
# Companion Guide

AZ-900 Bootcamp: Microsoft Azure Fundamentals

# Contents

# GETTING STARTED

## Course Overview

This AZ-900 bootcamp course covers all AZ-900 exam objectives and sub-objective, and ensures you are ready for the AZ-900 Microsoft Azure Fundamentals exam. The exclusive interactive hands-on labs from labIT PRO add a dimension to this course that you won't find with any other course on Udemy.

Even if you have no Azure experience, this course will prepare you for the AZ-900 exam. If you are looking for an entry point to Microsoft Azure, this AZ-900 exam prep course is the way to go!

## How to Use This Guide

This guide is designed to be a COMPANION to the actual course. More specifically, this guide provides an overview of each course topic, touching on some key pieces of information you should know, while the associated course lecture provides deeper detail. I recommend keeping this guide handy as you work through the course lectures, so you can take notes as you study.

After you've completed the course and taken all your notes in this guide, read through this guide, along with those notes. Re-watch any lecture that you feel you need more understanding of. Once you've done that, you can schedule your exam.

***NOTE:*** *Studying this companion guide, alone, IS NOT enough to pass the exam! It's designed to provide some structure to the course itself. The lectures in the course contain crucial information that's necessary to pass the exam. DO NOT skip the course lectures.*

# LEARNING TOOLS

This AZ-900 exam-prep course includes several fun activities, including flash cards, crossword puzzles, lab simulations, and more. Take advantage of them. You can do them whenever you like. Try them before you complete any of the lectures or try them AFTER you've completed your study. The idea with them is to make learning a little less tedious.

# BASIC CLOUD CONCEPTS

## Cloud Computing

Cloud computing is the delivery of compute services, like servers, storage, databases, networking over the Internet, allowing you to take advantage of economy of scale. When leveraging cloud computing resources, you generally pay only for the services that you use. This helps lower operating costs, while allowing you to run your infrastructure more efficiently, and scale as needed.

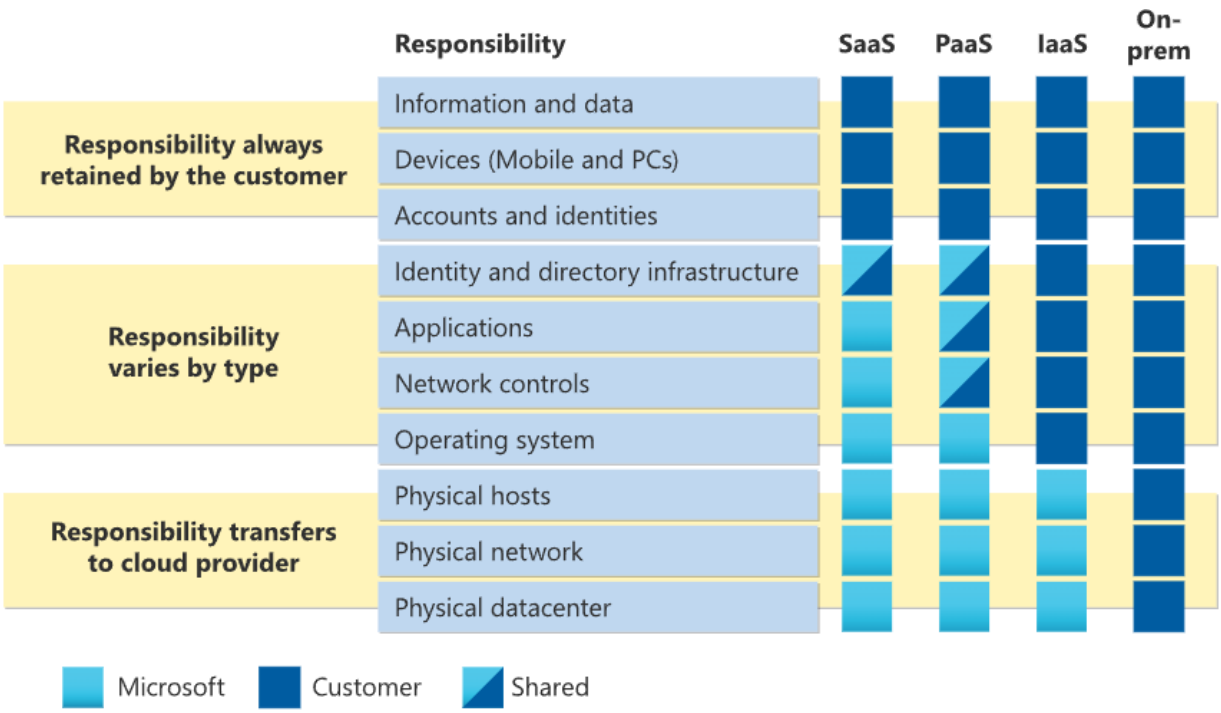
Organizations often move to the cloud to reduce CapEx costs, improve scalability, improve productivity, enhance performance, and increase security.

**Notes:**

_____
_____
_____
_____

## Shared Responsibility Model

The shared responsibility model breaks out which security tasks are handled by a cloud provider and which tasks are handled by the customer. Responsibilities will vary, depending on whether the particular workload is hosted on a SaaS platform, a PaaS platform, IaaS, or in a physical on-prem datacenter.




This graphic shows that in an on-premises datacenter, the customer owns the whole stack. However, when you move to the cloud, some of those responsibilities transfer to the cloud vendor.

It important to note that in ALL cloud deployments, the CUSTOMER owns the data and identities. The customer is also responsible for protecting their security. The customer is also responsible for maintaining any on-prem resources.

Regardless of the type of deployment, the customer is always responsible for data, endpoints, accounts, and access management.

**Notes:**

## Cloud Models

The three key deployment models for cloud computing include public cloud, private cloud, and hybrid cloud. Each model offers specific benefits.

**Public cloud**

In a public cloud deployment, services are offered over the public internet. These services are available to customers who wish to purchase them. The cloud resources, like servers and storage, are owned and operated by the cloud service provider.

**Private cloud**

In a private cloud, compute resources are accessed exclusively by users from a single business or organization. You can host a private cloud physically in your own on-prem datacenter, or it can be hosted by a third-party cloud service provider.

**Hybrid cloud**

A hybrid cloud is a complex computing environment. It combines a public cloud and a private cloud by allowing data and applications to be shared between them. This type of cloud deployment is often utilized by large organizations.

**Notes:**

_____
_____
_____
_____
_____
_____

## Consumption-Based Model

The consumption-based model refers to the way in which organizations only pay for the resources they use.

The consumption-based model offers the following benefits:

- No upfront costs
- No need to purchase or manage infrastructure
- Customer pays for resources only when they are needed
- Customer can stop paying for resources that are no longer needed

**Notes:**

_____
_____
_____
_____
_____
_____

## Benefits of Cloud Computing

Cloud computing offers several key advantages over a physical environment:

- **High availability:** Cloud-based apps can provide a continuous user experience with virtually no downtime.
- **Scalability:** Apps in the cloud can scale vertically and horizontally. When scaling vertically, compute capacity is added by adding RAM or CPUs to a virtual machine. When scaling horizontally, compute capacity is increased by adding instances of resources, such as adding VMs to a configuration.
- **Elasticity:** Allows you to configure apps to autoscale so they always have the resources they need.
- **Agility:** Deploy and configure cloud-based resources quickly as requirements change.
- **Geo-distribution:** Deploy apps to regional datacenters so that customers always have the best performance in their specific region.
- **Disaster recovery:** Cloud-based backup services, data replication, and geo-distribution allow you to deploy apps and know that their data is safe in the event of disaster.

**Capital Expenses vs. Operating Expenses**

Organizations have to think about two different types of expenses:

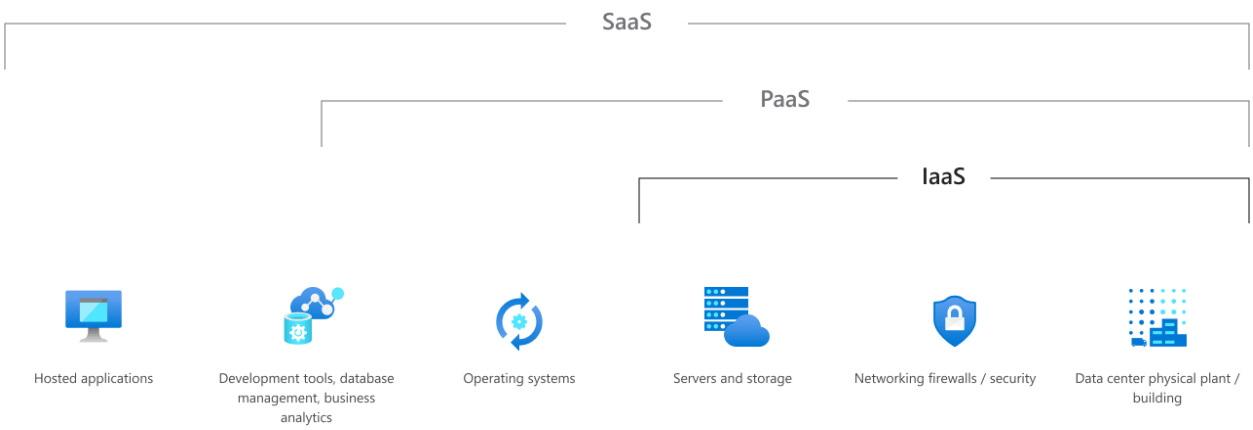
- **Capital Expenditure (CapEx):** The spending of money up-front on physical infrastructure. These expenses are deducted over time.
- **Operational Expenditure (OpEx):** The spending of money on services or products now and being billed for them now. These expenses are deducted in the same year they are incurred. Most cloud services are considered OpEx.

**Notes:**

_____
_____
_____
_____
_____
_____

## Infrastructure-as-a-Service (IaaS)

Infrastructure-as-a-Service is a cloud computing type that offers essential compute, storage, and networking resources on demand. Resources are offered on a pay-as-you-go basis.



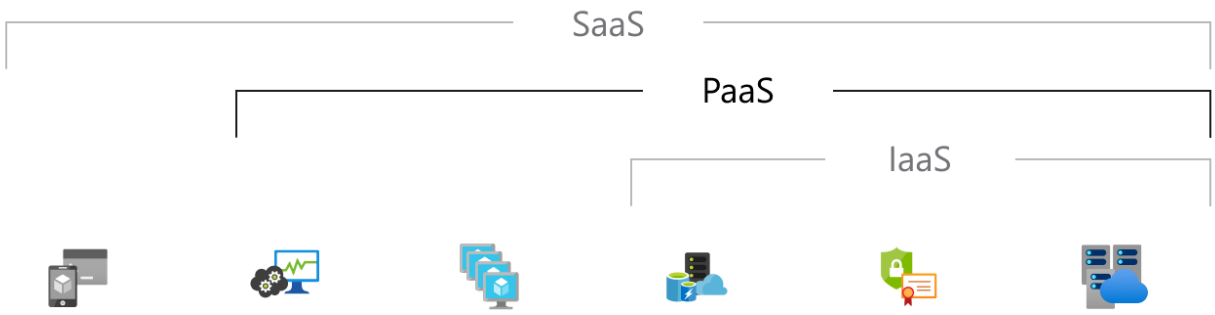

Migrating to IaaS helps reduce the need for maintenance of on-prem data centers and allows organizations to save money on hardware costs. IaaS solutions allow organizations to scale their IT resources up and down with demand, while also allowing them to quickly provision new applications and increase the reliability of their underlying infrastructure.

**Notes:**

_____
_____
_____
_____
_____
_____

## Platform-as-a-Service (PaaS)

Platform-as-a-Service is a complete development and deployment environment in the cloud. It can be used to deploy simple cloud-based apps and complex cloud-enabled enterprise applications. When leveraging PaaS, you purchase the resources you need from your cloud service provider on a pay-as-you-go basis. The resource you purchase are accessed over a secure Internet connection.




PaaS resources include the same resources included in IaaS (servers, storage, and networking) PLUS things like middleware, development tools, business intelligence services, and database management systems.

It's important to remember that PaaS is designed to support the complete web application lifecycle. It allows organizations to avoid the expense buying and managing software licenses, underlying infrastructure and middleware, container orchestrators, and development tools.

Ultimately, when leveraging PaaS offerings, you manage the applications and services, while the cloud service provider manages everything else.

**Notes:**

_____
_____
_____
_____
_____
_____

### Software-as-a-Service (SaaS)

Software-as-a-Service allows users to connect to cloud-based apps over the Internet. Microsoft Office 365 is a good example of SaaS in action. Gmail would be another good example.

SaaS provides a complete software solution that's purchased on a pay-as-you-go basis from a cloud service provider. It's essentially the rental of an app, that users can then connect to over the Internet, via a web browser.

The underlying infrastructure, middleware, app software, and app data for a SaaS solution are all hosted in the provider's data center, which means the service provider is responsible for managing the hardware and software.

SaaS allows organizations to get up and running quickly, with minimal upfront cost.

**Notes:**

_____
_____
_____
_____
_____
_____

## CORE ARCHITECTURAL COMPONENTS

### Azure Regions and Regional Pairs

Azure is made up of datacenters located around the world. When you create a resource (ie. Virtual machine, virtual network, etc), you're actually using physical equipment that's located in one or more of these locations. Azure organizes these locations into regions.

**Azure Regions**

A region is a geographical area that contains one or more datacenters that are relatively close and networked together with a low-latency network.


When you deploy a resource in Azure, you'll often need to choose the region where you want your resource deployed.

It’s important to note that some services or features are only available in certain regions.

A few examples of regions are East US, Canada Central, and North Europe.

**Region Pairs**

Every Azure region is paired with another region within the same geography (ie. US, Europe, or Asia) at least 300 miles away in order to allow replication of resources across that geography. Replicating resources across region pairs helps reduce interruptions due to events like natural disasters, civil unrest, power outages, or physical network outages that affect both regions at once.

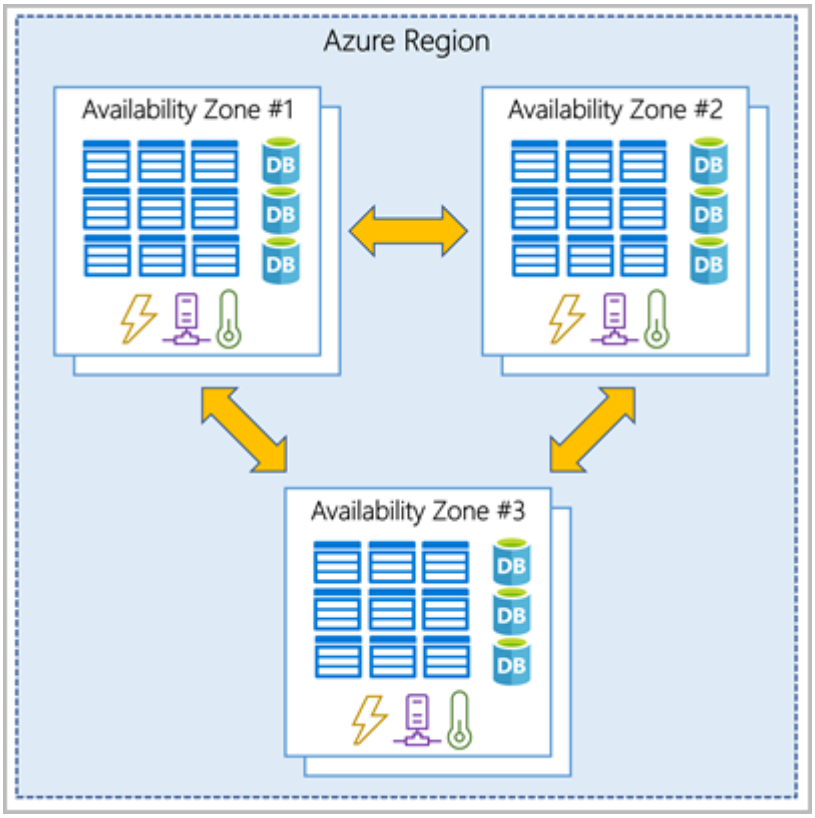
**Notes:**

_____
_____
_____
_____
_____
_____

## Availability Zones in Azure

Availability zones are physically separate datacenters within an Azure region. Every availability zone includes one or more datacenters that features independent power, cooling, and networking. In essence, an availability zone is designed to be an *isolation boundary,* meaning if one zone goes down, the other continues working.

It important to remember that availability zones are connected through private high-speed fiber-optic networks. The image below shows what availability zones look like within a region:




Availability zones are designed primarily for VMs, managed disks, load balancers, and SQL databases.

**Notes:**

_____
_____
_____
_____
_____
_____

## Azure Resources and Resource Groups

Before deploying an Azure resource, you need to create a resource group to deploy the resource into. The relationship of resources with resource groups is highlighted below:

- **Resource:** A resource is a manageable item in Azure. Virtual machines, storage accounts, web apps, and virtual networks are examples of resources.
- **Resource Group:** A resource group is a container that holds resources for an Azure solution. Resources within a resource group are typically managed as a group.

**Notes:**

_____
_____
_____
_____

_____
_____

## Azure Subscriptions

An Azure subscription provides authenticated and authorized access to Azure products and services and allows organizations to provision cloud resources. Every Azure subscription links to an Azure account, which is an identity in Azure AD or in a directory that Azure AD trusts.

Azure subscriptions can be used to define boundaries around Azure products, services, and resources:

- **Billing boundary:** Determines how an Azure account is billed for using Azure.
- **Access control boundary:** Create separate subscriptions to reflect different organizational structures.

An account can have one subscription or multiple subscriptions that have different billing models. You can also use subscription to apply different access-management policies when necessary.

**Notes:**

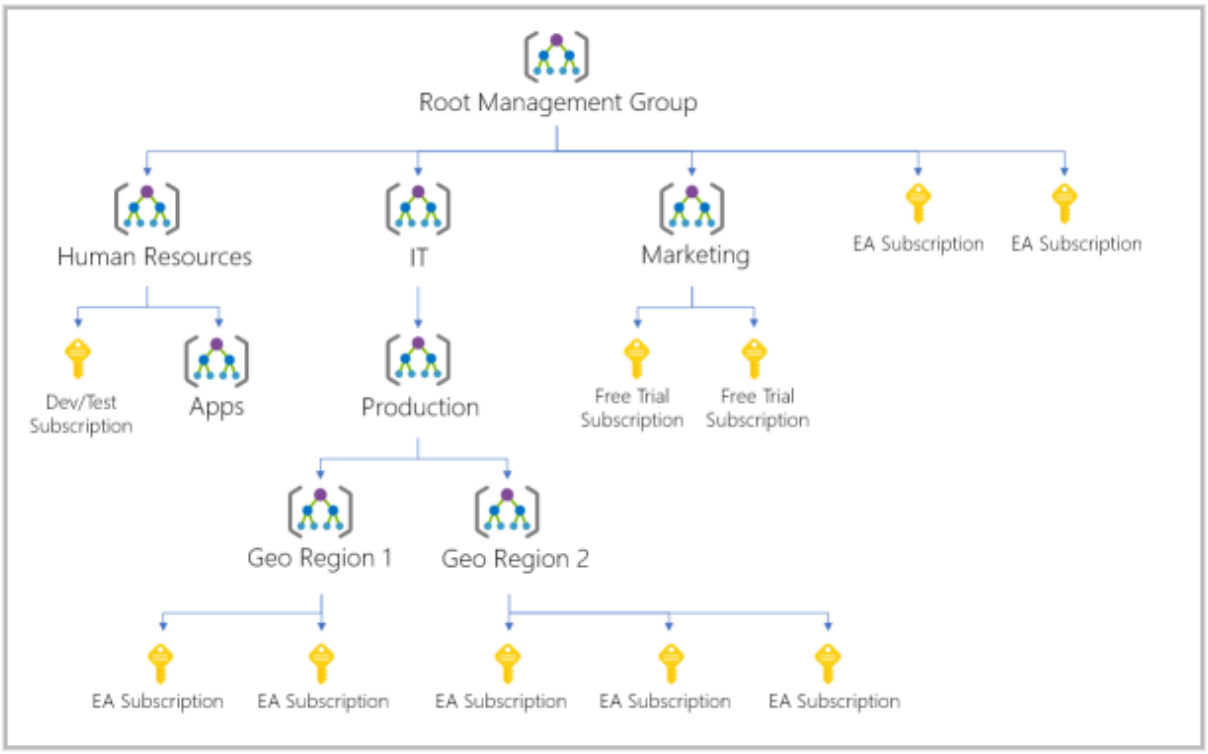
_____
_____
_____
_____
_____
_____

## Management Groups in Azure

To efficiently manage access, policies, and compliance when you manage multiple Azure subscriptions, you can use Management Groups, because management groups provide scope that sits above subscriptions.

When managing multiple subscriptions, you organize those subscriptions into management groups, to which you can then apply governance conditions. All subscriptions within a management group will, in turn, inherit the conditions you apply to the management group.

The image below highlights how you can create a hierarchy for governance through the use of management groups:




It's important to note that a single management group tree can support up to six levels of depth and while each management group can have many children, each management group and subscription can support only one parent.

**Notes:**

_____
_____
_____
_____
_____
_____

# CORE AZURE COMPUTE SERVICES AND PRODUCTS

## An Intro to Azure Compute

Azure compute is an on-demand computing service that organizations use to run cloud-based applications. It provides compute resources like disks, processors, memory, networking, and even operating systems.

Azure supports many types of compute solutions, including Linux, Windows Server, SQL Server, Oracle, IBM, and SAP. Each Azure compute service offers different options depending on your requirements. The most common Azure compute services are:

- Azure Virtual Machines
- VM Scale Sets

- Azure Container Instances
- Azure App Service
- Azure Functions

**Virtual Machines**

Virtual machines are virtual versions of physical computers that feature virtual processors, memory, storage, and networking resources. They host an operating system just like a physical computer, and you can install and run software on them just like a physical computer.

**Virtual Machine Scale Sets**

A virtual machine scale set allows you to deploy and manage a set of identical VMs that you can use to deploy solutions with true autoscale.

**Containers and Kubernetes**

Container Instances and Azure Kubernetes Service are both Azure compute resources that organizations can use to deploy and manage containers. Unlike VMs, which are full virtualized servers, containers are lightweight, virtualized application environments.

**App Service**

Azure App Service is a compute platform that you can use to quickly build, deploy, and scale enterprise-grade web, mobile, and API apps running on any platform.

**Functions**

Functions are a serverless technology that are best used in cases where you're concerned only about the code running your service and not the underlying platform or infrastructure.

**Notes:**

_____
_____
_____
_____
_____
_____

## ACI vs AKS

For many organizations, containers have become the preferred way to package, deploy, and manage cloud apps. Azure Container Instances (ACI) is the easiest way to run a container in Azure, without the need for any VMs or other infrastructure. However, if you require full container orchestration, Microsoft recommends Azure Kubernetes Service (AKS).

AKS simplifies the deployment of a managed Kubernetes cluster in Azure by offloading the operational overhead to Azure. Since it’s hosted, Azure handles the health monitoring and maintenance. The Kubernetes masters are managed by Azure, and you manage and maintain the agent nodes.

It’s important to note that AKS itself is free. You pay only for the agent nodes within your clusters, not for the masters.

**Notes:**

_____
_____
_____
_____
_____
_____

## Key Azure Management Tools

There are several tools at your disposal to manage Azure resources and environments. They include the Azure Portal, Azure PowerShell, Azure CLI, the Azure Mobile App, and ARM templates.

The Azure portal is a web-based user interface that you can use to access almost every feature of Azure. It can be used to visually understand and manage your Azure environment, while Azure PowerShell allows you to quickly perform one-off tasks and to script tasks as needed. Azure PowerShell is available for Windows, Linux, and Mac, and you can access it in a web browser via Azure Cloud Shell.

The Azure CLI is a command-line interface. It’s an executable program that you can use to execute commands in Bash. You can use the Azure CLI to perform every possible management task in Azure. Like Azure PowerShell, the CLI allows you to run one-off commands or you can combine them into a script and execute them together.

The Azure mobile app is available for iOS and Android devices. It allows you to access Azure resources when you're away from a computer. You can use the mobile app to monitor the health and status of Azure resources, check for alerts, diagnose and fix issues, and even restart a web app or virtual machine. The mobile app also allows you to run the Azure CLI or Azure PowerShell commands to manage Azure resources.

ARM templates allow you to declaratively describe the resources you want to use, using JSON format. The template will then create those resources in parallel. For example, need 25 VMs, all 25 VMs will be created at the same time.

**Notes:**

_____
_____
_____
_____
_____
_____

# CORE AZURE NETWORK SERVICES AND PRODUCTS

## Getting Started with Azure Virtual Networks

*Azure virtual networks* are used to allow Azure resources to communicate with each other, with users on the internet, and with on-prem computers.

A virtual network consists of an overarching address space and subnets that break up that address space into smaller blocks.

When you provision a vNet, you specify a custom IP address space using either public or private addresses. Azure will then assign resources within that virtual network addresses from the address space that you assign.

Subnets are used to segment a virtual network into one or more sub-networks. When you define a subnet, you allocate a portion of the virtual network's address space to that subnet. Resources are then deployed into the subnet.

Resources within subnets can be secured with Network Security Groups.

When you deploy a vNet, it is automatically scoped to a single region or location. That said, multiple vNets from different regions can be connected together, using Virtual Network Peering.

A vNet is also scoped to a single subscription. However, you can implement multiple vNets within each Azure subscription.

**Communicating With On-Prem Resources**

Azure vNets allow you to your on-prem environment with resources deployed in your Azure subscription. To do this, you can use a *point-to-site VPN*, a *site-to-site VPN*, or an *Azure ExpressRoute*, depending on your needs:

- **A Point-to-site VPN** allows a client computer to initiate an encrypted VPN connection to connect that computer to your Azure virtual network.
- **A Site-to-site VPN** links an on-prem VPN device to the Azure VPN gateway in a virtual network. This allows devices in Azure to appear as if they are on the local network. A site-to-site VPN is encrypted and works over the internet.
- **Azure ExpressRoute** is for situations where you need more bandwidth and higher levels of security. It provides a dedicated private connection to Azure that doesn't travel over the internet.

**Routing Network Traffic**

Azure automatically routes traffic between subnets on connected virtual networks, on-prem networks, and the internet. However, you can manually control this routing and override these settings with *route tables* and *Border Gateway Protocol.*

A route table allows you to define rules that control how traffic should be directed, while Border Gateway Protocol (BGP) works with Azure VPN gateways, Azure Route Server, or ExpressRoute to propagate on-premises BGP routes to Azure virtual networks.

**Filtering Network Traffic**

When working with Azure vNets, you can filter traffic between subnets via *network security groups* and *network virtual appliances*.

A network security group contains one or more inbound and outbound security rules that you define. These rules allow or block traffic, based on factors you define.

A network virtual appliance, on the other hand, is a specialized VM that's similar to a hardened network appliance. This device is used to carry out a particular network function (ie. run a firewall or perform WAN optimization).

**Connecting Virtual Networks**

vNets can be linked together via virtual network *peering*, while *User-defined routes* allow for enhanced control over network traffic flow. More specifically, user-defined routes allow you to control the routing tables between subnets within a VNet, as well as between VNets.

**Notes:**

_____
_____
_____
_____
_____
_____

## vNet Peering

vNet peering is used to seamlessly connect multiple vNets in Azure. When peered, the virtual networks appear as one for connectivity purposes. Traffic between VMs in peered virtual networks travels over the Microsoft backbone infrastructure, meaning traffic is routed through Microsoft's *private* network only.

There are two types of peering supported by Azure: *Virtual network peering* and *Global virtual network peering*. Virtual network peering allows you to connect virtual networks within the same Azure region, while Global virtual network peering allows the connection of virtual networks across Azure regions.

**Notes:**

_____
_____
_____
_____
_____
_____

## An Intro to Azure DNS

Azure DNS is a hosting service for DNS domains. It provides name resolution through the Microsoft Azure infrastructure. When you host a domain in Azure, you can manage its DNS records using the same credentials, APIs, tools, and billing as your other Azure services.

**Customizable Virtual Networks with Private Domains**

Azure DNS also supports private DNS domains, which allow you to use your own custom domain names in your private virtual networks.

**Alias Records**

Azure DNS supports alias record sets, which can be used to refer to an Azure resource, like an Azure public IP address or an Azure Traffic Manager profile endpoint. In the event the IP address of the underlying resource changes, the alias record will seamlessly update itself.

**Notes:**

_____

_____

_____

_____

_____

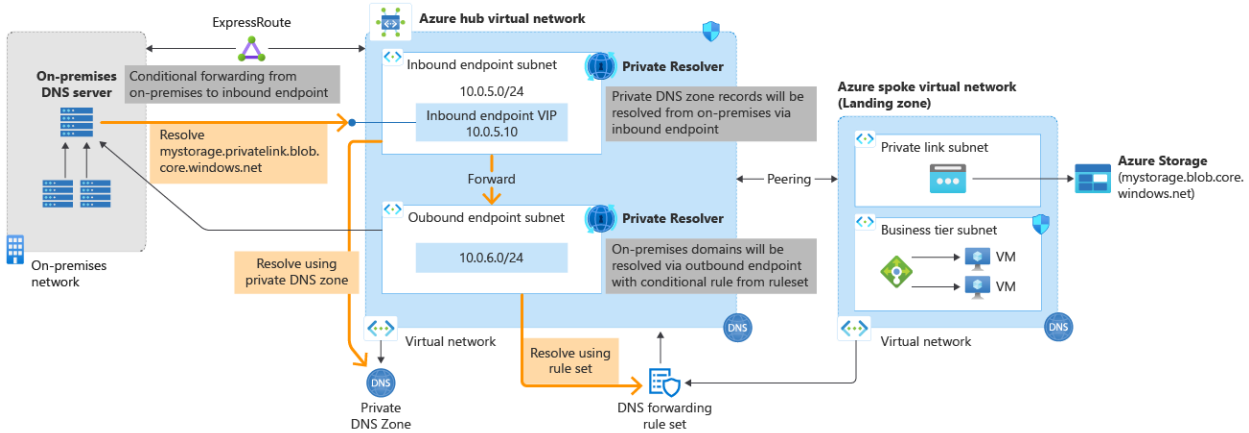
_____

## Azure DNS Private Resolver

The Azure DNS Private Resolver allows you to query Azure DNS private zones from an on-prem environment without deploying VM-based DNS servers in Azure.

Deploying Azure DNS Private Resolver requires an Azure vNet. When you create an Azure DNS Private Resolver inside a vNet, inbound endpoints are established. These can then be used as the destination for DNS queries. An outbound endpoint processes DNS queries based on a DNS forwarding ruleset that you define.

The image below depicts the architecture associated with Azure DNS Private Resolver:



**Notes:**

_____
_____
_____
_____
_____
_____

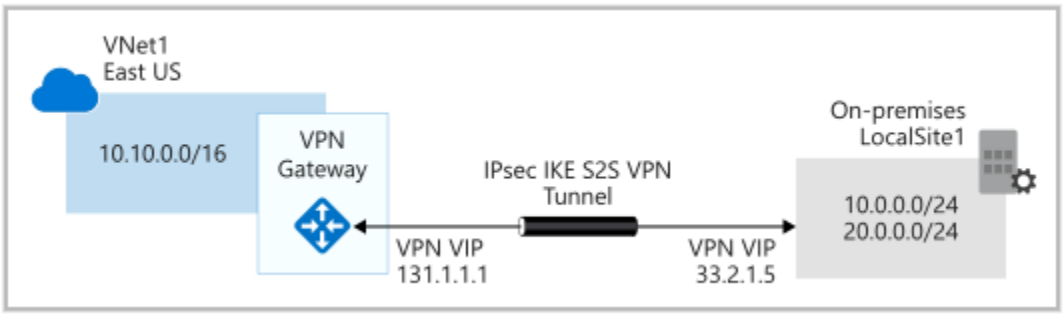
## A Deeper Dive into Azure VPN Gateways

VPNs (virtual private networks) use an encrypted tunnel within another network. They're typically used to connect multiple trusted private networks to one another over the public internet. The traffic over a VPN is encrypted while traveling over the untrusted network.

**VPN Gateways**

A VPN gateway is a type of virtual network gateway. Deploying an Azure VPN Gateway instance in a dedicated subnet of a vNet allows you to setup a few different VPN connections:

- ***site-to-site* connection:** Connect on-prem datacenter to virtual network.
- ***point-to-site* connection:** Connect individual devices to a virtual network.
- ***network-to-network* connection:** Connect virtual networks to other virtual networks




As data travels across the internet via a VPN, it's encrypted inside a private.

It's important to note that only one VPN gateway can be deployed in each vNet. However, you can use one gateway to connect to multiple locations.

VPN gateways come in two flavors: ***policy-based*** and ***route-based***.

**Policy-Based VPNs**

A policy-based VPN gateway specifies statically the IP address of packets that should be encrypted through the tunnel. It supports IKEv1 only and uses static routing.

When configuring a policy-based VPN, you must define the IP addresses that reside behind each tunnel.

**Route-based VPNs**

Route-based gateways can be used if defining which IP addresses are behind each tunnel is too difficult or not practical. Route-based VPNs are the preferred connection method for on-premises devices because they are more resilient to topology changes, including the creation of new subnets.

It should be noted that route-based VPN gateways support IKEv2 and can use *dynamic routing protocols*, where routing/forwarding tables direct traffic to different IPSec tunnels.

**Notes:**

_____
_____
_____
_____
_____
_____

## A Deeper Dive into Azure ExpressRoute

ExpressRoute is used to extend an on-prem network into the Microsoft cloud via a private connection. It allows you to establish connections to Microsoft cloud services, like Azure and Microsoft 365, with the help of a connectivity provider.

Because ExpressRoute connections don't go over the public Internet, they are more reliable, and they offer faster speeds. ExpressRoute connections also offer consistent latencies and higher security when compared to connections that go over the Internet.

**ExpressRoute connectivity models**

ExpressRoute supports several models that can be used to connect an on-prem network to the Microsoft cloud. These models include CloudExchange colocation, Point-to-point Ethernet connection, Any-to-any connection, and Directly from ExpressRoute sites

Because data doesn't travel over the public internet when using an ExpressRoute connection, it's not exposed to the risks typically associated with internet communications. An ExpressRoute connection is essentially a private connection from your on-prem infrastructure to your Azure infrastructure.

**Notes:**

_____
_____
_____
_____
_____
_____

## Private Links and Private Endpoints

Azure Private Link is a service that you can use to access Azure PaaS Services, like SQL Database or Azure Storage. It can also be used to connect to Azure-hosted customer-owned services over a private endpoint in your virtual network.

The private endpoint used by Private Links is a network interface that uses a private IP address from your virtual network. This interface connects privately and securely to a service that's powered by Azure Private Link. In essence, when you enable a private endpoint, you bring the Azure service into your virtual network.

It's important to note that traffic between a virtual network and the Azure service that you are connecting to always travels across the Microsoft backbone network.

**Notes:**

_____
_____
_____
_____
_____
_____

# CORE AZURE STORAGE SERVICES AND PRODUCTS

## An Intro to Azure Storage Accounts

The Azure storage account is the container that's used to host all Azure Storage data objects, including blobs, file shares, queues, tables, and disks. It provides a unique namespace for accessing Azure Storage data from anywhere in the world over HTTP or HTTPS.

**Types of storage accounts**

There are several types of storage accounts available, with each supporting different features and having a separate pricing model.

The *Standard general-purpose v2* storage account supports Blob Storage (including Data Lake Storage1), Queue Storage, Table Storage, and Azure Files, while the *Premium block blobs* storage account type supports Blob Storage (including Data Lake Storage1). The *Premium file shares* storage account is used to host Azure Files, and the *Premium page blobs* storage account is for Page blobs only.

Each storage account type offers different replication options. These are covered in detail in the lecture.

**Notes:**

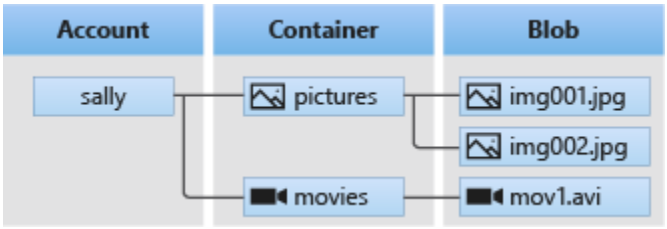
_____
_____
_____
_____
_____
_____

## A Look at Azure Blobs

Azure Blob storage is an Azure-based object storage solution. It's optimized for storing massive amounts of **unstructured** data, which is data that doesn't adhere to a particular data model or definition, such as text or binary data.

Organizations typically use blob storage to serve images or documents to a web browser, for storing files for distributed access, and for streaming video and audio. Blob storage is also used in cases where you have an app that needs to write to log files, or in case where you need to store data for backup and restore, disaster recovery, and archiving.

To use blob storage, you host your data blobs in a blob storage container, which resides inside the storage account. The image below shows this relationship:




**Blob Storage Tiers**

Azure offers different access tiers for blob storage:

- **Hot access tier**: Used to store data that is accessed frequently. Has the highest storage costs, but the lowest access costs.
- **Cool access tier**: Used to store data that is infrequently accessed and stored for at least 30 days Has lower storage costs than hot tier, but higher access costs.
- **Archive access tier**: Used to store data that is rarely accessed and stored for at least 180 days, Has the lowest storage costs, but also the highest access costs.

**Notes:**

_____
_____
_____
_____
_____
_____

## A Look at Azure Files

Azure Files is another storage offering. It provides fully managed file shares in Azure that can be accessed via SMB or NFS. You can mount Azure Files file shares concurrently in cloud and on-prem deployments.

You can access SMB Azure file shares from Windows, Linux, and macOS clients. However, NFS Azure Files shares are only accessible from Linux or macOS clients.

It should be noted that SMB Azure file shares can also be cached on Windows Servers via Azure File Sync.

Organizations typically use Azure file shares to replace or supplement on-prem file servers. They are also often used to lift and shift apps to the cloud.

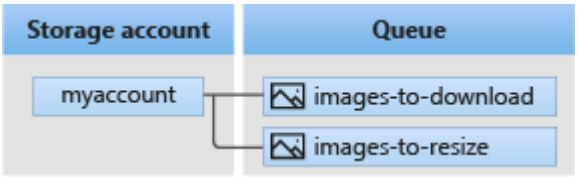
**Notes:**

_____
_____
_____
_____
_____
_____

## A Look at Azure Queues

Azure Queue Storage is designed for storing large numbers of messages used by distributed apps. These messages can be stored and accessed from anywhere in the world via authenticated calls using HTTP or HTTPS. In other words, it enables communication between the components of the distributed application that use it. Each queue maintains a list of messages that can be added by a sender component and processed by a receiver component. With a queue, your application can scale immediately to meet demand.

Queue Storage consists of the access URL, the storage account itself, the queue itself, and the messages. The image on your screen shows the architecture of typical queues.




To access the "images-to-download" queue above, you'd use the following URL:

*https://myaccount.queue.core.windows.net/images-to-download*

**Notes:**

_____
_____
_____
_____
_____
_____

## A Look at Azure Table Storage

Azure Table storage is used to store non-relational structured data (otherwise known as NoSQL data) in Azure. It provides a key/attribute store with a schemaless design, which makes it easy to adapt your data as the needs of your application change. Access to Table storage data is fast and is often less expensive than traditional SQL.

Organizations will often use Table storage to store flexible data like user data for web applications, address books, etc.

Azure Table storage accepts authenticated calls from inside and outside the Azure cloud.

Specific use cases are highlighted in the associated course lecture.

**Notes:**

_____
_____
_____
_____
_____
_____

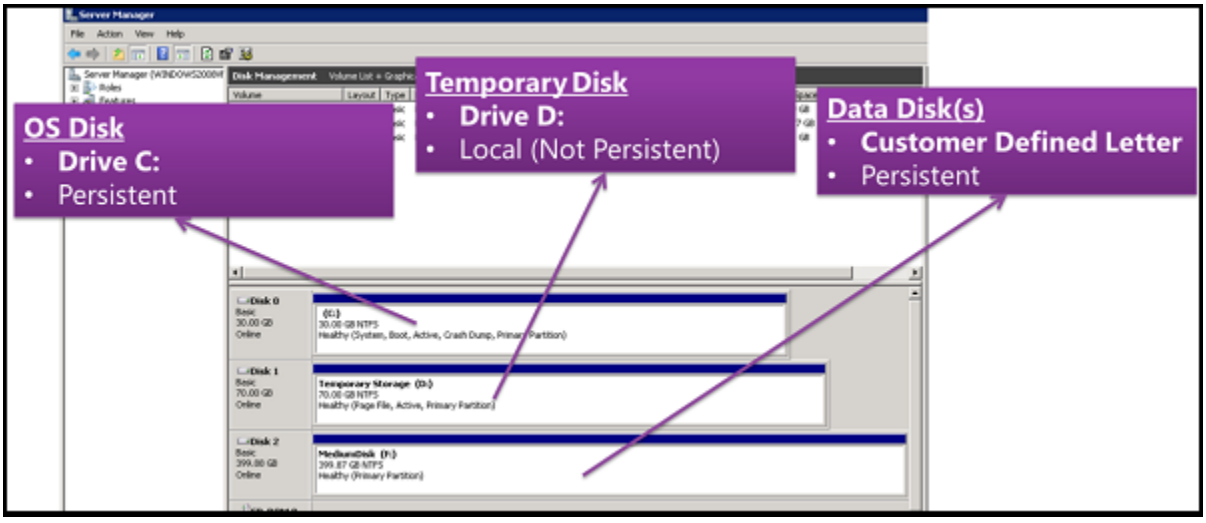
## Azure Managed Disks

Azure managed disks are block-level storage volumes. These storage volumes are managed by Azure and they are used with VMs. Managed disks are just like physical disks that you'd find in an on-prem server, except they are virtualized. To use a managed disk, you specify the disk size and the disk type, and then you provision the disk. Once provisioned, Azure handles the rest.

Azure managed disks come in a few different flavors: **ultra disks**, **premium solid-state drives (SSD)**, **standard SSDs**, and **standard hard disk drives (HDD)**.

Azure ultra disks are the highest-performing option for Azure VMs. Azure Premium SSDs offer high-performance and low-latency disks for VMs that require high IO. Azure Premium SSD v2 disks are designed for IO-intense enterprise workloads that require consistent sub-millisecond disk latencies and high IOPS and throughput at a low cost. Standard SSDs are best for web servers, and other low IOPS application servers, and non-production workloads, while standard HDD disks can be used for dev/test scenarios and less critical workloads. These disks are covered in detail in the course lecture.

There are three main disk roles in Azure: the **data disk**, the **OS disk**, and the **temporary disk**. These roles map to disks that are attached to your virtual machine. These, too, are covered in the lecture.




**Notes:**

_____
_____
_____

_____
_____
_____

## LRS Redundancy vs ZRS Redundancy

When you store data in an Azure Storage account, it's replicated three times in the primary region. Azure Storage provides two options for how this replication is performed:

- **Locally redundant storage (LRS)** copies the stored data synchronously three times within a single physical location in the primary region. This is the least expensive replication option. However, Microsoft does not recommend it for applications that require high availability.
- **Zone-redundant storage (ZRS)** copies the stored data synchronously across three Azure availability zones in the primary region. This replication option is recommended for applications that require high availability.

**Locally-redundant storage**

LRS provides 11 nines of durability of objects over a given year and is the lowest-cost redundancy option available. It protects data from server rack and drive failures. However, if a disaster (ie. fire/flood) occurs within the datacenter, all replicas of a storage account using LRS may be lost.

**Zone-redundant storage**

ZRS offers durability for storage resources of at least 12 nines over a given year. It replicates the storage account synchronously across three Azure availability zones in the primary region, and each availability zone is a separate physical location with independent power, cooling, and networking.

When using zone-redundant storage, data remains accessible for read and write operations even if a zone becomes unavailable.

**Notes:**

_____
_____
_____
_____
_____
_____

## GRS Redundancy vs GZRS Redundancy

For applications requiring high durability, you can choose to additionally copy the data in your storage account to a secondary region that is hundreds of miles away from the primary region. If your storage account is copied to a secondary region, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region isn't recoverable.

Azure Storage offers two options for copying your data to a secondary region: **Geo-redundant storage (GRS)** and **Geo-zone-redundant storage (GZRS)**.

**Geo-redundant storage** copies stored data synchronously three times within a single physical location in the primary region using LRS. It also copies the data asynchronously to a single physical location in the secondary region. The data is then copied synchronously three more times in the secondary region, using LRS. GRS offers at least sixteen 9's of durability over a given year.

**Geo-zone-redundant storage** copies stored data synchronously across three Azure availability zones in the primary region using ZRS. The data is then copied asynchronously to a single physical location in the secondary region. Within the secondary region, your data is copied synchronously three times more using LRS. GZRS is offers at least sixteen 9's of durability over a given year.

**Notes:**

_____
_____
_____
_____
_____
_____

# MOVING AND MIGRATING DATA IN AZURE

## Moving Files in Microsoft Azure

**AzCopy**

AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

**Storage Explorer**

Microsoft Azure Storage Explorer is a standalone app allows you to work with Azure Storage data on Windows, macOS, and Linux.

**Notes:**

_____
_____
_____
_____
_____
_____

## Azure File Sync

Azure File Sync is a cloud service that allows you to centralize your organization's file shares in Azure Files, while maintaining the flexibility of a Windows file server. It does this by allowing you to transform locally placed Windows file servers into quick caches of your Azure file shares.

You can access your data locally on file servers using SMB, NFS, and FTPS, while having as many caches as you need across the world.

Some of the key benefits of Azure File Sync include the ability to enable cloud tiering and the ability to perform cloud-side backups of your data.

**Cloud tiering**

Cloud tiering causes your most frequently accessed files to be cached on your local file server, while your least frequently accessed files get tiered to Azure. Since the tiered files can quickly be recalled on-demand, you only need to store a fraction of your data on-prem, reducing on-prem storage costs.

**Cloud-side backup**

Cloud-side backups reduce on-prem backup costs because they allow you to take centralized backups in the cloud using Azure Backup, instead of needing to backup local Windows file servers.

**Notes:**

_____
_____
_____
_____
_____
_____

## Azure Migrate

Azure Migrate is a suite of tools that you use to assess and migrate on-prem servers, infrastructure, applications, and data to Azure. It's a single portal that you use to start, run, and track migrations to Azure.

The Azure Migrate suite of tools includes:

- Azure Migrate: Discovery and assessment
- Azure Migrate: Server Migration
- Data Migration Assistant
- Azure Database Migration Service
- Movere
- Web app migration assistant
- Azure Data Box

**Azure Migrate: Discovery and assessment** allows you to discover and assess on-prem VMware, Hyper-V, and physical servers in preparation for migration to Azure.

**Azure Migrate: Server Migration** is used to migrate VMware VMs, Hyper-V VMs, physical servers, other virtualized servers, and public cloud VMs to Azure.

**Data Migration Assistant** is a stand-alone tool designed to allow you to assess SQL Server databases for migration to Azure SQL Database, Azure SQL Managed Instance, or Azure VMs running SQL Server.

The **Azure Database Migration Service** allows you to migrate on-prem databases to Azure VMs running SQL Server, Azure SQL Database, or SQL Managed Instances.

**Movere** is a Software as a Service platform that Microsoft acquired.

The **Azure App Service Migration Assistant** is standalone migration tool that is used to assess on-prem web apps and to migrate them to Azure.

**Azure Data Box** is used to migrate large amounts of offline data to Azure. The secure data transfer of data facilitated by a physical Data Box storage device that Microsoft ships to you.

**Notes:**

_____
_____
_____
_____
_____
_____

# SECURITY, PRIVACY, COMPLIANCE, AND TRUST

## Securing Network Connectivity

**Defense in Depth**

Instead of basing security on a single perimeter, a defense in depth strategy takes a multi-layered approach. Each individual layer provides additional protection so that, if one layer gets breached, the next layer prevents the attacker from getting unauthorized access to data.

**Azure Security Services and Resources**

- Azure Firewall
    - Azure Firewall is a managed cloud-based network security service that you use to protect Azure Virtual Network resources.
- DDoS Protection
    - Azure DDoS Protection is used protect applications and servers from outside threats by analyzing network traffic and dropping anything that looks like it could be a DDoS attack.
- Network and Application Security Groups
    - Azure Network Security Groups are used to allow and to deny traffic to and from Azure resources.
    - You can associate an Azure Network Security Group with subnets within a virtual network or even to specific network interfaces.
    - Application security groups allow you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups.

**Notes:**

_____
_____
_____
_____
_____
_____

## Core Azure Identity Services

**Authentication vs Authorization**

Authentication is the act of validating that users are whom they claim to be. This is the first step in any security process. Authorization in system security is the process of giving the user permission to access a specific resource or function. This term is often used interchangeably with access control or client privilege.

**Azure Active Directory**

Azure Active Directory (Azure AD) is a cloud-based identity and access management service. This service helps your employees access external resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications. Azure Active Directory also helps them access internal resources like apps on your corporate intranet network, along with any cloud apps developed for your own organization.

**Multi-Factor Authentication**

Multi-factor authentication is a process in which users are prompted during the sign-in process for an additional form of identification, such as a code on their cellphone or a fingerprint scan.

If you only use a password to authenticate a user, it leaves an insecure vector for attack. If the password is weak or has been exposed elsewhere, an attacker could be using it to gain access. When you require a second form of authentication, security is increased because this additional factor isn't something that's easy for an attacker to obtain or duplicate.

Azure AD Multi-Factor Authentication works by requiring two or more of the following authentication methods:

- Something you know, typically a password.
- Something you have, such as a trusted device that's not easily duplicated, like a phone or hardware key.
- Something you are - biometrics like a fingerprint or face scan.

**Notes:**

_____
_____
_____
_____
_____
_____

## Deeper Dive into Azure Active Directory

Azure Active Directory is Azure's cloud-based identity and access management service. Like traditional Active Directory, it's used to allow users to sign-in and access resources. You can use Azure AD to provide access to internal resources on your corporate network as well as to cloud applications. Azure AD is also used to grant access to external resources, like Microsoft 365 and the Azure portal.

IT administrators use Azure AD to control access to applications and resources, while application developers will often use it as a standards-based approach for adding single sign-on to applications.

Microsoft 365 subscribers, Office 365 subscribers, and Azure subscribers use it inherently because each of these tenants are automatically Azure AD tenants, since user access to these applications are controlled by Azure AD.

In addition to the free version of Azure Active Directory, there are also paid capabilities that you can get access to. By upgrading to Azure Active Directory premium P1 or to Azure Active Directory premium P2, these paid Azure AD licenses provide additional benefits such as self-service, enhanced monitoring, security, reporting, and secure access for mobile users. The Azure AD license that you choose determines what features you get access to.

**Notes:**

_____
_____
_____
_____
_____
_____

## Deeper Dive into Azure AD Domain Services

Azure Active Directory Domain Services (Azure AD DS) is essentially a managed version of a traditional on-prem active directory. It offers domain join, group policy, LDAP, and Kerberos and NTLM authentication, and it's very similar to a traditional on-prem Active Directory. However, it's hosted in the cloud and does not require you to deploy or manage any domain controllers.

Azure Active Directory Domain Services consists of a DNS namespace and a matching directory for that namespace. It essentially "rides on top of", or integrates with, your existing Azure AD tenant. You can look at the Azure AD tenant as the vehicle for users to sign-in with credentials, while Azure Active Directory Domain Services is the vehicle for providing advanced management.

Because Azure Active Directory Domain Services replicates the identity information from your Azure AD tenant, it's fully compatible with cloud only Azure AD tenants. However, it is also compatible with Azure AD tenants that are synchronized with an on-prem active directory environment. This means that if you have an existing on-prem active directory, you can synchronize your users from that on-prem directory into Azure AD. The users that are synced into Azure AD will show up in your Azure Active Directory Domain Services environment as well.

One of the biggest advantages of Azure Active Directory Domain Services is the support for Kerberos and NTLM authentication. Because Azure Active Directory Domain Services supports these types of authentication, you can deploy applications that rely on Windows integrated authentication. This means lift and shift of applications to the cloud becomes much easier.

**Notes:**

_____
_____
_____
_____

## An Introduction to Azure AD B2B

Azure Active Directory B2B allows you to invite guest users to collaborate with your organization. It lets you securely share your organization's applications and services with external users, while allowing you to retain control over your data.

Azure AD B2B  works on an invitation and redemption process that allows your external partners to use their own credentials to access your company's resources. After you've sent an invite to an external user, the user redeems the invite and completes signup. They're then represented in your Azure AD as a user object.

Developers often use Azure AD B2B APIs to customize the invitation process and to write applications like self-service sign-up portals.

**Notes:**

## An Introduction to Azure AD B2C

Azure Active Directory B2C is an identity offering that provides business-to-customer identity as a service. It allows users to use their social, enterprise, or local accounts to get single sign-on to your applications.

While Azure AD B2C is built on the same technology as Azure AD, it's not part of Azure AD. It's actually a separate service altogether. It's designed to allow organizations to build customer-facing applications that will allow users of those apps to sign in with no restrictions on user account.

The Azure AD B2C service supports standards-based authentication protocols, including OpenID Connect, OAuth 2.0, and Security Assertion Markup Language (SAML), and it integrates with most modern applications and commercial software.

**Notes:**

## A Closer Look at SSPR, MFA, and Passwordless Authentication in Azure AD

**Self-Service Password Reset**

SSPR allows users to change their passwords via a web browser from virtually any device.

**Multi-Factor Authentication**

Multi-factor authentication is a process in which users are prompted during the sign-in process for an additional form of identification, such as a code on their cellphone or a fingerprint scan.

If you only use a password to authenticate a user, it leaves an insecure vector for attack. If the password is weak or has been exposed elsewhere, an attacker could be using it to gain access. When you require a second form of authentication, security is increased because this additional factor isn't something that's easy for an attacker to obtain or duplicate.

Azure AD Multi-Factor Authentication works by requiring two or more of the following authentication methods:

- Something you know, typically a password.
- Something you have, such as a trusted device that's not easily duplicated, like a phone or hardware key.
- Something you are - biometrics like a fingerprint or face scan.

**Passwordless Authentication**

Makes it possible for end users to authenticate without the need for a password. User credentials are provided via methods like biometrics through Windows Hello for Business, or through a FIDO2 security key.

**Notes:**

_____
_____
_____
_____
_____
_____

## Azure AD Conditional Access

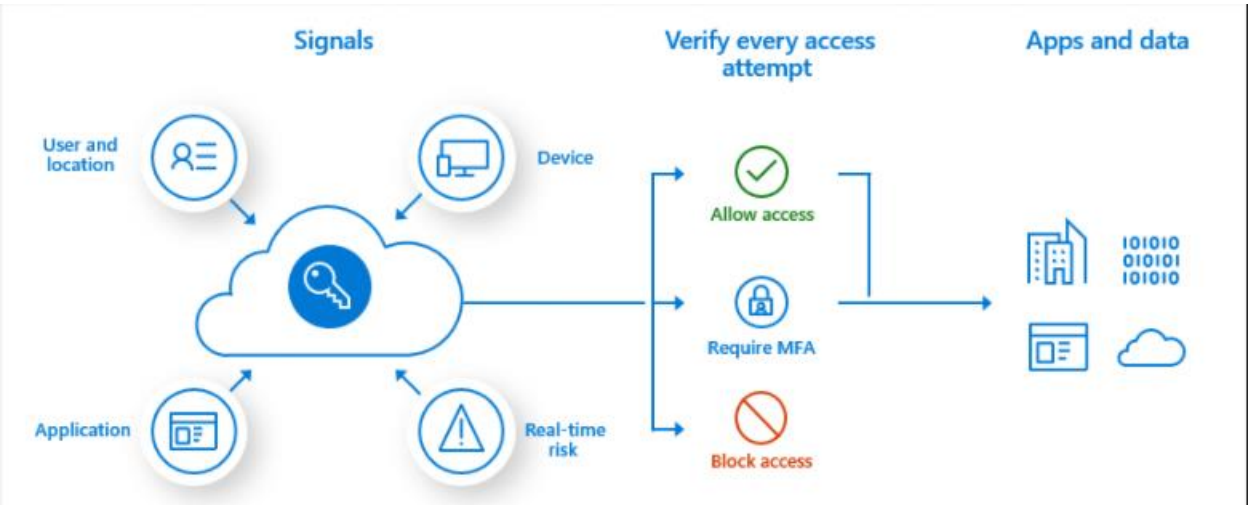
Conditional Access is a feature in Azure Active Directory that allows you to decide who can access apps and data and who can't, depending on conditions that you specify. It's essentially an added layer of security.

When you create a Conditional Access policy in Azure AD, the policy will look at signals like user, location, device, application, and risk, in order to automate access to apps and data.

Conditional Access policies at their simplest are if-then statements. If a user wants to access a resource, then they must complete an action. *Example:* A payroll manager wants to access the payroll application and is required to do multi-factor authentication to access it.

Use Conditional Access policies to apply the right access controls when needed to keep your organization secure.

The image on your screen shows how Conditional Access policies work.




In a typical use case, an admin might configure a Conditional Access policy so that users that are part of a particular group would be required to provide multifactor authentication before being able to sign in to a particular app.

Conditional Access is only available in the paid editions of Azure AD.

Using this feature requires an Azure AD Premium P1 license. Customers with Microsoft 365 Business Premium licenses also have access to Conditional Access features.

Risk-based policies require access to Identity Protection, which is an Azure AD P2 feature.

Other products and features that may interact with Conditional Access policies require appropriate licensing for those products and features.

**Notes:**

_____
_____
_____
_____
_____
_____

## Azure AD Role Based Access Control

To control permissions for Azure AD resource management, you use Azure AD roles. In the real world, for example, you'll have users who are responsible only for creating and managing user accounts, you'll have users who are responsible only for managing billing information, and you'll have users responsible for many other tasks. To support these requirements, Azure AD provide built-in roles and custom roles.

**Built-in roles**

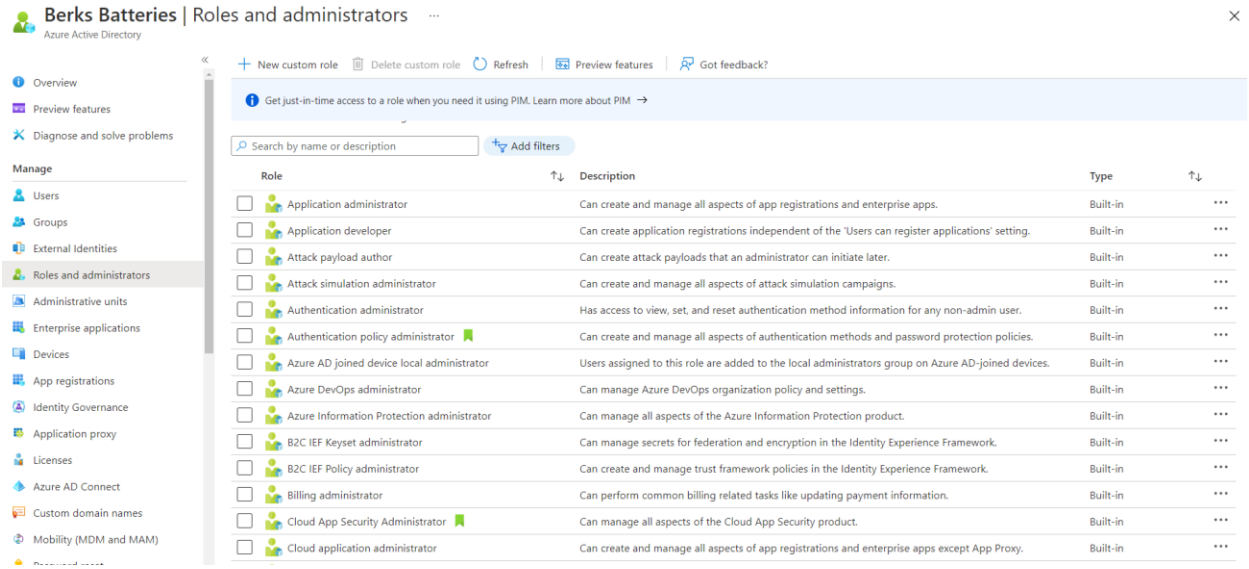
The most common built-in roles include the Global Administrator role, the User Administrator role, and the Billing Administrator role. There are others, but these are the most important ones to understand.

Global administrator provides access to all administrative features in Azure Active Directory. The person who signs up for the Azure AD tenant automatically becomes a global administrator for the tenant.

User administrators can create and manage all aspects of users and groups. This role also includes the ability to manage support tickets and to monitor service health.

Billing administrators are allowed to make purchases, manage subscriptions and support tickets, and to monitor service health.

There are many available built-in roles that apply to different areas of responsibility. Each built-in role is essentially a preconfigured bundle of permissions designed for specific tasks. The screenshot below is just a partial list of all of the available built-in roles.




While there ARE many built-in admin roles available in Azure AD that fit most needs, you can also create custom roles if you require more flexibility when granting access.

Using a custom Azure AD role to grant a user permissions to perform admin tasks is actually a two-step process. You first create the custom **role definition**. This custom role definition consists of a collection of permissions that you can add from a preset list. These permissions are actually the same ones that are used in the built-in roles. Once you've created the role definition, you assign it to a user by creating a **role assignment**.

**Notes:**

_____

_____

_____

_____

_____

_____

## The Zero-Trust Methodology

When we say, "zero trust", what we are referring to is the assumption that everything in the environment is connected to an open and untrusted network. This thought process even applies to resources that are placed behind firewalls.

In short, zero-trust equals “trust no one, and verify everything.” Taking this approach means you no longer trust the integrity of the corporate network. As a result, the organization’s security is strengthened.

In essence, zero-trust means that we no longer assume that our user passwords are enough to properly validate users. As a result, we add MFA, or multi-factor authentication to provide additional authentication checks. We also lock down access to devices on the corporate network. In other words, instead of allowing access to all devices, we configure security so that users can only access the specific apps or data that they need.

There are three principles that underpin the zero-trust model, and how security is implemented within it. These three principles include **verify explicitly**, **least privilege access**, and **assume breach**.

In addition to the three underlying principles that underpin the zero-trust model, there are also six foundational pillars that work together to provide end-to-end security.

These six foundational pillars of the Zero Trust model include identities, devices, applications, data, infrastructure, and networks.

**Notes:**

_____
_____
_____
_____
_____
_____

## Understanding Defense in Depth

Defense in depth is a layered approach to security. Instead of basing security on a single perimeter, a defense in depth strategy takes a multi-layered approach. It’s essentially a series of mechanisms that are used to slow the advance of an attacker. Each individual layer provides a separate layer of protection so that, if one layer gets breached, the next layer prevents the attacker from getting unauthorized access to data.

In a typical defense in depth strategy, there may be several layers of security, including the physical layer, identity and access, the perimeter, network security, the compute layer, the application layer, and then the data layer.

**Physical** security typically limits access to the datacenter to only authorized personnel, while **Identity and access** security controls access to infrastructure and change control.

**Perimeter** security often protects against DDoS attacks by filtering them before they can cause an actual denial of service for end users.

**Network** security can be achieved through segmentation and access controls. What network security does is limit communications between resources to only that communication that is necessary.

The **compute** layer can secure access to virtual machines either on-premises or in the cloud by closing certain ports, while **Application** layer security ensures that applications are secure and free of security vulnerabilities.

**Data** layer security controls access to business and customer data, and encryption to protect data.

**Notes:**

_____
_____
_____
_____
_____
_____

## What is Defender for Cloud?

Defender for Cloud security posture management and threat protection tool. It's used to strengthen the security posture of cloud resources. This is accomplished by leveraging the collection of offerings within the Microsoft Defender plan. You can use Defender for Cloud to protect workloads in Azure, hybrid workloads, and workloads on other cloud platforms.

The Defender plans of Microsoft Defender for Cloud offering includes:

- Microsoft Defender for Servers
- Microsoft Defender for Storage
- Microsoft Defender for SQL
- Microsoft Defender for Containers
- Microsoft Defender for App Service
- Microsoft Defender for Key Vault
- Microsoft Defender for Resource Manager
- Microsoft Defender for DNS
- Microsoft Defender for open-source relational databases
- Microsoft Defender for Azure Cosmos DB
- Defender Cloud Security Posture Management (CSPM)
- Security governance and regulatory compliance
- Cloud security explorer
- Attack path analysis
- Agentless scanning for machines
- Defender for DevOps

Defender for Cloud helps organizations harden their resources, track their security posture, protect against cyber-attacks, and streamline security management.

**Notes:**

_____
_____
_____
_____

## Monitoring and Reporting in Azure

**Tags**

Tags are metadata elements that you apply to your Azure resources. They're key-value pairs that help you identify resources based on settings that are relevant to your organization. If you want to track the deployment environment for your resources, add a key named Environment. To identify the resources deployed to production, give them a value of Production. Fully formed, the key-value pair becomes, Environment = Production.

You can apply tags to your Azure resources, resource groups, and subscriptions.

**Azure Monitor**

Azure Monitor collects, analyzes, and acts on telemetry from cloud and on-prem environments. This information helps organizations better understand how their apps are performing and proactively identifies issues affecting them.

Azure Monitor includes several key tools:

- Application Insights
- VM insights
- Container insights
- Smart alerts and automated actions
- Azure dashboards and workbooks.
- Azure Monitor Metrics

**Azure Service Health**

Azure Service Health is a set of tools that provides support when issues with Azure services crop up and affect your environment. It provides notifications and helps you understand the impact of such issues. It will also let you know when a particular issue is resolved. Service Health is actually a combination of three services. You have Azure Status, Service Health, and Resource Health.

**Azure Status** provides a global view of the health of Azure services that includes information on service availability.

**Notes:**

## Azure Governance Methodologies

**Azure Policy**

Azure Policy is used to enforce organizational standards and to assess compliance. The compliance dashboard in Azure Policy allows you to evaluate the overall state of your environment. It even allows you to drill down with per-resource, per-policy granularity. Azure Policy helps organizations bring resources into compliance through bulk remediation actions.

**Resource Locks**

Resource locks allow you to lock an Azure subscription, a resource group, or specific resources to protect them from accidental deletions and modifications. You can set locks that specifically prevent deletions, or you can set locks that prevent modifications. These locks are called **Delete** and **Read-only**. In the command line, these locks are called CanNotDelete and ReadOnly.

CanNotDelete allows users to read and modify a resource, but not delete it.

ReadOnly allows users to read a resource, but they can't delete or update it. Applying this lock is similar to restricting all authorized users to the permissions that the Reader role provides.

**Azure Blueprints**

Azure Blueprints allows you to define repeatable sets of Azure resources, or blueprints, that adhere to organizational standards and requirements. The blueprints that you create can be used to quickly deploy new environments that fall in line with organizational compliance.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts like Role Assignments, Policy Assignments, ARM templates, and Resource Groups.

**Notes:**

_____
_____
_____
_____
_____
_____

# AZURE PRICING AND SUPPORT

## Planning and Managing Costs

**Customer Types**

- Enterprise Customer
    - Typically signs an Enterprise Agreement with Azure.
- Web Direct Customer
    - Pays public prices for Azure resources.
- Cloud Solutions Provider
    - Are usually Microsoft partners that organizations hire.

**Factors that Affect Costs:**

- Resource Type
- Services
- Location

**Azure Pricing Calculator**

- Used to estimate the cost of different Azure products

**TCO Calculator**

- Allows you to estimate cost savings that you can realize by migrating your workloads to Azure.

**Notes:**

_____
_____
_____
_____
_____
_____

## LEGACY CONTENT

Video lectures, demonstrations, labs, and other resources are moved to the LEGACY CONTENT section of the course when they are no longer necessary for passing the exam, or when they've been replaced with updated videos.

I keep the legacy content around because I've been told it is still useful to lots of students. That said, nothing in the LEGACY CONTENT section is necessary for exam preparation. Just be sure you mark the videos as watched to ensure you can attain the 100% completion rate to get the Udemy course completion certificate.