

# CLC Exam Prep - Lesson 1: Cloud Computing

---

## Definition of Cloud Computing

What is the definition of Cloud Computing defined by NIST?

Cloud computing is a model for enabling ubiquitous, 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. (Source: NIST SP 800-145)

## Essential Characteristics of Cloud Computing

What are the five essential characteristics of cloud computing as defined by NIST? Provide a brief example for each.

- **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
  - *Example: A developer provisioning a new virtual server from a web console without needing to call or email the provider.*
- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
  - *Example: Accessing cloud-based email (SaaS) from a smartphone, laptop, or tablet through a web browser or dedicated app.*
- **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence.
  - *Example: Multiple customers' virtual machines running on the same physical server, or their data stored on a shared storage system, without them knowing the exact physical location.*
- **Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly commensurate with demand.  
To the consumer, the capabilities available for provisioning often appear to be unlimited.
  - *Example: An e-commerce website automatically scaling up the number of web servers during a holiday sale and scaling down after the peak.*
- **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).  
Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer.

- *Example: Paying for cloud storage based on the gigabytes consumed per month, or for compute instances based on hours of usage.*

Why is "on-demand self-service" important in cloud computing?

"On-demand self-service" empowers users to obtain and configure computing resources independently, without waiting for manual intervention from the service provider.

Explain the concept of "resource pooling" in cloud computing, including the role of multi-tenancy.

**"Resource pooling"** means that a cloud provider's computing resources (like processing power, memory, ...) are shared among multiple consumers (**tenants**).

This is typically achieved through a **multi-tenant model**, where different physical and virtual resources are dynamically assigned and reassigned according to consumer demand.

Consumers are generally unaware of the exact physical location of these resources but may be able to specify a general location (e.g., region or country).

**Multi-tenancy** is key to resource pooling as it allows the provider to efficiently utilize hardware, leading to economies of scale and lower costs for consumers.

It requires **strong isolation mechanisms** to ensure that one tenant's activities do not negatively impact or compromise another tenant.

How does "rapid elasticity" benefit cloud computing users?

**"Rapid elasticity"** benefits users by allowing them to dynamically match their computing resources to their actual demand. This means they can:

- **Handle Demand:** Quickly scale up resources to handle surges in workload and scale down resources when demand is low, so clients only pay for what they use.
- **Improve Agility:** Respond quickly to changing business requirements without slow requests for new hardware.
- **Appear Unlimited:** To the consumer, the available resources often seem unlimited.

What does "measured service" mean in the context of cloud computing, and why is it important?

**"Measured service"** means that cloud systems automatically control and optimize resource use by leveraging a metering capability. This ensures that usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer.

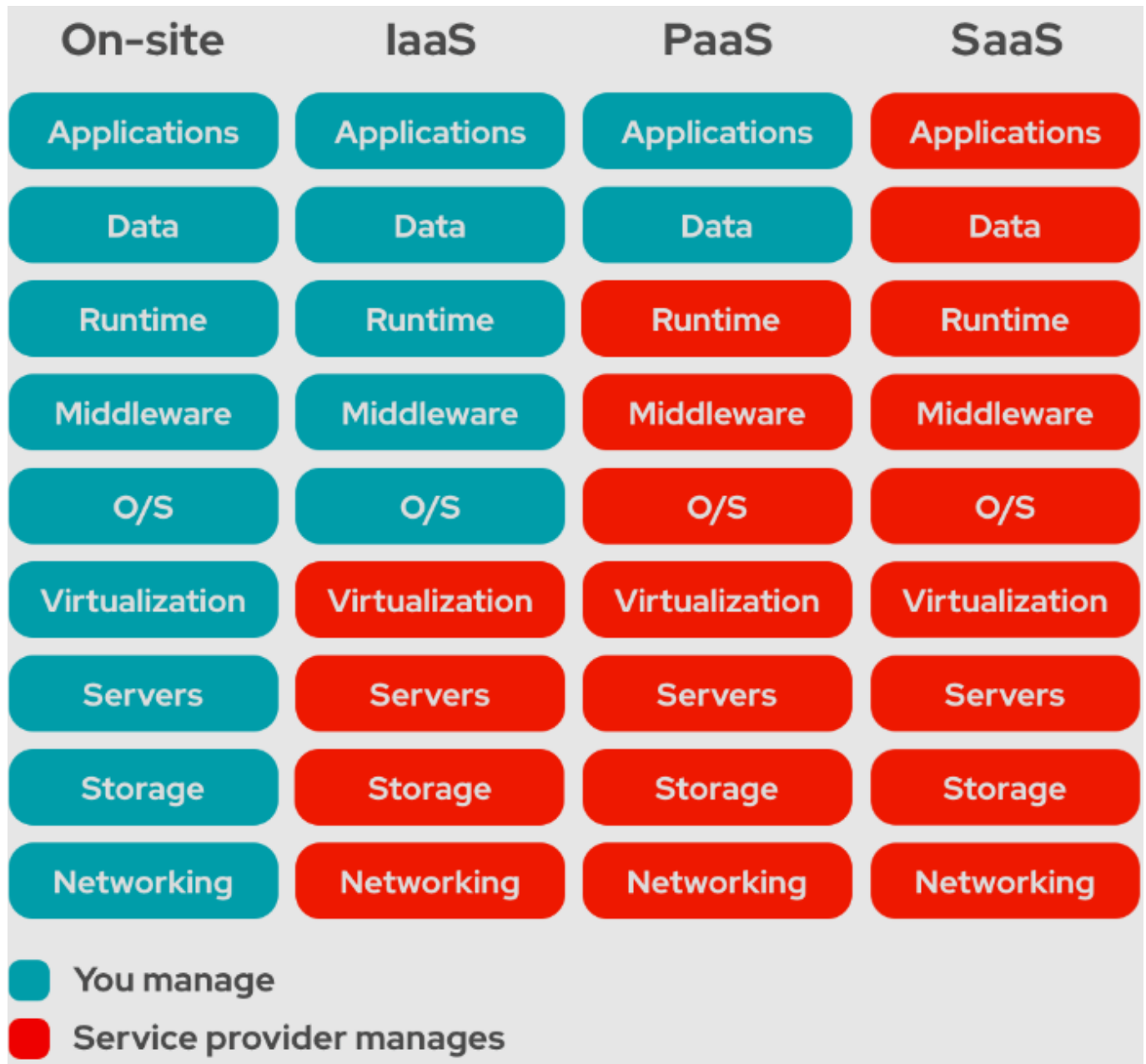
What is the difference between Scalability and Elasticity in cloud computing?

- **Scalability** is the ability of a system to handle a growing amount of work by adding resources. It can be:
  - **Vertical** (scaling up: adding more power like CPU/RAM to an existing machine)
  - **Horizontal** (scaling out: adding more machines to the pool).
- **Elasticity** is the ability to acquire or release resources, automatically and rapidly, depending on workload.

It focuses on matching the provisioned resources to the current demand in near **real-time**.

- **Scalability vs Elasticity:** While scalability is a prerequisite for elasticity, elasticity emphasizes the speed and automation of scaling actions (both up/out and down/in).

## Service Models



Describe the three main service models of cloud computing (SaaS, PaaS, IaaS).

- **Software as a Service (SaaS):** Consumer use the provider's applications running on a cloud infrastructure.

The applications are **accessible from various client devices** through either a thin client interface (like a web browser) or a program interface.

*Example: Google Workspace, Salesforce, Microsoft 365 (web versions).*

- **Platform as a Service (PaaS):** Consumer can deploy onto the provider cloud infrastructure consumer-created or acquired applications.

Consumer has control over the deployed applications and possibly configuration settings for the application-hosting environment.

*Example: AWS Elastic Beanstalk, Google App Engine, Heroku.*

- **Infrastructure as a Service (IaaS):** Delivers fundamental computing resources like virtual machines, storage, and networks.

The consumer has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components.

*Example: Amazon EC2, Microsoft Azure Virtual Machines, Google Compute Engine.*

What level of control does a consumer have in IaaS, PaaS, and SaaS?

- **IaaS:** The consumer has the **most control** over the computing resources.

**Consumers** manage the applications, OS, and have some control over networking components (like firewalls).

**Provider** manages the physical and virtualization layer.

- **PaaS:** The consumer has **moderate control**.

**Consumers** control the applications they deploy and can configure the environment settings.

**Provider** control OS, physical and virtualization layer.

- **SaaS:** The consumer has the **least control**.

**Consumers** control is typically limited to application configuration.

**Provider** manages almost everything: application, OS, servers, storage, and networking.

## Deployment Models

What are the four cloud deployment models?

- **Public Cloud:** Services offered over the public internet and available to anyone who wants to purchase them.
  - *Examples: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).*
- **Private Cloud:** Cloud infrastructure operated solely for a single organization. It can be managed by the organization or a third party and may exist on-premises, so it is directly managed by the organization, or off-premises, so the organization typically have less control over the infrastructure.
  - *Example: A company's internal data center running cloud technologies (like OpenStack or VMware vCloud) exclusively for its own business units.*
- **Hybrid Cloud:** A composition of two or more distinct cloud infrastructures (private, community, or public) bounded together by standardized or proprietary technology enabling data and application portability (e.g., cloud bursting for load balancing or workload migration).
  - *Example: An organization uses its private cloud for sensitive data and core applications, but uses a public cloud for development/testing, disaster recovery, or to handle peak loads.*


- **Community Cloud:** Cloud infrastructure shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party.
  - *Example: A cloud platform built for exclusive use by several government agencies to share specific applications and data related to a common mission, or a cloud for universities in a specific research field.*

## Cloud Computing Reference Architecture (NIST SP 500-292)

What are the major roles defined in the NIST cloud computing reference architecture?

- **Cloud Consumer: Person/Organization** that maintains a business relationship and uses services from Cloud Providers.
- **Cloud Provider (CSP): Person/Organization/Entity** responsible for making a service available to Cloud Consumers.

This two roles and responsibility of both roles are shown in blue and red, respectively:

On-site	IaaS	PaaS	SaaS
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking
 You manage			
 Service provider manages			

- **Cloud Auditor: Party** that can conduct independent assessment of cloud services about performance and security of the cloud implementation.
- **Cloud Broker: Entity** that manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.
  - **Example:** A cloud consumer may request service from a cloud broker instead of contacting a cloud provider directly.  
The cloud broker may create a new service by combining multiple services or by enhancing an existing service.
- **Cloud Carrier:** Intermediary that provides connectivity of cloud services from Cloud Providers to Cloud Consumers (e.g., network providers).

How do cloud auditors and cloud brokers contribute to the cloud ecosystem and service management?

#### Cloud Auditors:

- **Assurance & Compliance:** Provide independent assessment of cloud services against standards, security controls, privacy regulations. This help to ensures that providers meet their obligations.
- **Risk Assessment:** Help consumers understand the risks associated with a particular cloud service.
- **Transparency:** Their reports offer transparency into the provider's operations and controls.

**Cloud Brokers:** In general, a cloud broker can provide services in **three categories**:

- **Service Intermediation:** They can enhance a given service by adding specific capabilities (e.g., identity management, improved security) or providing value-added services on top of existing cloud offerings.
  - **Example:** *A broker offers enhanced identity management and single sign-on capabilities for multiple SaaS applications.*
- **Service Aggregation:** A cloud broker combines and integrates multiple services (also from different providers) into one or more new services. The broker provides data integration and ensures the secure data movement between the cloud consumer and multiple cloud providers.
  - **Example:** *A broker combines CRM (from provider A), marketing automation (from provider B), and analytics (from provider C) into a unified sales and marketing platform.*
- **Service Arbitrage:** They can switch between different cloud services or providers based on factors like cost and performance, aiming to provide the best value or terms to the consumer. Service arbitrage is similar to service aggregation except that the services being aggregated are not fixed, a broker has the flexibility to choose services from multiple agencies.
  - **Example:** *A web hosting broker automatically moves a customer's website between different IaaS providers based on which provider offers the lowest price for the required resources at any given time.*

## Security in Cloud Computing

What are the general security responsibilities of cloud providers and cloud consumers (Shared Responsibility Model)?

The **Shared Responsibility Model** dictates that security is a shared concern between the Cloud Provider (CSP) and the Cloud Consumer. The division of **responsibilities varies significantly based on the service model** (IaaS, PaaS, SaaS).

**Cloud Providers (CSP) are typically responsible for "Security OF the Cloud":**

- **Physical security** of data centers (access controls, environmental protections).
- **Security of the underlying infrastructure:** Hardware (servers, storage, networking equipment), software (hypervisors, cloud control plane), and network infrastructure (protecting against network-level attacks).
- **Virtualization infrastructure:** Ensuring isolation between tenants in a multi-tenant environment.

**Cloud Consumers are typically responsible for "Security IN the Cloud":**

- **Data Security:** Classifying and protecting their data, managing encryption keys (if applicable).
- **Identity and Access Management (IAM):** Account management and user permissions.
- **Operating System, Network, and Firewall Configuration (especially in IaaS and PaaS):** Patching guest OS, configuring firewalls and intrusion detection/prevention systems.

Why is physical security of data centers important in cloud computing?

Physical security of data centers is foundational to overall cloud security. It protects the hardware (servers, storage devices, network equipment) and the infrastructure that hosts cloud services from unauthorized physical access, theft, damage (due to environmental factors like fire, flood, or power failure), or interference. If physical security is compromised:

- **Data breaches.**
- **Service disruptions.**
- **Loss of data integrity or availability.**

Therefore, robust physical security measures (e.g., surveillance, biometric access controls, secure perimeters, environmental controls) are crucial for the CS Provider to ensure the confidentiality, integrity, and availability (CIA) of the services they provide.

If an IaaS Cloud consumer's application is compromised due to a vulnerability in the guest Operating System they manage, who is primarily responsible for the consequences and why?

In an IaaS model, the **Cloud Consumer** is primarily responsible. **Why:** According to the shared responsibility model for IaaS, the consumer has control over and responsibility for the guest Operating System, including patching, maintenance, and securing applications deployed on it. The Cloud Provider is responsible for the security *of* the cloud (the underlying infrastructure and hypervisor), but not for vulnerabilities within the consumer-managed guest OS or applications.

---

## Additional Potential Exam Questions

Categorize the following Cloud Service Management functions into Business Support, Provisioning/Configuration, or Portability/Interoperability:

- Managing customer billing and processing payments: **Business Support**
- Automatically deploying cloud systems based on requested resources: **Provisioning/Configuration**
- Supporting the migration of VM images to another cloud provider: **Portability/Interoperability**
- Monitoring virtual resources and generating performance reports: **Provisioning/Configuration**
- Providing a unified management interface to use data across multiple cloud providers: **Portability/Interoperability**

Given a scenario describing a computing service, analyze whether it qualifies as a cloud service according to the five essential NIST characteristics. Justify your answer for each characteristic.

*(This would require a specific scenario, similar to Task 1.2 in your assignment. The answer would involve evaluating the scenario against On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, and Measured service, explaining how well the scenario meets each point, referencing NIST SP 500-322 options if applicable.)*

What are the main layers involved in Service Orchestration within the NIST Cloud Computing Reference Architecture (SP 500-292)?

The main layers are:

- **Service Layer:** Defines interfaces for Cloud Consumers to access computing services (SaaS, PaaS, IaaS).
- **Resource Abstraction and Control Layer:** Contains components (e.g., hypervisors, virtual machines, virtual storage) that abstract physical resources and control their allocation, access, and monitoring. This layer enables resource pooling, dynamic allocation, and measured service.
- **Physical Resource Layer:** Includes all physical computing resources like hardware (CPUs, memory, networks, storage) and facilities (HVAC, power).