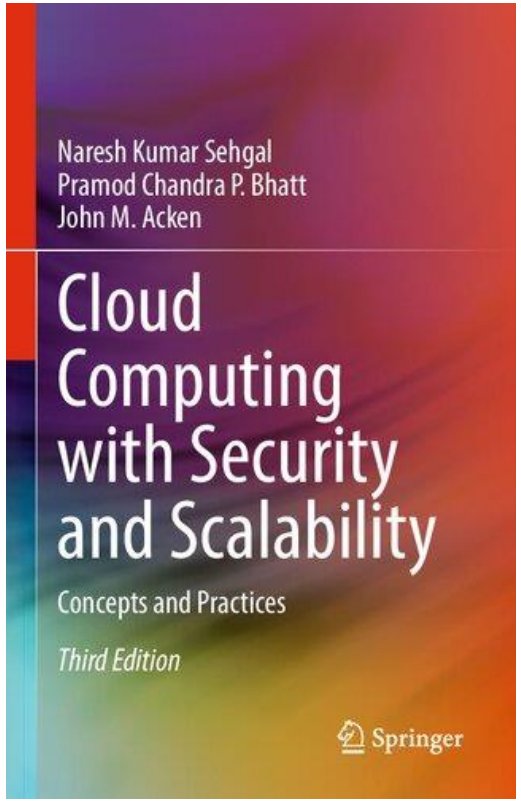
Cloud Computing

IF3110 – Web-based Application Development
School of Electical Engineering and Informatics
Institut Teknologi Bandung

Reference



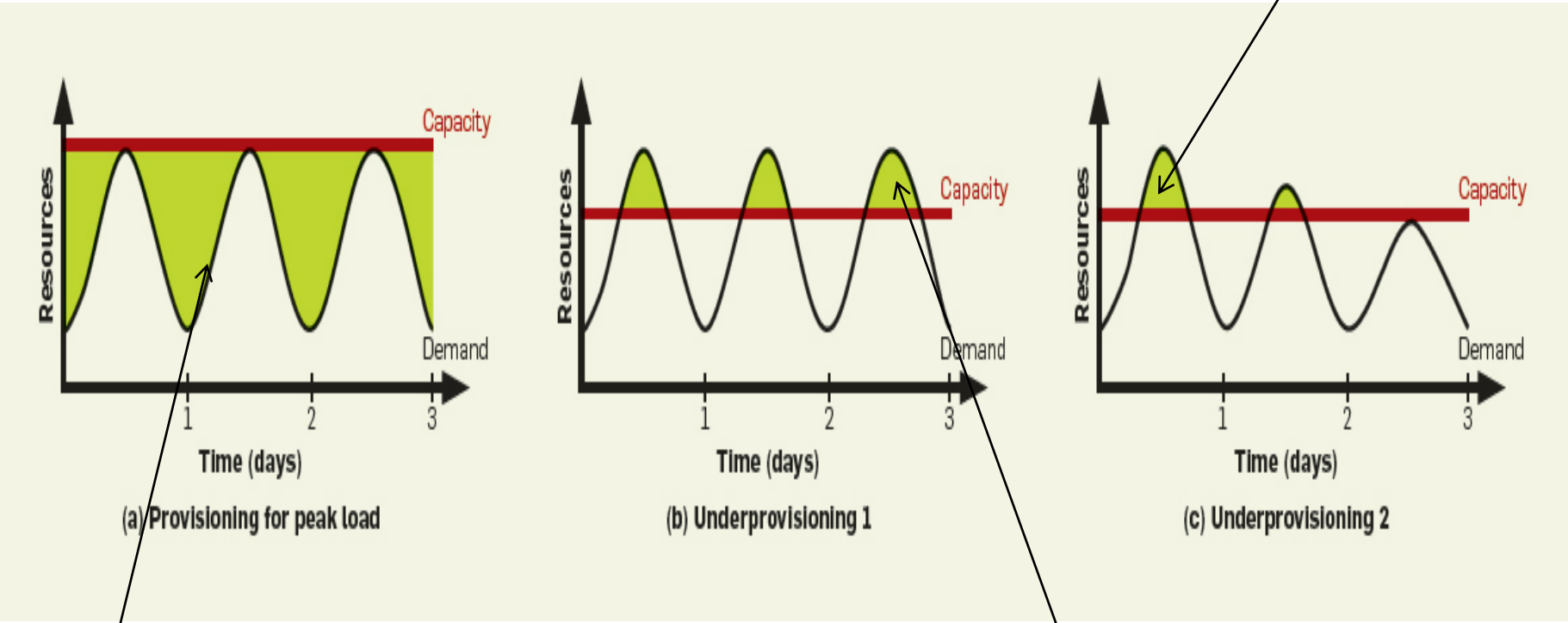
Naresh Kumar Sehgal, Pramod Chandra P. Bhatt, John M. Acken - Cloud Computing with Security and Scalability. Concepts and Practices-Springer (2023)

Divit Gupta - The Cloud Computing Journey_ Design and deploy resilient and secure multi-cloud systems with practical guidance-Packt Publishing Pvt. Ltd. (2024)

Suppose you have an innovative idea…

- You need a large capital outlay in hardware.
- You need talented humans to operate and maintain the system.
- There is an over provisioning risk – the new system may not be as popular as you hoped.
- There is an under provisioning risk – missing and losing potential users.
- Cloud computing allows you to start small and grow as needed.

Over or Under-Provisioning



Less and less demand.

Shaded area is unused capability.

Shaded area represents requests not served.

Real world estimates

- Average server utilization is 5% to 20%.
- Peak workload exceeds the average by factors of 2 to 10.
- Users provision for the peak.
- Peak loads may occur based on the time of day or based on other factors (e.g. photo sharing after the holidays, drop/add within two weeks of start of term, etc.)

What is Cloud Computing

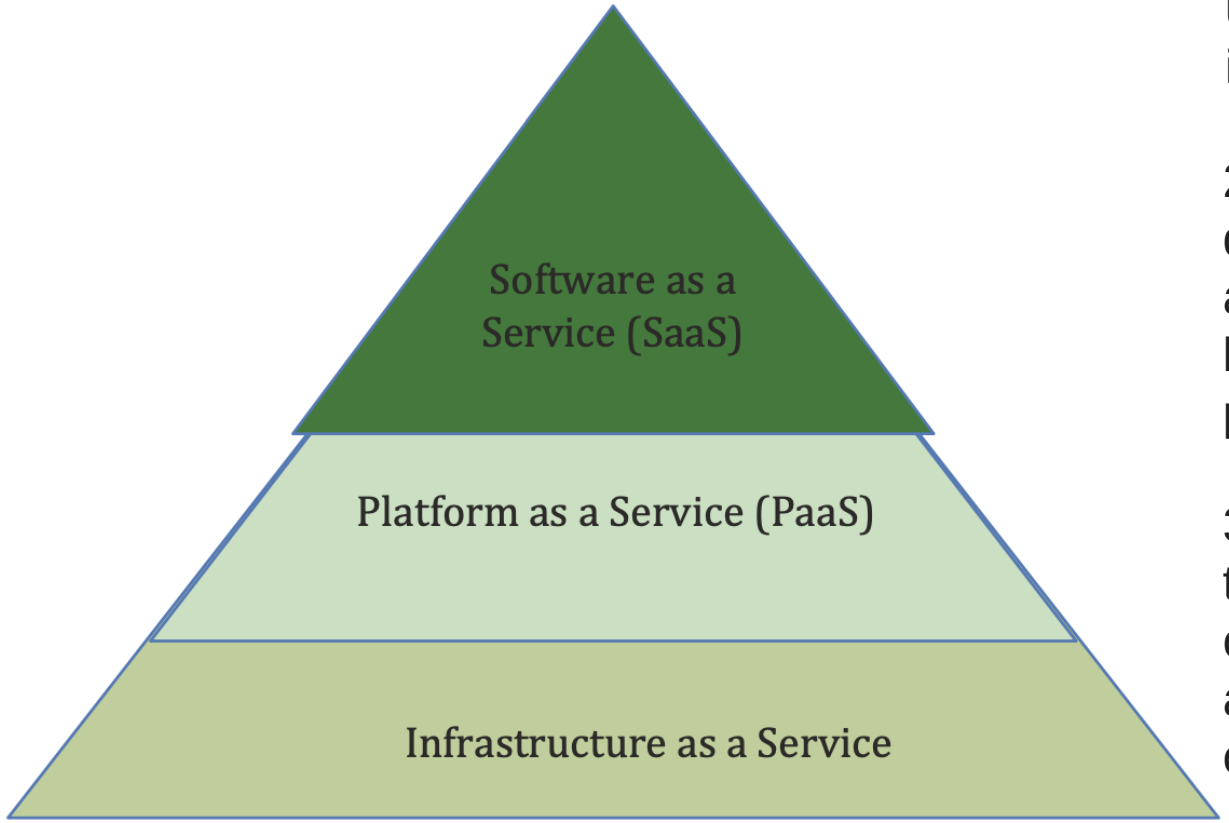
Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (US NIST)

Essential Characteristic of Cloud Computing

According to US NIST, any Cloud must have the following five characteristics

1. Rapid Elasticity: Elasticity is defined as the ability to scale resources both up and down as needed.
2. Measured Service: In a measured service, aspects of the Cloud service are controlled and monitored by the Cloud provider.
3. On-Demand Self-Service: The on-demand and self-service aspects of Cloud Computing mean that a consumer can use Cloud services as needed without any human interaction with the Cloud provider.
4. Ubiquitous Network Access: Ubiquitous network access means that the Cloud provider's capabilities are available over the network and can be accessed through standard mechanisms by both thick and thin clients.
5. Resource Pooling: Resource pooling allows a Cloud provider to serve its consumers via a multi-tenant model.

Cloud Computing Services Model

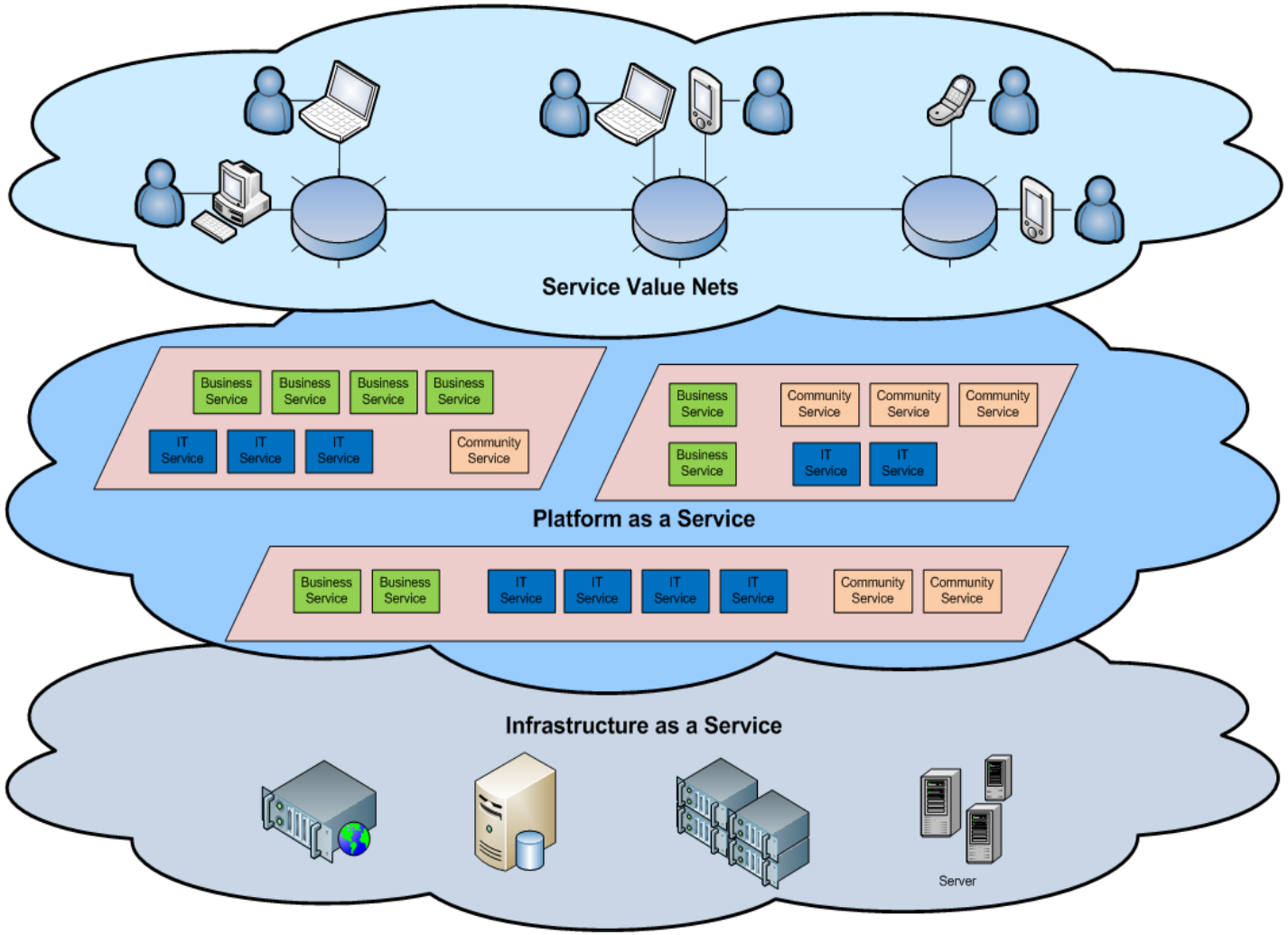


1. Software as a Service (SaaS): allows the consumer to use the provider's applications running on a Cloud infrastructure.

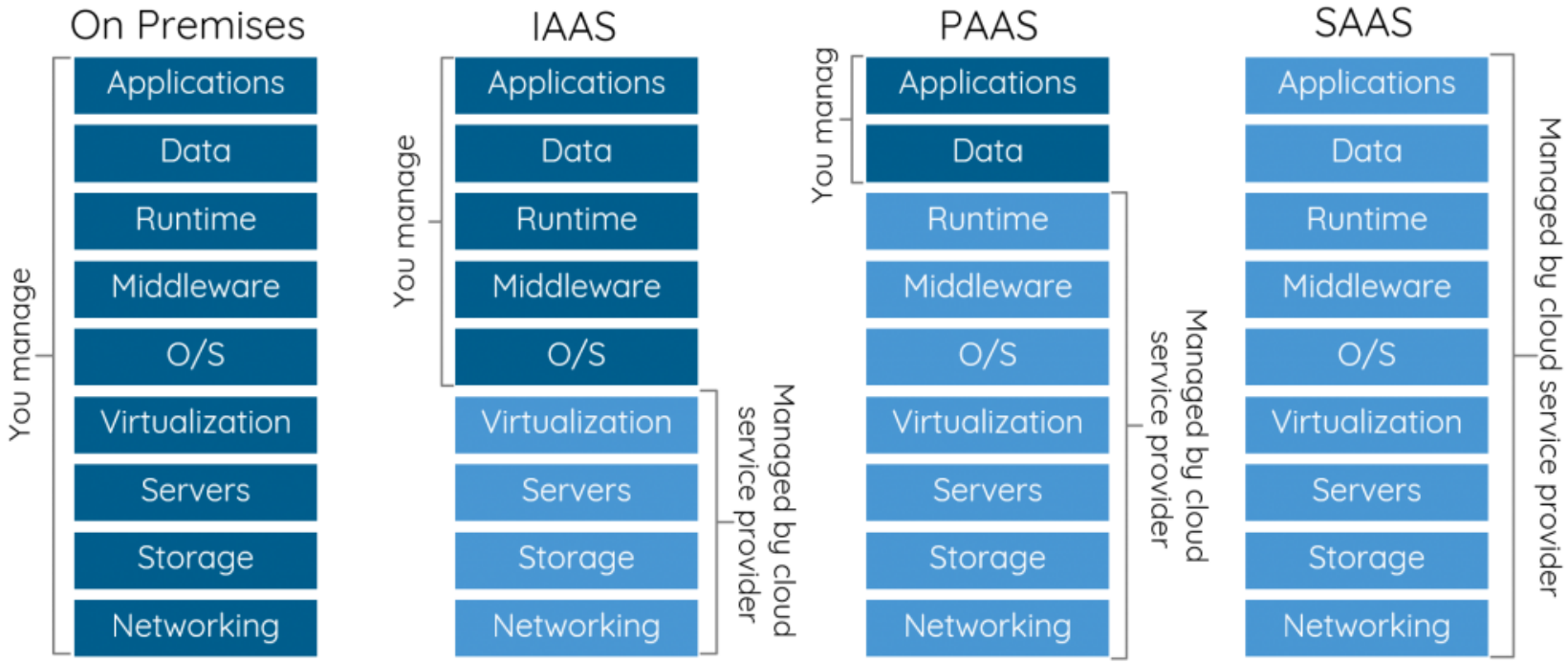
2. Platform as a Service (PaaS): allows the consumer to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

3. Infrastructure as a Service (IaaS): allows the consumer to provision CPU processing, storage, networks, and other computing resources at the lowest abstraction levels, with an ability to deploy and run software, which can include operating systems and applications.

Cloud Architecture



Cloud Architecture



Three Examples

SaaS: Dropbox and Salesforce allow users to use services without any hassles in setting up any computing infrastructure

PaaS: AppEngine (Google) Build scalable web applications fast. Not for general purpose computing.

PaaS: Azure (Microsoft) Use .NET and .NET libraries as needed. General purpose computing on a Microsoft platform.

IaaS: EC2 (Amazon) Elastic Compute Cloud (Choose OS and the entire software stack. General purpose computing

Cloud Computing Type

1. Public Cloud: Cloud infrastructure is made available to the general public.

2. Private Cloud: Cloud infrastructure is operated solely for an organization.

3. Hybrid Cloud: Cloud infrastructure is composed of two or more Cloud that interoperate or federate through technology.

Essential cloud infrastructure components

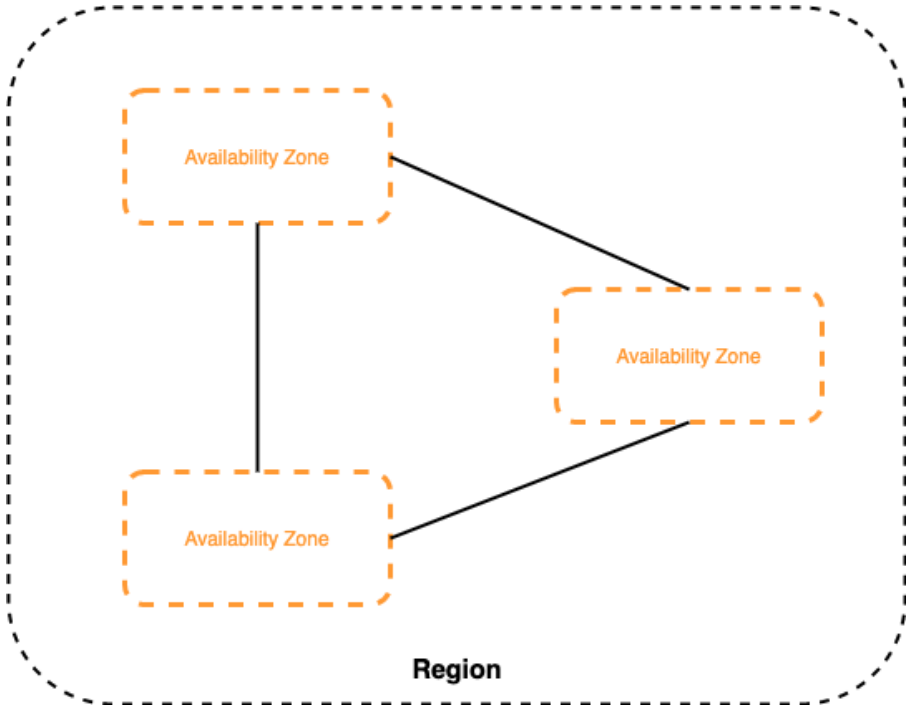
- Physical data centers
- Virtualization and hypervisors
- Networking
- Storage
- Security
- Management and orchestration
- Monitoring and analytics
- Disaster recovery and backup
- Compliance and governance

Physical data centers

Data centers form the foundation of cloud infrastructure as they house the necessary hardware, including servers, storage systems, and networking equipment. They provide the physical space, power, and cooling required to support the operation of cloud services.

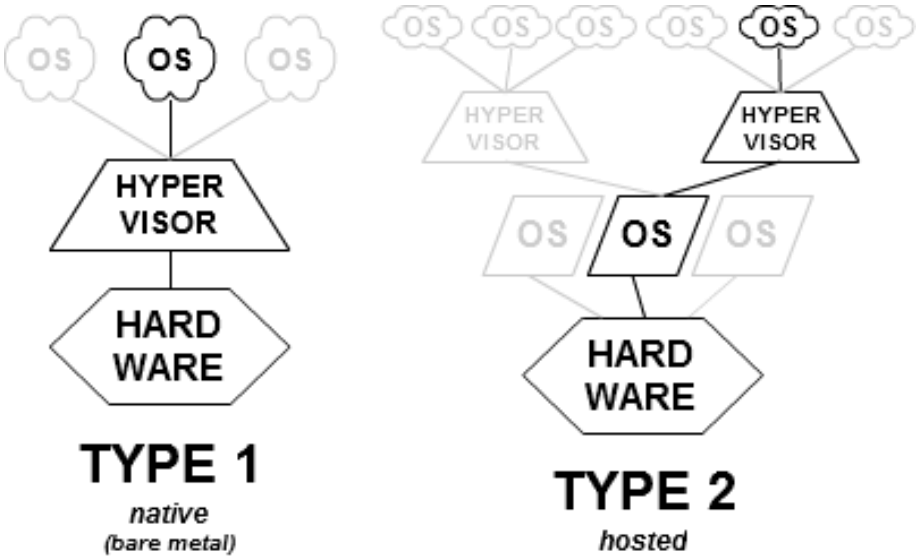
The design, maintenance, and management of physical data centers are critical to ensuring the availability, scalability, and reliability of cloud services.

Example: AWS



AWS has the concept of a Region, which are physical locations around the world where we cluster data centers. We call each group of logical data centers an Availability Zone (AZ). Each AWS Region consists of multiple, isolated, and physically separate AZs within a geographic area. Each AZ consists of one or more physical data centers, and we design each AZ to be completely isolated from the other AZs in terms of location, power, and water supply.

Virtualization and hypervisors



- Virtualization allows multiple VMs to run on a single physical server, enabling efficient resource utilization.
- Hypervisors, such as VMware ESXi and KVM, manage the creation, allocation, and management of these VMs.

Networking

Networking components include switches, routers, load balancers, and firewalls. They establish and maintain connections between different cloud components, enabling communication and data transfer.

- Protocols (TCP/IP, UDP)
- Virtual private networks (VPNs)
- Load balancing
- Firewalls
- Software-defined networking (SDN)

Storage

Storage is a fundamental component of cloud infrastructure that plays a crucial role in storing and managing vast amounts of data for cloud-based applications and services.

Cloud storage encompasses different types, such as block storage, file storage, and object storage. Block storage provides raw storage blocks, similar to traditional hard drives. File storage offers a hierarchical filesystem, while object storage provides scalable and durable storage for unstructured data.

Storage area networks (SANs) and network-attached storage (NAS) are commonly used in cloud environments.

Object Storage is often used for most of web application use cases

Security

Security components ensure the protection and integrity of cloud infrastructure and data. This includes encryption mechanisms, firewalls, access control, authentication, and intrusion detection systems.

- Authentication and access control
- Data encryption
- Network security
- Vulnerability management
- Security monitoring and logging
- Incident response and disaster recovery
- Compliance and regulatory requirements

Management and orchestration

Cloud management platforms enable centralized management and control of the cloud infrastructure. These platforms facilitate tasks such as provisioning and monitoring resources, managing user access, and implementing automation and orchestration for efficient resource allocation and deployment.

- Provisioning and resource allocation
- Monitoring and performance management
- Automation and orchestration
- Configuration and change management
- Cost management and billing
- Governance and compliance:

Monitoring and analytics

Monitoring tools track the performance, availability, and health of the cloud infrastructure and applications. They provide real-time insights, enabling the proactive identification and resolution of issues.

- Real-time monitoring
- Alerting and incident management
- Performance optimization
- Capacity planning
- Cost optimization
- Security monitoring
- Analytics and reporting

Disaster recovery and backup

Disaster recovery mechanisms ensure business continuity by replicating data and applications to alternate locations. Backup strategies involve regularly creating copies of data to protect against data loss or corruption.

- Data replication
- Backup and restore
- Disaster recovery planning
- Failover and high availability
- Testing and validation
- Data protection and compliance
- Cost-efficiency
- Rapid recovery

Compliance and governance

Cloud infrastructure components adhere to industry-specific compliance requirements and governance policies. This ensures the security, privacy, and regulatory compliance of data and services hosted in the cloud

- Regulatory compliance
- Data privacy and protection
- Security assessments and audits
- Risk management
- Policy management
- Auditing and reporting
- Legal and contractual compliance
- Incident response and forensics
- Continuous monitoring and compliance

Top Public Cloud Providers

- AWS (Amazon Web Services)
- Microsoft Azure
- GCP (Google Cloud Platform)
- Alibaba Cloud
- Oracle
- IBM Cloud

Service similarities between cloud service providers

Google Cloud Platform	Amazon Web Services[12]	Microsoft Azure[13]	Oracle Cloud[14]
Google Compute Engine	Amazon EC2	Azure Virtual Machines	Oracle Cloud Infra OCI
Google App Engine	AWS Elastic Beanstalk	Azure App Services	Oracle Application Container
Google Kubernetes Engine	Amazon Elastic Kubernetes Service	Azure Kubernetes Service	Oracle Kubernetes Service
Google Cloud Bigtable	Amazon DynamoDB	Azure Cosmos DB	Oracle NoSQL Database
Google BigQuery	Amazon Redshift	Azure Synapse Analytics	Oracle Autonomous Data Warehouse
Google Cloud Functions	AWS Lambda	Azure Functions	Oracle Cloud Fn
Google Cloud Datastore	Amazon DynamoDB	Azure Cosmos DB	Oracle NoSQL Database
Google Cloud Storage	Amazon S3	Azure Blob Storage	Oracle Cloud Storage OCI

Intellectual Exercises

- Identify common tasks in Web Developments
- Which tasks do need some adjustments because using clouds?