

Cloud Computing

Module 2

Architecture

1. Requirements
2. Introduction to Cloud computing architecture
3. Various kinds of Cloud computing architecture

Requirements

Cloud computing is required to meet the requirement of *scalability, cost efficiency, legal agreement and business.*

Architecture for Scalability

- **Vertical Scale-Up**

- ✓ When new resources are added in the existing system to meet the expectation.

- **Horizontal Scale-Up**

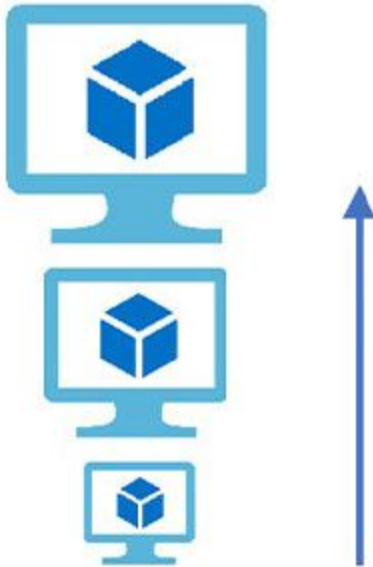
- ✓ When new server racks are added in the existing system to meet the higher expectation.

Note: Vertical scaling is easy and cheaper than Horizontal scaling. It also requires less time to be fixed.

Contd...

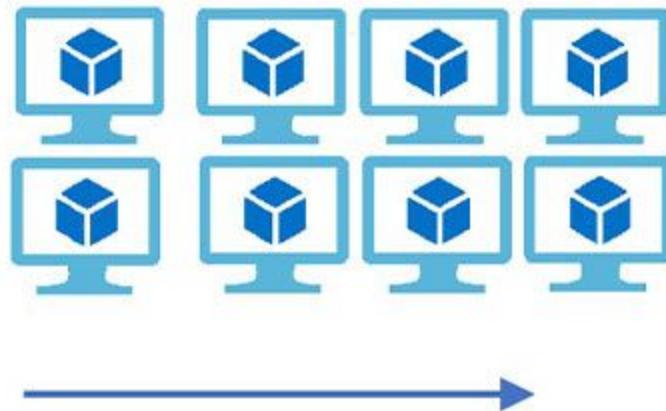
Vertical Scaling

(Increase size of instance (RAM , CPU etc.))

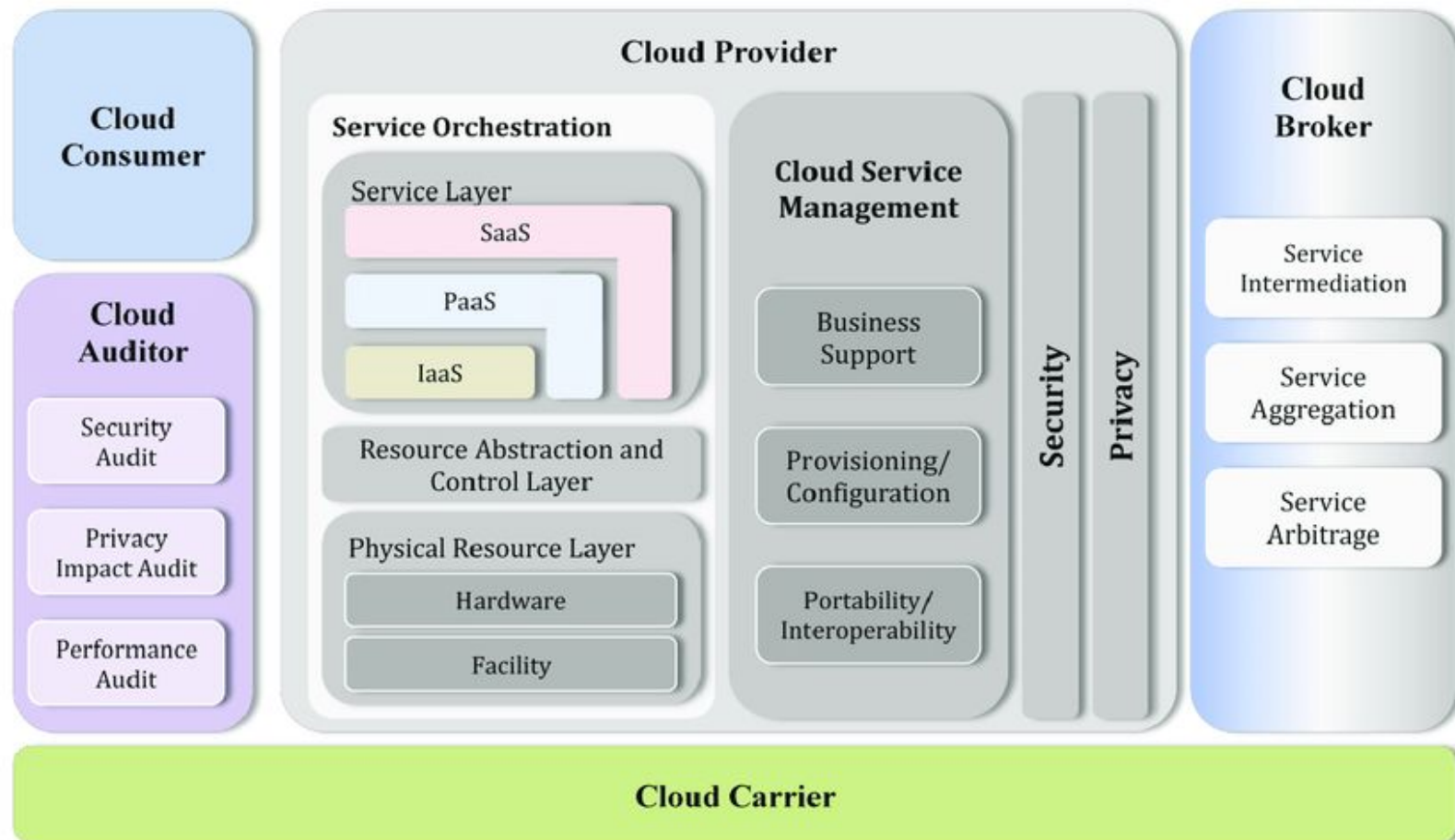


Horizontal Scaling

(Add more instances)

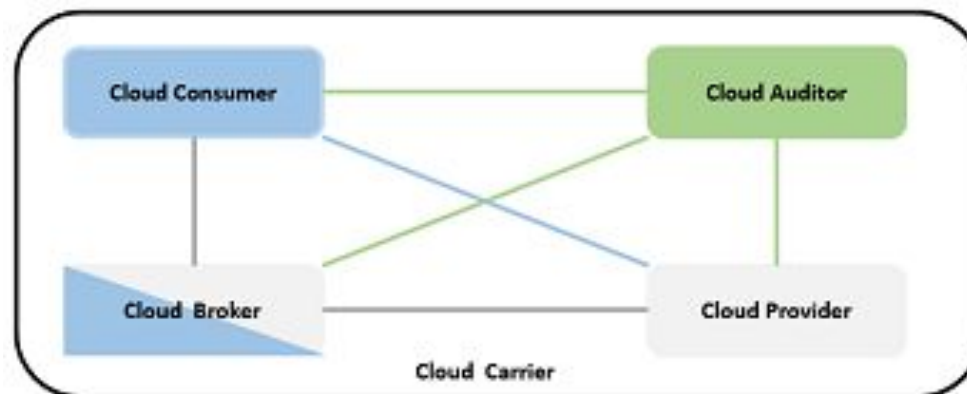


Cloud Conceptual Reference Model



Actors in Cloud Computing

- **Cloud Consumer** A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
- **Cloud Provider** A person, organization, or entity responsible for making a service available to interested parties.
- **Cloud Auditor** A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
- **Cloud Broker** An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
- **Cloud Carrier** An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.



Scenarios in Cloud: #1

1. Cloud consumer interacts with the cloud broker instead of contacting a cloud provider directly.
2. The cloud broker may create a new service (mash-up) by combining multiple services or by enhancing an existing service.
3. Actual cloud providers are invisible to the cloud consumer.



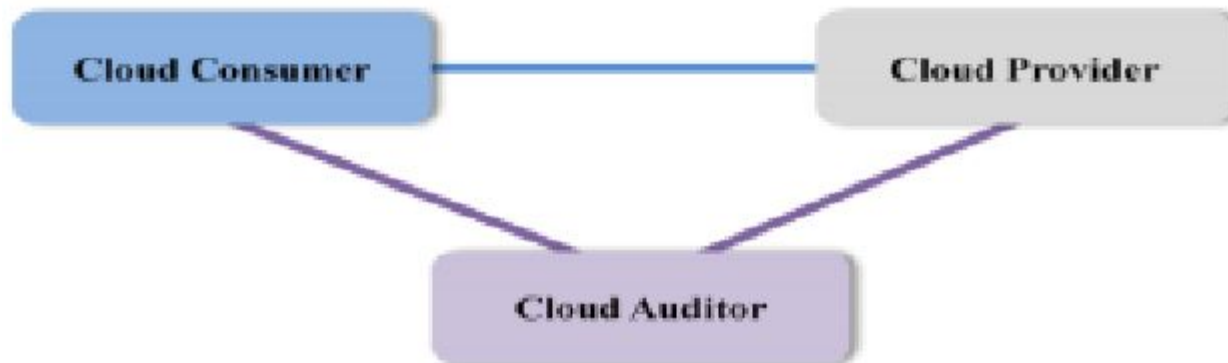
Scenarios in Cloud: #2

1. Cloud carriers provide the connectivity and transport of cloud services from cloud providers to cloud consumers.
2. Cloud provider participates in and arranges for two unique service level agreements (SLAs), one with a cloud consumer (e.g. SLA1) and one with a cloud carrier (e.g. SLA2).
3. A cloud provider may request cloud carrier to provide dedicated and encrypted connections to ensure the cloud services (SLA's).



Scenarios in Cloud: #3

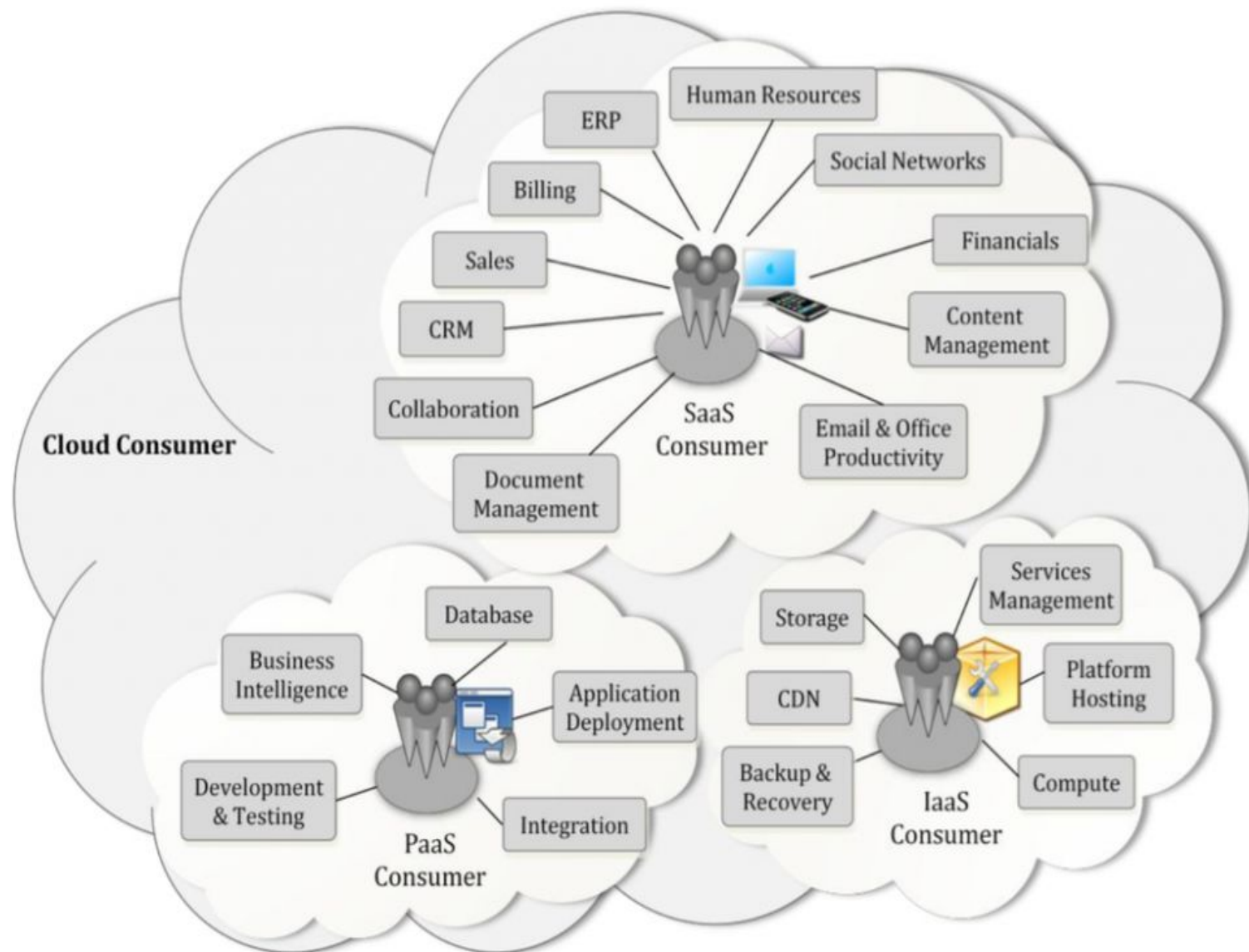
1. Cloud auditor conducts independent assessments for the operation and security of the cloud service.
2. The audit may involve interactions with both the Cloud Consumer and the Cloud Provider.



Cloud Consumer

- Cloud consumer **browses & uses the service.**
- Cloud consumer sets up contracts with the cloud provider.
- Cloud consumers need **SLAs to specify the technical performance requirements fulfilled by a cloud provider.**
- SLAs cover the quality of service, security, remedies for performance failures.
- Cloud consumer can freely choose a cloud provider with better pricing with favorable conditions.
- Pricing policy and SLAs are non-negotiable.

Contd...



SaaS Consumers

- SaaS consumers can be organizations that provide their members with **access to software applications**, end users who directly **use software applications**, or software application administrators who **configure applications for end users**.
- SaaS consumers can be **billed based on the number of end users, the time of use, the network bandwidth consumed, the amount of data stored or duration of stored data**.

PaaS Consumers

- PaaS consumers can be application developers or administrators.
 1. who **design and implement** application software
 2. who run and test applications - **application testers**
 3. who **publish applications** into the cloud
 4. who **configure and monitor application** performance.
- PaaS consumers can be **billed** according to, processing, database storage and network resources consumed by the PaaS application, and the duration of the platform usage.

IaaS consumer

- IaaS consumer can be system developers, system administrators and IT managers who are interested in creating, installing, managing and monitoring services for IT infrastructure operations.
- IaaS consumer can be billed according to the amount or duration of the resources consumed, such as CPU hours used by virtual computers, volume and duration of data stored, network bandwidth consumed, number of IP addresses used for certain intervals.

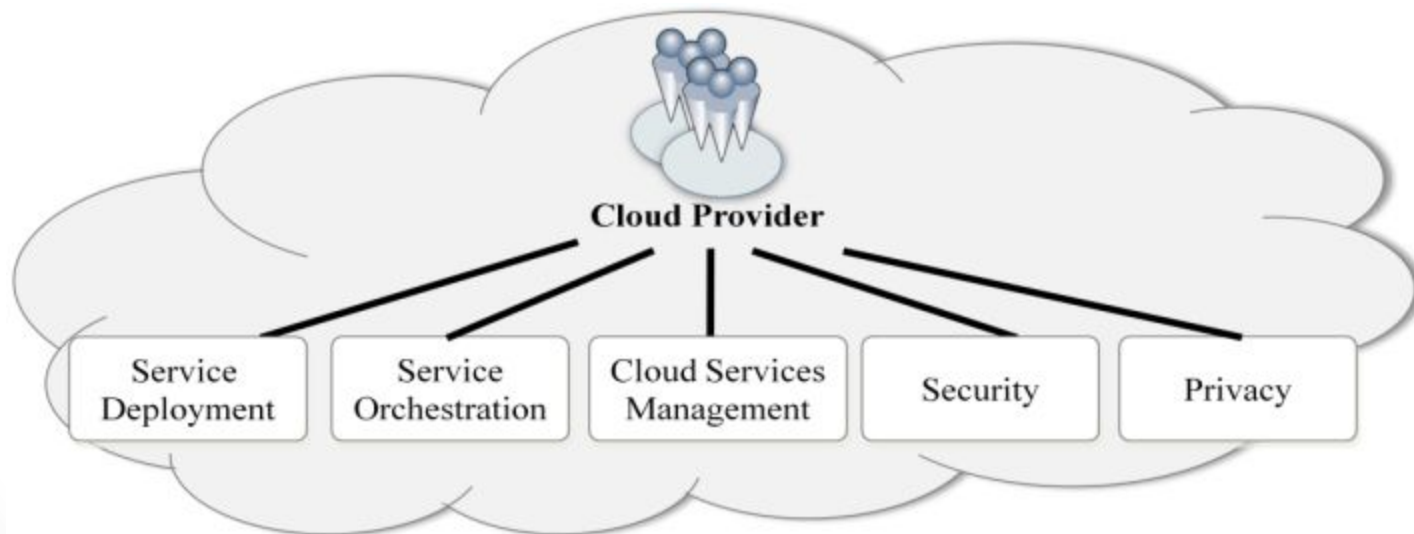
Cloud Provider

- Cloud Provider **acquires and manages the computing infrastructure** required for providing the services, **runs the cloud software** that provides the services, and **makes arrangement to deliver the cloud services** to the Cloud Consumers through network access.
- SaaS provider **deploys, configures, maintains and updates the operation of the software applications** on a cloud infrastructure. SaaS provider maintains the expected service levels to cloud consumers.
- PaaS Provider **manages the computing infrastructure for the platform** and components (runtime software execution stack, databases, and other middleware).
- IaaS Cloud Provider **provides physical hardware and cloud software** that makes the provisioning of these infrastructure services, for example, the physical servers, network equipments, storage devices, host OS and hypervisors for virtualization.

Contd...

- Five major activities of Cloud Provider's

1. Service deployment
2. Service orchestration
3. Cloud service management
4. Security
5. Privacy



Cloud Auditor

- Auditor evaluates the security controls, privacy impact, performance, etc.
- Auditing is especially important for federal agencies.
- Security auditing can make an assessment of the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome. This is done by verification of the compliance with regulation and security policy.
- Privacy audit helps in Federal agencies comply with applicable privacy laws and regulations governing an individual's privacy, and to ensure confidentiality, integrity, and availability of an individual's personal information at every stage of development and operation.

Cloud Broker

- Integration of cloud services can be complex for consumers. Hence cloud broker, is needed.
- Broker manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.
- In general, a cloud broker can provide services in three categories:
- **Service Intermediation:** Broker enhances a service by improving capability and providing value-added services to consumers. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.
- **Service Aggregation:** Broker combines and integrates multiple services into one or more new services. The broker provides data integration and ensures the secure data movement.
- **Service Arbitrage:** It is similar to service aggregation with the flexibility to choose services from multiple agencies. For example, broker can select service with the best response time.

Cloud Carrier

- Cloud carriers provide access to consumers through network, telecommunication, and other access devices.
- For example, cloud consumers can obtain cloud services through network access devices, such as computers, laptops, mobile phones, mobile internet devices (MIDs), etc.
- The distribution of cloud services is normally provided by network and telecommunication carriers or a transport agent, where a transport agent refers to a business organization that provides physical transport of storage media such as high-capacity hard drives.
- Cloud provider can set up SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers.

How to host the Cloud?

- Remember Bob from ABC Corporation?
- He has decided to outsource their business to the cloud!!
- But he faces some difficult decisions!
 - Should he approach a third party?
 - Should he ask his IT team to build a cloud infrastructure on their company premises?



- At its core, the cloud is simply a data-center, with software capable of managing virtualized resources according to user demand.
- While choosing a cloud solution, consider
 - Where will the data-center reside?
 - Who owns the data-center?
 - Who can use resources within the data-center?
 - Who operates and manages the data-center?



Cloud Deployment Models



HYBRID CLOUD

- Combination of both public and private cloud
- Shared security responsibility
- Helps maintain tighter controls over sensitive data and processes



PUBLIC CLOUD

- Offered by third-party providers
- Available to anyone over the public internet
- Scales quickly and convenient



PRIVATE CLOUD

- Offered to select users over the internet or a private internal network
- Provides greater security controls
- Requires traditional datacenter staffing and maintenance

Private Cloud

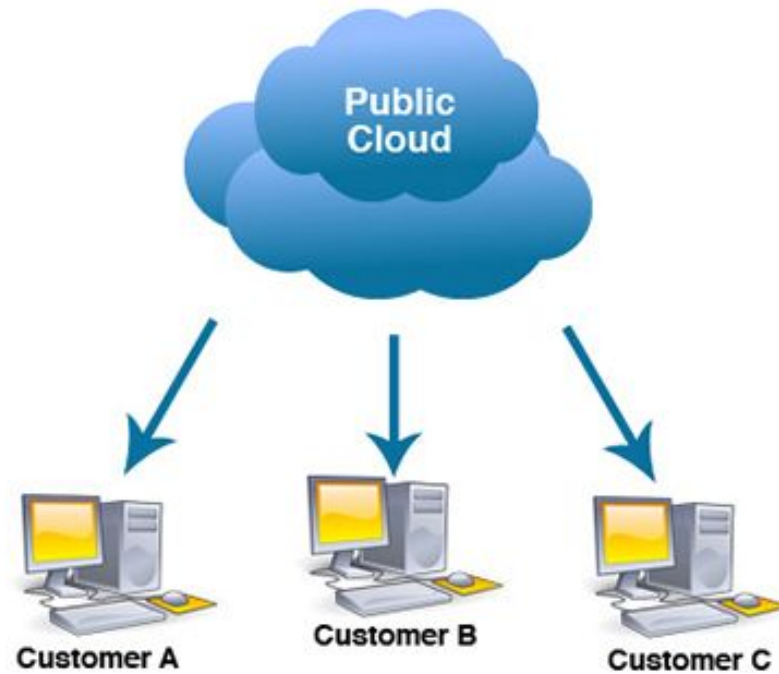
Internal Private Cloud



Hosted Private Cloud



Public Cloud



Public vs Private Cloud

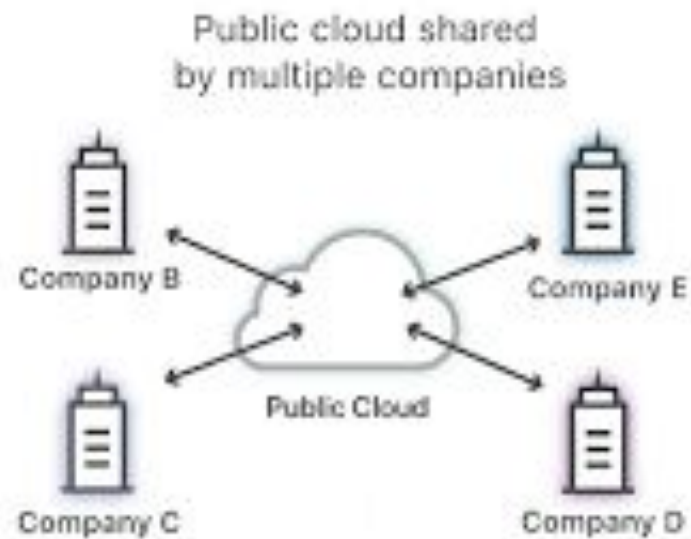
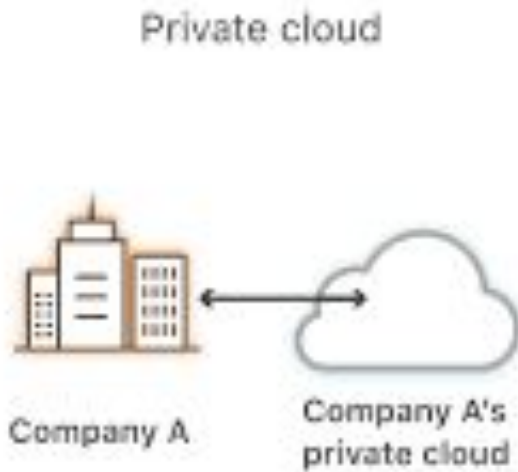
Public Cloud

- Provisioned for open use by general public
- Owned, managed and operated by business, academic or government organizations
- Eg: Gmail, Microsoft Azure, Dropbox etc.

Private Cloud

- Exclusively used by an organization
- Usually managed, operated and owned by the organization
- Usually resides on the organization premises
- Open source tools like OpenStack and Eucalyptus can be used to build private clouds

Contd...



Here are the facts!

- ABC Corp. website has a significant user base right now, and is expected to grow over time
- The data maintained by the company is related to product details, and no financial details are maintained (assume)
- Which cloud model – private or public – would you recommend?

Here are the facts!

- What would be the case where there is also sensitive data that has to be maintained?
 - Credit card details
 - Company expansion plans
 - Other customer and employee data

Public Cloud Features

- Scalable
- Affordable
- Always available
- Stringent SLAs
- Less secure

When should one opt for Public Clouds?

- Larger user base
- Varying resource usage
- Lack of infrastructure
- Financial constraints

Private Cloud Features

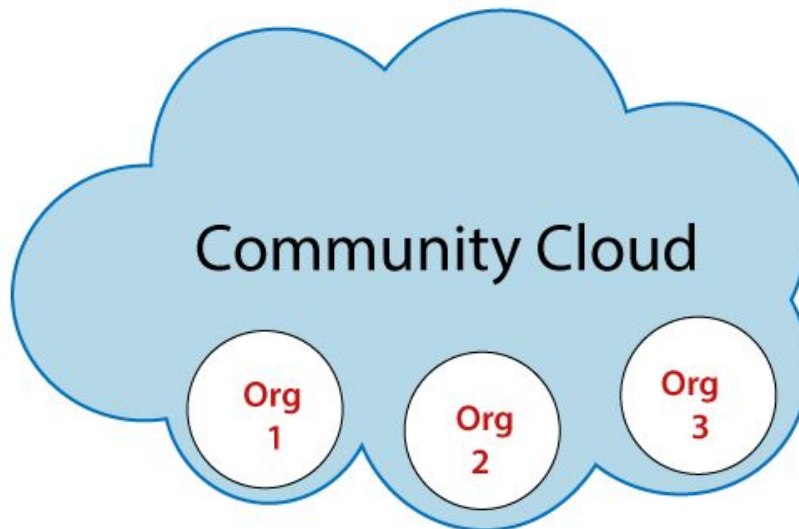
- Secure
- More control available
- Weak SLAs

When should one opt for Private Clouds?

- Sufficient Funds
- Security and autonomy is paramount
- Few users
- Sufficient resources are available

Community Cloud

- A **community cloud** in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific **community** with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.



Features of Community Cloud

- Collaborative effort
- No party has full control
- Partially secure
- Cost effective

When should one opt for Community Clouds?

- Need for collaboration
- Financial constraints
- Less maintenance costs

Hybrid Cloud

- Organization manages both private and public clouds.
- Services can be used from either cloud, depending on organizational policies.
- Sometimes, a private cloud could be used till its capacity is met, after which the workload spills over to the public cloud – **Cloud Bursting**.

THE BENEFITS OF HYBRID CLOUD



PUBLIC CLOUD

- ✓ High Scalability
- ✓ Low complexity
- ✓ Pay as you go



PRIVATE CLOUD

- ✓ Dedicated & Secure
- ✓ Good Performance
- ✓ High Reliability
- ✓ Regulatory Compliance



PUBLIC CLOUD PRIVATE CLOUD




HYBRID CLOUD

- ✓ High Scalability
- ✓ Very Secure
- ✓ Improved Cost
- ✓ High Reliability
- ✓ A lot of Flexibility
- ✓ High Performance

Cloud Deployment Models - Summary

- Depending on who owns and operates the cloud, and who can access the cloud, there are 4 deployment models
 - Public Cloud
 - Private Cloud
 - Community Cloud
 - Hybrid Cloud

Comparison

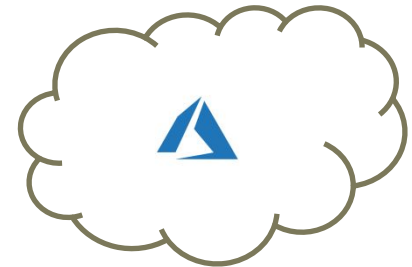
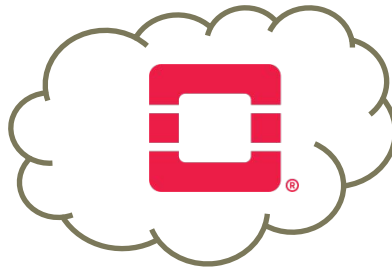
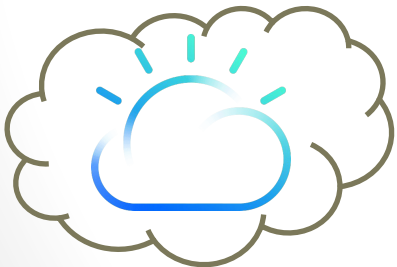
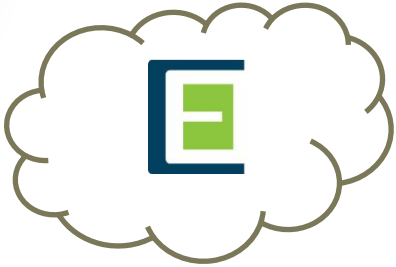
	Infrastructure Managed By ¹	Infrastructure Owned By ²	Infrastructure Located ³	Accessible and Consumed By ⁴
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or Organization Third Party Provider	 Organization Third Party Provider	 On-Premise Off-Premise	 Trusted
Hybrid	<u>Both</u> Organization & Third Party Provider	<u>Both</u> Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

Contd...

Deployment model	scope of services	owned by	managed by	security level	location
public	general public and large industry groups	CSP	CSP	low	off premise
private	single organization	single organization	single organization or CSP	high	off or on premise
community	organizations that share the same mission, policy and security requirements	several organizations	several organizations or CSP	high	off or on premise
hybrid	organizations and public	organizations and CSP	organizations and CSP	medium	off and on premise

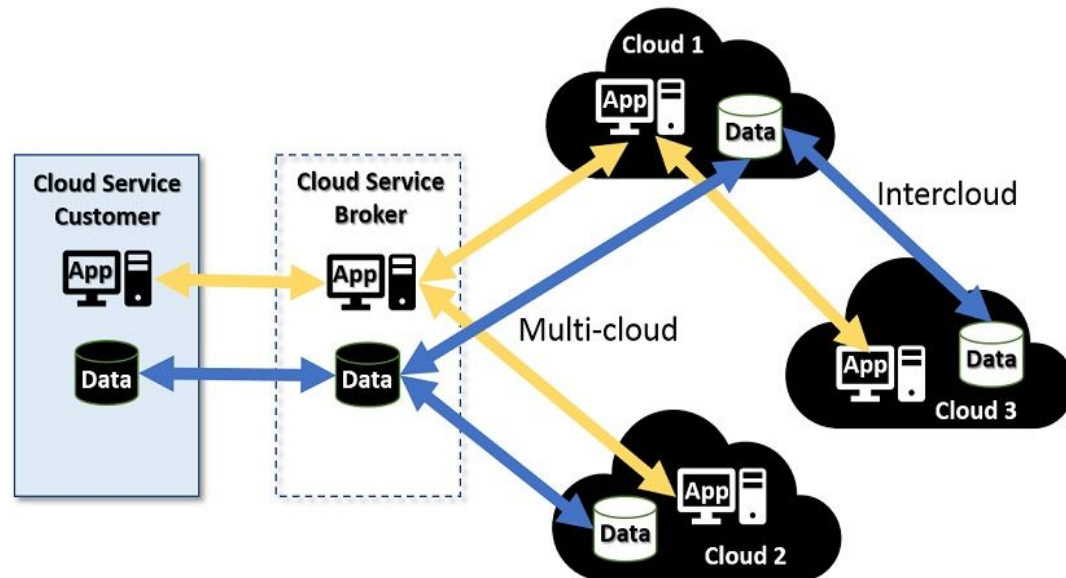
Can a cloud run out
of resources?

Can we connect the Clouds?



Intercloud

- Intercloud – “Cloud of Clouds”
- Mesh of clouds, unified based on open standard protocols to provide interoperability
- Interconnects multiple cloud providers’ infrastructures.
 - Focus is on direct interoperability between public cloud service providers



Need for Intercloud

- Scalability + wider resource availability
- Interoperability + avoiding vendor lock-in
- Availability and disaster recovery
- Geographic distribution and low latency access

Types of Interclouds

- **Federation Clouds:** A set of cloud providers willingly interconnect their cloud infrastructures in order to share resources
 - Voluntary contribution
 - Suitable for collaboration of governmental clouds or private cloud portfolios
 - Types of federation clouds are **Peer to Peer** and **Centralized clouds**.
- **Multi-Cloud:** A client or service uses multiple independent clouds
 - No voluntary interconnection and sharing
 - Managing resource provisioning and scheduling is the responsibility of client or their representatives.
 - Used to utilize resources from both governmental clouds and private cloud portfolios.

Types of Federated Clouds

- **Peer to peer Inter-Cloud federation**
 - Clouds collaborate directly with each other but may use distributed entities for directories or brokering.
 - Eg: RESERVOIR (Resources and Services Virtualization without Barriers Project), Open Cirrus etc
- **Centralized Inter-Cloud federation**
 - Clouds use a central entity to perform or facilitate resource sharing.
 - The central entity acts as a storehouse where the available cloud resources are registered.
 - Eg: Contrail, Dynamic Cloud Collaboration (DCC) and Federated Cloud Management.

Few Questions...

- Need of multi-cloud strategy.
- Challenges in multi-cloud.
- Security in multi-cloud.