**Azure Fundamentals**

The Azure Fundamentals exam covers three topics:

* Describe Cloud Concepts (25%-30%)
* Describe Azure Architecture and Services (35%-40%)
* Describe Management and Governance (30%-35%)

**Index**

[**1. Cloud Concepts** 3](#_Toc113891874)

[1.1. Azure Cloud Computing 3](#_Toc113891875)

[1.2. Advantages of Cloud 6](#_Toc113891876)

[1.3. Cloud Services 8](#_Toc113891877)

[**2. Azure Architecture and Services** 10](#_Toc113891878)

[2.1. Azure Physical Infrastructure 11](#_Toc113891879)

[2.2. Azure Management Infrastructure 13](#_Toc113891880)

[2.3. Azure Compute Services 14](#_Toc113891881)

[2.4. Azure Containers 16](#_Toc113891882)

[2.5. Azure Functions 16](#_Toc113891883)

[2.6. Azure App Service 16](#_Toc113891884)

[**3. Azure Network** 17](#_Toc113891885)

[3.1. Azure Networking Services 17](#_Toc113891886)

[3.2. Azure Virtual Private Networks 20](#_Toc113891887)

[3.3. Azure Express Route 21](#_Toc113891888)

[3.4. Azure DNS 21](#_Toc113891889)

[**4. Azure Storage** 22](#_Toc113891890)

[4.1. Azure Storage Redundancy 22](#_Toc113891891)

[4.2. Azure Storage Services 23](#_Toc113891892)

[4.3. Azure Migration Options 25](#_Toc113891893)

[4.4. File Movement 26](#_Toc113891894)

[**5. Azure Access** 27](#_Toc113891895)

[5.1. Azure Directory Services 27](#_Toc113891896)

[5.2. Azure Authentication 28](#_Toc113891897)

[5.3. External Identities 29](#_Toc113891898)

[5.4. Conditional Access 29](#_Toc113891899)

[5.5. Role-Based Access Control 30](#_Toc113891900)

[5.6. Zero Trust Model 30](#_Toc113891901)

[5.7. Defense In Depth 30](#_Toc113891902)

[5.8. Microsoft Defender for Cloud 31](#_Toc113891903)

# 1. Cloud Concepts

## 1.1. Azure Cloud Computing

Cloud computing allows you to have your services in the Cloud data center instead of in a physical location. This way, you can easily adjust the resources you need and delegate maintenance to the Cloud provider.

Services: Computer Power (CPU, RAM), Virtual Machines, Storage, Databases, Networking, Internet of Things (IoT) and Machine Learning (ML).

### 1.1.1. Shared Responsibility Model

When you have an on-premises datacenter you are responsible for everything. On the contrary, when you use Cloud computing you can decide how much responsibility you want to delegate to the Cloud provider. This depends on the types of service you select: Infrastructure as a Service(IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Is important to clarify that sometimes the responsibility depends on the situation. For example, if you user a cloud SQL database, the cloud provider is responsible for maintaining the database. However, if you deployed a virtual machine and installed an SQL database on it, you’d be responsible for database patches and updates.

### 1.1.2. Cloud Models

The cloud model defines the deployment type of cloud resources.

#### Private Cloud

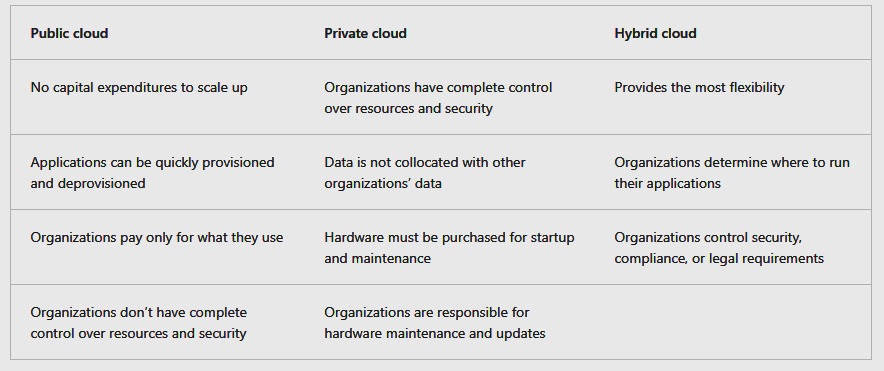
Is the natural evolution from the corporate datacenter. Is a cloud that is built, controlled and maintained by a single entity. This allows greater control but higher cost since you need to pay for all the available resources even if you’re not using them at all times. You may host you own datacenter, a dedicated offsite datacenter or a third party may have a dedicated datacenter for your company.

#### Public Cloud

A public cloud is built, controlled and maintained by a third-party cloud provider. Anyone that wants to purchase cloud services can access and user resources.

#### Hybric Cloud

Hybrid cloud is a computing environment where both public and private clouds get interconnected. You may need private cloud only for certain highly sensible services and may be comfortable having the rest in a public cloud. Thus, hybrid cloud allows balancing security and affordability.



#### Multi Cloud

Multi Cloud is when you have services with more than one cloud provider. It may be due to your organization migrating from one provider to another, or because you need to use features from both providers.

In any case, **Azure Arc** can help you manage your cloud environment, whether it’s a public Azure cloud, a private cloud in your datacenter, a hybrid configuration or a multi-cloud environment.

There is also a specialized **Azure VMware Solution** for running VMware workloads with seamless integration and scalability. This is useful when you have previously stablished a VMware private cloud environment but want to migrate to a publich or hybrid cloud.

### 1.1.3. Consumption base model

Cloud computing operates on a consumption-based model using operation expenditure (OpEx). On the contrary, a traditional datacenter uses capital expenditure (CapEx) because you need to estimate your current and future capacity and pay for it upfront.

The advantages of cloud services are:

* No upfront cost.
* No need to purchase or manage infrastructure.
* You can add or remove resources whenever you need to and adjust payment (easy to scale).

Cloud computing is a way to rent computer power and storage from someone else’s datacenter. You can treat cloud resources like you would resources in your own datacenter. However, unlike your own datacenter, when you’re done using cloud resources, your give them back.

## 1.2. Advantages of Cloud

Cloud computing allows you to have your services in the Cloud data center instead of in a physical location

### 1.2.1. High Availability

One of the most important considerations when deploying an application to the cloud is availability. Azure provides different SLA (Service Level Agreements) which are agreements between provider and customer for guaranteeing a stated level of service.

SLAs are related to service availability or uptime. The client may be credited if the SLA is not met. Common values for uptime in Azure are 99% (7.2 hrs per month), 99.9% (43 min per month), 99.95% (22 min per month) and 99.99% (4.32 min per month).

### 1.2.2. Scalability

Scalability refers to the ability to adjust resources to meet demand and is another important advantage of cloud services. Scalability allows the client to response to a system overload and to avoid overpaying for additional services.

Scaling usually has two varieties: vertical and horizontal. Vertical scaling focuses on increasing or decreasing the capabilities of resources. Horizontal scaling adds or subtracts the number of resources.

### 1.2.3. Reliability

Reliability is the ability of a system to recover from errors and continue to function. The cloud, due to its decentralized design, naturally supports reliable and resilient infrastructure because you can deploy resources in different regions around the world. In some cases, the cloud environment can automatically switch to another region.

### 1.2.4. Prediction

Predictability in the cloud lets you move forward with confidence. Predictability can be focused on performance or costs.

**Performance predictability** focuses on predicting the resources required to deliver a positive experience for customers. If you suddenly need more resources, **autoscaling** can deploy additional resources to meet demand, then scale back when it decreases. Or, if traffic is mostly concentrated in one area, **load balancing** will help redirect some of the overhead to areas with less stress.

**Cost forecasting** focuses on forecasting the cost of cloud spending. With the cloud, you can track resource usage in real time, monitor resources to ensure you're using them most efficiently, and apply data analytics to find patterns and trends to help better plan resource deployments. By operating in the cloud and using cloud insights and analytics, you can predict future costs and adjust resources as needed. You can even use tools like total cost of ownership (TCO) or pricing calculators to get an estimate of your potential cloud spend.

### 1.2.5. Security and Governance

Cloud provides several useful **governance** features. You can set a **template** to help ensure the deployed resources meet corporate standards and requirements. Plus, you can **update** all your deployed resources to new standards. Cloud-based **auditing** helps flags any resource that’s out of compliance and provides mitigation strategies. This process can also be automated.

On the **security** side, **infrastructure as a service** provides the maximum security since you’re able to handle physical resources, operative system and installed software, including patches and maintenance. **Platform as a service** and **software as a service** both take care of patches and maintenance automatically. Also, cloud is prepared to deal with attacks such as DDoS (distributed denial of service).

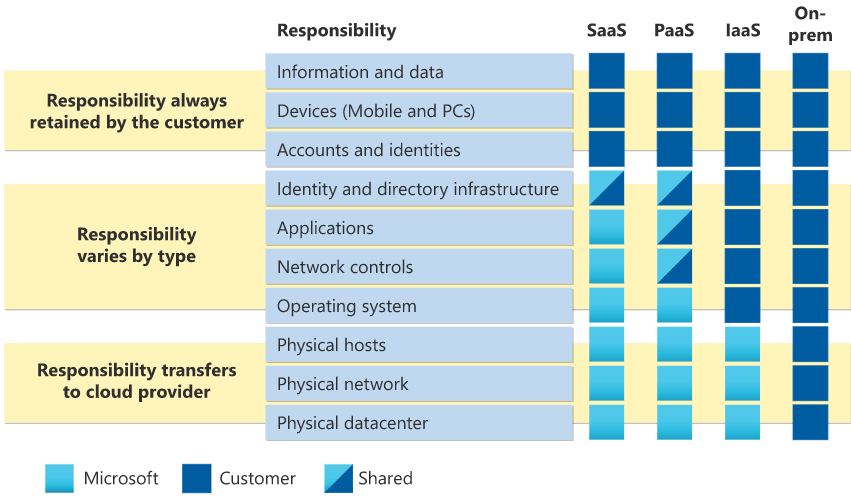
### 1.2.6. Manageability

Management comes in two forms. **Management of the cloud** is about controlling cloud resources such as: automatic **scale**, **templates**, **monitoring** and **alerts** based on configured metrics.

**Management in the cloud** refers to the way you can manage resources: through a **web portal**, using a **CLI**, using **APIs** or using **PowerShell**.

## 1.3. Cloud Services

Cloud services are IaaS, PaaS and SaaS. Each of them have particular advantages. Responsibility of cloud services is always shared.



### 1.3.1. IaaS

Infrastructure as a Service places most of the responsibility on the client. The provider is responsible for maintaining the physical infrastructure and its access to the internet. The client is responsible for the installation, configuration, patching, updates and security.

Common scenarios are:

* Lift-and-shift migration: You’re standing up cloud resources similar to your on-prem datacenter, and then simply moving the things running on-prem to running on the IaaS infrastructure.
* Testing and development: You have established configurations for development and test environments that you need to rapidly replicate. You can stand up or shut down the different environments rapidly with an IaaS structure, while maintaining complete control.

### 1.3.2. PaaS

In Platform as a Service the cloud provider maintains the physical infrastructure, physical security and connection to the internet, as well as the operating systems, middleware, development tools and business intelligence services that make up a cloud solution. In a PaaS scenario, you don’t have to worry about the licensing or patching for operating systems and databases. Common scenarios are:

* Development framework: PaaS provides a framework that developers can build upon to develop or customize cloud-based applications. Cloud features like scalability, high-availability and multi-tenant capability are included, reducing the amount of coding that developer must do.
* Analytics or business intelligence: Tools provided as a service allow organizations to analyze and mine their data, finding insights and patterns and predicting outcomes to improve forecasting, product design decisions, investments returns, and other business decisions.

### 1.3.3. SaaS

Software as a Service is the most complete cloud service where you’re basically renting or using a fully developed application. Email, financial software, messaging applications and connectivity software are all common examples of SaaS implementation:

* Email and messaging.
* Business productivity applications.
* Finance and expense tracking.

#### Azure Command Line

PowerShell:

Get-date

bash // change to bash CLI

Azure Commands:

az version // shows Azure version

az upgrade

az interactive // interactive mode where you can hit tab for displaying options.

// no need to use az in interactive mode

exit // exit interactive mode

# 2. Azure Architecture and Services

In this module, the main architectural components of Azure will be introduced. You'll learn about the physical organization of Azure: data centers, availability zones, and regions; and also about the organizational structure of Azure: resources and resource groups, subscriptions, and management groups.

## 2.1. Azure Physical Infrastructure

The Azure physical infrastructure is divided into physical and management infrastructure.

The physical infrastructure starts with datacenters which are facilities with resources arranged in racks, with dedicated power, cooling and networking infrastructure. Azure has datacenters around the world that are grouped into Azure Regions or Azure Availability zones.

### 2.1.1. Regions

A region is a geographical are on the planet that contains one or more datacenters that are nearby and networked together with a low-latency network. When you deploy a resource with Azure, you’ll often choose the region where you want your resource deployed.

### 2.1.2. Availability Zones

Availability zones are physically separate datacenters within an Azure region and are set up to be an isolation boundary. If one zone goes down, the others continue working because they have independent power, cooling and networking. Availability zones are connected through high-speed, private fiber-optic networks. Every Azure region that supports zones has at least 3 of them to guarantee resiliency.

* Zonal services: You pin the resource to a specific zone (for example, VMs, managed disks, IP addresses)
* Zone-redundant services: The platform replicates automatically across zones (for example, zone-redundant storage, SQL Database)
* Non-regional services: Service are always available from Azure geographies and are resilient to zone-wide outages as well as region-wide outages.

### 2.1.3. Region Pairs

Most Azure regions are paired with another region within the same geography (such as US, Europe, or Asia) at least 300 miles away. This approach allows for the replication of resources across a geography that helps reduce the likelihood of interruptions because of events such as natural disasters, civil unrest, power outages, or physical network outages that affect an entire region. For example, if a region in a pair was affected by a natural disaster, services would automatically fail over to the other region in its region pair.

* If an extensive Azure outage occurs, one region out of every pair is prioritized to make sure at least one is restored as quickly as possible for applications hosted in that region pair.
* Planned Azure updates are rolled out to paired regions one region at a time to minimize downtime and risk of application outage.
* Data continues to reside within the same geography as its pair (except for Brazil South) for tax- and law-enforcement jurisdiction purposes.

Most regions are paired in two directions, meaning they are the backup for the region that provides a backup for them (West US and East US back each other up). However, some regions, such as West India and Brazil South, are paired in only one direction. In a one-direction pairing, the Primary region does not provide backup for its secondary region. So, even though West India’s secondary region is South India, South India does not rely on West India. West India's secondary region is South India, but South India's secondary region is Central India. Brazil South is unique because it's paired with a region outside of its geography. Brazil South's secondary region is South Central US. The secondary region of South Central US isn't Brazil South.

### 2.1.4. Sovereign Regions

In addition to regular regions, Azure also has sovereign regions. Sovereign regions are instances of Azure that are isolated from the main instance of Azure. You may need to use a sovereign region for compliance or legal purposes.

Azure sovereign regions include:

* US DoD Central, US Gov Virginia, US Gov Iowa and more: These regions are physical and logical network-isolated instances of Azure for U.S. government agencies and partners. These datacenters are operated by screened U.S. personnel and include additional compliance certifications.
* China East, China North, and more: These regions are available through a unique partnership between Microsoft and 21Vianet, whereby Microsoft doesn't directly maintain the datacenters.

## 2.2. Azure Management Infrastructure

The management infrastructure includes Azure resources and resource groups, subscriptions and accounts.

### 2.2.1. Resources and resource groups

A resource is the basic building block of Azure. Anything you create, provision, deploy is a resource. Virtual machines, virtual networks, databases, cognitive services are all considered resources within Azure.

Every resource needs to be in a resource group which is just a grouping of resources. A single resource can only be in one group at the time and resource groups can’t be nested (not possible to have groups inside groups). When you apply an action to a resource group, that action will apply to all resources within, including deleting or granting access.

### 2.2.2. Subscriptions

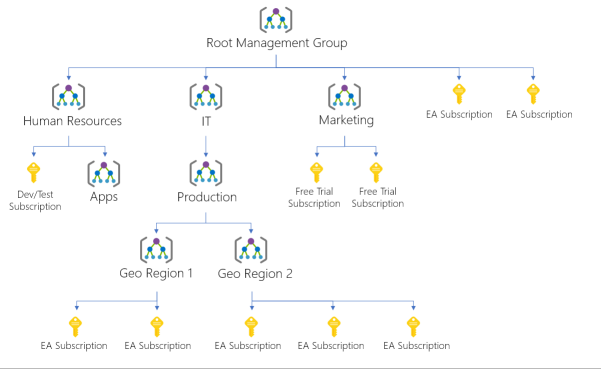
Subscriptions are a unit of management, billing and scale. Subscriptions allow you to logically organize resource groups and facilitate billing.

Using Azure requires an Azure subscription which provides you with access to products and services. An Azure subscription links to an Azure account, which is an identity in Azure Active Directory (Azure AD) or in a directory that Azure AD trusts. An account it’s required to have at least one subscription but it can contain multiple ones. Multi-subscriptions are used to define boundaries of two types:

* Billing boundary: Determines how an Azure account is billed for using Azure. You might want to create one subscription for your production workload and another for you development and testing workloads.
* Access control boundary: Used to limit access to products and functionalities. You can choose to separate environments for developing and testing. You can also reflect the organization structure: limit one team to lower-cost resources and enable full access for the IT department.

### 2.2.3. Management groups

Resources are grouped into resource groups which are then grouped into subscriptions. Subscriptions can be further contained into management groups. Management groups can be nested giving you enterprise-grade management at a large scale. A limit of 10,000 management groups can be supported in a single directory supporting until six levels of depth.



## 2.3. Azure Compute Services

Compute services are virtual machines, containers and similar.

### 2.3.1. Azure Virtual Machines

VMs are a way to provide infrastructure as a Service (IaaS) in the form of a virtualized server. Just like a physical computer, you can customize all of the software running on your VM. This makes it a perfect choice when you need to have total control over the operative system, the ability to run custom software and to use custom hosting configurations.

Using virtual machines you don’t have to worry about buy and maintain physical hardware but you’ll still need to configure, update and maintain the software that runs on the VM.

You can use an image to rapidly provision a VM. An image is a template that may already include OS and specialized software for a given task.

#### Scale Sets

You can group VMs together to provide high availability, scalability and redundancy. Scale sets is one of the two possible ways of grouping VMs.

Scale sets let you create and manage a group of identical, load-balanced VMs. You just need to create one virtual machine and Azure helps you automatize the replication and monitoring to automatically decide when to scale up or down based on preconfigured parameters. Scale sets also deploy a load balancer that makes sure your resources are being used efficiently.

#### Availability Sets

Availability sets are conceived to help you build a more resilient, highly available environment. Availability sets group VMs in two ways: update domain and fault domain.

The update domain groups VMs that can be rebooted at the same time. When applying updates only one update domain is offline at the time. Then, 30 minutes are given before the update begins in the next update domain.

Fault domains group the VMs by common power source and network switch. By default, an availability set will split you VMs across up to three fault domains. This helps protect against a physical power or networking failure. There is no extra cost for configuring an availability sets.

#### When to use VMs

During testing and development because you can combine different OS and application configurations. After using then you can easily remove the VMs.

When you need to run certain applications in the cloud like SharePoint to extend you on-premises network. Is also useful when you want to make lift and shift which means moving applications from your physical servers to the cloud.

During disaster recovery you can extend your on-premises network to the cloud to cover for the service your own network is missing.

#### VM Resources

When you create a VM you have the chance to pick resources including:

* Size (purpose, number of processor cores, and amount of RAM)
* Storage disks (hard disk drives, solid state drives, etc.)
* Networking (virtual network, public IP address, and port configuration)

#### VM commands

Create a virtual machine:

az vm create \

--resource-group learn-f7bf9502-0169-4d33-8ba7-8f95838e5008 \

--name my-vm \

--image UbuntuLTS \

--admin-username azureuser \

--generate-ssh-keys

Configure Nginx:

This commang uses a github script to download the latest package from internet using apt-get update. Then it installs Nginx and then sets the home page to /var/www/html/index.html to print a welcome message.

az vm extension set \

--resource-group learn-f7bf9502-0169-4d33-8ba7-8f95838e5008 \

--vm-name my-vm \

--name customScript \

--publisher Microsoft.Azure.Extensions \

--version 2.1 \

--settings '{"fileUris":["https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-nginx.sh"]}' \

--protected-settings '{"commandToExecute": "./configure-nginx.sh"}'

#### Azure Virtual Desktop

Azure Virtual Desktop is a type of virtual machine that provides a desktop and application virtualization service running on the cloud. It allows you to use a cloud-hosted version of Windows from any location. Is compatible across devices and operating systems and works with apps that you use to access remote desktops or most modern browsers.

Azure Virtual Desktop provides centralized security management for users' desktops with Azure Active Directory (Azure AD). You can enable multifactor authentication to secure user sign-ins. You can also secure access to data by assigning granular role-based access controls (RBACs) to users.

With Azure Virtual Desktop, the data and apps are separated from the local hardware. The actual desktop and apps are running in the cloud, meaning the risk of confidential data being left on a personal device is reduced. Additionally, user sessions are isolated in both single and multi-session environments.

Azure Virtual Desktop lets you use Windows 10 or Windows 11 Enterprise multi-session, the only Windows client-based operating system that enables multiple concurrent users on a single VM.

## 2.4. Azure Containers

Unlike virtual machines, you don’t manage the operating system for a container. Containers are lightweight and designed to be created, scaled out and stopped dynamically. Also VMs can also implement this, is always more efficient to do it with containers. Tasks like taking snapshots are also a lot faster with containers. While VMs virtualize the hardware, containers virtualize the operative system. One of the most popular container engines is Docker, which is supported by Azure.

### 2.4.1. Azure Container Instances

Azure container instances offer the fastest and simples way to run a container in Azure offering Platform as a Service. Azure Container Instances allow you to upload your containers and then the service will run the containers for you.

Containers are mostly used to create solutions by using a microservice architecture. This architecture is where you break solutions into smaller, independent pieces.

## 2.5. Azure Functions

Azure functions allow you to set triggers to perform work in response to an event (often via a REST request), timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less. Functions scale automatically based on demand, so they may be a good choice when demand is variable because resources are deallocated when the function is finished and you’re only charged for the CPU time used while your function runs.

Functions can be either stateless or stateful. When they're stateless (the default), they behave as if they're restarted every time they respond to an event. When they're stateful (called Durable Functions), a context is passed through the function to track prior activity.

## 2.6. Azure App Service

Azure App Service is a simplified hosting version provided in addition to VMs and containers. The goal is to let you focus on building and maintaining your app while Azure focuses on keeping the environment up and running.

App service enables you to build and host web apps, background jobs (WebJobs), mobilie back-ends and RESTful APIs in the programming language of your choice without managing infrastructure. It offers automatic scaling and availability supporting both Windows and Linux. It enables automated deployments from Github, Azure DevOps, or any Git repo to support a continuous deployment model.

# 3. Azure Network

## 3.1. Azure Networking Services

Networking services include Azure virtual networks, Azure DNS and Azure ExpressRoute.

### 3.1.1. Azure Virtual Networking

Azure virtual networks and virtual subnets enable Azure resources to communicate with each other, with internet users and you on-premises client computers. They allow public endpoints with a public IP as well as private endpoints within the virtual network.

### 3.1.2. Azure Isolation and segmentation

Azure virtual network allows you to create multiple isolated virtual networks with IP ranges existing only within Azure infrastructure. You can further divide IP address into subnets. For name resolution, you can use the Azure built in service or you can configure the virtual network to use either an internal or an external DNS Server.

### 3.1.3. Internet communications

You can enable incoming connections from the internet by assigning a public IP address to an Azure resource, or putting the resource behind a public load balancer

### 3.1.4. Communicate between Azure resources

There are two ways of achieving secure resource communication:

* Virtual networks that can connect VMs and other Azure services such as App Services, Azure Kubernetes Service and Azure virtual machine scale sets.
* Service endpoints can connect to other Azure resource types, such as Azure SQL databases and storage accounts. This approach enables you to link multiple Azure resources to virtual networks to improve security and provide optimal routing between resources.

### 3.1.5. Communicate with on-premises resources

Azure virtual networks enable you to link resources together in your on-premises environment and within your Azure subscription. In effect, you can create a network that spans both your local and cloud environments. There are three mechanisms for you to achieve this connectivity:

* Point-to-site virtual private network connections are from a computer outside your organization back into your corporate network. In this case, the client computer initiates an encrypted VPN connection to connect to the Azure virtual network.
* Site-to-site virtual private networks link your on-premises VPN device or gateway to the Azure VPN gateway in a virtual network. In effect, the devices in Azure can appear as being on the local network. The connection is encrypted and works over the internet.
* Azure ExpressRoute provides a dedicated private connectivity to Azure that doesn't travel over the internet. ExpressRoute is useful for environments where you need greater bandwidth and even higher levels of security.

### 3.1.6. Route Network Traffic

By default, Azure routes traffic between subnets on any connected virtual networks, on-premises networks, and the internet. You also can control routing and override those settings, as follows:

* Route tables allow you to define rules about how traffic should be directed. You can create custom route tables that control how packets are routed between subnets.
* Border Gateway Protocol (BGP) works with Azure VPN gateways, Azure Route Server, or Azure ExpressRoute to propagate on-premises BGP routes to Azure virtual networks.

### 3.1.7. Filter Network Traffic

Azure virtual networks enable you to filter traffic between subnets by using the following approaches:

* Network security groups are Azure resources that can contain multiple inbound and outbound security rules. You can define these rules to allow or block traffic, based on factors such as source and destination IP address, port, and protocol.
* Network virtual appliances are specialized VMs that can be compared to a hardened network appliance. A network virtual appliance carries out a particular network function, such as running a firewall or performing wide area network (WAN) optimization.

### 3.1.8. Connect Virtual Networks

You can link virtual networks together by using virtual network peering. Peering allows two virtual networks to connect directly to each other. Network traffic between peered networks is private, and travels on the Microsoft backbone network, never entering the public internet. Peering enables resources in each virtual network to communicate with each other. These virtual networks can be in separate regions, which allows you to create a global interconnected network through Azure.

User-defined routes (UDR) allow you to control the routing tables between subnets within a virtual network or between virtual networks. This allows for greater control over network traffic flow.

### 3.1.9. Networking in the Command Line

Store the list of IP from your network in a variable.

IPADDRESS="$(az vm list-ip-addresses \

--resource-group learn-292acb42-c63d-4e1d-a214-0c1119c21332 \

--name my-vm \

--query "[].virtualMachine.network.publicIpAddresses[\*].ipAddress" \

--output tsv)"

Try connecting to the web page returns an error message because the machine has no internet access.

curl --connect-timeout 5 http://$IPADDRESS

Print ip address:

echo $IPADDRESS

Get the security group associated with your network (my-vmNSG):

az network nsg list \

--resource-group learn-292acb42-c63d-4e1d-a214-0c1119c21332 \

--query '[].name' \

--output tsv

List the rules associated with that group:

az network nsg rule list \

--resource-group learn-292acb42-c63d-4e1d-a214-0c1119c21332 \

--nsg-name my-vmNSG \

--query '[].{Name:name, Priority:priority, Port:destinationPortRange, Access:access}' \

--output table

Create a rule that allows access using port 80:

az network nsg rule create \

--resource-group learn-292acb42-c63d-4e1d-a214-0c1119c21332 \

--nsg-name my-vmNSG \

--name allow-http \

--protocol tcp \

--priority 100 \

--destination-port-range 80 \

--access Allow

Verify list of rules is updated:

az network nsg rule list \

--resource-group learn-292acb42-c63d-4e1d-a214-0c1119c21332 \

--nsg-name my-vmNSG \

--query '[].{Name:name, Priority:priority, Port:destinationPortRange, Access:access}' \

--output table

Name Priority Port Access

----------------- ---------- ------ --------

default-allow-ssh 1000 22 Allow

allow-http 100 80 Allow

Now you can access the web page.

## 3.2. Azure Virtual Private Networks

A virtual private network (VPN) uses an encrypted tunnel within another network. VPNs are typically deployed to connect two or more trusted private networks to one another over an untrusted network (typically the public internet). Traffic is encrypted while traveling over the untrusted network to prevent eavesdropping or other attacks. VPNs can enable networks to safely and securely share sensitive information.

### 3.2.1. VPN Gateways

A VPN gateway is a type of virtual network gateway. Azure VPN Gateway instances are deployed in a dedicated subnet of the virtual network and enable the following connectivity:

* Connect on-premises datacenters to virtual networks through a site-to-site connection.
* Connect individual devices to virtual networks through a point-to-site connection.
* Connect virtual networks to other virtual networks through a network-to-network connection.

All data transfer is encrypted inside a private tunnel as it crosses the internet. You can deploy only one VPN gateway in each virtual network. However, you can use one gateway to connect to multiple locations, which includes other virtual networks or on-premises datacenters.

When you deploy a VPN gateway, you specify the VPN type: either policy-based or route-based. The main difference between these two types of VPNs is how traffic to be encrypted is specified. In Azure, both types of VPN gateways use a pre-shared key as the only method of authentication.

Policy-based VPN gateways specify statically the IP address of packets that should be encrypted through each tunnel. This type of device evaluates every data packet against those sets of IP addresses to choose the tunnel where that packet is going to be sent through.

In Route-based gateways, IPSec tunnels are modeled as a network interface or virtual tunnel interface. IP routing (either static routes or dynamic routing protocols) decides which one of these tunnel interfaces to use when sending each packet. Route-based VPNs are the preferred connection method for on-premises devices. They're more resilient to topology changes such as the creation of new subnets.

Use a route-based VPN gateway if you need any of the following types of connectivity:

* Connections between virtual networks
* Point-to-site connections
* Multisite connections
* Coexistence with an Azure ExpressRoute gateway

### 3.2.1. High Availability Scenarios

* **Active/Standby**: Is the default configuration that assigns two instances of VPN Gateways to each VPN resource in Azure. If the connection is interrupted because of an error the second Gateway begins working and is usually restored within a 90 seconds. The same happens for planned maintenance but the original is expected to be restored in just a few seconds.
* **Active/Active**: With the introduction of support for the BGP routing protocol, you can also deploy VPN gateways in an active/active configuration. In this configuration, you assign a unique public IP address to each instance. You then create separate tunnels from the on-premises device to each IP address. You can extend the high availability by deploying an additional VPN device on-premises.
* **ExpressRoute failover**: Another high-availability option is to configure a VPN gateway as a secure failover path for ExpressRoute connections. ExpressRoute circuits have resiliency built in. However, they aren't immune to physical problems that affect the cables delivering connectivity or outages that affect the complete ExpressRoute location. In high-availability scenarios, where there's risk associated with an outage of an ExpressRoute circuit, you can also provision a VPN gateway that uses the internet as an alternative method of connectivity. In this way, you can ensure there's always a connection to the virtual networks.
* **Zone-redundant gateways**: In regions that support availability zones, VPN gateways and ExpressRoute gateways can be deployed in a zone-redundant configuration. This configuration brings resiliency, scalability, and higher availability to virtual network gateways. Deploying gateways in Azure availability zones physically and logically separates gateways within a region while protecting your on-premises network connectivity to Azure from zone-level failures. These gateways require different gateway SKUs and use Standard public IP addresses instead of Basic public IP addresses.

## 3.3. Azure Express Route

Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection, with the help of a connectivity provider. This connection is called an ExpressRoute Circuit. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365. This allows you to connect offices, datacenters, or other facilities to the Microsoft cloud. Each location would have its own ExpressRoute circuit.

Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility. ExpressRoute connections don't go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet.

## 3.4. Azure DNS

The main benefits of the Azure DNS are reliability and performance, security, easy of use, customizable virtual network and alias records.

# 4. Azure Storage

## 4.1. Azure Storage Redundancy

Azure Storage always stores multiple copies of your data so that it's protected from planned and unplanned events such as transient hardware failures, network or power outages, and natural disasters. Redundancy ensures that your storage account meets its availability and durability targets even in the face of failures.

When deciding which redundancy option is best for your scenario, consider the tradeoffs between lower costs and higher availability. The factors that help determine which redundancy option you should choose include:

* How your data is replicated in the primary region.
* Whether your data is replicated to a second region that is geographically distant to the primary region, to protect against regional disasters.
* Whether your application requires read access to the replicated data in the secondary region if the primary region becomes unavailable

### 4.1.1. Redundancy in the Primary Region

Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage offers two options for how your data is replicated in the primary region, locally redundant storage (LRS) and zone-redundant storage (ZRS).

Locally Redundant Storage (LRS): Make three copies in the same datacenter for 11 nines durability over a year. LRS protects your data against server rack and drive failures. However, if a disaster such as a fire or flooding occurs within the data center, all replicas of a storage account using LRS may be lost or unrecoverable.

Zone-Redundant Storage (ZRS): Replicates your Azure Storage data synchronously across three Azure availability zones in the primary region offering a 12 nines durability. The data will be accessible to read and write even if a zone becomes unavailable because Azure undertakes networking updates such as DNS repointing to access the new pieces of data. ZRS is recommended for high availability scenarios of for restricting replication of data within a country or region to meet data governance requirements.

### 4.1.2. Redundancy in the Secondary Region

If you want to guarantee your data will persist even in the event of a catastrophic failure Azure provides redundancy in the secondary region which has to be the pair of your region inevitably. Is important to note that data is replicated asynchronously to the secondary region so some data may be lost if an event occurs. Azure Recovery Point Objective (RPO – time between saves) is typically less than 15 minutes. Two possible schemes:

* Geo-Redundant Storage(GRS): First copy data three times in the same zone in the primary region using LRS and then replicate it to the secondary region for 16 nines durability.
* Geo-Zone-Redundant Storage(GZRS): Data is copied across the three availability zones in the primary region using ZRS and is also replicated to a secondary geographic region also for 16 nines durability.

#### Read Access to Data in Secondary Region

Geo-redundant storage (with GRS or GZRS) replicates your data to another physical location in the secondary region to protect against regional outages. However, that data is available to be read only if the customer or Microsoft initiates a failover from the primary to secondary region. However, if you enable read access to the secondary region, your data is always available, even when the primary region is running optimally. For read access to the secondary region, enable read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS).

## 4.2. Azure Storage Services

The Azure Storage platform includes 4 main data services: Azure Blobs, Azure Files, Azure Queues and Azure Disks.

### 4.2.1. Blob Storage

Azure Blob Storage is unstructured, meaning that there are no restrictions on the kinds of data it can hold. Blob Storage purpose is to contain massive amounts of data. Therefore, it can manage thousands of simultaneous uploads, massive amounts of video data, constantly growing log files, and can be reached from anywhere with an internet connection.

One advantage of blob storage over disk storage is that it doesn't require developers to think about or manage disks. Data is uploaded as blobs, and Azure takes care of the physical storage needs. This makes blobs ideal for:

* Serving images or documents directly to a browser.
* Storing files for distributed access.
* Streaming video and audio.
* Storing data for backup and restore, disaster recovery, and archiving.
* Storing data for analysis by an on-premises or Azure-hosted service.

Objects in Blob storage can be accessed from anywhere in the world via HTTP or HTTPS. Users or client applications can access blobs via URLs, the Azure Storage REST API, Azure PowerShell, Azure CLI, or an Azure Storage client library. The storage client libraries are available for multiple languages, including .NET, Java, Node.js, Python, PHP, and Ruby.

#### Blob Storage Tiers

Data stored in the cloud can grow at an exponential pace. To manage costs for your expanding storage needs, it's helpful to organize your data based on attributes like frequency of access and planned retention period. Data stored in the cloud can be handled differently based on how it's generated, processed, and accessed over its lifetime. Some data is actively accessed and modified throughout its lifetime. Some data is accessed frequently early in its lifetime, with access dropping drastically as the data ages. Some data remains idle in the cloud and is rarely, if ever, accessed after it's stored. To accommodate these different access needs, Azure provides several access tiers, which you can use to balance your storage costs with your access needs.

Azure Storage offers different access tiers for your blob storage, helping you store object data in the most cost-effective manner. The available access tiers include:

* Hot access tier: Optimized for storing data that is accessed frequently (for example, images for your website).
* Cool access tier: Optimized for data that is infrequently accessed and stored for at least 30 days (for example, invoices for your customers).
* Archive access tier: Appropriate for data that is rarely accessed and stored for at least 180 days, with flexible latency requirements (for example, long-term backups).

### 4.2.2. Azure Files

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) or Network File System (NFS) protocols. Azure Files file shares can be mounted concurrently by cloud or on-premises deployments. SMB Azure file shares are accessible from Windows, Linux, and macOS clients. NFS Azure Files shares are accessible from Linux or macOS clients. Additionally, SMB Azure file shares can be cached on Windows Servers with Azure File Sync for fast access near where the data is being used.

The key benefits are:

* **Shared access**: Azure file shares support the industry standard SMB and NFS protocols, meaning you can seamlessly replace your on-premises file shares with Azure file shares without worrying about application compatibility.
* **Fully managed**: Azure takes care of hardware and OS.
* **Scripting and tooling**: PowerShell cmdlets and Azure CLI can be used to create, mount, and manage Azure file shares as part of the administration of Azure applications.
* **Resiliency**: Given the strong Azure infrastructure.
* **Familiar programmability**: Applications running in Azure can access data in the share via file system I/O APIs. Developers can therefore leverage their existing code and skills to migrate existing applications. In addition to System IO APIs, you can use Azure Storage Client Libraries or the Azure Storage REST API.

### 4.2.3. Queue Storage

Azure Queue Storage is a service for storing large numbers of messages. Once stored, you can access the messages from anywhere in the world via authenticated calls using HTTP or HTTPS. A queue can contain as many messages as your storage account has room for (potentially millions). Each individual message can be up to 64 KB in size. Queues are commonly used to create a backlog of work to process asynchronously.

Queue storage can be combined with compute functions like Azure Functions to take an action when a message is received. For example, you want to perform an action after a customer uploads a form to your website. You could have the submit button on the website trigger a message to the Queue storage. Then, you could use Azure Functions to trigger an action once the message was received.

### 4.2.4. Disk Storage

Disk storage, or Azure managed disks, are block-level storage volumes managed by Azure for use with Azure VMs. Conceptually, they’re the same as a physical disk, but they’re virtualized – offering greater resiliency and availability than a physical disk. With managed disks, all you have to do is provision the disk, and Azure will take care of the rest.

## 4.3. Azure Migration Options

There are two ways to get data into Azure storages: Azure Migrate and Azure Data Box. Azure Migrate allows real-time migration of infrastructure, applications and data while Azure Data Box supports asynchronous migration of data.

### 4.3.1. Azure Migrate Tools

Azure Migrate helps you migrate from an on-premises environment to the cloud providing a unified migration platform to start, run and track the process. The following tools are provide by Azure for migration:

* **Azure Migrate: Discovery and assessment**. Discover and assess on-premises servers running on VMware, Hyper-V, and physical servers in preparation for migration to Azure.
* **Azure Migrate: Server Migration**. Migrate VMware VMs, Hyper-V VMs, physical servers, other virtualized servers, and public cloud VMs to Azure.
* **Data Migration Assistant**. Data Migration Assistant is a stand-alone tool to assess SQL Servers. It helps pinpoint potential problems blocking migration. It identifies unsupported features, new features that can benefit you after migration, and the right path for database migration.
* **Azure Database Migration Service**. Migrate on-premises databases to Azure VMs running SQL Server, Azure SQL Database, or SQL Managed Instances.
* **Web app migration assistant**. Azure App Service Migration Assistant is a standalone tool to assess on-premises websites for migration to Azure App Service. Use Migration Assistant to migrate .NET and PHP web apps to Azure.
* **Azure Data Box**. Use Azure Data Box products to move large amounts of offline data to Azure.

### 4.3.2. Azure Data Box

Azure Data Box is a physical migration service that helps transfer large amounts of data in a quick, inexpensive, and reliable way. The secure data transfer is accelerated by shipping you a proprietary Data Box storage device that has a maximum usable storage capacity of 80 terabytes. The Data Box is transported to and from your datacenter via a regional carrier. A rugged case protects and secures the Data Box from damage during transit.

You can order the Data Box device via the Azure portal to import or export data from Azure. Once the device is received, you can quickly set it up using the local web UI and connect it to your network. Once you’re finished transferring the data (either into or out of Azure), simply return the Data Box. If you’re transferring data into Azure, the data is automatically uploaded once Microsoft receives the Data Box back. The entire process is tracked end-to-end by the Data Box service in the Azure portal.

Data Box is ideally suited to transfer data sizes larger than 40 TBs in scenarios with no to limited network connectivity. The data movement can be one-time, periodic, or an initial bulk data transfer followed by periodic transfers.

## 4.4. File Movement

In addition to large scale migration using services like Azure Migrate and Azure Data Box, Azure also has tools designed to help you move or interact with individual files or small file groups. Among those tools are AzCopy, Azure Storage Explorer and Azure File Sync.

### 4.4.1. AzCopy

AzCopy is a command-line utility that you can use to copy blobs or files to or from your storage account. With AzCopy, you can upload files, download files, copy files between storage accounts, and even synchronize files. AzCopy can even be configured to work with other cloud providers to help move files back and forth between clouds. Is important to note that Synchronizing with AzCopy is one-direction only.

### 4.4.2. Azure Storage Explorer

Azure Storage Explorer is a standalone app that provides a graphical interface to manage files and blobs in your Azure Storage Account. It works on Windows, macOS, and Linux operating systems and uses AzCopy on the backend to perform all of the file and blob management tasks. With Storage Explorer, you can upload to Azure, download from Azure, or move between storage accounts.

### 4.4.3. Azure File Sync

Azure File Sync is a tool that lets you centralize your file shares in Azure Files and keep the flexibility, performance, and compatibility of a Windows file server. It’s almost like turning your Windows file server into a miniature content delivery network. Once you install Azure File Sync on your local Windows server, it will automatically stay bi-directionally synced with your files in Azure.

# 5. Azure Access

## 5.1. Azure Directory Services

Azure Active Directory (Azure AD) is a directory service that enables you to sign in and access both Microsoft cloud applications and cloud applications that you develop. Azure AD can also help you maintain your on-premises Active Directory deployment.

One method of connecting Azure AD with your on-premises AD is using Azure AD Connect. Azure AD Connect synchronizes user identities between on-premises Active Directory and Azure AD. Azure AD Connect synchronizes changes between both identity systems, so you can use features like SSO, multifactor authentication, and self-service password reset under both systems.

Azure AD provides services such as:

* **Authentication**: This includes verifying identity to access applications and resources. It also includes providing functionality such as self-service password reset, multifactor authentication, a custom list of banned passwords, and smart lockout services.
* **Single sign-on**: Single sign-on (SSO) enables you to remember only one username and one password to access multiple applications. A single identity is tied to a user, which simplifies the security model. As users change roles or leave an organization, access modifications are tied to that identity, which greatly reduces the effort needed to change or disable accounts.
* **Application management**: You can manage your cloud and on-premises apps by using Azure AD. Features like Application Proxy, SaaS apps, the My Apps portal, and single sign-on provide a better user experience.
* **Device management**: Along with accounts for individual people, Azure AD supports the registration of devices. Registration enables devices to be managed through tools like Microsoft Intune. It also allows for device-based Conditional Access policies to restrict access attempts to only those coming from known devices, regardless of the requesting user account.

### 5.1.1. Azure Domain Services

Azure Active Directory Domain Services (Azure AD DS) is a service that provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. Just like Azure AD lets you use directory services without having to maintain the infrastructure supporting it, with Azure AD DS, you get the benefit of domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.

When you create an Azure AD DS managed domain, you define a unique namespace. This namespace is the domain name. Two Windows Server domain controllers are then deployed into your selected Azure region. This deployment of DCs is known as a replica set. You don't need to manage, configure, or update these DCs. The Azure platform handles the DCs as part of the managed domain, including backups and encryption at rest using Azure Disk Encryption.

A managed domain is configured to perform a one-way synchronization from Azure AD to Azure AD DS. You can create resources directly in the managed domain, but they aren't synchronized back to Azure AD. In a hybrid environment with an on-premises AD DS environment, Azure AD Connect synchronizes identity information with Azure AD, which is then synchronized to the managed domain.

## 5.2. Azure Authentication

Azure supports multiple authentication methods, including standard passwords, single sign-on (SSO), multifactor authentication (MFA), and passwordless.

### 5.2.1. Single Sign-On

Single sign-on (SSO) enables a user to sign in one time and use that credential to access multiple resources and applications from different providers. For SSO to work, the different applications and providers must trust the initial authenticator.

With SSO, you need to remember only one ID and one password. Access across applications is granted to a single identity that's tied to the user, which simplifies the security model. As users change roles or leave an organization, access is tied to a single identity. This change greatly reduces the effort needed to change or disable accounts. Using SSO for accounts makes it easier for users to manage their identities and for IT to manage users.

### 5.2.2. Multifactor Authentication

Multifactor authentication is the process of prompting a user for an extra form (or factor) of identification during the sign-in process. MFA helps protect against a password compromise in situations where the password was compromised but the second factor wasn't.

Multifactor authentication provides additional security for your identities by requiring two or more elements to fully authenticate. These elements fall into three categories:

* Something the user knows – this might be a challenge question.
* Something the user has – this might be a code that's sent to the user's mobile phone.
* Something the user is – this is typically some sort of biometric property, such as a fingerprint or face scan.

#### Azure AD Multi-Factor

Azure AD Multi-Factor Authentication is a Microsoft service that provides multifactor authentication capabilities. Azure AD Multi-Factor Authentication enables users to choose an additional form of authentication during sign-in, such as a phone call or mobile app notification.

### 5.2.3. Passwordless Authentication

Passwordless authentication needs to be set up on a device before it can work. For example, your computer is something you have. Once it’s been registered or enrolled, Azure now knows that it’s associated with you. Now that the computer is known, once you provide something you know or are (such as a PIN or fingerprint), you can be authenticated without using a password.

Each organization has different needs when it comes to authentication. Microsoft global Azure and Azure Government offer the following three passwordless authentication options that integrate with Azure Active Directory (Azure AD):

* **Windows Hello for Business**: Windows Hello for Business is ideal for information workers that have their own designated Windows PC. The biometric and PIN credentials are directly tied to the user's PC, which prevents access from anyone other than the owner.
* **Microsoft Authenticator app:** The Authenticator App turns any iOS or Android phone into a strong, passwordless credential. Users can sign-in to any platform or browser by getting a notification to their phone, matching a number displayed on the screen to the one on their phone, and then using their biometric (touch or face) or PIN to confirm.
* **FIDO2 security keys:** The FIDO (Fast Identity Online) Alliance helps to promote open authentication standards and reduce the use of passwords as a form of authentication. FIDO2 is the latest standard that incorporates the web authentication (WebAuthn) standard.

FIDO2 security keys are an unphishable standards-based passwordless authentication method that can come in any form factor. Fast Identity Online (FIDO) is an open standard for passwordless authentication. FIDO allows users and organizations to leverage the standard to sign-in to their resources without a username or password by using an external security key or a platform key built into a device.

Users can register and then select a FIDO2 security key at the sign-in interface as their main means of authentication. These FIDO2 security keys are typically USB devices, but could also use Bluetooth or NFC. With a hardware device that handles the authentication, the security of an account is increased as there's no password that could be exposed or guessed.

## 5.3. External Identities

An external identity is a person, device, service, etc. that is outside your organization. Azure AD External Identities refers to all the ways you can securely interact with users outside of your organization. If you want to collaborate with partners, distributors, suppliers, or vendors, you can share your resources and define how your internal users can access external organizations. If you're a developer creating consumer-facing apps, you can manage your customers' identity experiences.

External identities may sound similar to single sign-on. With External Identities, external users can "bring their own identities." Whether they have a corporate or government-issued digital identity, or an unmanaged social identity like Google or Facebook, they can use their own credentials to sign in. The external user’s identity provider manages their identity, and you manage access to your apps with Azure AD or Azure AD B2C to keep your resources protected.

The following capabilities make up External Identities:

* **Business to business (B2B) collaboration** - Collaborate with external users by letting them use their preferred identity to sign-in to your Microsoft applications or other enterprise applications (SaaS apps, custom-developed apps, etc.). B2B collaboration users are represented in your directory, typically as guest users.
* **B2B direct connect** - Establish a mutual, two-way trust with another Azure AD organization for seamless collaboration. B2B direct connect currently supports Teams shared channels, enabling external users to access your resources from within their home instances of Teams. B2B direct connect users aren't represented in your directory, but they're visible from within the Teams shared channel and can be monitored in Teams admin center reports.
* **Azure AD business to customer (B2C)** - Publish modern SaaS apps or custom-developed apps (excluding Microsoft apps) to consumers and customers, while using Azure AD B2C for identity and access management.

## 5.4. Conditional Access

Conditional Access is a tool that Azure Active Directory uses to allow (or deny) access to resources based on identity signals. These signals include who the user is, where the user is, what device the user is requesting access from or the application the user is trying to access.

Conditional Access also provides a more granular multifactor authentication experience for users. For example, a user might not be challenged for second authentication factor if they're at a known location. However, they might be challenged for a second authentication factor if their sign-in signals are unusual or they're at an unexpected location. In some cases is also useful to forbid access from outside of a certain area.

## 5.5. Role-Based Access Control

Azure provides built-in roles that describe common access rules for cloud resources. You can also define your own roles. Each role has an associated set of access permissions that relate to that role. When you assign individuals or groups to one or more roles, they receive all the associated access permissions. So, if you hire a new engineer, all you have to do is add him to the Azure RBAC (Azure Role-Based Access Control) for engineers.

Role-based access control is applied to a scope, which is a resource or set of resources that this access applies to. Scopes include:

* A management group (a collection of multiple subscriptions).
* A single subscription.
* A resource group.
* A single resource.

Observers, users managing resources, admins, and automated processes illustrate the kinds of users or accounts that would typically be assigned each of the various roles. Azure RBAC is hierarchical, in that when you grant access at a parent scope, those permissions are inherited by all child scopes.

## 5.6. Zero Trust Model

Zero Trust is a security model that assumes the worst case scenario and protects resources with that expectation. Zero Trust assumes breach at the outset, and then verifies each request as though it originated from an uncontrolled network.

Today, organizations need a new security model that effectively adapts to the complexity of the modern environment; embraces the mobile workforce: and protects people, devices, applications, and data wherever they're located.

To address this new world of computing, Microsoft highly recommends the Zero Trust security model, which is based on these guiding principles:

* Verify explicitly - Always authenticate and authorize based on all available data points.
* Use least privilege access - Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
* Assume breach - Minimize blast radius and segment access. Verify end-to-end encryption. Use analytics to get visibility, drive threat detection, and improve defenses.

Traditionally, corporate networks were restricted, protected, and generally assumed safe. Only managed computers could join the network, VPN access was tightly controlled, and personal devices were frequently restricted or blocked.

The Zero Trust model flips that scenario. Instead of assuming that a device is safe because it’s within the corporate network, it requires everyone to authenticate. Then grants access based on authentication rather than location.

## 5.7. Defense In Depth

You can visualize defense-in-depth as a set of layers, with the data to be secured at the center and all the other layers functioning to protect that central data layer. Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. This approach removes reliance on any single layer of protection. It slows down an attack and provides alert information that security teams can act upon, either automatically or manually.

Here's a brief overview of the role of each layer:

* The physical security layer is the first line of defense to protect computing hardware in the datacenter.
* The identity and access layer controls access to infrastructure and change control.
* The perimeter layer uses distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
* The network layer limits communication between resources through segmentation and access controls.
* The compute layer secures access to virtual machines.
* The application layer helps ensure that applications are secure and free of security vulnerabilities.
* The data layer controls access to business and customer data that you need to protect.

## 5.8. Microsoft Defender for Cloud

Defender for Cloud is a monitoring tool for security posture management and threat protection. It monitors your cloud, on-premises, hybrid, and multi-cloud environments to provide guidance and notifications aimed at strengthening your security posture.

Because Defender for Cloud is an Azure-native service, many Azure services are monitored and protected without needing any deployment. However, if you also have an on-premises datacenter or are also operating in another cloud environment, monitoring of Azure services may not give you a complete picture of your security situation.

When necessary, Defender for Cloud can automatically deploy a Log Analytics agent to gather security-related data. For Azure machines, deployment is handled directly. For hybrid and multi-cloud environments, Microsoft Defender plans are extended to non-Azure machines with the help of Azure Arc. Cloud security posture management (CSPM) features are extended to multi-cloud machines without the need for any agents.

Defender for Cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises:

* **Continuously assess** – Know your security posture. Identify and track vulnerabilities.
* **Secure** – Harden resources and services with Azure Security Benchmark.
* **Defend** – Detect and resolve threats to resources, workloads, and services.

Defender for cloud provides advanced threat protection features for many of your deployed resources, including virtual machines, SQL databases, containers, web applications, and your network. Protections include securing the management ports of your VMs with just-in-time access, and adaptive application controls to create allowlists for what apps should and shouldn't run on your machines.