Azure Fundamentals

In this document, I share the highlights of my first week working with Azure. It's a personal log, detailing my exploration of key areas such as data centers, cloud computing, Azure core services, virtualization, resource management, and both foundational and advanced networking concepts. As someone new to this platform, this is more about documenting my learning process rather than offering expert insights.

Introduction

Before jumping straight into Azure, let's first understand why it became important.

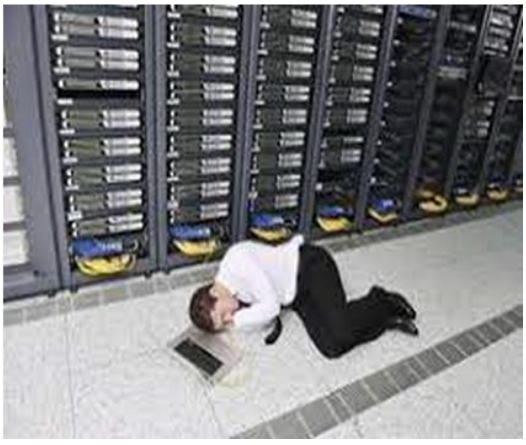
Data Centres and Servers

In the beginning, companies needed physical servers to run their applications and store data. These servers were placed in large buildings called data centres. As businesses grew, they needed more and more servers, which made data centres bigger and harder to manage. Running all these servers became expensive and complicated.

How Do Data Centres work?

To store, move, and digitally access information, data centres contain real or virtual servers that are connected internally and externally by networking and communication equipment. An organization can gather its equipment and resources for data processing, storage, and communications in a data centre facility, which consists of the following:

- Systems for handling, processing, exchanging, and storing data throughout the enterprise.
- Physical infrastructure facilitating data communications and processing.
- Utilities include network security access, cooling, energy, and uninterruptible power supply (UPS)



The Move to the Cloud

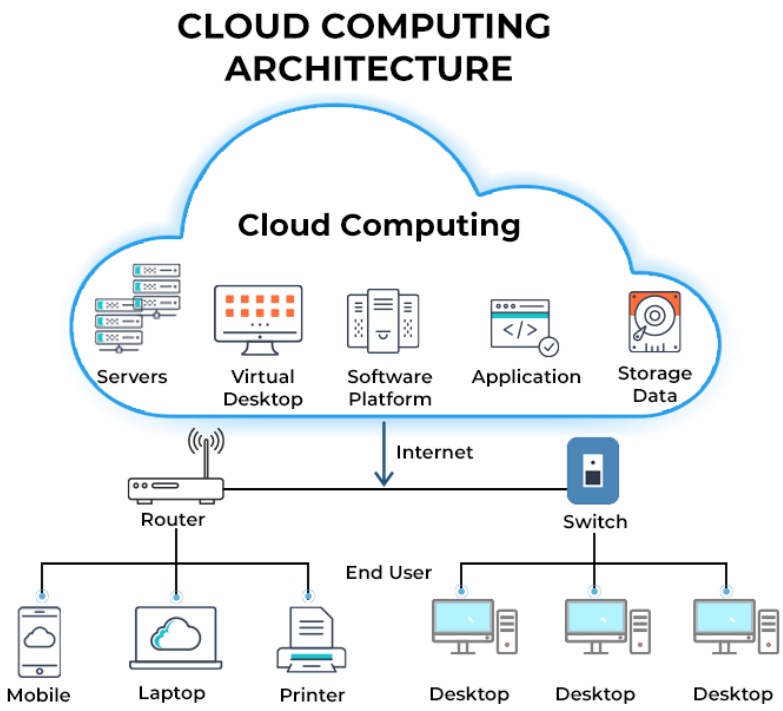
To solve these problems, cloud computing was created. Instead of buying and maintaining physical servers, companies could rent virtual servers from cloud providers like Microsoft Azure, AWS, GCP etc. This change made it cheaper and easier to scale (grow) the infrastructure.

Cloud

Think of the cloud as a massive online storage and computing space. It's like a powerful computer which you can access from anywhere using the internet, without needing to own or manage the hardware. You can store files, run apps, and access services all through the cloud.

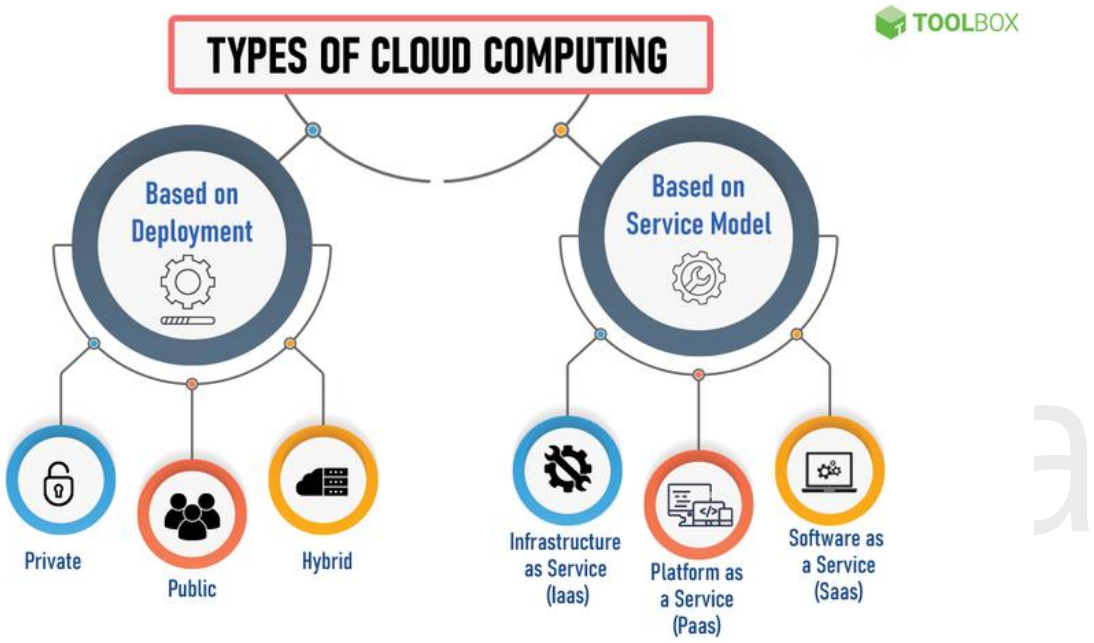
What is Cloud Computing?

Cloud computing is the delivery of computing services like servers, storage, databases, networking, software, and more over the internet ("the cloud"). Instead of buying and maintaining physical servers or computers, you can rent computing power and storage from a cloud providers like Microsoft (Azure), Google (GCP) or Amazon (AWS). These services are run from large data centres around the world.



Types of Cloud Computing

Cloud computing can either be classified based on the deployment model or the type of service. Based on the specific deployment model, we can classify cloud as public, private, and hybrid cloud. Based on the service the cloud model offers, it can be classified as infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS).

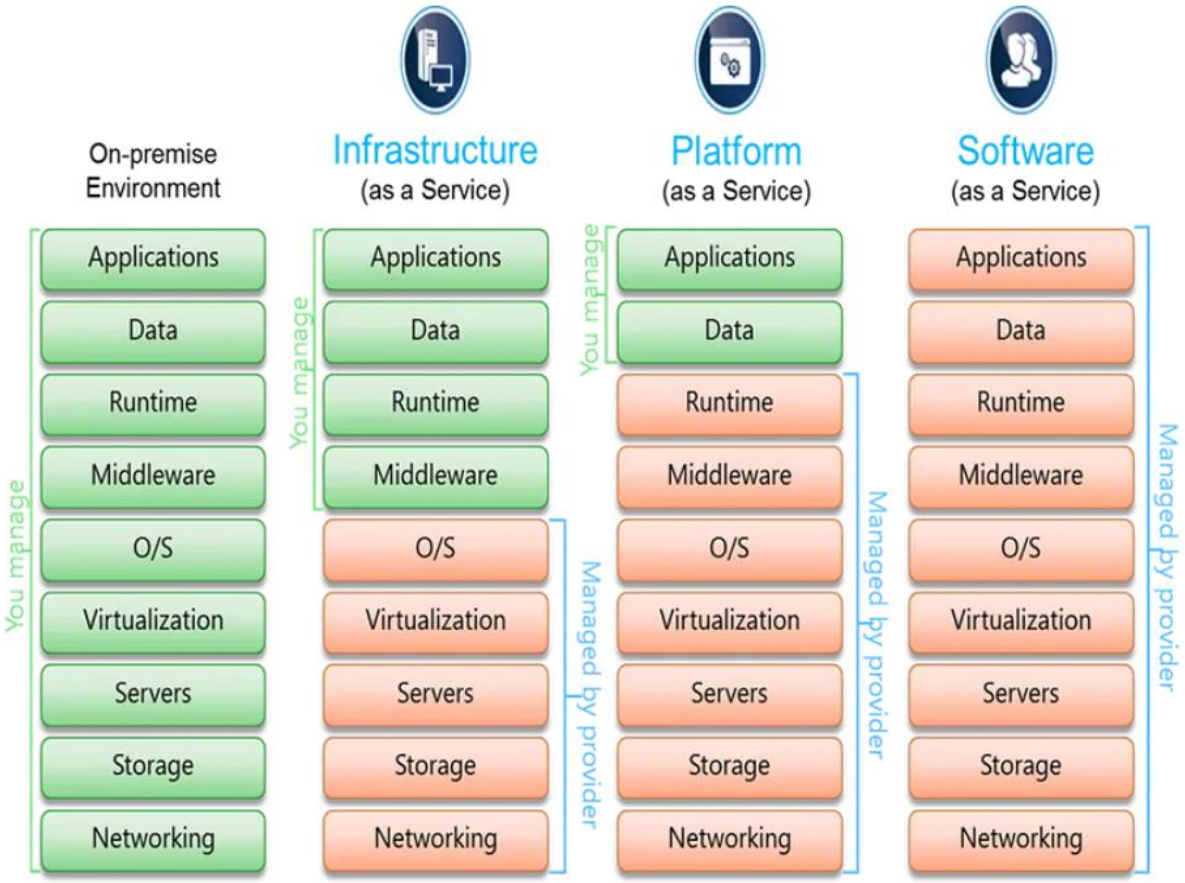


Based on Deployment

1. **Public Cloud**: This is the most common type of cloud. Companies like Microsoft, Google, and Amazon own public clouds, and anyone can use them by paying for the service. You share the cloud resources (like storage and processing power) with other users.
2. **Private Cloud**: This cloud is used exclusively by one organization. It's more secure because the resources are not shared with others, but it can be more expensive.
3. **Hybrid Cloud**: A mix of public and private clouds. For example, a company might use a private cloud for sensitive data and a public cloud for less critical applications.

Based on Service Model

When you use the cloud, you're likely using one of three main service models: IaaS, PaaS, or SaaS. Let's break these down into simple terms.



1. IaaS (Infrastructure as a Service)

- Imagine you need a computer, but instead of buying physical hardware (like a server), you rent it from a cloud provider.
- IaaS gives you access to virtual machines, storage, and networks over the internet. You get to control the operating system, software, and everything else, but the physical infrastructure is managed by the provider.
- **Example:** Think of IaaS like renting an empty house. You get the space (infrastructure), but you need to bring in your furniture (operating system, software) and set everything up yourself.
- **Use Case:** Ideal for businesses that need flexibility in building their own applications but don't want to manage physical hardware.

2. PaaS (Platform as a Service)

- PaaS provides you with a platform to develop, run, and manage applications without worrying about the underlying infrastructure. The cloud provider takes care of everything from servers to storage, so you can focus on building your app.
- **Example:** Imagine renting a fully furnished house. Everything you need is already there you just move in and start living (developing). The provider handles the setup, so you can focus on what you want to do.
- **Use Case:** Perfect for developers who want to create applications without dealing with the complexities of managing hardware and software.

3. SaaS (Software as a Service)

- SaaS is when you use software over the internet without needing to install or manage it yourself. The software runs on the cloud provider's servers, and you access it through a web browser or app.
- **Example:** SaaS is like staying in a hotel. Everything is taken care of for you—you just use the service. You don't need to worry about maintenance or updates.
- **Use Case:** Great for businesses or individuals who want to use software without the hassle of installation, maintenance, or updates.
-

Summary

- **IaaS:** You manage the software; the provider manages the hardware.
- **PaaS:** You focus on building your app; the provider manages everything else.
- **SaaS**: You use ready-made software; the provider takes care of everything.

Key Benefits of Cloud Computing

The most important reason why cloud computing is growing rapidly is the various benefits it offers. It saves businesses the time and resources required to set up full-fledged physical IT infrastructure. Let's look at all the benefits cloud offers:

Scalability

Scalability is the ability to increase or decrease computing resources based on demand. For example, if your website suddenly gets a lot of traffic, cloud computing can automatically allocate more resources to handle the load.

Elasticity

Elasticity is similar to scalability but focuses on the ability to quickly add or remove resources. It's like a rubber band that can stretch when needed and return to its original size afterward. This ensures that you're only using what you need and not paying for unnecessary resources.

Reliability

Reliability in cloud computing means that the services are consistently available and perform well. Cloud providers often have multiple backups and fail-safes to ensure reliability.

Agility

Agility is the ability to quickly and easily adapt to changes. In cloud computing, this means being able to deploy new applications or services quickly, without waiting for new hardware or software.

High Availability

High availability means that a service is always available, even if something goes wrong. Cloud providers achieve this by having multiple copies of your data in different locations (availability zones) so that if one goes down, the others can take over.

Fault Tolerance

Fault tolerance is the ability of a system to continue working even if some parts fail. In cloud computing, this means that if one server or component fails, another can automatically take over without interrupting the service.

Disaster Recovery

Disaster recovery refers to the strategies and processes that allow a business to recover quickly after a disaster, like a natural calamity or cyberattack. In cloud computing, disaster recovery often involves keeping copies of data in multiple locations to ensure it can be restored if something goes wrong.

Load Balancing

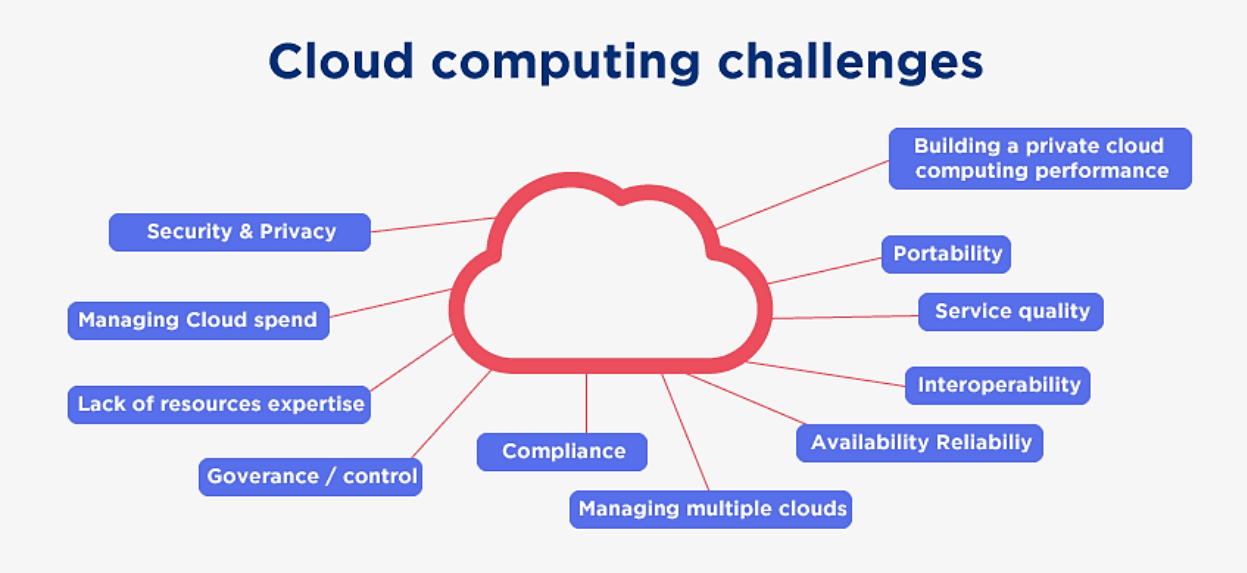
Load balancing is like a traffic cop that directs requests to different servers to ensure no single server gets overwhelmed. It helps distribute work evenly across multiple servers, improving performance and reliability.

Security

cloud computing involves protecting data, applications, and systems from unauthorized access and threats. Key aspects include encryption, identity and access management, network security, and threat detection. Effective security also requires compliance with regulations and regular updates to address vulnerabilities.

Challenges of Cloud Computing

While cloud computing offers numerous advantages, it also comes with its set of challenges. Here are some key concerns:



Security Concerns

Security remains a top worry for cloud users. Despite cloud service providers' assurances of robust security protocols and certifications, storing data on the cloud inherently involves some level of risk. Ensuring that your data remains safe requires vigilance and proactive measures.

Downtime Issues

One common challenge with cloud computing is downtime. Cloud services, while generally reliable, can occasionally experience outages. These interruptions may occur when providers face high demand or technical difficulties, leading to temporary disruptions in access to your applications.

Internet Dependency

Accessing cloud data requires a stable internet connection and compatible devices. Public Wi-Fi networks, if not secured properly, can pose additional risks when accessing cloud services. Reliable connectivity and secure access are crucial for uninterrupted cloud usage.

Financial Considerations

Cloud providers typically operate on a pay-as-you-go model. While this can be cost-effective, businesses must often commit to monthly or annual subscription plans, which can add up over time. It's essential to consider these expenses in your overall budget.

Security Risks

Even with strong security measures in place, the risk of data breaches or loss remains. Hackers increasingly target cloud storage, making it vital for businesses to implement additional security practices and safeguards to protect sensitive information.

Limited Control

Cloud users often have limited control over the underlying infrastructure. The cloud provider manages the hardware and software, leaving users with control primarily over applications rather than backend systems. This means users must rely on the provider for security, firmware updates, and overall management.

Virtualization

Virtualization is a technology that allows you to create and run virtual versions of physical resources, such as servers or operating systems. This means you can have multiple "virtual" computers running on a single physical machine. The key component in virtualization is the **hypervisor**.

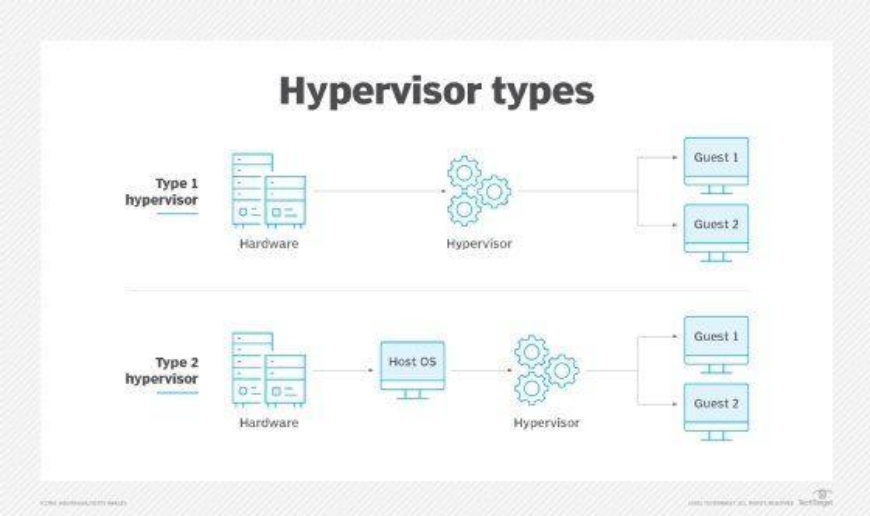
1. Hypervisor

A hypervisor is software that manages and allocates resources to virtual machines (VMs). It sits between the hardware and the VMs, creating and running these virtual environments. There are two main types of hypervisors:

- **Type 1 Hypervisor (Bare-Metal):** Runs directly on the hardware. It's more efficient and has better performance because it doesn't need a host operating system. Examples include VMware ESXi and Microsoft Hyper-V.

- **Type 2 Hypervisor (Hosted):** Runs on top of an existing operating system. It's easier to set up but can be less efficient because it relies on the host OS. Examples include VMware Workstation and Oracle VirtualBox.

Example: If the physical server is like a big, powerful machine, the hypervisor is like a smart manager that allocates space and resources to different virtual machines as needed.

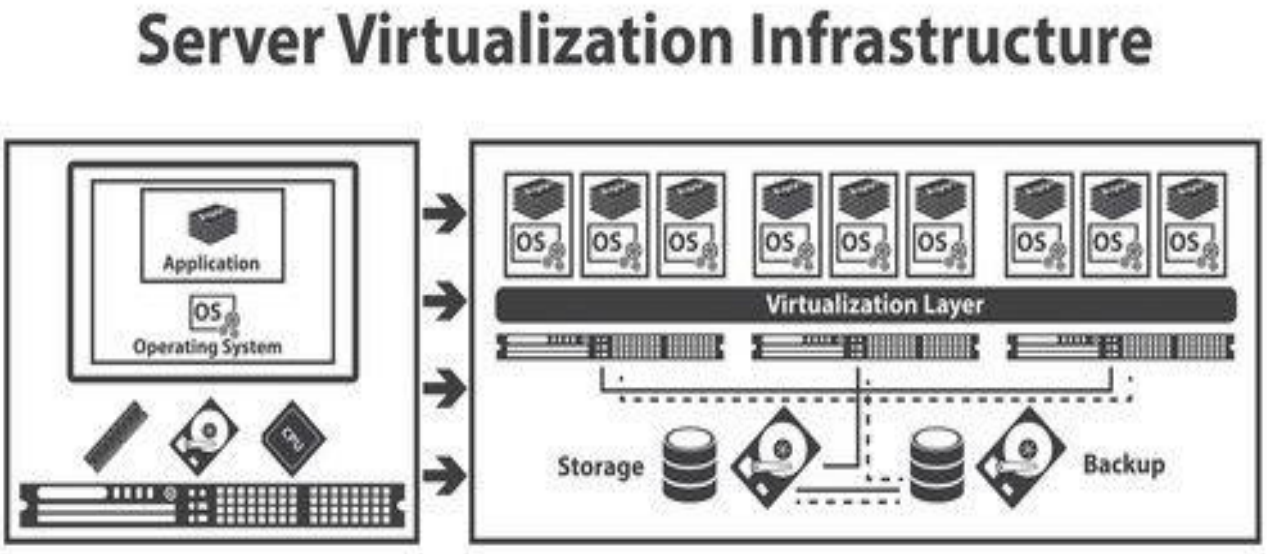


Concepts in Virtualization

1. Server Virtualization: In server virtualization, a physical server is divided into multiple VMs, each running its own OS. This allows for better utilization of hardware resources and easier management of servers.

2. Resource Pooling: Virtualization enables the pooling of physical resources, such as CPU, memory, and storage. These resources can be dynamically allocated to VMs based on demand.
3. Isolation: VMs operate independently of each other. This isolation ensures that issues in one VM do not affect others, providing a more secure and stable environment.

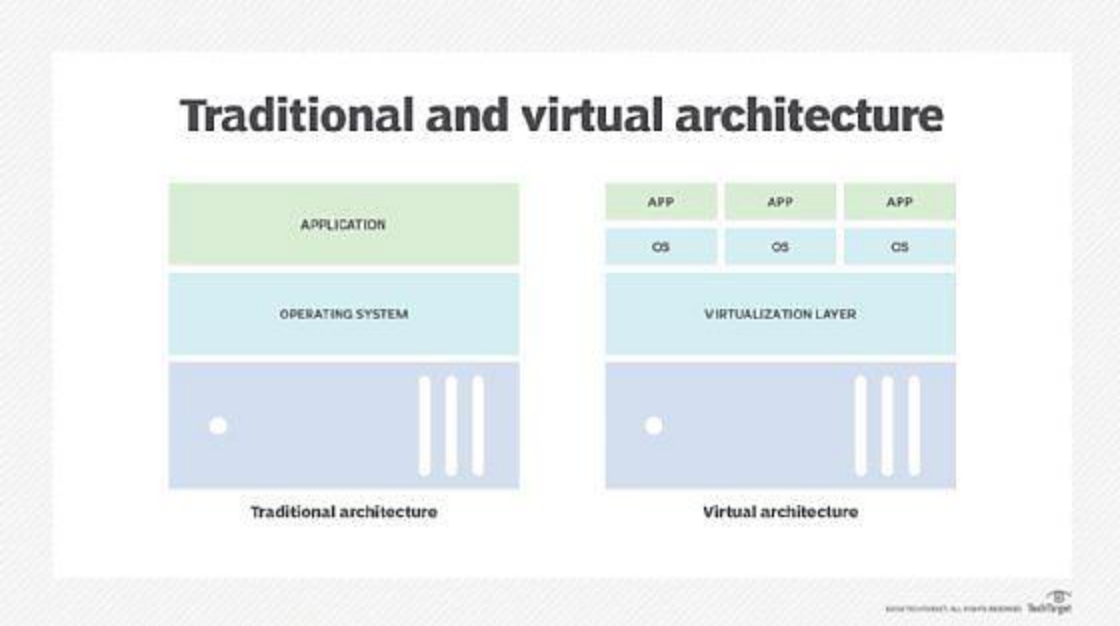
Benefits of Virtualization



1. Server Consolidation: Multiple VMs can run on a single physical server, reducing the need for a large number of physical machines. This leads to cost savings and energy efficiency.
2. Flexibility and Scalability: Virtualization allows for the easy creation, modification, and scaling of VMs. This flexibility is essential in dynamic computing environments.
3. Disaster Recovery: Virtualization simplifies disaster recovery by enabling the quick restoration of VMs from snapshots or backups.
4. Resource Optimization: Resources can be allocated and deallocated dynamically based on workload, optimizing resource utilization.
5. Testing and Development: Virtualization provides a sandbox for testing and development. VMs can be easily created, modified, and discarded without affecting the production environment.

Virtual Machines (VMs)

A virtual machine is like a computer within a computer. It has its own operating system and applications, but it runs inside a larger, physical computer. VMs are used in cloud computing to provide flexible and efficient computing power.



Virtual Machine Types

- **General-Purpose VMs:** These are versatile and can handle a variety of workloads. They are good for testing and development, small databases, and low to moderate traffic websites.
- **Compute-Optimized VMs:** Designed for applications that require high processing power, like complex calculations or simulations.
- **Memory-Optimized VMs:** Ideal for applications that need large amounts of memory, such as big databases or data analytics.
- **Storage-Optimized VMs:** Best for applications that require high disk throughput, like large data processing or high-performance databases.
- **GPU VMs:** Equipped with graphics processing units (GPUs) for tasks like machine learning, 3D rendering, or other GPU-intensive operations.

Let's get started with AZURE!!!

Now that we've covered the challenges of cloud computing, it's time to dive into Azure! Azure is Microsoft's cloud computing platform, designed to address many of the issues mentioned above while offering powerful solutions for modern businesses. Let's explore what Azure has to offer and how it can help you navigate the cloud landscape effectively.

1. Introduction to Azure

Azure is Microsoft's cloud platform, offering a range of services from virtual machines and databases to analytics and networking. As organizations adopt cloud strategies, understanding Azure is crucial for handling infrastructure, scaling, and security needs.

1.1 Core Azure Services

Azure provides services across several domains, including computing, networking, storage, and databases. Some of the core services include:

1. Virtual Machines (VMs):

Allow you to create and manage powerful virtual servers in the cloud. You can run Windows, Linux, and other operating systems without needing to maintain physical hardware.

2. Azure App Service (PaaS):

A platform for hosting web apps, REST APIs, and mobile backends. With Azure App Service, you can build and deploy scalable web applications without managing infrastructure.

3. Azure SQL Database:

A fully managed, scalable database service. You can use it to store and manage relational data without worrying about the underlying hardware.

4. Azure Blob Storage:

Designed for storing large amounts of unstructured data like text or binary data. Common use cases include storing backups, media files, or logs.

5. Azure Virtual Network (VNet):

This service allows you to create isolated cloud networks and connect them to on-premises infrastructure. VNet's let you define security rules and network routes for your applications.

6. Azure Functions:

A serverless compute service that allows you to run small pieces of code (functions) in response to events, without needing to manage infrastructure.

7. Azure Kubernetes Service (AKS):

A managed container orchestration service based on Kubernetes. It simplifies deploying, managing, and scaling containerized applications.

8. Active Directory (AD):

A cloud-based identity and access management service. Azure AD helps manage user access to resources and applications within your organization.

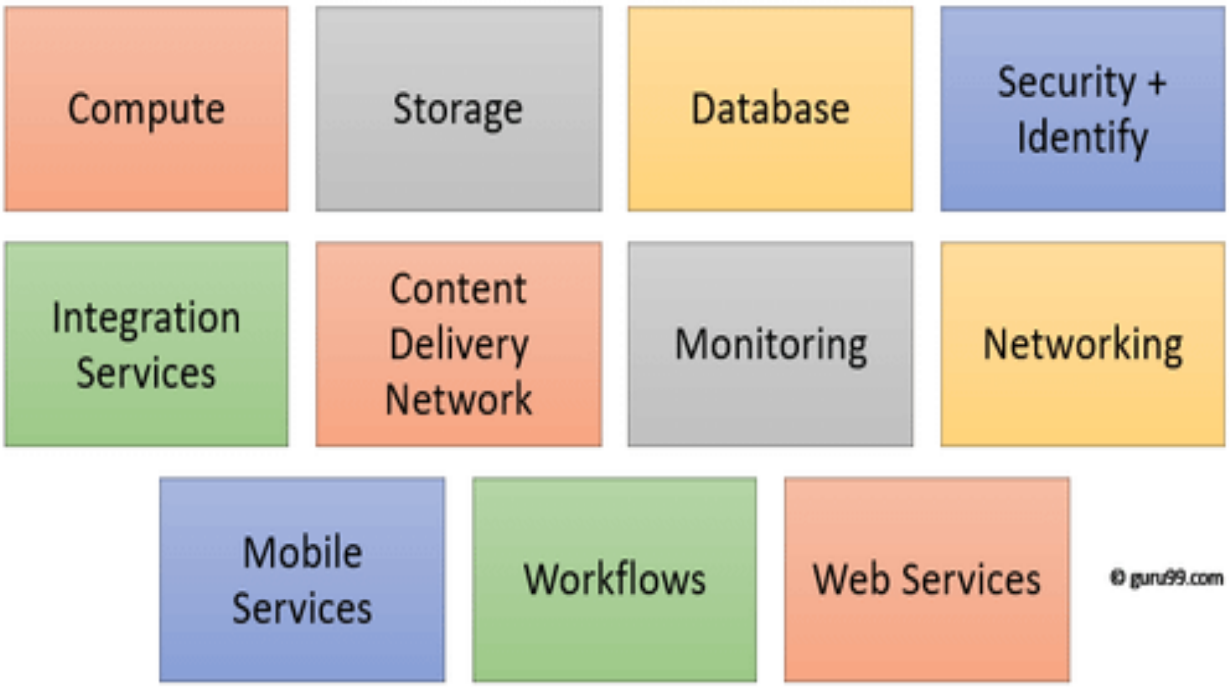
9. Azure Cosmos DB:

A globally distributed, multi-model database service that allows you to build highly responsive and scalable applications.

10. Azure DevOps:

A suite of development tools to plan work, collaborate on code, build, and deploy applications. It includes Azure Pipelines, Azure Repos, Azure Boards, and more.

1.2 Azure Infrastructure



Azure's infrastructure is the backbone that supports its cloud services. Here's how it works:

1. Data Centers:

Azure operates data centers across the globe, often in groups called "regions". Each Azure region is a set of data centers deployed within a defined geographic area, and it is designed to provide low-latency access to Azure services for users and applications in that region.

2. Regions and Region Pairing:

"Regions" are physical locations around the world where Azure data centers are clustered. "Region Pairing" means that each Azure region is paired with another region in the same geography. This provides redundancy in case of a failure in one region. For instance, if a region goes down, the paired region can ensure services stay online.

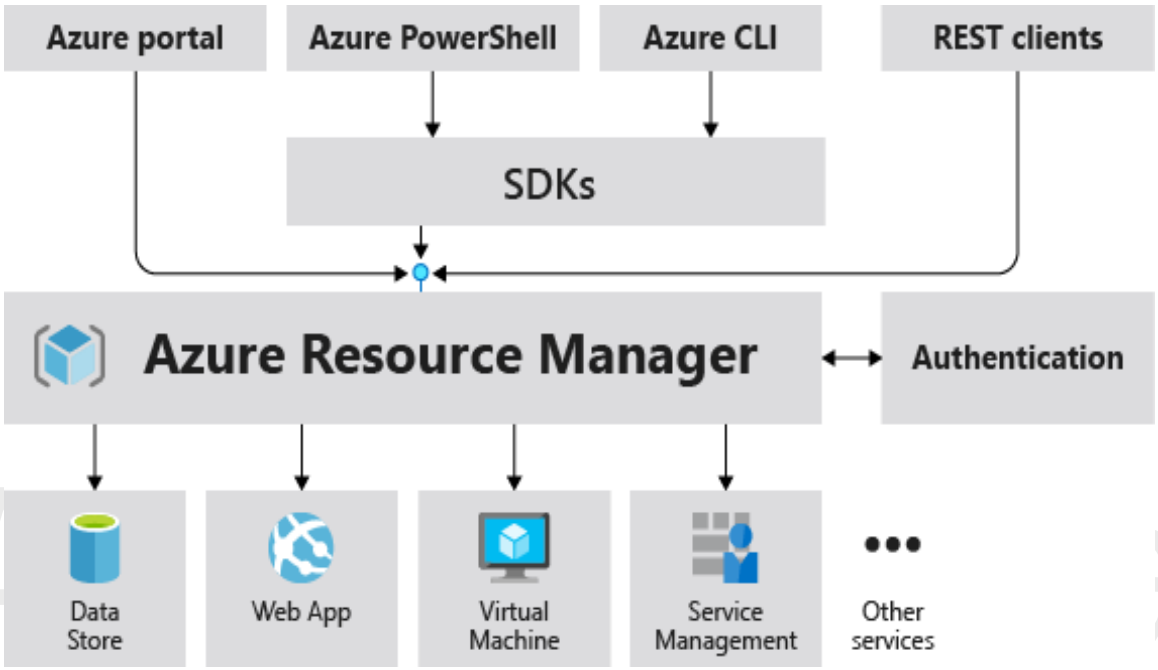
3. Availability Zones:

Each Azure region is divided into "Availability Zones", which are separate physical locations within the region. These zones are designed to offer isolation from failures, such as power outages or hardware failures. If one zone goes down, others remain available, keeping applications running smoothly

.

4. Azure Resource Manager (ARM):

ARM is the management layer for Azure. It organizes your resources (like virtual machines, databases, etc.) into groups, making it easier to deploy, manage, and monitor them. ARM ensures that resources in the same group can interact securely and efficiently.

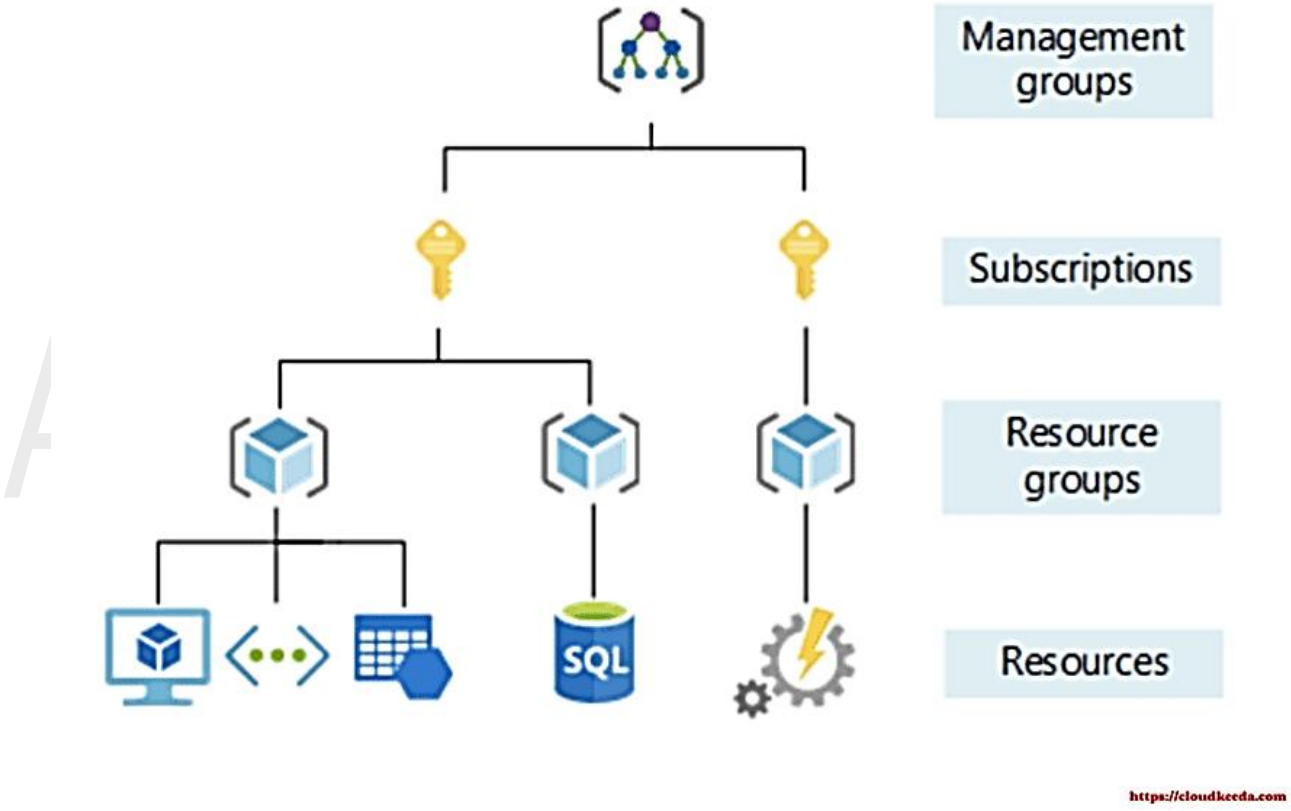


5. Networking:

Azure provides powerful networking services that allow users to create virtual networks (VNets), connect on-premises networks to the cloud (VPN gateways), and manage network traffic (load balancers). This flexible networking infrastructure allows organizations to build secure, scalable cloud networks.

1.3 Azure Resources

- In Azure, a "resource" is anything you create or use within the platform, such as virtual machines, storage accounts, databases, or networks. These resources are the building blocks of your cloud environment.
- Example: Think of Azure resources like individual appliances in your home—each one has a specific purpose, like a fridge for storing food or a washing machine for cleaning clothes.



1.4 Azure Resource Groups

- When you create resources in Azure, is (mandatory) to place them in a resource group. This grouping makes it easier to manage, monitor, and organize your resources.
- Why They're Mandatory: Resource groups are mandatory because they provide a way to manage resources collectively. For example, you can apply the same settings,

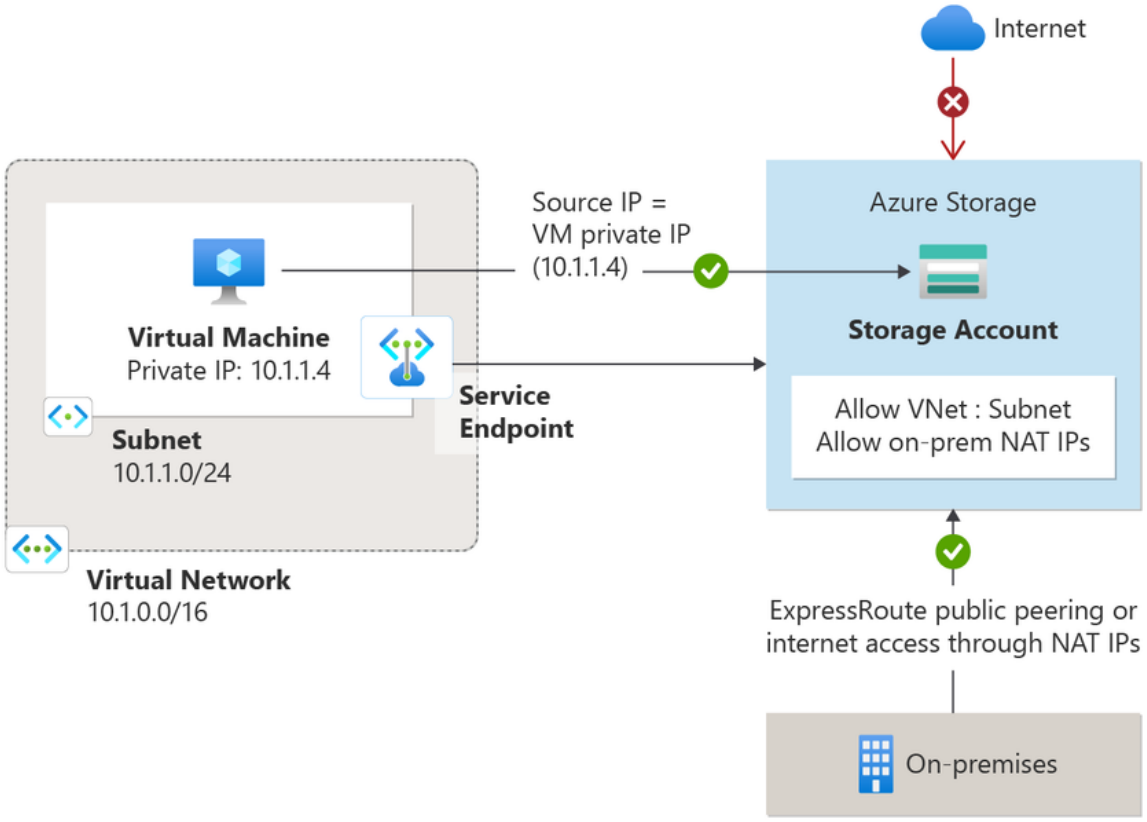
permissions, or policies to all resources in a group, and when it's time to delete the project, you can remove all related resources at once by deleting the resource group.

1.5 Azure Networking

Virtual Network (VNet)

A Virtual Network (VNet) in Azure is a private network that connects Azure resources securely and can be extended to on-premises networks.

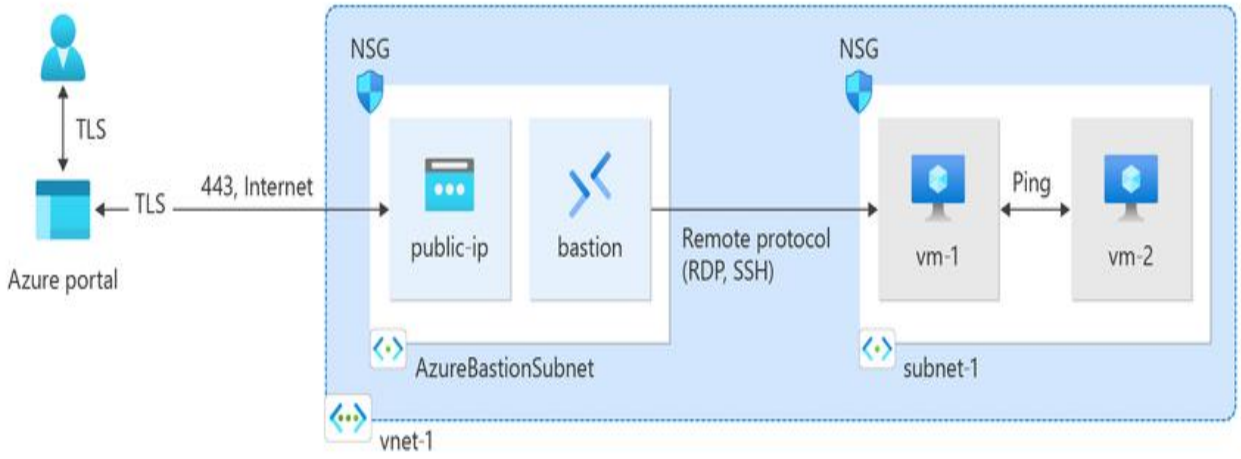
- Isolation: A VNet provides network-level isolation, ensuring that resources in one VNet can't directly communicate with resources in another unless explicitly allowed.
- Subnetting: You can divide a Virtual Network into smaller segments called subnets. Subnets allow you to organize resources, control traffic, and improve network efficiency.
- Address Space: Each VNet has an IP address range defined using CIDR (Classless Inter-Domain Routing) notation. The address space determines the range of IP addresses available for resources within the network.



Subnets

Subnets are subdivisions of a Virtual Network that allow for better resource organization and control over traffic flow. By separating resources into subnets, you can:

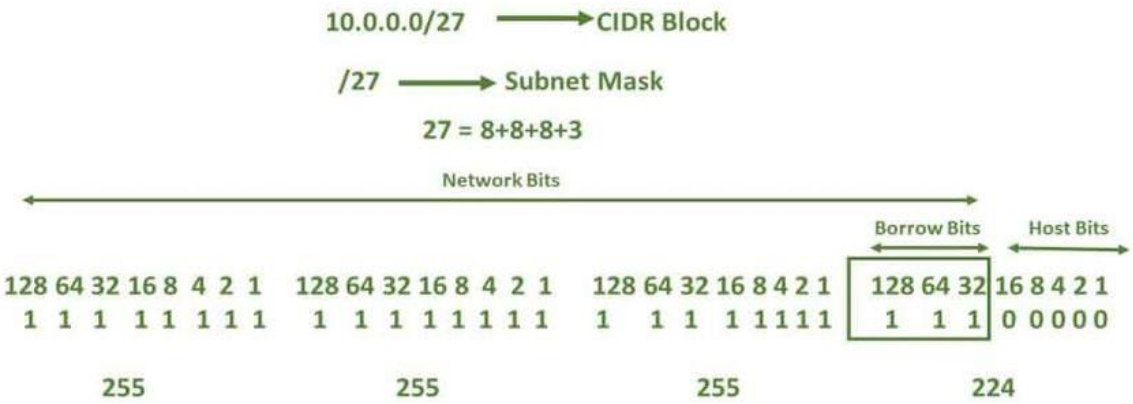
- Apply different security rules to each subnet.
- Control traffic flow between subnets within the same VNet.
- Distribute workloads based on their function (e.g., front-end and back-end servers).



CIDR (Classless Inter-Domain Routing)

CIDR is a method for allocating IP addresses and routing. It helps define the range of IP addresses used in a network or subnet. CIDR notation (e.g., 192.168.1.0/24) specifies:

- The base IP address of the network.
- The network prefix length, which defines how many IP addresses are available in the network or subnet.



Routes

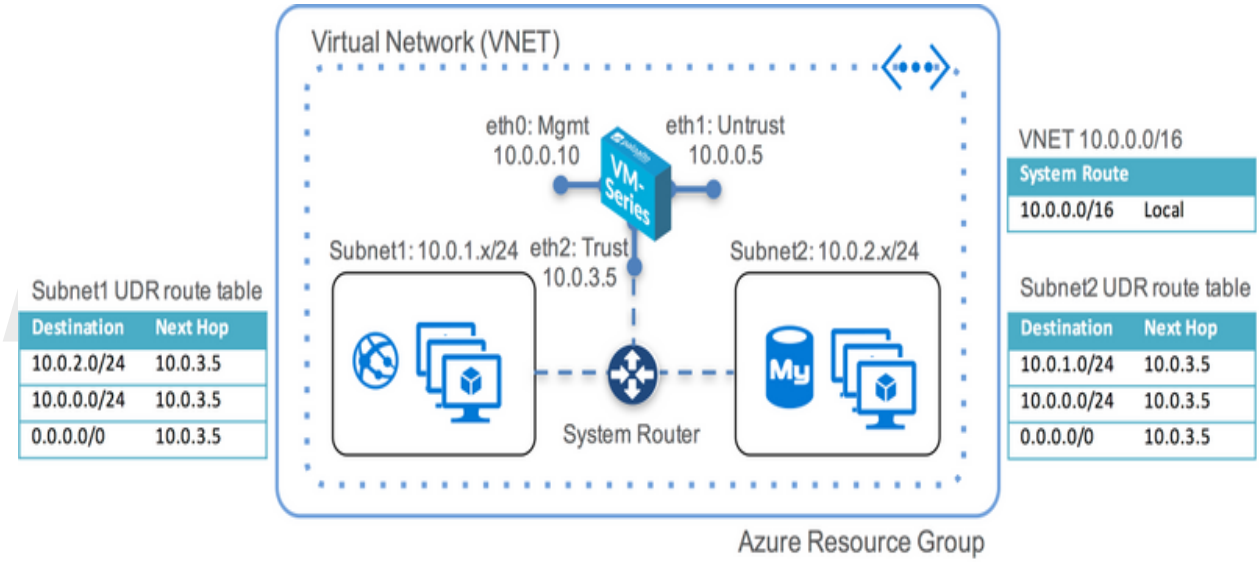
Routes determine how network traffic is directed from one place to another. Each route specifies:

- The destination (where the traffic is going).
- The next hop (the next point that the traffic passes through on its way to the destination).

Route Tables

Route Tables are collections of routes that are associated with subnets. They allow you to create custom routing rules for how traffic flows within the VNet or to external networks. For example:

- You can route traffic from one subnet to another within the VNet.
- You can specify routes to on-premises networks via VPN gateways or ExpressRoute.



1.6 Network Security Groups (NSGs)

Network Security Groups are a key component of Azure's network security framework. They help manage and filter traffic at the network level.

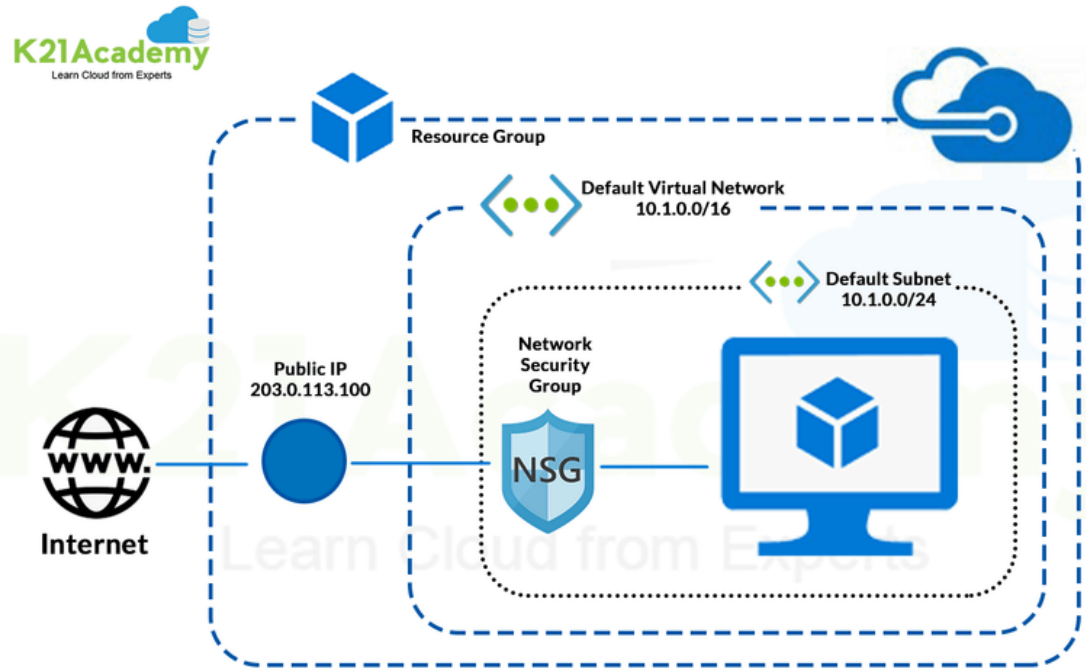
Security Rules: NSGs use rules to allow or block traffic based on source/destination IP address, port, and protocol (e.g., TCP/UDP). Each rule specifies:

- Priority: The order in which rules are applied (lower numbers are processed first).
- Direction: Whether the rule applies to inbound or outbound traffic.
- Action: Allow or deny the traffic.

Default Rules: NSGs come with default security rules that help control traffic within the Virtual Network and between subnets. These include:

- Allow traffic between resources in the same VNet.
- Block inbound traffic from the internet by default.

Association: NSGs can be applied to both subnets and individual network interfaces (NICs) on virtual machines. This flexibility allows you to apply different security rules at different levels.

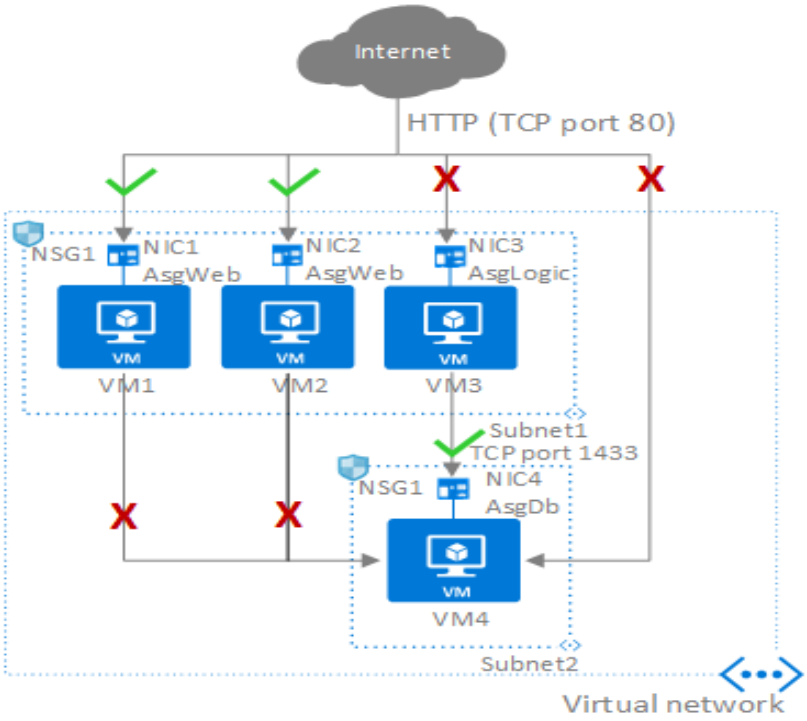


1.7 Application Security Groups (ASGs)

Application Security Groups simplify the process of managing network security by grouping virtual machines based on their application or role.

Simplification: Instead of managing security rules for individual IP addresses, you can assign rules to a group of VMs that serve the same function. This makes it easier to manage security for large-scale applications.

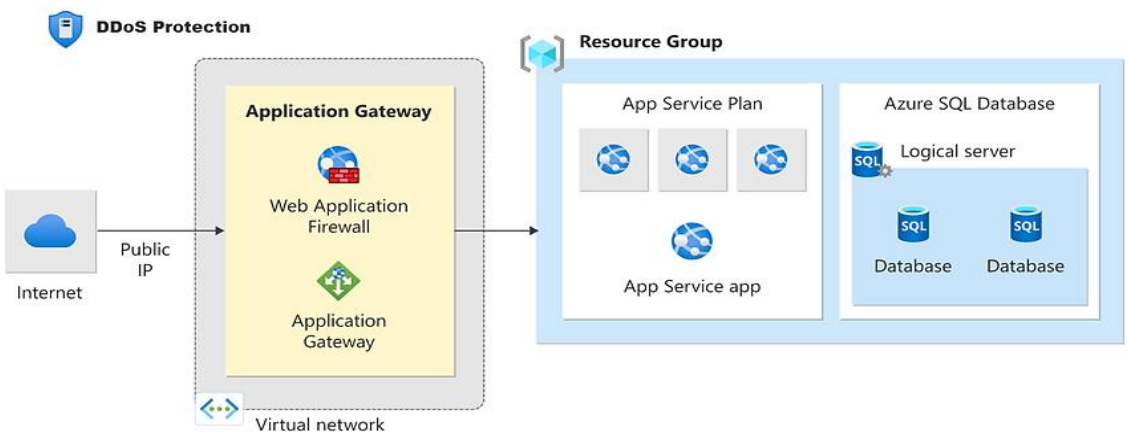
Rule Association: You can create security rules that apply to an entire ASG, allowing for more intuitive network security management. For example, you can create a rule that allows traffic between a web server ASG and a database ASG, without needing to specify individual IP addresses.



1.6 Azure Networking Advanced

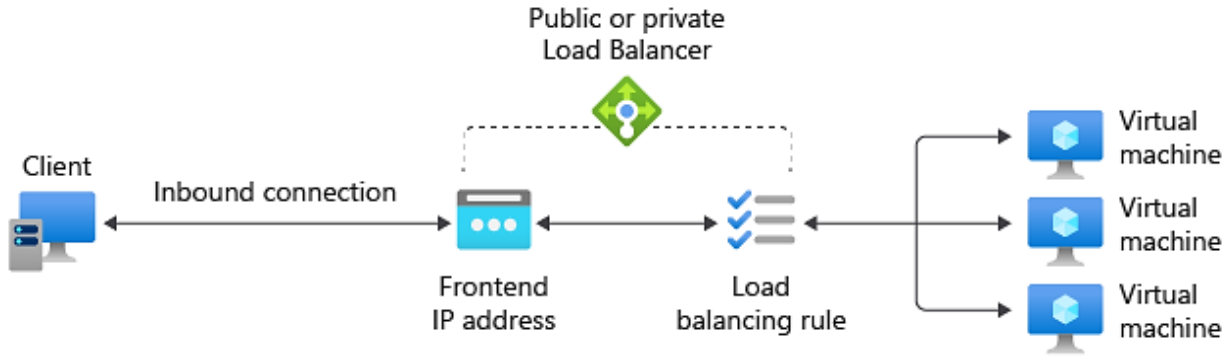
Azure Application Gateway & Web Application Firewall (WAF)

Azure Application Gateway is a web traffic load balancer designed to manage and route traffic to web applications. It includes features like load balancing to distribute traffic evenly across multiple servers, SSL termination to offload SSL processing from servers, and Web Application Firewall (WAF) to protect against web vulnerabilities.



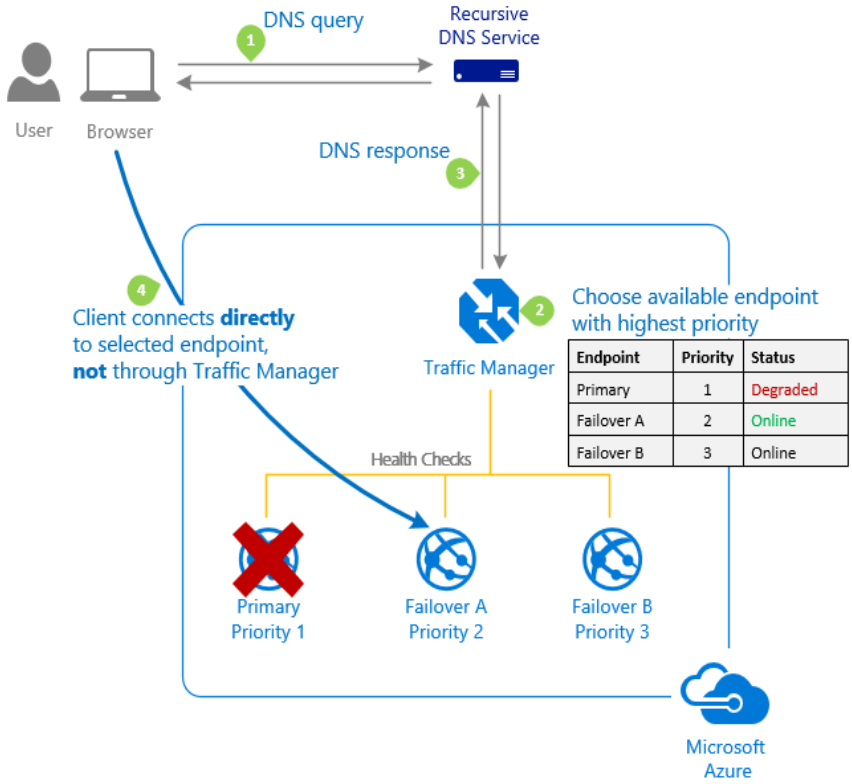
Azure Load Balancer

Azure Load Balancer distributes incoming network traffic across several servers, ensuring no single server is overwhelmed. It supports various load balancing algorithms, works with availability sets for high availability, and manages both inbound and outbound traffic



Azure DNS

Azure DNS is a scalable domain hosting service providing name resolution using Azure's infrastructure. It integrates well with other Azure services, offers global availability for low-latency responses, and handles domain name management efficiently.



Azure Firewall

Azure Firewall is a managed network security service that protects Azure Virtual Network resources. It offers stateful firewall capabilities, application FQDN filtering, and integrates with threat intelligence feeds to enhance security.

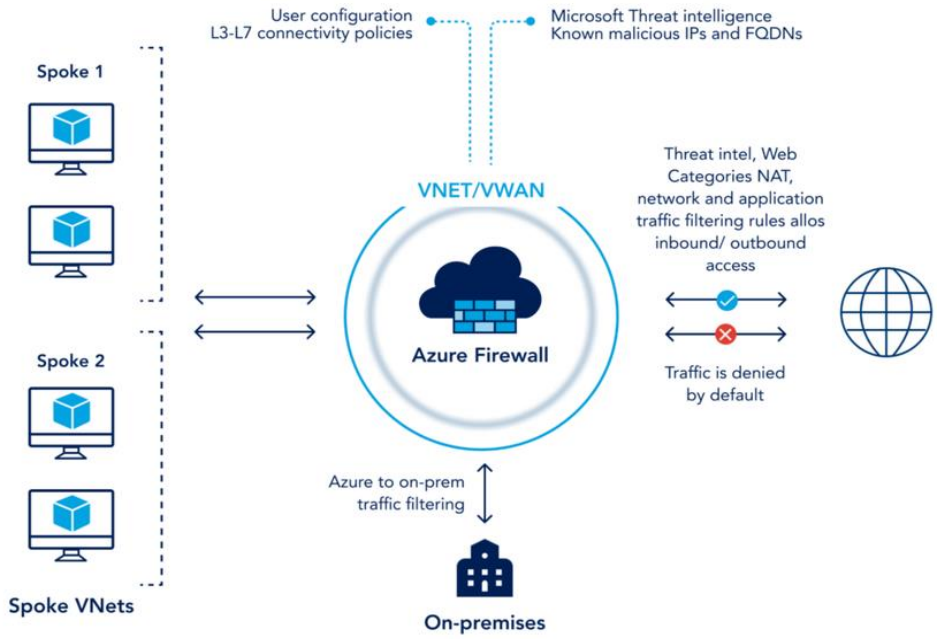
Virtual Network Peering and VNet Gateway

Virtual Network Peering connects Azure Virtual Networks, enabling resources in different VNets to communicate directly. It supports global peering and transitive routing for improved performance.

VNet Gateway provides secure communication between on-premises networks and Azure Virtual Networks. It supports Site-to-Site VPN for encrypted connections and Point-to-Site VPN for remote access.

VPN Gateway

Azure VPN Gateway ensures secure site-to-site connectivity between on-premises networks and Azure. It uses IPsec/IKE VPN protocols for secure communication, supports high availability with active-active and active-passive configurations, and allows dynamic routing via BGP.



NOTE: The images used in this document are taken from the internet