# 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%)

# 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.

### 1.1.2.1 Private Cloud

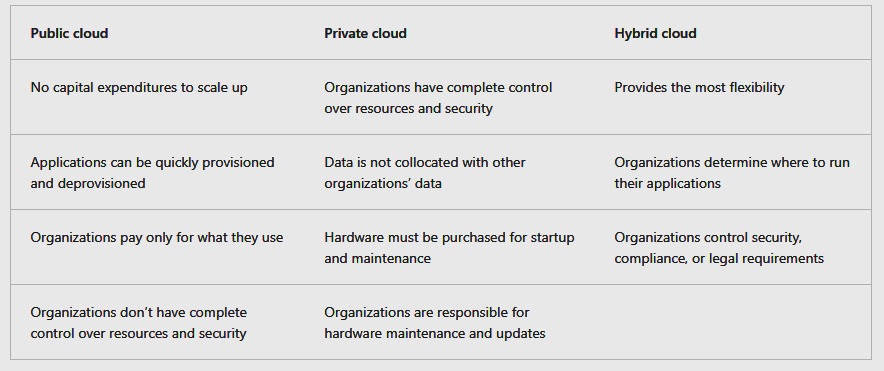
Is the natural evolution from the corporate datacenter. Is a cloud that is built, controlled and maintained by a single entity. This allows greater control but higher cost since you need to pay for all the available resources even if you’re not using them at all times. You may host you own datacenter,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

### 1.1.2.2 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.

### 1.1.2.3 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.



### 1.1.2.4 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).

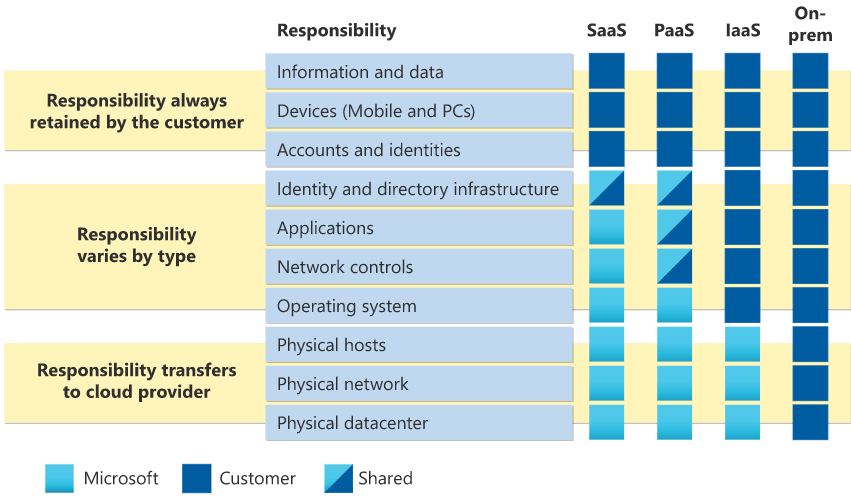
## 1.2.6. Manageability

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.

# 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.

After completing this module, you will be able to:

* Describe Azure regions, region pairs, and sovereign regions.
* Describe Availability Zones.
* Describe Azure data centers.
* Describe Azure resources and resource groups.
* Describe subscriptions.
* Describe management groups.
* Describe the hierarchy of resource groups, subscriptions, and management groups.

## 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

# 2.1. Azure Physical Infrastructure

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

## 2.1. Physical 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

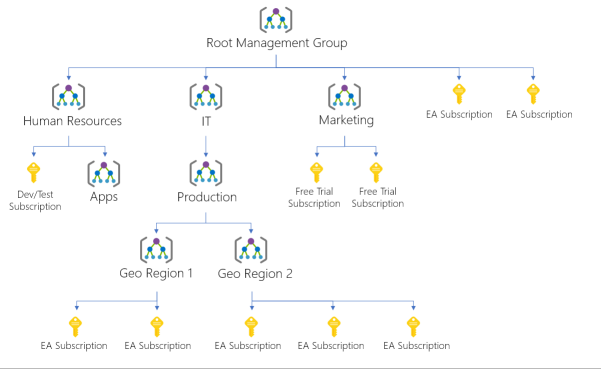
Subscriptions are a unit of management, billing and scale. Subscriptions allow you to logically organize resource groups and facilitate billing.

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.

### 2.3.1.1. 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.

### 2.3.1.2. 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.

### 2.3.1.3. 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.

### 2.3.1.4. 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)

### 2.3.1.5. 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"}'

### 2.3.1.6. 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.

# 3.1. 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 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. 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.

# 4.2. 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).