**Microsoft Azure Fundamentals: Describe cloud concepts.**

**What is cloud computing?**

Basically, is a way to rent compute power and storage from someone else datacentre.

Cloud computing is the delivery of computing services over the internet.

In essence, cloud computing is like having a virtual restaurant for your IT needs. You choose what services you want from the menu, enjoy additional innovative offerings, and can easily expand your "restaurant" without dealing with the limitations of physical kitchens or waiting for construction.

**What is shared responsibility model?**

As the name suggests, responsibilities get shared between the cloud provider and the consumer.

For example, physical security, power, cooling, and network connectivity are the responsibility of the cloud provider, wouldn’t make sense for the consumer to have any of those responsibilities.

The consumer is responsible for the data and information stored in the cloud.

Also, for some things, the responsibility depends on the situation.

**There is a graph that helps to visualize it:**

A screen shot of a computer

Description automatically generated

**Traditional Home Ownership (On-Premises Datacenter):**

Imagine owning a house. You're responsible for everything - from the security of your property, fixing the roof, maintaining the garden, to making sure all the appliances inside are working smoothly. It's a lot on your plate.

**Renting an Apartment (Cloud Computing):**

Now, think of moving into an apartment. The property owner takes care of the building's security, repairs, and utilities like water and electricity. You, as the tenant, are responsible for your personal belongings inside the apartment, ensuring only trusted people have access.

**Shared Responsibility Model in Cloud Computing:**

Cloud computing is like renting an apartment. The cloud provider (property owner) manages physical security, power, cooling, and network connectivity. You focus on what's inside - your data and applications.

**According to the shared responsibility model, which cloud service type places the most responsibility on the customer?**

IaaS places the most responsibility on the consumer, with the cloud provider being responsible for the basics of physical security, power, and connectivity.

**What are the types of cloud models?**

private, public, and hybrid.

**Let’s explain a bit about each one of those models:**

* Private: It is a cloud used by a single entity, given great control for the company, but there is a greater cost.
* Public: it is a cloud built, controlled, and maintained by a third-party (cloud provider). Anyone that wants to purchase cloud services can access and use resources.
* Hybrid: as imagined, uses both public and private clouds, that can allow a private cloud to use extra temporary resources, also can provide extra layer of security
* *Multi-cloud: in that scenario the company uses multiple public cloud providers, for example when you are migrating from one service to another, or when you need to use different features from different cloud providers.*

A screenshot of a computer

Description automatically generated**There is a graph that can help you to visualize it:**

Private Cloud: Think of it as building your dream house—your exclusive digital space, fully customized but with higher costs. You decide if it's on your own land or in a dedicated neighborhood, possibly managed by a third party.

Public Cloud: Imagine renting an apartment in a tower block—a shared space open to everyone. It's widely available, cost-effective, and offers shared benefits like security and infrastructure managed by the building owner.

Hybrid Cloud: Picture living in a diverse suburban neighborhood with different house styles. A hybrid cloud lets you choose between your custom home (private cloud) and renting apartments (public cloud) as needed, providing flexibility, security, and scalability for varying demands.

**Which cloud model uses some datacentres focused on providing cloud services to anyone that wants them, and some data centres that are focused on a single customer?**

The hybrid cloud model is a combination of public cloud and private cloud, using both datacentres dedicated solely to one customer and datacentres that are shared with the public.

**What is Capital expenditure (Capex)?**

It is an expense (expenditure), that usually is initial and made one-time, for example: build a datacentre, buy a new building.

**What is Operational Expenditure (OpEx)?**

It is an expense on products or services over time, for example, rent a convention centre, sign up for cloud services.

**What is consumption-based model?**

In that model (used in cloud computing), you don’t pay for physical infrastructure / electricity… you pay for the IT resources you use, if you don’t use, you don’t pay for it.

(If you find that you need more virtual machines, you add more. If the demand drops and you don’t need as many virtual machines, you remove machines as needed. Either way, you’re only paying for the virtual machines that you use)

**What are the benefits of consumption-based model?**

1. No upfront cost
2. Ability to pay more resources when you need them.
3. Ability to stop paying resources when you no longer need them.
4. No need buy/manage infrastructure.
5. Helps to plan and manage operating costs.
6. Helps to scale your business.

Imagine setting up a home office. Buying a desk, chair, and computer upfront (like building a datacentre) is like Capital Expenditure (Capex) – a one-time expense for tangible things. On the other hand, Operational Expenditure (OpEx) is like paying monthly for internet services – an ongoing cost for a continuous benefit.

Now, think about cloud computing. It's like renting a laptop instead of buying one. You only pay for the time you use it, and you don't worry about fixing or upgrading it – that's the cloud provider's job. This pay-as-you-go approach is OpEx in action. It's flexible – need more computing power? Rent more. Don't need it anymore? Stop renting. It's like paying for electricity – you only pay for what you use, not for the power plant.

**In cloud applications, what means high availability?**

That ensures the resources are available when needed (regardless of disruptions or events that may occur.), another term related to availability is uptime.

**In cloud applications, what means scalability?**

It is the ability to adjust resources to handle demand, that means you can add or reduce resources as your business needs.

**What are the 2 types of scalabilities?**

* Vertical- ability of scale the capabilities of resource, adding or removing CPU /RAM for example.
* Horizontal- ability of scale number of resources, for example adding or removing virtual machines or containers.

**Which type of scaling involves adding or removing resources (such as virtual machines or containers) to meet demand?**

Horizontal scaling is adding or subtracting the number of resources.

High Availability:

Imagine you're ordering food delivery from your favourite restaurant. High availability is like knowing that no matter what, they'll always have chefs ready to cook and deliver your meal. Even if there's a busy evening or a sudden surge in orders, you're confident the restaurant's service won't be disrupted, and you'll get your food on time.

Scalability:

Now, think of scalability as having a magical kitchen that adjusts based on your dinner party size. If more friends unexpectedly join, you can magically expand the kitchen (scale up resources) by adding more chefs or cooking spaces to handle the increased demand. On the flip side, if fewer friends show up, you can shrink the kitchen back to its usual size (scale down resources) to avoid unnecessary costs.

**What means reliability in the cloud?**

It is the ability of a system to recover from failures and continue to function. For example, if happens a catastrophic event in one region, your data is safe in another region and maintain the service.

**What means predictability in the cloud?**

It is the ability to move forward with confidence, that can be focused on performance or cost.

* Cost predictability – focused on the cost of the cloud spend.
* Performance predictability- focused on the resources needed to deliver a positive experience for the customers.

Reliability:

Imagine a reliable courier service delivering your packages. If one delivery person encounters an issue, another quickly takes over, ensuring your packages reach you on time.

Predictability:

Think of predictability as using a GPS for your travel plans. It not only tells you the best route but also estimates the time and fuel cost, helping you plan your journey confidently.

**What are the benefits of security and governance in the cloud?**

1. Enhanced Data Protection:

Measures to safeguard sensitive data, reducing the risk of breaches and unauthorized access.

1. Compliance Assurance:

Help organizations meet regulatory requirements, ensuring adherence to industry-specific standards and data protection laws.

1. Continuous Monitoring:

Enable real-time monitoring and threat detection, allowing for quick response to potential security incidents.

1. Automation and Orchestration:

Automation in the cloud streamlines security processes, reducing human error and improving overall efficiency.

**What is Management OF the cloud?**

That means managing your cloud resources, for example automatically scale resource deployment based on need or receive automatic alerts based on configured metrics, Monitor the health of resources.

**What is Management IN the cloud?**

Management in the cloud is how you can manage your cloud environment and resources. For example: Through a web portal or using a command line interface.

**What is characterized as the ability of a system to recover from failures and continue to function?**

Reliability is the ability of a system to recover from failures and continue to function, and it is one of the pillars of the Microsoft Azure Well-Architected Framework.

**Which type of scaling involves adding or removing resources (such as virtual machines or containers) to meet demand?**

Horizontal scaling is adding or subtracting the number of resources.

**What is Azure SLA?**

That is a kind of contract that guarantees the % of uptime (services are available) and downtime, more guarantee of uptime (100%) is also more expensive, usually the Azure SLA is 99% (can have a downtime of max 1.68 hour per week), 99.9% (can have a downtime of max 10 min per week), there is also 99.95%, 99.99% options available.

Governance and Compliance:

Think of governance and compliance as a set of rules for your office. You create templates for how desks, chairs, and computers should be arranged to meet company standards and government regulations. These templates ensure consistency and can be easily updated if there are changes in the rules. Auditing is like a regular check to make sure everything follows the rules, and if something is out of line, there are suggestions on how to fix it. It's like ensuring all office spaces comply with safety and organizational standards.

**Describe Infrastructure as a Service (IaaS):**

* It is most flexible category of cloud service.
* Provides maximum of control for user.
* Cloud controls: hardware / network connectivity/ physical security.
* You are basically renting hardware in datacentre.
* You’re responsible for installation and configuration, patching and updates, and security.

**Describe Software as a Service (SaaS):**

* Most complete cloud service from a product perspective.
* It is the least flexible.
* Requires least amount of technical knowledge (easiest to get up and running).
* You are essentially renting a fully developed application (email / financial software, for example).
* You are responsible for the data that you put into the system, the devices that you allow to connect to the system, and the users that have access.

**Describe Platform as a Service (PaaS):**

* is a middle ground between renting space in a datacentre (infrastructure as a service) and paying for a complete and deployed solution (software as a service).
* Cloud controls: hardware / network connectivity/ physical security /operating systems / middleware / development tools / business intelligence service.

**Which cloud service type is most suited to a lift and shift migration from an on-premises datacentre to a cloud deployment?**

With an IaaS service type, you can approximate your on-premises environment, making a lift-and-shift transition to the cloud relatively straightforward.

**What type of cloud service type would a Finance and Expense tracking solution typically be in?**

SaaS provides access to software solutions, such as finance and expense tracking, email, or ticketing systems.

**On-Premises:** Running an on-premises data centre is like owning your own pizzeria. You have full control over the entire pizza-making process. You make the pizza dough from scratch, choose the toppings, manage the oven (physical hardware), and handle all aspects of pizza creation.

**Infrastructure as a Service (IaaS):** is like buying the pizza base. The provider gives you the fundamental foundation (the pizza base). You choose the toppings, sauce, cheese, and bake it to your liking. It is Your responsibility for managing the operating system, applications, and configurations.

**Platform as a Service (PaaS):** is like buying a frozen pizza. The cloud provider delivers a pre-configured pizza (platform) with a set of toppings (development tools and middleware). You pop it into the oven, and it's ready to eat. You have the flexibility to customize certain aspects but don't have to worry about the complexities of creating the entire pizza.

**Software as a Service (SaaS):** is like going out to a pizza restaurant. You simply order the pizza (software) from the menu, and it's served to you. You enjoy the final product without any involvement in the cooking process. Users only need to access and utilize the software without concern for the underlying complexities.

**Microsoft Azure Fundamentals: Describe Azure architecture and services.**

**What is Microsoft Azure?**

Azure is a continually expanding set of cloud services that help you meet current and future business challenges.

**What can I do with Azure?**

With Azure you can, for example, run your existing applications on virtual machines to explore artificial intelligence (AI) and machine-learning (ML), and allow you to accommodate your storage for data as you needed.

**What does Azure offer?**

* Continuous innovation.
* Security.
* Support for all languages and frameworks (Build on your terms).
* You can use private/public or hybrid, what suits you.

Let's say you run a library. Moving your library's catalogue and services to Azure's virtual machines (VMs) is like digitizing your catalogue and services, making them accessible from anywhere. Beyond that, Azure provides additional services, like AI and machine learning, allowing you to implement innovative solutions such as a recommendation system for book selections or a chatbot to help library users.

**How to create an Azure account?**

1. You need an Azure subscription.

* You can use a temporary subscription, while you are learning, via Learn sandbox.

1. You can add more than 1 subscription, depending on what your business needs.
2. Each subscription can have one or more resource groups.
3. That resource group will have access to specific Azure resources (virtual machine, SQL database…).

**That graph can illustrate it better:**

A diagram of a diagram of a company

Description automatically generated

**What is the Microsoft Learn sandbox?**

It is a sandbox, where you can use for free when you are learning how to use the Azure resources.

**Describe Azure physical infrastructure:**

In simple words, that means the physical datacentres, with resources arranged in racks, with dedicated power, cooling, and networking infrastructure.

**How Azure is designed to help to achieve resiliency and reliability in physical infrastructure?**

The Azure datacentres are grouped in regions or availability zones.

**What is region in Azure?**

A region is a geographical area on the planet that contains at least one, but potentially multiple datacentre that are nearby and networked together with a low-latency network.

**What is availability zone in Azure?**

Availability zones are physically separate datacentres within an Azure region. Each availability zone is made up of one or more datacentres.

**That is a graph for better visualization of the combination of availability zone and region:**

A diagram of a computer

Description automatically generated

**What availability zones can do to help you?**

You can protect your information through redundancy, that way is created a duplicate hardware environment in different availability zones.

**What are the Azure services that support availability zones?**

1. Zonal service.
2. Zone-redundant services.
3. Non-regional services.

**What is region pairs?**

* Most Azure regions are paired with another region within the same geography (for tax- and law-enforcement jurisdiction purposes), but at least 300 miles away.
* This approach allows for the replication of resources across a geography.
* That is done to help reduce the interruptions because of events such as natural disasters or power outages for example, that affect an entire region.
* Azure updates use paired regions to minimize downtime and risk of application outage.

Imagine Microsoft Azure as a factory, a complex where each building represents a datacentre.

As this company expands, it establishes itself in various cities worldwide **(REGIONS).** Each city, or region, has its own set of factories.

Within these cities, the factory takes precautions to ensure continuous operation. It divides each location into separate production lines, known as **(AVAILABILITY ZONES).** If one line encounters an issue, the others continue operations.

To increase resilience, Azure implements a strategy like having duplicate factories in different locations **(REGION PAIRS).**

**Describe Azure management infrastructure.**

The Azure management infrastructure is based on Azure resources/ groups / subscriptions / account.

**What is Azure resource?**

It is basically anything you create on Azure. Examples: Virtual Machine, database, cognitive services, virtual network

**What is resource group?**

It is basically a way to group that resources, when you create a resource, you need to place it into a resource group.

**Rules about resource group**

* 1 resource group can have 1 or more resources.
* 1 resource can only be in 1 group, but you can move on resource to another group.
* If you delete a resource group, all the resources will be deleted.
* Resource group cannot be nested (you cannot put resource group B inside of resource group A).
* If you grant or deny access to a resource group, you’ve granted or denied access to all the resources within the resource group.

**What is Azure subscription?**

* In simple words, it is a logically way to organize your resource groups and facilitate billing.
* A subscription provides you with authenticated and authorized access to Azure products and services.
* An account can have multiple subscriptions, but it’s only required to have one.

**What Azure feature replicates resources across regions that are at least 300 miles away from each other?**

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.

**What are the types of subscription boundaries? (boundaries == limits)**

1. Billing boundary: determines how an Azure account is billed, makes easier to organize and manage costs.
2. Access control boundary: determines the access-management policies, makes easier to manage and control the access to the resource.

**Why could you create additional Azure subscription?**

1. For control access of different teams on organizational structures.
2. Set up separate environments for development / testing / security.
3. For billing purposes.

**What is Azure management groups?**

That is way to organize subscription into containers, when you are dealing multiple development teams in multiple geographies for example.

That can be nested if necessary.

That helps to create a hierarchy that applies a business policy.

That provide user access to multiple subscription.

**That graph can help to visualise the hierarchy:**

A diagram of a company

Description automatically generated

**What happens to the resources within a resource group when an action or setting at the Resource Group level is applied?**

The setting is applied to current and future resources.

Resources inherit permissions from their resource group.

**How many resource groups can a resource be in at the same time?**

A resource can only be in one group at a time.

Imagine managing a kitchen with different dishes like, lasagne, cake, fish pie - each dish is a **RESOURCE** in Azure, like a Virtual Machine or a database. To keep things organized, group these kitchen sections into areas focused on specific sections (desserts, main course, appetizer), like **RESOURCE GROUPS** in Azure where you organize different resources.

Now, overseeing the whole kitchen – Azure uses **SUBSCRIPTIONS**, acting like a manager for billing and organization. It helps logically arrange your cuisine sections (resource groups).

But as you expand, managing multiple kitchens (subscriptions) can be tricky. Enter Azure **MANAGEMENT GROUPS** – like a corporate headquarters overseeing kitchens in various cities, making it easy to organize and govern efficiently.

**What is a virtual machine?**

It is just like a physical computer, where you can customize all software running.

When you create a virtual machine, you also can manage its resources like, number of processors, amount of RAM, if it is hard disk or SSD, port configuration, virtual network.

**When could you use virtual machine?**

* During testing and development: because it provides a quick and easy way to create different OS and application configurations.
* When running applications in the cloud, that can provide economic benefits, opposed to create a traditional infrastructure, using extra resources only when needed.
* When extending your datacentre to the cloud or when you move from a physical server to the cloud (also known as lift and shift).
* During disaster recovery

**What a virtual machine can offer to you?**

1. Control over the operating system.
2. Customize hosting configuration.
3. Run custom software.

**What is virtual machine scale sets?**

Virtual machine scale sets let you create, update, configure and manage a group of identical, load balanced VMs, all centrally managed.

Automatically determine increase or decrease number of Virtual Machines, based on demand or schedule.

It is used to build large scale services for areas as big data, compute and container workloads.

**What is virtual machine availability sets?**

Availability sets prevents you from losing all your VMs with a single network or power failure.

That is achieved using 2 characteristics:

1. Update domains:

That separate the virtual machines in different domains, allows you to apply updates on one domain while knowing that only one update domain grouping will be offline at a time. (different chefs take breaks in different times to keep the kitchen always running)

1. Fault domain:

By default, an availability set will split your VMs across up to three fault domains protecting against a physical power or networking failure.

A virtual machine is like a customizable, high-speed car, where you decide how powerful its engine is, what kind of tires it uses, and even its colour. It's like customizing your car for optimal performance, you even can add unique features to your car, making it one of a kind.

In that car scenario compared to a virtual machine, you can use it for testing, like taking your car for a test drive, trying out different features and configurations and only paying for your car when you use it, also you can take your physical car to a digital highway – that's like moving your data centre to the cloud with virtual machines.

And there's more! Virtual machine scale sets – it's like managing a convoy of identical, high-speed cars that automatically adjusts its size based on demand or schedule, perfect for digital services on a large scale.

**Describe Azure virtual desktop:**

It is another type of virtual machine; it enables you to use different devices and operating systems to access windows versions. (lets you use Windows 10 or Windows 11).

You can enable multifactor authentication.

You can also secure access to data by assigning granular role-based access controls (RBACs) to users.

**Describe Azure containers:**

If you want to run multiple copies of an application on a single host machine, containers are an excellent choice.

They are like a digital storage box, you can store file, data, anything you need, that keeps it safe and organized with access anywhere.

Containers are designed to be created, scaled out, and stopped dynamically.

Containers are designed to allow you to respond to change on demand.

The most popular is docker.

**What are Azure container instances? (instances = copies)**

Fastest and simplest way to run container in Azure. It is as Paas (platform as a service)

You upload your containers and the service run the containers for you.

**What are Azure container apps?**

They are very similar with container instance but with extra benefits such as the ability to incorporate load balancing and scaling.

**What is Azure Kubernetes service?**

Known as AKS is a container orchestration service. It manages the lifecycle of containers, making the management simpler and more efficient.

**Why could you use containers?**

Containers helps you to break solutions into smaller pieces, for example, you can split a website into containers of front end / back end / storage. That allows you to scale specific containers to achieve better performance, without impacting other components.

Imagine you're moving to a new house, and you have lots of stuff – furniture, clothes, kitchen items. Now, think of all your belongings as pieces of a big application. If you want to organize and move these things efficiently, you'd use containers.

**Azure Container Instances:** Think of these as super-fast-moving trucks. It's like a moving that handles the transportation, and you only need to worry about packing.

**Azure Container Apps:** Like container instances, but with some cool extra features, because for example they also help with things like balancing the load (ensuring everything is evenly distributed) and adjusting the size if needed.

**Azure Kubernetes Service (AKS):** This is like having a team of expert movers and organizers, that not only transports your containers but also manages their entire journey. It ensures they get to the new house safely, efficiently, and in the right order.

**What is Azure function?**

Azure Functions is an event-driven, serverless compute option that doesn’t require maintaining virtual machines or containers. They scale automatically based on demand and you are charged only when CPU is used to run the function.

Functions are commonly used when you need to perform work in response to an event (often via a REST request), timer, or message from another Azure service.

In other words, think of them as your digital helpers that work behind the scenes, only showing up when there's work to be done, if you need more helpers, they will show up. You can use them to automate tasks, process data, or respond to events in your applications. They make your life easier by handling tasks automatically and quickly.

**Describe application hosting options:**

Application hosting options are like different places to showcase and run your software or websites. Think of it as choosing where to have a party.

In Azure you can use Virtual machine or containers to host.

Virtual machines give you more control of the hosting environment and it is the most familiar.

But in Azure you also have the hosting option: Azure app service.

**What is Azure app service?**

Enable you to host your software or websites, in the programming language of your choice without managing the infrastructure.

Offers automatic scaling and high availability.

Azure App Service lets you focus on building and maintaining your app, and Azure focuses on keeping the environment up and running.

Imagine you're planning a big event, like a wedding, and you need a place to host it. With Virtual Machine It's like renting an entire customizable banquet hall. You have full control over the space, and you can configure it exactly the way you want. With Containers is like having separate rooms for different parts of your event. But with Azure App Service is like hiring a professional event planner. You don't need to worry about the details of the venue, that allows you to focus on your celebration (building and maintaining your app), while Azure takes care of keeping the environment up and running smoothly.

**Describe Azure virtual networking:**

Azure virtual networks and virtual subnets are like pathways that help different things in the cloud talk to each other, like virtual computers, websites, and data storage. It's a bit like how roads and streets let people, cars, and houses connect with each other.

**What are the benefits of Azure Virtual Network?**

* Isolation and segmentation.
* Internet communications.
* Communicate between Azure resources.
* Communicate with on-premises resources.
* Route network traffic.
* Filter network traffic.

**What is an endpoint?**

Endpoint is a specific point where data or information begins or ends its journey. It can be a physical device, such as a computer, smartphone, or server, or a virtual location like a web address or a specific service within a network.

Endpoints are essential for data transfer and communication in various technological systems.

**What is IP address?**

IP stands for "Internet Protocol." An IP address is like a unique code for devices connected to the internet, like how your home has a specific mailing address.

**Explain public and private endpoints on azure virtual networking:**

Azure virtual networking supports both public and private endpoints to enable communication between external or internal resources with other internal resources.

* Public endpoint: public IP address and can be accessed anywhere.
* Private endpoint: exist inside a virtual network and have private IP address inside of the address space of that virtual network (You have a special home with a secret address, and all your neighbours are also in that hidden neighbourhood. Your home's address is only known to the people living there, and it's not a regular public address in the city.)

**What is public load balancer?**

In the context of the internet, a public load balancer helps websites and online services handle a large number of users and deliver content without any server getting too busy. Think of it as a restaurant with many waiters. When customers come in (internet users making requests) the manager (the load balancer) assigns each customer's order to an available waiter (server). This ensures that customers are served quickly and efficiently, and the restaurant runs smoothly.

**Describe Azure virtual private networks.**

VPN stands for virtual private network, that uses an encrypted tunnel within another network.

VPNs can enable networks to share sensitive information safely and securely.

Basically, it connects 2 or more trusted networks over an untrusted network (internet for example), traffic is encrypted while travelling over the untrusted network to prevent any attack.

**Why people use VPN?**

1. Privacy: A VPN keeps your online actions private.
2. Security: It adds an extra layer of protection.
3. Bypass Restrictions: You can access websites and services that might be restricted in your location.
4. Anonymity: It can make it harder for websites to track your online behaviour.

**What is VPN Gateway?**

A VPN gateway is like the entrance to your private tunnel on the internet. It's the point where your device connects to a Virtual Private Network (VPN) to create a secure and encrypted pathway for your online traffic. Ensuring that only authorized users can enter the private tunnel.

**Policy-based Azure VPN Gateway**

Specify statically the IP address of packets that should be encrypted through each tunnel.

**Route-based Azure VPN Gateway**

Tunnels are modelled as a virtual tunnel interface. IP routing decides which one of these tunnel interfaces to use when sending each packet.

**When should you choose for route-based VPN gateway?**

1. They are the preferred connection method for on-premises devices.
2. Connections between virtual networks
3. Point-to-site connections
4. Multisite connections
5. Coexistence with an Azure ExpressRoute gateway

**How to keep high availability for VPN?**

These are strategies to keep it’s a highly available and fault tolerant VPN configuration:

* Active/Standby:

Think of this like a backup generator for a building. The main electricity supply (the active instance) powers everything, but if there's a problem or maintenance work, the backup generator (the standby instance) kicks in automatically to keep the lights on. For a few moments during the switch, the power might flicker, but it's quickly restored. So, the main power source and the backup are there, but one is actively running, and the other is ready to take over.

When planned maintenance or unplanned disruption affects the active instance, the standby instance automatically assumes responsibility for connections without any user intervention.

* Active/Active:

Imagine a busy fast-food restaurant with two cash registers (instances). Both cash registers are open and serving customers at the same time (active/active). This speeds up service because more people can order and pay simultaneously. If one cash register has an issue or needs a break, the other one continues without interruption. Each cash register has its own line, and the restaurant can even add a third cash register if needed. It's all about efficiency and not depending on just one.

You assign a unique public IP address to each instance.

You create separate tunnels from the on-premises device to each IP address.

* ExpressRoute Failover:

Think of this like a backup route for your daily commute. You usually take the main highway (ExpressRoute) to work because it's faster and more reliable. However, sometimes, there might be an accident or road closure, which is like a disruption in ExpressRoute. So, you have a backup route (the VPN gateway) that uses different roads (the internet) to make sure you can still get to work even if the main highway has a problem. It's a reliable alternative route for those rare situations.

* Zone-Redundant Gateways:

Picture a big company with offices in different parts of a city. Each office has its own power source just in case there's a blackout in one area. Now, the company also has an even more robust backup system. It has power sources in different zones, like different neighbourhoods within the city. So, even if there's a problem in one neighbourhood, the other zones keep the power running for the offices. This way, they're prepared for almost any situation, and the offices never lose electricity. It's all about having multiple layers of backup and protection.

**Describe Azure ExpressRoute**

Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection, that 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.

**What are the benefits of Azure ExpressRoute?**

1. Faster Internet Highway:

Normally, when you access Azure (the cloud), you use the public internet, which is like the regular roads everyone uses. It can get busy and slow sometimes. But with Azure ExpressRoute, it's like having your own private highway. It's less crowded, so your data travels faster and more securely.

1. Secure Data Delivery:

Think of your data as precious cargo. Using the public internet is like sending it in an open truck, where anyone can see or tamper with it. With ExpressRoute, it's like sending your data in an armoured car – secure and protected from prying eyes.

1. Stable Connection:

The regular internet can be unpredictable, like a road with lots of potholes. Sometimes it's fast, and other times it's slow or even down. ExpressRoute is like having a smooth, well-maintained road. It's always there, so your connection to Azure is stable and reliable.

1. Privacy and Control:

Sometimes, you want to keep your data private and not let it go out in the open. With ExpressRoute, it's like having a private tunnel from your house to Azure. Only you and Azure can use it, so your data stays under your control.

1. Global Connectivity to Microsoft Services across all regions with ExpressRoute Global Reach:

ExpressRoute Global Reach means that you can reach these stores, not just in your local area, but all around the world. It's like having a pass that lets you shop in any Microsoft store, no matter where they are.

1. Dynamic Routing between your network and Microsoft via Border Gateway Protocol (BGP):

BGP is like a smart system that figures out the fastest and most efficient way to deliver your packages, means that your data takes the best and quickest route to reach Microsoft's services. It's like your packages always taking the fastest roads to get to their destination.

1. Built-in Redundancy in Every Peering Location for Higher Reliability:

Built-in redundancy means that even if one entry point has a problem, there's another one ready to take over. It's like having more than one door to a building. If one door is blocked, you can use the other door to get in.

**Explain the types of ExpressRoute connectivity models:**

1. CloudExchange colocation

Imagine there's a big building called the "CloudExchange." Inside this building, there are lots of different internet service providers and cloud providers, including Microsoft.

With this model, you physically place your networking equipment inside the CloudExchange building.

By being in the same building as Microsoft's cloud services, your data can quickly and directly connect to their services.

1. Point-to-point Ethernet connection

Think of this like a direct cable between your place (on-premises network) and Microsoft's data centre. You have a dedicated, private connection, from your office to Microsoft's cloud.

1. Any-to-any connection

This is like having multiple exits to a highway. Your network connects to multiple ExpressRoute locations, and from there, you can reach various Microsoft services.

1. Directly from ExpressRoute sites

In this model, you connect to Microsoft's cloud directly from an ExpressRoute site. These sites are like special entry points to Microsoft's network.

It's like having multiple doors to access different parts of Microsoft's cloud, and you can choose the one that's most convenient for your needs.

**What is DNS?**

DNS stands for Domain Name System. It's like the phone book of the internet.

You look up the name of the website (like looking up a person's name in a phone book), and it tells you the IP address (like a phone number) your computer needs to connect to the website's server.

* Domain Names: Every website or computer connected to the internet has a unique address called an IP address. It's a series of numbers like 192.168.1.1.
* Domain Names to the Rescue: DNS is a system that translates human-friendly domain names (like www.example.com) into IP addresses. So, when you type a website's name into your browser, DNS helps your computer find the correct IP address to connect to.

**What is Azure DNS?**

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure, that makes easier to connect your resources, services, and applications on the Azure platform.

**What are the Benefits of Azure DNS?**

1. Reliability and performance

* Azure DNS is like having multiple pizza shops in different parts of your town. This means that no matter where you are, you can order pizza from the nearest shop, ensuring it arrives quickly and hot.
* Each DNS query is answered by the closest available DNS server to provide fast performance and high availability for your domain.

1. Security

* Azure DNS is like having a special lock on your front door. It only lets the right people in, and it keeps track of who enters and when, like a security system for your house.
* It provides security features like Azure role-based access control (Azure RBAC).
* This feature allows you to control who can access and perform specific actions within your organization.
* It also offers activity logs, which allow you to monitor changes made by users within your organization.
* Resource locking is another security feature that prevents accidental modifications or deletions.

1. Ease of Use

* Azure DNS is like having all your tools neatly organized in one toolbox. It means you can easily grab the right tool for the job.
* Azure DNS is integrated in the Azure portal and uses the same credentials, support contract, and billing as your other Azure services.

1. Customizable virtual networks

* With Azure DNS, it's like you get to choose the name for this room. Instead of being stuck with what someone else decided, you can give it a name that's meaningful to you.
* Allows you to use your own custom domain names in your private virtual networks, rather than being stuck with the Azure-provided names.

1. Alias records

* Suppose you have a favourite restaurant you like to go to for burgers, but the restaurant moves to a new location. Azure DNS is like having a GPS system that automatically updates the address of the restaurant in your phone's map app. So, even if the restaurant moves, you can still find it without any trouble.
* Azure DNS supports alias record sets. These allow you to refer to Azure resources using DNS records.
* If the IP address of the underlying resource changes, the alias record set automatically updates itself during DNS resolution, ensuring that your DNS records stay up to date and accurate.

**Describe Azure storage:**

A storage account provides a unique namespace for your Azure Storage data that's accessible from anywhere in the world over HTTP or HTTPS. Data in this account is secure, highly available, durable, and massively scalable.

**What are the rules for naming Azure storage account?**

* Storage account names must be between 3 and 24 characters in length.
* May contain numbers and lowercase letters only.
* No two storage accounts can have the same name.

**That graph can show the different types of storage available:**

A screenshot of a computer

Description automatically generated

**What are the benefits of Azure storage?**

* Durable and highly available.

Redundancy ensures that your data is safe if transient hardware failures occur. You can also opt to replicate data across data centres or geographical regions for additional protection.

* Secure.

All data written to an Azure storage account is encrypted by the service and you have control over who has access to your data.

* Scalable

Azure Storage is designed to be massively scalable to meet the data storage and performance needs.

* Managed.

Azure handles hardware maintenance, updates, and critical issues for you.

* Accessible.

Data in Azure Storage is accessible from anywhere in the world over HTTP or HTTPS.

**Describe 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. There are different redundancy options you should choose what is best for your scenario.

**Explain 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:

* A screenshot of a computer

  Description automatically generatedlocally redundant storage (LRS)
* replicates your data three times within

a single data centre in the primary.

* lowest-cost redundancy option and

offers the least durability.

* A screenshot of a computer

  Description automatically generatedzone-redundant storage (ZRS)
* replicates your Azure Storage data

synchronously across three Azure availability

zones in the primary region.

* 3 different datacentres in same region.
* recommended for scenarios that require

high availability.

* recommended for restricting replication

of data within a country or region to meet data governance requirements.

**Explain Redundancy in the secondary region:**

For applications requiring high durability, you can choose to additionally copy the data in your storage account to a secondary region that is hundreds of miles away from the primary region, then your data is durable even in the event of a catastrophic failure.

By default, data in the secondary region isn't available for read or write access.

The paired secondary region is based on Azure Region Pairs and can't be changed.

Azure Storage offers two options for copying your data to a secondary region:

* geo-redundant storage (GRS)
* A diagram of a storage system

  Description automatically generatedlike locally redundant storage (LRS).
* replicates your data three times within a

single data centre in the primary.

* then copies your data to a single physical

location in the secondary region (the region pair)

* geo-zone-redundant storage (GZRS)
* A screenshot of a computer

  Description automatically generatedLike zone-redundant storage (ZRS).
* Data in a GZRS storage account is copied across

three Azure availability zones in the primary region.

* then copies your data to a single physical location in

the secondary region (the region pair)

Locally Redundant Storage (LRS): This is like making three photocopies of your album and keeping them in the same room. It's the most budget-friendly option but not the most secure.

Zone-Redundant Storage (ZRS): Imagine you're making three copies, but this time you're placing them in three separate rooms in the same building. It's a bit safer, especially if something goes wrong in one room.

Geo-Redundant Storage (GRS): Like LRS, but after making three copies in the main room, a fourth copy is sent to a secure room in a different city. It's like having a backup album in a different location, providing extra safety.

Geo-Zone-Redundant Storage (GZRS): Like ZRS, but after creating three copies in the main region across different rooms, a fourth copy is sent to a secure room in a different city. This is like having both local and remote backups for maximum security.

**What are the data services included in Azure Storage platform?**

* Azure Blobs:
* Blob stands for Binary Large Object
* It is designed to store unstructured data (meaning that there are no restrictions on the kinds of data it can hold), such as documents, images, videos, and backups.
* Also includes support for big data analytics. Serving images or documents directly to a browser.
* Streaming video and audio.
* Azure Files:
* Managed file shares for cloud or on-premises deployments.
* It provides shared file storage that multiple virtual machines (VMs) can access concurrently.
* It's handy for scenarios where you need to share files between different parts of an application or team members.
* Azure Queues:
* It is a service for storing large numbers of messages. Once stored, you can access the messages from anywhere in the world.
* Queue storage can be combined with compute functions like Azure Functions to take an action when a message is received.
* Suppose you're running a food delivery service. Azure Queue Storage is like your digital order queue. When someone places an order, it goes into the queue, and your delivery drivers can pick up tasks from there. It ensures smooth and organized food deliveries without confusion.
* Azure Disks:
* Conceptually, they’re the same as a physical disk, but they’re virtualized.
* It's essential for virtual machines that need storage for running software.
* Azure Tables:
* NoSQL table option for structured, non-relational data.

**What are the Azure Files key benefits?**

Shared access: Azure file shares are like a shared digital workspace you can access the files using familiar tools and methods, just like if you were working on the same project in a physical office.

Fully managed: It's like having a computer where someone else takes care of all the technical stuff updating software, fixing issues, and making sure it's always working.

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. You can create and manage Azure file shares using Azure portal and Azure Storage Explorer.

Resiliency: Azure Files means you don't have to wake up in the middle of the night to deal with local power outages or network issues.

Familiar programmability: With Azure Files, you can use your existing software and skills to access and manage your files. It's like being able to communicate with your files using the language you already know, so you don't have to learn a new one.

**Explain more about BLOB storage:**

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.

Objects in blob storage can be accessed from anywhere in the world via HTTP or HTTPS.

**What is Access Tier?**

Access Tier refers to the storage class or level of access and pricing associated with Azure Blob Storage.

The choice of access tier allows you to optimize your storage costs based on the access patterns and usage characteristics of your data. You can transition data between these tiers as your access patterns change.

It's important to note that the choice of access tier is specific to Azure Blob Storage and is not applicable to other Azure storage services.

**Explain the different access tier options:**

* Hot access tier:

Optimized for storing data that is accessed frequently (for example, images for your website).

Data stored in this tier is more expensive to store, but the cost of data retrieval is lower.

* Cool access tier:

Optimized for data that is infrequently accessed and stored for at least 30 days (for example, invoices for your customers).

Data stored in this tier is less expensive to store, but the cost of data retrieval is higher compared to the Hot Access.

* Cold access tier:

Optimized for storing data that is infrequently accessed and stored for at least 90 days.

* 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).

The lowest storage costs, but also the highest costs to rehydrate and access data.

**How to get your data and information into Azure?**

Azure supports:

* real-time migration with Azure Migrate
* Asynchronous migration with Azure Data Box

**Explain Azure Migrate:**

Azure Migrate is a service that helps you migrate from an on-premises environment to the cloud.

For that it uses a single portal to start, run, and track your migration to Azure known as Unified migration platform and a range of tools for assessment and migration.

**Explain 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 Data Box is transported to and from your datacentre via a regional carrier. A rugged case protects and secures the Data Box from damage during transit.

That system can be used to import or export data from Azure.

**How can you move or interact with small file groups?**

* AzCopy
* It is a command-line utility that you can use to copy blobs or files to or from your storage account.
* That can also work between different cloud providers.
* It is one-direction synchronization.
* Azure Storage Explorer
* It is an independent app that provides a graphical interface to manage files and blobs in your Azure Storage Account.
* It uses AzCopy on the backend to perform all the file and blob management tasks.
* Azure File Sync
* Once you install Azure File Sync on your local Windows server, it will automatically stay bi-directionally synced with your files in Azure.
* You can Use any protocol that's available on Windows Server to access your data locally.
* You can configure cloud tiering, so the most frequently accessed files are replicated locally.

**Which tool automatically keeps files between an on-premises Windows server and an Azure cloud environment updated?**

Azure File Sync maintains a bidirectional synchronization of files between your on-premises and cloud Windows servers.

**Which storage redundancy option provides the highest degree of durability, with 16 nines of durability?**

Geo-redundant storage (GRS) and geo-zone-redundant storage (GZRS) both provide 16 nines of durability.

**Which Azure Storage service supports big data analytics, as well as handling text and binary data types?**

Azure Blobs is a massively scalable object store for text and binary data. Azure Blobs also includes support for big data analytics through Data Lake Storage Gen2.

**What is Microsoft Entra ID? (Azure directory services)**

Microsoft Entra ID is a directory service that enables you to sign in and access both Microsoft cloud applications and cloud applications that you develop.

Microsoft Entra ID can detect sign-in attempts from unexpected locations or unknown devices.

**What does Microsoft Entra ID do?**

1. 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.
2. Single sign-on (SSO): Instead of remembering a bunch of usernames and passwords for different apps, you just remember one. This is like having a magic key that opens lots of doors. It makes things easy and secure. When you change roles or leave a place, it's also much simpler to update who gets access to what.
3. Application management: You can manage your cloud and on-premises apps, you can easily add new apps and sign in without fuss.
4. Device management: It supports the registration of devices restricting access attempts to only those coming from known devices. So even if someone knows the password, they can't get in unless they're using an approved device.

**What is Microsoft Entra Connect?**

That is a tool that allows you to synchronize user identities between on-premises Active Directory and Microsoft Entra ID.

**What is Microsoft Entra Domain Services?**

Microsoft Entra Domain Services is like having a digital assistant for your online world.

Your digital assistant manages important things, like organizing your files, setting rules making sure everyone has the right access and ensuring everything runs smoothly in your online workspace.

When you decide to get your digital assistant, you define its name and what it should focus on. Similarly, with Microsoft Entra Domain Services, you create a special digital space with a unique name and purpose.

If you have old ways of doing things (like using an old computer), your digital assistant helps you smoothly shift to a new and improved setup. Likewise, Microsoft Entra Domain Services lets you move your old applications to a new "digital space" without dealing with complicated setups.

Your digital assistant comes with all the tools it needs, and you don't have to worry about managing or updating them. In the same way, with Microsoft Entra Domain Services, you don't need to handle technical details like configuring servers.

If you write down a note, your digital assistant makes sure it's saved. Similarly, Microsoft Entra Domain Services keeps your digital information safe and accessible, syncing it smoothly between your digital spaces.

**Describe Azure authentication methods:**

Authentication is like presenting ID when you’re traveling. It doesn’t confirm that you’re ticketed, it just proves that you're who you say you are.

Azure supports multiple authentication methods, including:

* Standard Passwords
* Single Sign-On (SSO)

You need to remember only one ID and one password.

The more passwords a user must manage, the greater the risk of a credential-related security incident.

Enables a user to sign in one time and use that credential to access multiple resources and applications from different providers.

* MultiFactor Authentication (MFA)

It is the process of prompting a user for an extra form of identification during the sign-in.

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:

* 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 phone.
* Something the user is – this is typically some sort of biometric property, such as a fingerprint or face scan.
* Passwordless

Passwordless authentication methods are more convenient because the password is removed and replaced with something you have, plus something you are, or something you know.

These are 3 passwordless authentication options that integrate with Microsoft Entra ID:

* Windows Hello for Business

It is ideal for 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) 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.

**What is Microsoft Entra External ID?**

It refers to all the ways you can securely interact with users outside of your organization.

If you want to collaborate with external partners, you can share your resources and define how external users can access your organization.

External users can "bring their own identities", they can use their own credentials to sign in, like Google or Facebook.

Depending on how you want to interact with external organizations and the types of resources you need to share, you can use a combination of these capabilities:

* 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 apps.

Think of it like inviting friends from other neighbourhoods to your party. They can wear whatever they like (use their preferred identity), and during the party, they're part of your group.

* B2B direct connect.

Establish a mutual, two-way trust with another Microsoft Entra organization for perfect collaboration.

It's like building a special bridge to connect with a nearby town. People from both sides can easily visit each other for shared activities. These visitors aren't permanent residents, but they are visible and monitored during shared events.

* Microsoft Entra business to customer (B2C)

Publish modern SaaS apps or custom-developed apps to consumers and customers.

Imagine opening a shop, with special entrance door, that attracts customers from different areas. Each customer has their own key to enter (Azure AD B2C identity), and while they're shopping, everything behind the scenes works smoothly. These customers have their preferences, and you use Azure AD B2C to manage their experience.

A diagram of a company

Description automatically generated

**What is Azure conditional access?**

This is a tool that Microsoft Entra ID uses to allow (or deny) access to resources based on identity signals. These signals include who the user is, where the user is, and what device the user is requesting access from.

**When should I use conditional access?**

* Require multifactor authentication (MFA) to access an application depending on the requester’s role, location, or network, that gives a balance between security and user convenience.
* Require access to services only through approved client applications. For example, you could limit which email applications are able to connect to your email service.
* Require users to access your application only from managed devices. A managed device is a device that meets your standards for security and compliance.
* Block access from untrusted sources, such as access from unknown or unexpected locations.

The following diagram illustrates this flow:

A diagram of a document

Description automatically generated

During sign-in, Conditional Access collects signals from the user.

Signal might be the user's location, the user's device, or the application that the user is trying to access.

Then enforces that decision by allowing or denying the access request or challenging for a multifactor authentication response.

Makes decisions based on those signals.

What is Azure role-based access control (RBAC)?

Azure Role-Based Access Control (RBAC) is a system used to manage and control access to resources within Microsoft Azure. It is to decide who gets to do what in a cloud environment.

The RBAC helps to manage the level of permissions for an entire team. Each role has an associated set of access permissions that relate to that role, that makes all easier and you can also define your own roles.

So, if you hire a new engineer and add them to the Azure RBAC group for engineers, they automatically get the same access as the other engineers in the same Azure RBAC group.

When you're assigned a role:

* If one role assignment grants you read permissions to a resource group.
* a different role assignment grants you write permissions to the same resource group.
* you have both read and write permissions on that resource group.

**What is zero trust model?**

In simple words is like treating every interaction with people and devices as if you've never met them before.

Imagine you have a high-security vault in a bank it doesn't matter if someone is a long-time employee. Every person who wants to enter the vault area must go through a background check each time they approach and is granted access only to the specific compartment that someone needs to access, also their movements and activities are constantly monitored.

You don't assume that because someone is in the vault, they can be trusted with everything.

**What are the Principles of Zero trust model?**

1. Verify explicitly:

Always authenticate and authorize based on all available data points.

1. Use least privilege access:

Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.

Only give someone the exact keys they need to open specific rooms, not the whole building.

1. Assume breach:

Always be ready for the possibility of a security breach and improve defences.

Minimize blast radius and segment access (Keep sensitive things separate and locked).

Verify end-to-end encryption.

Use analytics to get visibility, drive threat detection (constantly monitor for anything unusual).

**What is defence-in-depth?**

It is a strategy that uses a series of mechanisms to slow the advance of an attack, for example as a set of layers, each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. That protect information and prevent it from being stolen by those who aren't authorized to access it.

**That is a graph to see the layers to protect the data:**

A diagram of a security system

Description automatically generated

|  |
| --- |
| The first line of defense, safeguarding computing hardware in the datacenter. |
| Controls infrastructure access, ensuring secure sign-ins and change tracking. |
| Defends against large-scale attacks, preserving system availability. Use DDoS protection and firewalls |
| Restricts resource communication, reducing the risk of spreading attack and implement secure connectivity to on-premises networks. |
| Focuses on securing virtual machine access and endpoint protection. |
| Integrating security into the application development lifecycle helps reduce the number of vulnerabilities introduced in code |
| Protects sensitive data as in almost all cases, attackers are after data, needs to ensure the confidentiality, integrity, and availability of the data. |

**What is Microsoft Defender for Cloud?**

In simple terms, it watches over your computer, warns you about potential dangers, and takes steps to keep your computer safe.

Defender for Cloud is a monitoring tool for security posture management and threat protection.

It monitors your cloud and on-premises environments to provide guidance and notifications aimed at strengthening your security posture.

**What are the 3 pillars of defender for cloud?**

1. Continuously assess:

Know your security posture. Identify and track vulnerabilities.

1. Secure:

Harden resources and services with Azure Security Benchmark.

1. Defend:

Detect and resolve threats to resources, workloads, and services.

**Understanding the Protection everywhere you’re deployed:**

Imagine you're responsible for security in your neighbourhood. You want to make sure everyone's homes are safe.

* Azure services:
* are monitored and protected without needing any deployment.
* Your home is like an Azure service, and it's already well-protected. You have a security system that covers your house. It's all set up and ready to go, just like how Azure services are monitored and protected without extra deployment.
* on-premises datacentre or are also operating in another cloud environment:
* To extend protection to on-premises machines, deploy Azure Arc and enable Defender for Cloud's enhanced security features.
* Defender for Cloud can also protect resources in other clouds.
* Your neighbour’s home represents an on-premises or different cloud environment. They have a different security system in place, and it's not directly connected to yours.
* To ensure their home is secure too, you need to help them set up a security system like yours. This is like when Microsoft Defender for Cloud deploys a security agent to gather data in places outside of Azure.
* Multi-cloud:
* Now, you have another neighbour who uses multiple security systems for their different homes. You want to help them manage and monitor all their homes' security.
* Microsoft Defender for Cloud extends its protection to these different homes, even if they use various security systems. It's like offering a unified security management solution.

**A user is simultaneously assigned multiple roles that use role-based access control. What are their actual permissions? The role permissions are: Role 1 - read || Role 2 - write || Role 3 - read and write.**

Read and write.

Role-based access control, using an allow model, grants all the permissions assigned in all the assigned roles.

**Which security model assumes the worst-case security scenario, and protects resources accordingly?**

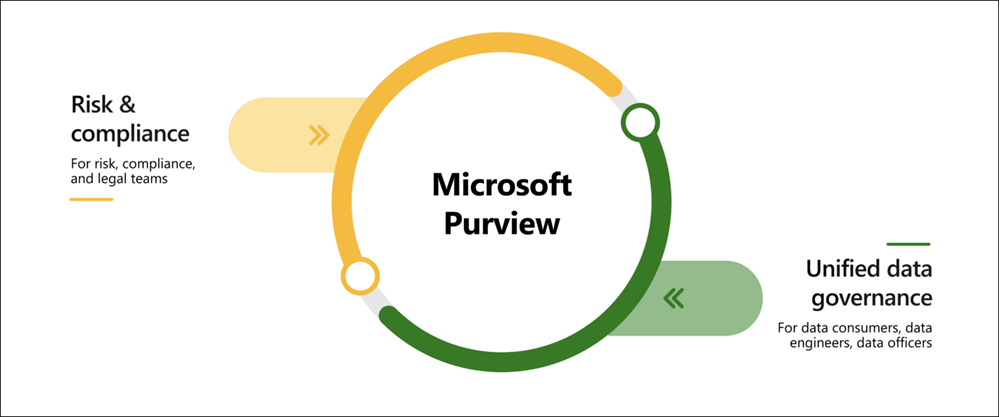
Zero Trust is a security model that assumes the worst-case scenario and protects resources with that expectation.

**Which Microsoft Entra tool can vary the credentials needed to log in based on signals, such as where the user is located?**

Conditional Access is a tool that Microsoft Entra ID uses to allow (or deny) access to resources based on identity signals. Conditional Access might challenge you for a second authentication factor if your sign-in signals are unusual or from an unexpected location.

**What is Microsoft pureview?**

It is a set of tools that helps you manage and understand your data better. It gives you a single view of your data, whether it's stored on your premises, in the cloud, or through software services.

There are two main parts to Microsoft Purview:

* one focuses on managing risks and ensuring compliance.

1. Protect sensitive data across clouds, apps, and devices.
2. Identify data risks and manage regulatory compliance requirements.

* the other concentrates on bringing together and organizing your data in a unified way.

1. Create an up-to-date map of your entire data.
2. Identify where sensitive data is stored.
3. Create a secure environment for data.
4. Understand how your data is stored and used.

**What is Azure Policy?**

It is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources. If you have a specific resource that you don’t want Azure Policy to automatically fix, you can flag that resource as an exception – and the policy won’t automatically fix that resource.

**How Azure Policy helps you?**

* Enables you to define both individual policies and groups of related policies.
* Enables you to set policies on a specific resource, resource group, subscription, and so on.
* Highlights resources that aren't compliant with the policies you've created.
* Prevent noncompliant resources from being created.

**What are Azure Policy initiatives?**

An Azure Policy initiative is a way of grouping related policies together.

**What is a resource lock?**

It is a tool that prevents resources from being accidentally deleted or changed.

They can be applied to individual resources, resource groups, or even an entire subscription.

Types of resource lock:

Delete – users can read and modify a resource, but they can’t delete a resource.

Read-only – users can read a resource, but they can’t delete or modify it.

**How do I delete or change a locked resource?**

First remove the lock, then, you can apply any action you have permission.

**How can you prevent creation of non-compliant resources, without having to manually evaluate each resource?**

Azure policy lets you create policies and initiatives (groups of policies) that prevent non-compliant resource from being created.

**What's the best way to prevent inadvertent deletion of a resource?**

A resource lock can be used to prevent a resource from accidentally being deleted.

Different ways to interact with Azure environment:

* Azure portal -- web-based console that provides an alternative to command-line tools.
* Azure PowerShell -- It is a shell where you can run commands (cmdlets), these commands call the Azure REST API to perform management tasks in Azure, that can make some process repeatable and automatable.
* Azure Command Line Interface (CLI) – It is functionally equivalent to Azure PowerShell, with the primary difference being the syntax of commands. While Azure PowerShell uses PowerShell commands, the Azure CLI uses Bash commands.

**What is Azure Arc?**

It is a set of technologies that helps manage your cloud environment, independent if it is public / private / hybrid. Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.

**Why Azure Arc is useful?**

Arc lets you extend your Azure compliance and monitoring to your hybrid and multi-cloud configurations, as if they are running in Azure.

**What resource Arc can manage outside Azure?**

* Servers
* Kubernetes clusters
* Azure data services
* SQL Server
* Virtual machines (preview)

**What is ARM (Azure Resource Manager)?**

Anytime you do anything with your Azure resources, ARM is involved. It provides a management layer that enables you to create, update, and delete resources in your Azure account.

**Explain the ARM process when a user sends a request.**

ARM receive the request -> ARM authenticates -> ARM authorize -> ARM sends the request to Azure service -> Azure service takes the requested action.

**What are the benefits of Azure Resource Manager (ARM)?**

* Use of template. Instead of giving your computer step-by-step instructions (like a recipe), you use a special plan (a JSON file) that says what you want to create.
* Deploy, manage, and monitor all the resources for your solution as a group, not individually.
* Define the dependencies between resources, so they're deployed in the correct order.
* Apply tags to resources to logically organize.

**Explain about ARM (Azure Resource Manager) Template.**

You can describe the resources you want to use in a declarative JSON format.

The deployment code is verified before any code is run (to ensure all is correct).

Can create resources in parallel, example, 50 instances can be created at the same time.

You need only to define the desired state and configuration of each resource in the ARM template, and the template does the rest. ARM templates and Bicep are two examples of using infrastructure as code with the Azure Resource Manager to maintain your environment.

**What are the benefits of Template?**

1. Declarative syntax: you declare what you want to deploy but don’t need to write the actual programming commands.
2. Orchestration: You don't have to worry about the complexities of ordering operations. Azure Resource Manager orchestrates the deployment of interdependent resources, so they're created in the correct order.
3. Modular files: You can break your templates into smaller, reusable components and link them together at deployment time.
4. Repeatable: ensure repeatable and consistent results across different environments.

**What is Bicep?**

Bicep is a user-friendly way to talk to Azure. Instead of using the more complex JSON language (like ARM templates), Bicep lets you describe your Azure environment in a simpler and shorter way.

**What are the benefits of Bicep?**

Basically, the same benefits as the Template, but with a simple syntax: no previous knowledge of programming languages.

**What service helps you manage your Azure, on-premises, and multicloud environments?**

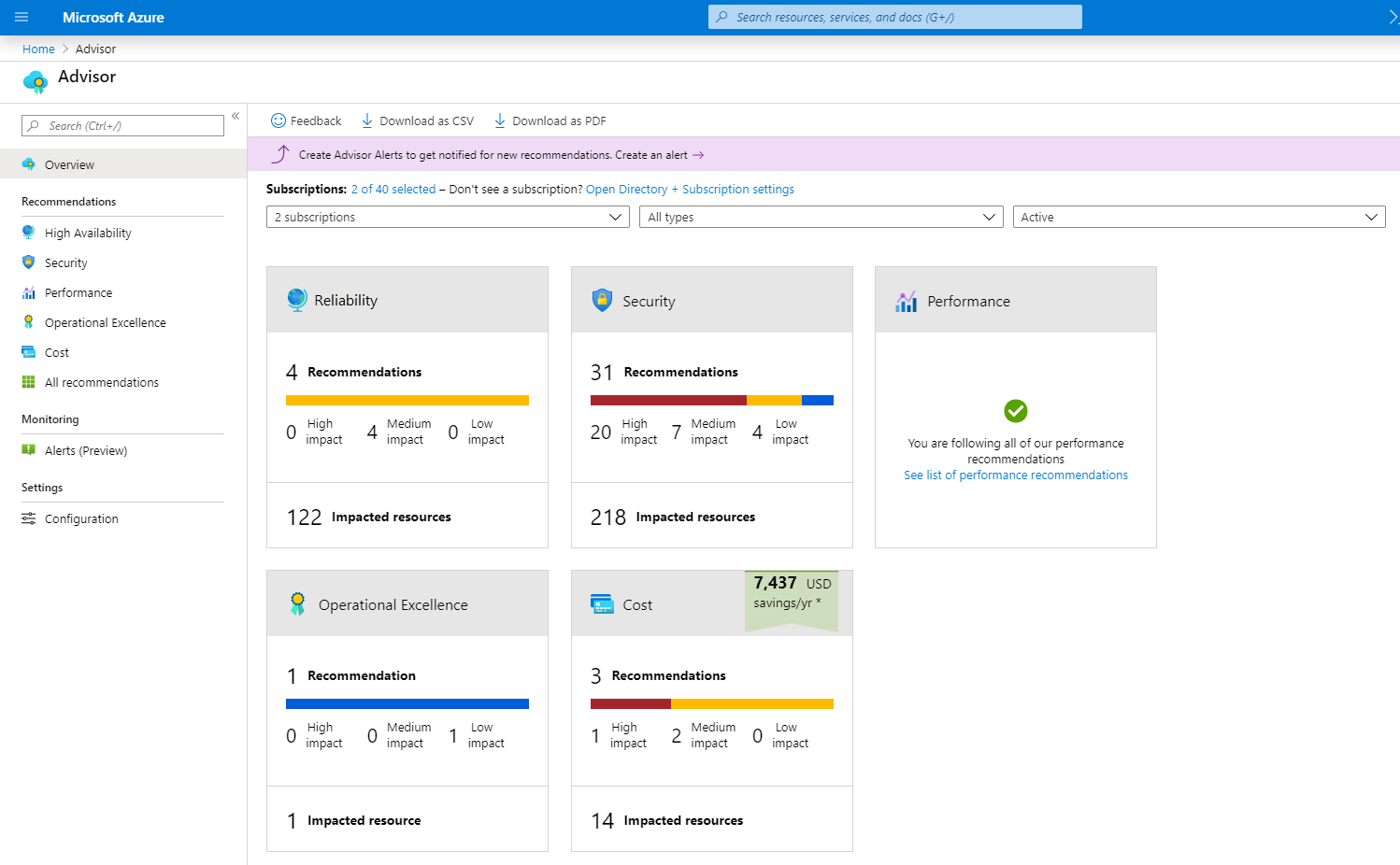
Azure Arc, working with Azure Resource Manager, lets you extend your Azure compliance and monitoring to your hybrid and multicloud configurations.

**What two components could you use to implement a “infrastructure as code” deployment?**

Bicep and ARM Templates allow you to deploy your resource as code.

**What are the recommendations from Azure Advisor?**

* Reliability: ensure and improve the continuity of your applications.
* Security: detect threats and vulnerabilities.
* Performance: improve the speed of your applications.
* Cost: optimize and reduce your overall Azure spending.
* Operational Excellence: help you achieve process and workflow efficiency, resource manageability, and deployment best practices.



**What is the Azure service Health?**

Based on the 3 pillars you can have a full picture of what is happening in Azure

1. Azure Status:

It's like the big map showing if everything in Azure is working worldwide. If there's a big issue that's affecting a lot of people, you'll find it here.

1. Service Health:

It is a personalized view for you. It focuses on what you're using in Azure. It's where you get info about outages, maintenance plans, and other stuff that might affect what you're doing.

1. Resource Health:

This is like looking at the health report of each tool in your Azure toolbox. It tells you how each specific thing you're using is doing. And you can set up alerts to know if anything changes.

**What are the benefits of Azure Service Health?**

* Stay Informed: Keep track of both the big picture (global Azure status) and the specifics (your individual resources).
* Customized Alerts: Set up alerts to get a heads up when something might affect your Azure services and regions.
* Historical Insights: Look back at past alerts to understand trends and investigate any issues.
* Support Links: In case something goes wrong, easily access links to get the support you need.

**What is Azure Monitor?**

It is a platform for collecting data on your resources, analysing that data, visualizing the information, and even acting on the results.

**What are Azure Log Analytics.**

It is a tool in the Azure Portal where you’ll write and run log queries on the data gathered by Azure Monitor.

Example:

You can write a simple query that returns a set of records and then use features of Log Analytics to sort, filter, and analyse the records.

You can write an advanced query to perform statistical analysis and visualize the results in a chart.

Imagine Log Analytics as your recipe book – you can ask it questions about your digital data, from simple queries to intricate culinary investigations.

You can sort, filter, and analyse, like adding the perfect seasonings to create a delightful dish.

Log Analytics can turn your findings into a digital menu, presenting data in charts and graphs that are easy to digest.

**What are Azure Monitor Alerts?**

They are automated way to stay informed when Azure Monitor detects a threshold being crossed.

You set the alert conditions and the notification actions.

Azure Monitor Alerts notifies when an alert is triggered.

Azure Monitor Alerts can also attempt corrective action (Depending on your configuration)

**What are application insights?**

It is capable of monitoring web applications that are running in Azure, on-premises, or in a different cloud environment.

You can monitor:

* **Requests and Responses:** How many times your app is being used, how fast it responds.
* **Dependencies:** Checks if your app relies on other services and how they're performing.
* **User Experience:** how quickly your app loads in their browsers.
* **User and Session Info:** Counts how many users are hanging out and what they're doing in each session.
* **Server Health:** Monitors the health of the machines running your app – checks if they're using too much CPU, memory, or network.

**You receive an email notification that virtual machines (VMs) in an Azure region where you have VMs deployed is experiencing an outage. Which component of Azure Service Health will let you know if your application is impacted?**

Resource Health is a tailored view of your actual Azure resources. It provides information about the health of your individual cloud resources.

**What are the factors that can affect costs in Azure?**

* **Resource** (The type of resources, the settings for the resource, licensing for the operating system)
* **Consumption** (If you use more compute, you pay more.)
* **Geography** (cost of power, labour, taxes, and fees vary depending on the location.)
* **Network traffic** (it’s less expensive to move information within Europe than to move information from Europe to Asia or South America.)
* **Subscription type** (Azure free trial subscription provides access to a few Azure products that are free for 12 months.)
* Maintenance (keeping an eye on your resources and making sure you’re not keeping around resources that are no longer needed)
* **Azure Marketplace** (lets you purchase Azure-based solutions and services from third-party vendors.)

**What is Pricing calculator?**

It is a tool designed to give you an estimated cost for provisioning resources in Azure.

The prices are only an estimate. Nothing is provisioned when you add resources to the pricing calculator, and you won't be charged for any services you select.

**What is TCO calculator?**

It is a tool designed to help you compare the costs for running an on-premises infrastructure compared to an Azure Cloud infrastructure.

**What is Microsoft Cost Management tool?**

It is a tool that provides the ability to quickly check Azure resource costs, create alerts based on resource spend, and create budgets that can be used to automate management of resources.

**What are the different cost alerts?**

1. Budget alerts

Notify you when spending, based on usage or cost, reaches or exceeds the amount defined in the alert condition.

1. Credit alerts

Notify you when your Azure credit monetary commitments are consumed. They are generated automatically at 90% and at 100% of your Azure credit balance.

1. Department spending quota alerts.

Notify you when department spending reaches a fixed threshold of the quota.

**Why is important to use tags?**

That helps to keep everything organized.

* **Cost management and optimization** (enable you to group resources so that you can report on costs)
* **Security** (enable you to classify data by its security level, such as public or confidential.)
* **Operations management** (enable you to group resources according to how critical their availability is to your business.)
* **Governance and regulatory compliance** (enable you to identify resources that align with governance or regulatory compliance requirement.)

**How do I manage resource tags?**

You can add, modify, or delete resource tags through Windows PowerShell, the Azure CLI, Azure Resource Manager templates, the REST API, or the Azure portal.

EXAMPLE TAGGING STRUCTURE

A resource tag consists of a name and a value.

Name Value

AppName The name of the application that the resource is part of.

\*\* You can assign one or more tags to each Azure resource.

**What Azure feature can help stay organized and track usage based on metadata associated with resources?**

Tags allow you to associate metadata with a resource to help keep track of resource management, costs and optimization, security, and so on.

**What’s the best method to estimate the cost of migrating to the cloud while incurring minimal costs?**

The Total Cost of Ownership calculator lets you input your current infrastructure and requirements and provides you with an estimate for running in the cloud.