and improvement of information security management.
- You can use **Service Trust Portal** to provide audited compliance reports.
    - A portal where customers can find information and resources about the security, privacy, and compliance practices associated with Microsoft cloud services.
    - It includes the following categories:
        - **Certifications, Regulations and Standards** - provide documentation and information about Microsoft's services' comreportsentrapliance with various regulatory requirements and industry-specific standards.
        - **Reports, Whitepapers and Artifacts** - contain detailed information about the measures and controls implemented by Microsoft to protect customer data and ensure regulatory compliance.
        - **Industry and Regional Resources** - industry-specific guidelines, regional regulatory frameworks, and other relevant materials to help organizations navigate compliance requirements specific to their industry or geographical location.
        - **Resources for your Organization** - provides templates, checklists, and guidance on implementing and maintaining robust security and compliance practices within an organization's Azure environment.

AZ-900 Exam Notes:

We suggest that you read the following information before taking the exam:

- Microsoft Privacy Statement helps you understand the personal data Microsoft processes, how they process it, and for what purposes.
- Have a look at Microsoft Trust Center if you are concerned about data security and how Microsoft is complying with privacy and legal requirements.
- Explore all the audit reports of Microsoft Cloud services about data protection standards and regulatory requirements in the Microsoft Service Trust Portal.

Sources:
https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-nist-csf?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-iso-27001?view=o365-worldwide

MONITORING AND MANAGEMENT

Azure Resource Manager (ARM)

- A service that allows you to create, update, and delete resources in your Azure account.
- Enables you to manage access control, locks, and tags for your resources after they have been deployed.

Features

- All requests are authenticated and authorized by ARM before being routed to the appropriate Azure service.
- Manage infrastructure using declarative templates and deploy it in a repeatable manner.
- Deploy, manage, and monitor all resources as a group.
- Tag resources to logically organize all the resources in your subscription.
- You can check the costs for a group of resources sharing the same tag.
- Define the dependencies between resources, so they're deployed in the correct order.

Resource groups

- A container that holds related resources.
- You can create a resource group using the Azure Portal, PowerShell, CLI, or an ARM template.
- Each resource can only exist in a single resource group.
- You can add or remove resources to any resource group at any time.
- Allows you to move a resource from one resource group to another.
- Resources from multiple regions can be in one resource group.
- You can give users access to a resource group.
- Resources can interact with other resources in different resource groups.
- A resource group has a location, or region, as it stores metadata about the resources.
- When you delete a resource group, it also deletes all of its resources.

Resource locks

- Protect critical Azure resources from accidental deletion or modification.
- There are two types of resource locks:
    - **CanNotDelete** - prevents a resource from being deleted or modified.
    - **ReadOnly** - only allows read-only access to a resource.
- You can set locks at the subscription, resource group, or resource level.
- When you apply a lock to a parent scope, it is applied to all resources within that scope.
- Users with appropriate permissions can remove or update locks.

ARM templates

- The **template** is a JSON file with declarative syntax that defines the properties and configuration of your resources. It is divided into the following sections:
    - **Parameters** - values that allow the same template to be used in multiple environments.
    - **Variables** - values that can be reused in templates.
    - **User-defined functions** - customized functions to simplify the template.
    - **Resources** - define the resources to be deployed.
    - **Outputs** - values from deployed resources.
- When a template is deployed, ARM converts it into REST API operations.
- You can specify an apiVersion so that you can reuse the template without worrying about breaking changes introduced in later versions.
- To make sure your template adheres to suggested best practices, use an **ARM template toolkit (arm-ttk)**.
- Before deploying the template, you can preview changes using the **what-if** operation.
- To deploy a template, you can use the following:
    - Azure Portal
    - Azure CLI
    - Azure Cloud Shell
    - PowerShell
    - REST API
    - Button in GitHub repository
- An application can be defined in a single template or divided into a purpose-specific template (modular files). You can also create a parent template that links all the nested templates.
- You can share the template using **template specs** and manage access using role-based access control (RBAC).
    - **Link template** - a different template file that is linked from the primary template.
    - **Nested template** - an embedded template syntax within the main template.
- You can also get the template of an existing resource group by exporting it.
- With **Azure Pipelines**, you can continuously build and deploy ARM template projects.

Pricing

- You are only charged for the resources deployed by the ARM template.

References:
https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview
https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/overview

Azure Monitor

- Monitoring tool for your Azure resources and applications.
- A service to display the metrics of your resources. You can also configure alerts that send notifications when a threshold is breached.

Features

- Metrics represents a time-ordered set of data points that are published to Azure Monitor.
- The metrics collected are stored for a maximum of 93 days.
- Share your dashboards with other users using Azure Dashboards.
- The data is stored as a set of records in either the Log Analytics or Application Insights.
- You may use **log analytics** to collect and store the data from various log sources and use a custom query language to query them.
- Application Insights helps you detect and diagnose issues across applications and dependencies.
- When important conditions are found in your monitoring data, you can create an **alert rule** to identify and address issues.
- You can export basic usage metrics from your CDN endpoint with diagnostic logs.

Alerts

- An alert rule is a combination of **resources, signal/telemetry,** and **conditions**.
- The **condition** is evaluated independently for each resource.
- Alerts are fired for each resource and consist of the following:
    - **Alert processing rules** - can be used to add or suppress action groups, apply filters, or have the rule run on a predefined schedule.
    - **Action groups** - send notifications or start an automated workflow to notify users that an alert has been triggered.
    - **Alert conditions** - set by the system (fired or resolved).
    - **User response** - it is the response set by the user.
- Types of alerts:
    - **Metric alerts** - evaluate resource metrics at regular intervals.
    - **Log alerts** - enable users to evaluate resource logs at a predefined frequency using a Log Analytics query.
    - **Activity log alerts** - triggered whenever a new activity log event takes place and matches the defined conditions. An example of activity log alerts is Resource Health alerts and Service Health alerts.
    - **Smart detection alerts** - smart detection in an Application Insights resource can provide automatic alerts about potential performance issues and failures in your application.
    - **Prometheus alerts** - used for alerting on the performance and health of Kubernetes and AKS clusters.
- When creating an alert rule, you need to have read and write permissions. You can only access, create, and manage alerts for resources if you have permissions.

- Types of alerts states:
    - **Stateless alerts** - trigger an action whenever the condition is met, regardless of whether it has previously been triggered.
        - It can be configured to log, metric, and activity log alerts.
        - Frequency of notifications:
            - Alert frequency of less than 5 minutes
            - Alert frequency of more than 5 minutes
    - **Stateful alerts** - trigger an action when the condition is met, and remain inactive until the conditions are resolved.
        - It can be configured to both log and metric alerts.
- When an alert is deemed resolved, the corresponding alert rule sends an email or webhook notification of its resolution, and the monitor state in the Azure portal is updated to reflect the resolved status.

Log Analytics

- All log data obtained by Azure Monitor shall be stored in a Log Analytics workspace.
- You can also use Log Analytics workspace to collect log data from on-premises systems and third-party services.
- Configure data retention policies to control how long log data is kept in the workspace.
- Enables you to write queries to sort, filter, and analyze a set of records.
- The language used for searching and analyzing log data is called Kusto Query Language (KQL).
- If the query includes workspaces in 20 or more regions, your query will be blocked from running.
- With a log analytics agent, you can collect logs and performance data from virtual or physical devices outside Azure.
- Build custom dashboards, alerts, and visualizations to gain insights into the log data.
- You can configure data collection from a variety of sources using agents, APIs, or custom data collectors.

Application Insights

- An application performance monitoring (APM) tool to monitor and analyze the performance and usage of applications. It has the following capabilities:
    - **Live Metrics** - real-time monitoring of your deployed application.
    - **Availability** - conduct continuous tests on your application's external endpoint(s) to assess its availability and responsiveness over time.
    - **GitHub or Azure DevOps integration** - integrate telemetry data into the DevOps workflow and tools.
    - **Usage** - gain insights into which features are most used by your users and understand their interactions and usage patterns within your application.
    - **Smart Detection** - proactively analyze telemetry data to automatically detect failures and anomalies.
- Enables you to collect metrics and application telemetry data.
- Monitor diagnostic trace logs from your application.

- You can use Application Insights through Auto-Instrumentation (agent) or by adding the SDK to the application code.
- Supports distributed tracing to enable the search and visualization of the end-to-end flow of a particular execution or transaction.
- The Application Map enables you to identify performance bottlenecks or areas of failure across all components of your distributed application.

Pricing

- You pay for the ingestion and retention of data in Log Analytics (per GB/month).
- You are billed for the number of metrics you have per month.
- There are no charges for health criteria alerts.

Sources:
https://docs.microsoft.com/en-us/azure/azure-monitor/overview
https://azure.microsoft.com/en-us/services/monitor/

Azure Service Health

- Gives you a personalized view of the status of your Azure services and regions.
- Azure Service Health is composed of three services:
    - Azure status - informs you of service outages in Azure.
    - Service Health - helps you to have a customized view of your services' health in a region.
    - Resource Health - provides health information on your Azure resources.
- Active events in service health:
    - Service issues
    - Planned maintenance
    - Health advisories
    - Security advisories
- Track any alerts and issues in real-time and get full reports once resolved.
- You can configure alerts to notify you about active and upcoming service issues.
- Azure users can use Service Health at no additional cost.

Sources:
https://docs.microsoft.com/en-us/azure/service-health/overview
https://azure.microsoft.com/en-us/features/service-health/

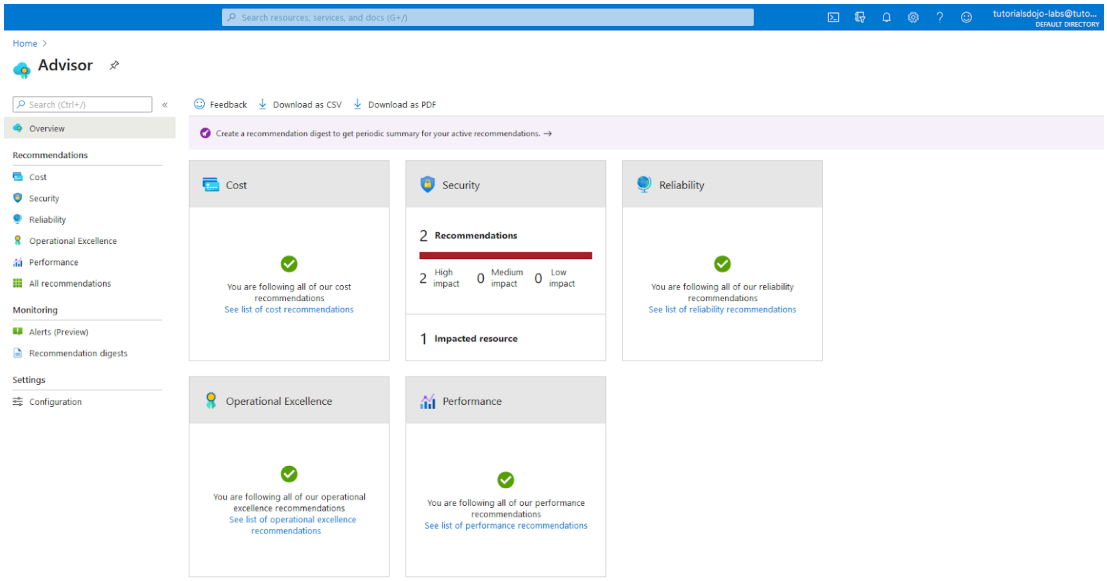
Azure Policy

- Ensure resources are compliant with a set of rules.
- Manage your policies in a centralized location where you can track their compliance status and verify the non-compliant resources.
- Select between **built-in policies** and **custom policies**.
- Implement proper guardrails and assess compliance across the organization
- Policy vs. RBAC
    - A policy maintains compliance with the resource state, while RBAC focuses on controlling user actions at different scopes.
    - Even if the user has access to perform an action, if the result is a non-compliant resource, the policy will still block the create or update option.
- JSON format is used to create a policy.
- You can manage the evaluation and outcome with **resource provider**, and the results are reported to Azure Policy.
- Policy order of evaluation: Disabled, Append/Modify, Deny and Audit
- Azure Policy effects:
    - Append - add additional fields to the requested resource.
    - Audit - a warning event for a non-compliant resource.
    - AuditIfNotExists - audit the resources when the condition is met.
    - Deny - prevents the request before being sent to the Resource Provider.
    - DeployIfNotExists - if the condition is met, it allows you to execute a template deployment.
    - Disabled - allows you to disable a single assignment, rather than disabling all assignments under that policy.
    - Modify - manage tags of resources.
- Determine the assigned resources with **policy assignments**.

Sources:
https://azure.microsoft.com/en-us/services/azure-policy/
https://docs.microsoft.com/en-us/azure/governance/policy/overview

Azure Advisor

- Advisor analyzes your configurations and offers personalized, actionable recommendations.
- It provides relevant best practices to help you improve:
  - Cost
  - Security
  - Reliability
  - Operational Excellence
  - Performance
- Access recommendations are available at no additional cost.



Sources:
https://azure.microsoft.com/en-us/services/advisor/
https://docs.microsoft.com/en-us/azure/advisor/advisor-overview

Azure Blueprints

- Creates templates for standard and repeatable Azure environments that comply with an organization's compliance requirements and operational standards.
- It supports the following resources as artifacts:
    - Role Assignments
    - Policy Assignments
    - Azure Resource Manager (ARM) templates
    - Resource Groups
- It provides **resource locking** to prevent unwanted changes.
- A Blueprint may have its own parameters, but these can only be created if a Blueprint is developed from the REST API rather than Azure Portal.
- Blueprints role: Owner, Contributor, Blueprint Contributor, Blueprint Operator
- With Blueprints, you have a centralized location for environment management, including deployment, versioning, and update.
- If your subscriptions are in the same Azure Blueprint, you can upgrade multiple subscriptions at once.
- You can also use Blueprints to set up resource groups within subscriptions.
- Set up multiple environments within the same shared environment, when you assign a Blueprint to a subscription.

Sources:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview
https://azure.microsoft.com/en-us/services/blueprints/

Azure Compliance Manager

- A dashboard and monitoring tool that summarizes data protection, compliance score, and recommendations.
- It allows you to assign, track, and record compliance and assessment-related activities.
- Recommendations for industry regulations: **GDPR**, **ISO,** and **NIST**
- You can upload and manage artifacts or evidence in a secure repository.

Sources:
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/policy-compliance/regulatory-compliance
https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud

Azure Arc

- A hybrid cloud management platform for managing servers, Kubernetes clusters, and applications across on-premises, multi-cloud, and edge environments.
- Centralize resource management and deploy consistent Azure services anywhere.

Features

- You can deploy Azure services (Azure Policy, Azure Monitor, and Azure Defender) anywhere, allowing them to use the same tools and processes across their entire hybrid cloud estate.
- Enforce policies, audit logs, and detect threats to your servers and Kubernetes clusters.
- GitOps can be used to deploy configurations from Git repositories across one or more clusters.
- Using Azure Policy, you can achieve zero-touch compliance and configuration for Kubernetes clusters.
- Custom locations can be created on top of your Azure Arc-enabled Kubernetes clusters and used as target locations for deploying Azure services instances.
- You can configure Azure VM extensions to monitor, secure, and update your servers using Azure management services.
- You can manage the following resource types in Azure Arc:
    - Servers (Windows and Linux)
    - Kubernetes Clusters
    - Azure Data Services
        - SQL Managed Instance
        - PostgreSQL
    - SQL Server
    - Virtual Machines
        - VMware vSphere
        - Azure Stack HCI
- It can be integrated with other Azure services, allowing users to automate tasks, backup data, and recover from disasters using the following services:
    - Azure Automation
    - Azure Backup
    - Azure Site Recovery
- Using Azure RBAC and Azure Lighthouse, you can delegate access and manage security policies for resources.

Pricing

- You are charged for the license of Azure Arc-enabled SQL Server.
  - Standard Edition
  - Enterprise Edition
- You are charged for the add-on use of Azure Policy (guest configuration), Azure Monitor, and Azure Defender.
- You are charged for the additional Kubernetes Configuration (6 vCPUs are free).
- You are charged for SQL Managed Instance tiers:
  - General Purpose
  - Business Critical

Source:
https://azure.microsoft.com/en-us/products/azure-arc
https://learn.microsoft.com/en-us/azure/azure-arc/overview

Azure RBAC

- A role-based access control service to manage user's access to Azure resources including what they can do with those resources and what areas they can access.
- It is an authorization system based on **Azure Resource Manager**, which provides fine-grained access management of Azure resources.

Concepts

- A role assignment is composed of security principal, role definition, and scope.
    - **Security Principal** - an object representing a user, group, service principal, and managed identity that requests access to Azure resources.
    - **Role Definition** - a list of permissions that can be performed, such as read, write and delete.
    - **Scope** - set of resources to which access applies.

- Attaching a role definition to a user, group, service principal, and managed identity to grant access to a particular scope is called **role assignment**.
- You can attach multiple role assignments since RBAC is an additive model.
- Azure RBAC supports both allow and deny assignments.

Roles

- Azure Roles - Azure RBAC has over 70 built-in roles. The following are the four fundamental Azure roles:
    - Owner
    - Contributor
    - Reader
    - User Access Administrator

- Microsoft Entra built-in roles - Provide access to manage Microsoft Entra ID resources in a directory such as create users, assign administrative roles to others, manage licenses, reset passwords, and manage domains.

Azure Roles	Microsoft Entra Roles
Manage access to Azure resources.	Manage access to Microsoft Entra ID resources.
It supports custom roles.	It supports custom roles.
The scope can be specified at multiple levels (management group, subscription, resource group, resource).	The scope is only at the tenant level.

Role information can be accessed through Azure Portal, CLI, PowerShell, Resource Manager templates, and REST APIs.	Role information can be accessed through Azure Admin Portal, Microsoft 365 Admin Center, Microsoft Graph, and Azure AD PowerShell.

Best Practices

- Use Azure RBAC to segregate duties within your team and only grant the access your users need.
- Limit the number of subscription owners (*max of 3*) to reduce the potential for breach by a compromised owner.
- You can use Microsoft Entra PIM to protect privileged accounts from malicious cyber-attacks.

Source:
https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

SOLUTIONS

Azure Internet of Things (IoT)

- A service that allows you to connect, monitor, and control one or more IoT devices that can communicate with back-end services hosted in the cloud.

Azure IoT Hub

- A PaaS solution that provides complete control over the collection and processing of IoT data.
- To create a complete end-to-end solution, you can integrate the IoT Hub with other Azure services.
    - Azure Event Grid
    - Azure Logic Apps
    - Azure Machine Learning
    - Azure Stream Analytics
- Message routing integration automatically helps you respond to a device-reported state change.
- You can use IoT Hub scaling if you are approaching the message limit on your IoT Hub.

Azure IoT Central

- A SaaS solution that provides a collection of industry-specific application templates.
- You can create your own device template to define the characteristics and behavior of a device.
- Configure custom dashboards to monitor your device's health and telemetry.
- Build custom rules when device telemetry crosses a specified threshold.
- You can apply single or bulk updates by creating jobs.

Azure Sphere

- An IoT security solution that helps you protect your data, privacy, and infrastructure.
- Components:
    - Azure Sphere chip - a microcontroller unit that provides real-time processing capabilities.
    - Azure Sphere OS - an operating system based on Linux that runs on an Azure Sphere chip.
    - Azure Sphere Security Service - it supports certificate-based authentication, automatic software updates, and failure reporting. By default, the data is encrypted at rest.
- The Azure Sphere devices can run on two types of applications:
    - High-level applications for containers.
    - Real-time capable applications (RTApps) for bare metals.

Azure IoT Products

- Azure IoT solution accelerators allow you to customize solution templates for common IoT scenarios.
- Azure IoT Edge enables you to deploy cloud analytics and custom business logic locally on IoT edge devices.
- Create knowledge graphs based on digital models of entire environments using Azure Digital Twins.
- If you need to monitor, analyze, and visualize your IoT data in real-time, you can use Azure Time Series Insights.
- A real-time operating system for IoT devices, powered by MCUs is called Azure RTOS.
- Azure SQL Edge is an optimized SQL database engine for IoT and IoT Edge deployments.

Sources:
https://docs.microsoft.com/en-us/azure/iot-hub/about-iot-hub
https://docs.microsoft.com/en-us/azure/iot-central/core/overview-iot-central
https://azure.microsoft.com/en-us/product-categories/iot/

Azure Big Data

- A service to store and process large amounts of data sets.
- Create big data clusters for Hadoop, Spark, and Kafka with **Azure HDInsight**.
    - Reduce costs by scaling your workloads up and down.
    - Monitor all your clusters with Azure Monitor.
- **Azure Databricks** is based on Apache Spark capabilities that provide an interactive workspace and streamlined workflows.
    - Enables you to read data from multiple sources and use Spark to create breakthrough insights.
- **Azure Synapse Analytics** is a data warehousing and big data analytics service.
    - Allows you to ingest, prepare, manage, and serve data for BI and ML needs..

AZ-900 Exam Notes:

Azure Synapse Analytics is formerly known as *Azure SQL Data Warehouse*. It includes SQL pool as the data warehouse solution. This platform also combines data exploration, ingestion, transformation, preparation, and a serving analytics layer.

- You can use **Azure Event Hubs** for big data streaming and event ingestion service.
    - Enables you to receive and process millions of events per second.
- **Azure Stream Analytics** provides you real-time analytics and a complex event-processing engine.
    - Simultaneously analyze and process large volumes of streaming data from multiple sources.

Sources:
https://docs.microsoft.com/en-us/azure/data-lake-analytics/data-lake-analytics-overview
https://docs.microsoft.com/en-us/azure/hdinsight/hdinsight-overview
https://docs.microsoft.com/en-us/azure/databricks/scenarios/what-is-azure-databricks
https://docs.microsoft.com/en-us/azure/synapse-analytics/sql-data-warehouse/sql-data-warehouse-overview-what-is
https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-about
https://docs.microsoft.com/en-us/azure/stream-analytics/stream-analytics-introduction

Azure Machine Learning

- A service to train, deploy, automate, manage, and track machine learning models.
- Azure ML offers **Basic** and **Enterprise** editions.
- You can use **Azure ML SDK for Python**, **Azure ML Studio**, and **ML CLI** to manage your deployed models.
- You can automate and accelerate the ML lifecycle using **MLOps**.
- Azure ML **designer** allows you to visually connect (drag-and-drop) datasets and modules without writing any code.
- ML **pipelines** provide a complete logical workflow and an ordered sequence of steps.
- **AutoML** uses the target metric you specify to train and tune a model.
- **Azure Cognitive Services** enables developers to build cognitive intelligent applications without having AI or data science skills. The following are the Azure Cognitive REST APIs that you can use:
    - Vision, Speech, Language, Search, and Decision APIs.

Azure Bot Service

- Build a bot that uses natural language and speech capabilities to communicate with your users.
- You can integrate Bot Service across multiple communication channels such as Microsoft Teams, Slack, and Facebook Messenger.
- Use Bot Framework Composer if you need a visual editing canvas for conversation flows.
- With Bot Framework SDK, you can create a bot that uses speech, understands natural language, and handles questions and answers.

Sources:
https://docs.microsoft.com/en-us/azure/machine-learning/overview-what-is-azure-ml
https://azure.microsoft.com/en-us/services/machine-learning/

Azure Serverless

- Enables you to build applications without managing infrastructure.

Azure Functions

- Enables you to run a small piece of code to do a task.
- A single task is performed for each invocation.
- Supported languages: C#, Java, JavaScript, Python, and PowerShell
- You can run your code based on the HTTP requests or schedule when your function runs.
- You are only charged for the time you run your code.

Azure Logic Apps

- Allows you to automate your workflows without writing a single line of code.
- Build your workflow using a logic app designer.
- Components:
    - **Workflow** helps you create a series of steps for your logic app.
    - **Managed connectors** allow you to access and work with your data.
    - **Trigger** is the first step to run your logic app.
    - **Actions** are steps that happen after the trigger and perform tasks in the workflow of your logic app.
    - **Enterprise Integration Pack** allows you to create an automated, scalable enterprise integration workflow.

Azure Event Grid

- A network to route events between applications
- Route custom events to different endpoints.
- Components:
    - **Events** - The information that happened in the system.
    - **Event sources** - Where the event comes from.
    - **Topics** - It provides an endpoint where the publisher sends events.
    - **Event subscriptions** - Filter the events that are sent to you.
    - **Event handlers** - The service that will process the event.
- You must provide a SAS token or key authentication before publishing a topic.

Sources:
https://docs.microsoft.com/en-us/azure/azure-functions/functions-overview
https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-overview
https://docs.microsoft.com/en-us/azure/event-grid/overview

Azure DevOps

- A service that offers a set of tools for planning, building, and deploying applications.

Features

- **Azure Boards**
  - It allows you to track features, user stories, tasks, and bugs associated with your project.
  - You can also customize your dashboards and track progress easily during your project lifecycle.
- **Azure Pipelines**
  - A CI/CD service that helps you build and test your code automatically.
  - Enables you to deploy your codes to multiple targets at the same time.
- **Azure Repos**
  - Store and manage your codes using a set of version control tools.
  - It supports a version control system to track every change you made in your code.
- **Azure Test Plans**
  - A test management solution that supports end-to-end traceability.
  - Run tests simultaneously using exploratory test sessions.
- **Azure Artifacts**
  - Allows you to create, host, and share your code/packages with your team or other organization.
  - You can share your code by storing Maven, npm, NuGet, and Python packages together.

Azure DevTest Labs

- A self-service sandbox that helps you create Dev/Test environments.
- You can quickly provision different environments by using reusable templates and artifacts.
- It also has a cost management feature to track your VMs and PaaS resources to stay within the allocated budget.

GitHub Actions for Azure

- Automates software development workflows.
- A **workflow** enables you to build, test, package, release, and deploy projects on Azure.
- Each workflow is composed of individual actions that run after a particular event. These **actions** are defined in YAML files.
- You can find all the available actions in the Marketplace for GitHub Actions for Azure.

Sources:
https://docs.microsoft.com/en-us/azure/devops/user-guide/what-is-azure-devops?view=azure-devops
https://azure.microsoft.com/en-us/services/devops/

OTHER AZURE NOTES

Azure Service Bus

- A fully managed message broker service.
- It allows you to decouple applications and services.
- Provides a reliable and secure platform for asynchronous data and state transfer.
- Enables you to deliver messages to multiple subscribers and fan-out message delivery to downstream systems.

Features

- **Message Sessions** for implementing first in, first out (FIFO) and request-response patterns to ensure the order of messages in the queue.
- **Autoforwarding** allows you to remove messages from a queue or subscription and transfer it to a different queue or topic (*must be in the same namespace*).
- A dead-letter queue holds the messages that can't be delivered to any receiver.
- It supports a scheduled delivery of messages.
- You can set aside a message using **message deferral**.
- With **client-side batching**, you can delay the sending of messages for a certain period of time.
- **Autodelete on idle** enables you to set an idle interval to automatically delete a queue. Five minutes is the minimum duration.
- **Duplicate detection** allows you to resend the same message and discard any duplicate copies.
- You can continue the operation of your environment in a different region or datacenter with **geo-disaster recovery**.

Components

- A container for all messaging components is called a **namespace**.
- You send and receive messages from **queues** (*point-to-point communication*).
- Multiple queues and topics are supported in a single namespace, and namespaces often serve as application containers.
- **Topics** also allow you to send and receive messages and mainly used in publish/subscribe scenarios. It contains multiple independent subscriptions called **entities**.
- To filter specific messages, you can use rules and filters to define conditions that trigger optional actions.

Security

- **Shared Access Signatures (SAS)** guards access to Service Bus based on authorization rules.
- You can authenticate and authorize an application to access Service Bus entities such as queues, topics, subscriptions, and filters using **Microsoft Entra ID**.

- Create a security identity using **Managed identities for Azure resources** and associate that identity with access-control roles to grant custom permissions for accessing specific Azure resources.

Pricing

- You are charged based on the following:
  - The number of operations
  - The number of AMQP connections or HTTP calls
- For hybrid connections, you are charged based on the number of listeners.
- With Windows Communication Foundation (WCF) relays, you are charged based on the message volume and relay hours.

Sources:
https://azure.microsoft.com/en-us/services/service-bus/
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-messaging-overview

COMPARISON OF AZURE SERVICES

Azure Virtual Machines vs Web App

	Azure Virtual Machine	Azure Web App
Description	Infrastructure as a service, if you need to have full control over your computing environment.	Platform as a service, it allows you to integrate the app without managing the underlying infrastructure.
Deploy	Uses an OS image.	Uses a runtime stack.
State Management	Stateful or stateless	Stateless
Autoscaling	You need to use VM scale sets to support autoscaling in virtual machines.	Autoscaling is a built-in service in App Service.
Scale Limit	1000 nodes per scale set for platform image and 600 nodes per scale set for custom image	20 instances and 100 with App Service Environment
Traffic Distribution	Distribute the incoming network traffic using Azure load balancer.	Load balancing is integrated into App Service.
Architecture Styles	The supported architecture styles are N-Tier and Web-Queue-Worker.	The supported architecture styles are N-Tier and Big compute (HPC).

Azure Container Instances (ACI) vs Azure Kubernetes Service (AKS)

	ACI	AKS
Description	Run containers without managing servers.	Orchestrate and manage multiple container images and applications.
Deployment	For event-driven applications, quickly deploy from your container development pipelines, run data processing, and build jobs.	Uses clusters and pods to scale and deploy applications.
Web Apps (Monolithic)	Yes	Yes
N-Tier Apps (Services)	Yes	Yes
Cloud-Native (Microservices)	Yes	Yes, recommended for Linux containers
Batch/Jobs (Background tasks)	Yes	Yes
Use cases	• Dev/Test scenarios • Task automation • CI/CD agents • Small/scale batch processing • Simple web apps	• Containers and application configuration portability • Enables you to select the number of hosts, size, and orchestrator tools • Transfer container workloads to the cloud without changing your current management practices.
Major Difference	You should use AKS if you need full container orchestration, such as service discovery across multiple containers, automatic scaling, and coordinated application upgrades.	

Azure Functions vs Logic Apps vs Event Grid

	Functions	Logic Apps	Event Grid
Service	Serverless Compute	Serverless Workflows	Serverless Events
Description	Run a small piece of code to do a task	Automate your workflows without writing a single line of code.	Route custom events to different endpoints.
Features	• Serverless applications • Choice of language • Bring your own dependencies • Integrated security • Flexible development tools • Stateful serverless architecture	• Built-in and managed connectors • Control your workflows • Manage or manipulate data • App, data and system integration • Enterprise application integration • B2B communication in the cloud or on-premises	• Advanced filtering • Fan-out to multiple endpoints • Supports high-volume workloads • Built-in Events • Custom Events
Development	Code-first	Designer-first	Event Source and Handlers
Use case	Big data processing, microservices reference architecture, and serverless messaging	Connect legacy, modern, and cutting-edge systems with pre-built connectors.	Serverless application architectures, Ops Automation, and Application integration
Pricing	You are only charged for the time you run your code.	You are charged for the execution of triggers, action, and connectors.	You are charged for each operation, such as ingress events, advanced matches, delivery attempts, and management calls.

Azure Scale Set vs Availability Set

	Scale Set	Availability Set
Description	A group of identically configured virtual machines spread across fault domains.	A group of discrete virtual machines spread across fault domains.
Workloads	Use Scale Set for unpredictable workloads (autoscale).	Use Availability Set for predictable workloads.
Domain default	Has 5 fault domains and 5 update domains by default	Has 3 fault domains and 5 update domains by default
Configuration	Virtual machines are created from the same image and configuration.	Virtual machines are created from different images and configurations.
Distribution	Virtual machine scale sets can be distributed within a single datacenter or across multiple data centers.	Virtual machines are automatically distributed within a data center.
Number of VMs	Scale sets can increase the number of virtual machines based on demand.	You can only add a virtual machine to the availability set when it is created.
Pricing	Scale sets have no additional charge. You only pay for the computing resources.	Availability set has no additional charge. You only pay for the computing resources.

Azure Blob vs Disk vs File Storage

	Blob Storage	Disk Storage	File Storage
Type of storage	Object storage to store all types of data formats.	Block storage for virtual machines.	File system across multiple machines.
Max Storage Size	Same as maximum storage account capacity	65,536 GiB for ultra disk 32,767 GiB for standard and premium drives	Scale up to 100 TiB
Max File Size	190.7 TiB for block blob 195 GiB for append blob 8 TiB for page blob	Equivalent to the maximum size of your volumes	4 TiB for a single file
Performance (Throughput)	500 requests per second for a single blob	Up to 2000 MBps per disk.	6,204 MiB/s for egress 4,136 MiB/s for ingress
Data Accessing	Objects can be accessed via HTTP/HTTPs.	A single virtual machine in a single AZ.	Share your files either on-premises or in the cloud.
Encryption Methods	Encrypt your data using Azure SSE (256-bit AES)	SSE by storage service and ADE for OS and data disks.	Encrypt your data using Azure SSE (256-bit AES)
Backup and Restoration	Versioning, snapshots and object replication	You can back up your managed disks at any point in time using snapshots.	Uses file share snapshots
Pricing	You are billed based on the stored data per month, operations performed, data transfer, and redundancy.	You pay for the disk size, snapshots, and number of transactions.	You pay for the provisioned GiB per month and the number of servers connected to the cloud endpoint.
Use Cases	Static website, media and log files, backups, analytics workloads	Boot volumes and transaction-intensive workloads	Central location of your files, monitoring logs and applications

Locally Redundant Storage (LRS) vs Zone-Redundant Storage (ZRS) vs (GRS)

	Locally-Redundant Storage (LRS)	Zone Redundant Storage (ZRS)	Geo-redundant storage (GRS)
Replication	Replicates your data 3 times within a single physical location synchronously in the primary region.	Replicates your data across 3 Azure Availability Zones synchronously in the primary region	Replicates your data in your storage account to a secondary region
Redundancy	Low	Moderate	High
Cost	Provides the least expensive replication option	Costs more than LRS but provides higher availability	Costs more than ZRS but provides availability in the event of regional outages
Percent durability of objects over a given year	At least 99.999999999% (11 9's)	At least 99.9999999999% (12 9's)	at least 99.99999999999999% (16 9's)
Availability SLA for read requests	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier) for GRS At least 99.99% (99.9% for cool access tier) for RA-GRS
Availability SLA for write requests	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)
Available if a node went down within a data center?	Yes	Yes	Yes
Available if the entire data center (zonal or non-zonal) went down?	No	Yes	Yes

Available on region-wide outage in the primary region?	No	No	Yes
Has read access to the secondary region if the primary region is unavailable?	No	No	Yes
Supported storage account types	General-purpose v2 General-purpose v1 Block blob storage Blob storage File storage	General-purpose v2 Block blob storage File storage	General-purpose v2 General-purpose v1 Blob storage

Azure Load Balancer vs App Gateway vs Trentraaffic Manager

	Load Balancer	App Gateway	Traffic Manager
Service	Network load balancer.	Web traffic load balancer.	DNS-based traffic load balancer.
Network Protocols	Layer 4 (TCP or UDP)	Layer 7 (HTTP/HTTPS)	Layer 7 (DNS)
Features	Internal and public load balancer	SSL/TLS termination and cookie-based session affinity	Traffic-routing methods, Traffic manager profile, endpoint monitoring options
Routing	Source/Destination (IP & Port), and Protocol	URI path or Host headers	Offers various routing methods such as: Priority, Weighted, Performance, Geographic, Multivalue and Subnet
Security	Integrate Azure Firewall with Standard LB.	Web Application Firewall	Use locks to protect your traffic manager profile.

Network Security Group (NSG) vs Application Security Group

	Network Security Group	Application Security Group
Description	A network security group is used to enforce and control network traffic.	An application security group is an object reference within an NSG.
Features	Controls the inbound and outbound traffic at the subnet level.	Controls the inbound and outbound traffic at the network interface level.
Rules	Rules are applied to all resources in the associated subnet.	Rules are applied to all ASGs in the same virtual network.
Direction	Has separate rules for inbound and outbound traffic.	Has separate rules for inbound and outbound traffic.
Limits	NSG has a limit of 1000 rules.	ASGs that can be specified within all security rules of an NSG have a limit of 100 rules.
Action	Supports `ALLOW` and `DENY` rules.	Supports `ALLOW` and `DENY` rules.
Constraints	You are not allowed to specify multiple IP addresses and IP address ranges in the NSG created by the classic deployment model.	You are not allowed to specify multiple ASGs in the source or destination.

Microsoft Defender for Cloud vs Microsoft Sentinel

	Microsoft Defender for Cloud	Microsoft Sentinel
Description	Unified infrastructure security management system	Intelligent security analytics and threat intelligence service.
Category	Cloud Security Posture Management (CSPM) / Cloud Workload Protection Platform (CWPP)	Security Information Event Management (SIEM) / Security Orchestration Automated Response (SOAR)
Function	Provides security alerts, scores, vulnerability assessment, recommendations, and security posture management.	Provides alert detection, threat visibility, proactive hunting, and threat response.
Features	• Microsoft Defender ATP Integration • Network map • Virtual Machine Behavioral Analytics • Adaptive network hardening • Regulatory Compliance dashboard & reports • Missing OS patches assessment • Security misconfigurations assessment • Endpoint protection assessment • Disk encryption assessment • Third-party vulnerability assessment • Network security assessment	• Custom analytics rules • Multiple Workspace View • Azure Monitor Workbooks Integration • Security playbook • Investigation Graph • Hunting search and query tools
Provides Security Recommendation?	Yes	No
Threat Response Management	Manual	Automated
Integration	You may use the Microsoft Defender for Cloud to provide Microsoft Sentinel with more information to identify, investigate, and remediate threats.	

Azure Policy vs Azure Role-Based Access Control (RBAC)

	Azure Policy	Role-based Access Control (RBAC)
Description	Ensure resources are compliant with a set of rules.	Authorization system to provide fine-grained access controls.
Focus	Policy is focused on the properties of resources.	RBAC focuses on what resources the users can access.
Implementation	You specify a set of rules to prevent over-provisioning of resources.	You grant permission on what users can create.
Default access	By default, rules are set to `ALLOW`.	By default, all access is denied.
Scope	Policy within the resource group or subscription.	Grant access to users or groups within a subscription.
Integration	Both services work hand-in-hand to provide governance around your environment.	

Microsoft Entra ID vs Azure Role-Based Access Control (RBAC)

	Microsoft Entra	Azure RBAC
Description	An identity and access management service that helps you access internal and external resources.	An authorization system that manages user's access to Azure resources including what they can do with those resources and what areas they can access.
Focus	Grants permissions to manage access to Microsoft Entra ID resources.	Grants permissions to manage access to Azure resources.
Scope	Tenant level	Specify at multiple levels (management group, subscription, resource group, and resource)
Roles	Important Microsoft Entra built-in roles: 1. Global Administrator – manage access to all the administrative features in Microsoft Entra ID. 2. User Administrator – create and manage different types of users and groups in Azure. 3. Billing Administrator – it can manage subscriptions, support tickets, make purchases, and monitor service health. Supports custom roles. You can assign multiple roles to a user.	Fundamental Azure RBAC built-in roles: 1. Owner – full access to all Azure resources. 2. Contributor – create and manage all types of resources in Azure. 3. Reader – a user with this role can only view Azure resources 4. User Access Administrator – it has permissions to manage user access to all types of resources. Supports custom roles in P1 and P2 licenses. You can assign multiple roles on a user.
Role information	You can access the role information in the Azure Portal, Microsoft 365 admin center, Microsoft Graph, and AzureAD PowerShell.	You can access the role information in the Azure Portal, CLI, PowerShell, Resource Manager templates, and REST API.
Pricing	Microsoft Entra ID has three editions: Free, P1, and P2. For the P1 and P2 licenses, you are charged on a monthly basis.	Azure RBAC is free and included in your Azure subscription.

AWS vs AZURE SERVICES

To help you learn the different Microsoft Azure services, we've come up with this **AWS vs Azure services comparison**. If you already have some background in AWS (or cloud computing in general) either through work experience or AWS certifications then you won't have a hard time learning Microsoft Azure.

The following sections show the related AWS and Azure services based on function and capabilities. Each AWS service in this list has a similar service in Azure.

Compute

Amazon EC2 vs. Azure Virtual Machine

	Amazon EC2	Azure VM
Description	A virtual server that supports both Linux and Windows operating systems.	A Linux-based / Windows-based virtual server that you can provision.
Configurations	EC2 configurations are called **instance types.**	Virtual machine configurations are called **VM series.**
Images	**AMI** or operating systems are stored in a root volume.	**VM images** or operating systems are stored in an OS disk.
OS Volumes	Root volume type: General Purpose SSD (gp2), Provisioned IOPS SSD (io1 and io2), and Magnetic (standard)	OS disk type: Standard HDD, Standard SSD, and Premium SSD
Storage Volumes	Persistent storage volumes for your data using **Elastic Block Storage volumes.**	Persistent storage volumes for your data using **Azure Disk.**
Encryption	Encrypt EBS volumes with **AWS KMS.**	Encrypt OS and data disks with **Azure SSE.**

Script	Add a script that will be run on an instance boot called **user-data.**	Add a script that will be run into the virtual machine while it is being provisioned called **custom data.**
Security	**Security group** enables you to create security rules to allow the traffic going to your instances.	**NIC network security group** enables you to create security rules to allow or deny the traffic going to your virtual machine.
Monitoring	Monitor the performance of your EC2 instances with **Amazon CloudWatch.**	Monitor the performance of your virtual machines with **Azure Monitor.**
Network	All EC2 instances are launched in an isolated network called **VPC**.	All virtual machines are launched in an isolated network called **VNet.**

Other Compute Services Comparison

- **AWS Batch** and **Azure Batch** - provision tens, hundreds, or thousands of compute resources based on the job requirements.
- **AWS Auto Scaling** and **Azure VM Scale Sets** - increase or decrease the number of your resources as demand changes.
- **AWS Lambda** and **Azure Functions** - a serverless computing platform to run code in response to events.
- **Amazon ECS, AWS Fargate,** and **Azure Container Instances** - run containerized applications without managing any servers.
- **Amazon ECR** and **Azure Container Registry** - a repository to store and manage container images.
- **Amazon EKS** and **Azure Kubernetes Service** - simplify the management of your containerized applications across a cluster of nodes.

Storage

Amazon S3 vs. Azure Blob

Feature	Amazon S3	Azure Blob
Description	Object storage service of AWS	Object storage service of Azure
Components	S3 is composed of **buckets** and **objects**.	Blob storage resources: **Storage Account, Container**, and **Blob**
Max File Size	The maximum file size for each object is 5 TB.	The maximum file size for each blob: Block (190.7 TiB), Append (195 GiB), and Page (8 TiB).
Max Storage Size	Bucket capacity is virtually unlimited.	Single blob container size is the same as the maximum storage account capacity.
Tiers	S3 tiers: Standard, Standard-IA, One Zone-IA, Intelligent-Tiering, Glacier, and Glacier Deep Archive	Blob tiers: Hot, Cool, and Archive.
Durability	Data durability across multi-AZ is 11 9's.	Data durability across LRS (11 9's), ZRS (12 9's), GRS, and RA-GRS (16 9's).
Replication	Copy objects across S3 buckets in different AWS Regions using **Cross-Region Replication.**	Copy block blobs between a source and destination account using **Object Replication**.
CDN	Cache content from a static website with **Amazon CloudFront.**	Cache content from a static website with **Azure CDN.**
Encryption	Encrypt objects using Client-Side and Server-Side Encryption.	Encrypt storage account using Microsoft- and Customer-managed keys.

Endpoint	Endpoint: <tutorialdojo>.s3.<region>.amazonaws.com	Endpoint: <tutorialdojo>.blob.core.windows.net

Other Storage Services Comparison

- **Amazon EBS** and **Azure Disk** - a disk storage to store your data and operating system.
- **Amazon EFS** and **Azure Files** - create and configure file systems and share your files across multiple resources.
- **AWS Storage Gateway** and **Azure StorSimple** - simplify storage management by using a hybrid cloud storage solution.
- **AWS Snow Family** and **Azure Data Box** - transfer petabytes and exabytes of data to the cloud.

Databases

Amazon RDS vs. Azure SQL

	Amazon RDS	Azure SQL
Description	Configure and scale a relational database in the cloud.	Fully managed and intelligent relational database in the cloud.
DB Engines	Database engines: Amazon Aurora, PostgreSQL, MySQL, Oracle, MariaDB, and Microsoft SQL Server	Database Engine: Microsoft SQL Server
Serverless	The serverless database is called **Amazon Aurora Serverless**.	The serverless database is called **Azure SQL Database serverless.**
Templates	DB templates are Free Tier, Dev/Test, and Production.	DB templates are Basic, Standard, and Premium.
Performance	DB performance: Standard, Memory-Optimized, and Burstable Classes	DB performance: General Purpose, Hyperscale, and Business Critical
High Availability	Eliminate a single point of failure with **Multi-AZ deployment.**	Eliminate a single point of failure with **zone redundant configuration.**
Secondary DB	Create readable secondary databases in the same or different regions with **read replicas.**	Create readable secondary databases in the same or different regions with **active geo-replication.**
Backup	Automated backups retention period up to 35 days.	Automated backups retention period up to 35 days.

Monitoring	Monitor the metrics of your database with **Amazon CloudWatch.**	Monitor the metrics of your database with **Azure Monitor.**
Endpoint	Endpoint: rds.<region>.amazonaws.com	Endpoint: <server_name>.database.windows.net

Other Database Services Comparison

- **Amazon DynamoDB** and **Azure Cosmos DB** - a database model for document and key-value stores.
- **Amazon Redshift** and **Azure Synapse Analytics** - a cloud data warehouse service used for analytics and business intelligence tools.
- **Amazon ElastiCache** and **Azure Cache for Redis** - an in-memory-based caching service to improve the performance of your existing database.
- **AWS DMS** and **Azure DMS** - automate the migration of your data from multiple databases.

Networking

Amazon VPC vs. Azure VNet

	Amazon VPC	Azure VNet
Description	A virtual network service in AWS where you can launch your resources.	An isolated network service in Azure to run your VMs and applications.
Default	Default VPC in each region.	Default VNet is not existing.
Reserved IP address	AWS reserves 5 IP addresses within each subnet.	Azure reserves 5 IP addresses within each subnet.
Subnets	Subnets are from **/28** to **/16.**	Subnets are from **/29** to **/8.**
Subnet Types	Subnet types: Private, Public and VPN-only	Subnet types: Private, Public and Gateway
Static IP address	You can assign a static IPv4 to your resources with **Elastic IP addresses.**	You can assign a static IPv4 and IPv6 address to your resources.
Security	Secure your network using **NACLs** and **Security Groups**.	Secure your network using **NSGs** and **ASGs**.
Gateways	Types of gateways: Internet Gateway, Egress-only, NAT Gateway, Virtual Private Gateway, and Customer Gateway	Types of gateways: VPN Gateway and ExpressRoute Gateway
Route Table	By default, subnets are automatically associated with the main route table.	Route tables are not automatically associated with your subnets.
Peering	A **VPC peering** enables communication between two VPCs.	A **VNet peering** enables communication between virtual networks.

Other Networking Services Comparison

- **AWS VPN Gateway** and **Azure VPN Gateway** - secure connection from your on-premises network to your cloud private network.
- **Amazon Route 53** and **Azure DNS** - helps you manage your DNS records.
- **AWS Direct Connect** and **Azure ExpressRoute** - dedicated private connection between the cloud provider and your data center.
- **Amazon ELB: NLB** and **Azure Load Balancer** - layer 4 load balancer for TCP and UDP protocols.
- **Amazon ELB: ALB** and **Azure Application Gateway** - load balancer for layer 7 traffic (SSL termination, cookie stickiness, and round-robin routing).

Security and Identity

AWS Identity & Access Management (IAM) vs. Microsoft Entra ID & RBAC

	AWS IAM	Microsoft Entra ID & RBAC
Description	Create and manage users, groups, roles, and policies in your account.	Create users and groups with **Microsoft Entra ID**.
MFA	Secure your account by activating MFA.	Secure your account by activating MFA in Microsoft Entra ID.
Groups	IAM groups allow you to organize a large number of IAM users.	Microsoft Entra ID allows you to assign a large number of users to groups.
Roles	Delegate administrator roles using identity-based policies.	Delegate administrator roles using Microsoft Entra ID.
Access	Access resources only in the AWS console.	Microsoft Entra ID supports **hybrid identity** to access resources in the cloud or on-premises.
Monitoring	Monitor the status of your user accounts with a **credential report.**	Monitor the security and usage patterns of your environm ent with **Microsoft Entra monitoring and health**.
Domain	Unique account sign-in page URL: https://<My_AWS_Account_ID>.signin .aws.amazon.com/console/	The domain name of Microsoft Entra tenant: <Azure_Tenant>.onmicrosoft.com
Permission	Grant users temporary permission using **IAM roles.**	**RBAC** enables you to grant users certain roles to access specific resources.
Policy	A collection of permissions written in JSON is called **IAM policies.**	A collection of permissions written in JSON is called **role definition** in RBAC.

Multiple roles	You can assign multiple permissions to an IAM user.	You can assign multiple roles to a resource group with RBAC.

Other Security and Identity Services Comparison

- **AWS WAF** and **Azure WAF on Application Gateway** - protects web applications from common exploits and vulnerabilities.
- **AWS Shield** and **Azure DDoS Protection** - protect your resources from denial of service attacks.
- **AWS KMS** and **Azure Key Vault** - create and manage the keys used to encrypt your data.
- **AWS Trusted Advisor** and **Azure Advisor** - provides recommendations in operational excellence, security, performance, reliability, and cost.

Sources:
https://aws.amazon.com/
https://docs.microsoft.com/en-us/azure/architecture/aws-professional/

FINAL REMARKS

If you are a student or a non-technical person who wants to pursue the IT industry, cloud computing is one of the most in-demand skills that will help you become a competitive candidate. Microsoft Azure is one of the top cloud service providers that can help you build, deploy, and manage applications quickly. Creating new solutions for startups to enterprise companies requires skills and knowledge. Since this is an emerging technology, a lot of people aspire to become Microsoft Azure Certified. These certifications are investments in yourself and also to improve your skills. Everyone in the community acknowledges Microsoft Certifications.

We at Tutorials Dojo are dedicated to help you upgrade your skills and your career. We have various collections of technical blogs, guides, cheat sheets, and practice exams that are constantly updated based on our experiences and our students' feedback. If you are preparing in your journey to become an AZ-900 certified, we provide valuable content to achieve the results you desire.

If you are reading this right now, we are very happy to help you on your journey towards the cloud. Thank you for choosing Tutorials Dojo, and we hope you'll continue supporting us. If you wish to validate what you have learned so far, now is a great time to check out our AZ-900 Microsoft Azure Fundamentals Practice Exams. You can also try the free sampler version of our full practice test course here. We also wish you the very best in your future Azure certification exams.

Good luck on your exam, and we hope to see you in our other practice test courses.

ABOUT THE AUTHORS

Jon Bonso

Born and raised in the Philippines, Jon is the Co-Founder of **Tutorials Dojo**. Now based in Sydney, Australia, he has over a decade of diversified experience in Banking, Financial Services, and Telecommunications. He's 8x AWS Certified and has worked with various cloud services such as Google Cloud, and Microsoft Azure. Jon is passionate about what he does and dedicates a lot of time creating educational courses. He has given IT seminars to different universities in the Philippines for free and has launched educational websites using his own money and without any external funding.

Gerome Pagatpatan

Gerome is certified in AWS, Azure, and Oracle. After graduating from college with a degree in Electronics Engineering, he decided to pursue the field of Information Technology through self-study. He is passionate about education, and now it's his turn to share his knowledge, experiences, and passion in Cloud Computing.