



Q. Cloud Deployment Models

A cloud deployment model is a specific configuration of environment parameters such as accessibility and proprietorship of deployment infrastructure and technology used.

There are 4 types

1. Public Cloud

The name speaks itself. Public clouds are available to general public and data are stored on third party servers.

Examples

- ~~Amazon~~ Amazon EC2
- Azure
- Heroku
- Digital Ocean

Advantages

- High Scalability
- Reduced costs
- 24/7 running

Private Cloud

There is a subtle difference between Private and Public cloud.

Here, Only one company owns a private cloud of which is also called internal or corporate model.

Examples

- IBM
- Cisco
- Red Hat
- S a M Cloud Box.

Advantages

- Flexible
- High security
- Privacy.

2. Community cloud

Here, several organizations with similar background share the infra structure and related resources of community cloud.

Example

IBM

Advantages

- Cost reduction
- Reliability
- Ease of collaboration

↳ Hybrid

It is a mixture of two or more above discussed clouds

It allows companies to mix and match facets of styles that suits their requirements



Benefits

- Reasonable Price
- Improved Privacy
- Enhanced Scalability

Q3

Virtualization

- It is a technique of how to separate a service from underlying physical delivery of that service.
- It is process of creating a virtual version of something like computer & hardware.

o

Types

Q4

Application Virtualization

- It helps a user to have remote access of an application from a server.
- The server stores all personal info and other characteristics of app but can still run on local workstation through internet.





(2)

Network Virtualization

- The ability to run multiple virtual networks with each has separate context and data plan
- It can be managed by individual parts that are confidential to each other.

(3)

Desktop Virtualization

- It allows users OS to be remotely stored on server in data center.
- It allows user to access desktop virtually from any location.

(4)

Storage Virtualization

- It is an array of servers that are managed by virtual storage system.
- It makes managing storage from

PAGE NO. _____
DATE: _____

multiple sources to be managed
as single repos.

① Server Virtualization

- In this, masking of server resources takes place.
- Here, physical server is divided into multiple virtual servers by changing identity no and processors.



Q8 what is CDN

A CDN aka Content Delivery Network refers to geographically distributed group of servers which work together to provide fast delivery of Internet content.

A CDN allows quick transfer of assets needed for loading Internet content including -

- HTML Pages
- Javascript Files
- Stylesheets
- Images
- Videos

→ The popularity of CDN services continues to grow and today the majority of web traffic is served from CDN

like -

- Facebook
- Netflix
- Amazon

Advantages

(1) Improves website load Time

- By distributing content closer to visitors by using a nearby CDN server visitors get faster loading experience.
- Thus bounce-rate increases the amount of time that people spend on the site.

(2) Reducing Band width costs

CDNs are able to reduce the amount of data on origin server must upload, thus reducing hosting costs for website owners.

(3) Increasing Content availability and Redundancy

large amount of traffic or

hardware failures can interrupt a normal pipeline.

This distributed nature of CDN handles node failure and can easily withstand such failures.

(C) Implementing Security

CDN may improve security by providing DDoS mitigation → improvements in security certificates and other optimizations.

(D) Other Benefits

- Decrease Silver load
- saves lot of Money
- Perfect Analysis
- Good response time.



(1)

Cloud Security Issues

1.

Data loss

Cloud based env makes it easy to share data stored and accessible directly from public. Thus possibility of data loss is high.

(2)

Data Privacy

The lot of sensitive data is also on clouds. And thus exposure of such data can lead to bad results.

(3)

FISS configuration

Cloud is designed to easily use and to enable data sharing, making it difficult for organizations to ensure that data is only accessible to authorized parties.

(C) Weaknesses In Unauthorized Access

→ An attacker can gain any access if improper configuration is done or if user's or any credentials are compromised.

(D) Insecure APIs

If improper API and CSP are used, it can exploit potential methods for exfiltrating sensitive data.

(E) Hijacking of Account

It is one serious problem and often lack the ability to detect and respond to these threats.

(F) Lack of Visibility

It can limit an organization's

ability to monitor their cloud based resources and protect them against attack.

③ Dos Attacks

- Denial of Service is having a major impact of different companies.
- It also demands a ransom money to any individual, firm or organization.

④ Cyber attacks

Such attacks can likely be repeated many times with a high probability of success.

Thus, they are common target of all users.



(1) Open Cloud services

1. Cloud Foundry

It outstands for being available as an open-source, stand-alone software application, which makes it independent of cloud providers.

It can be deployed on VMs.

(2) WSO 2

There is lot of clients of internal and external APIs. This scenario when WSO 2 sits, is capable of full lifecycle.

- It's easy integration with WSO 2 Identity Server or API-driven IAM (Identity across regions).
for authentication access stored environments.

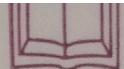
Cloudify

It is an orchestration framework designed to model applications from services while automating their lifecycles.

This includes ability to deploy on any cloud environment or data center and perform continuous maintenance.

OpenShift

- It is "Kubernetes" based platform
- It is build with security in mind where containers run as non-root user and when not the case.
- Its fast installation and configuration procedure as well as easy to maintain.



Stackato

It is a polyglot PaaS product based on Cloud Foundry and runs on top of your cloud infrastructure and serves as delivery platform for your application.

- Each application has its own LXC (Linux Container) which guarantees an efficient and secure sharing of resources.

16

② Load Balancing

It is a method that allows you to create proper balance of amount of work that is being performed on various pairs of servers or hardware equipment.

Different Types

1. Static Algorithm

→ They are made for those when user have low variation in load.

→ It is major drawback that load shifting does not depend on state of system.

2. Dynamic Algorithm

It first searches the lightest server in entire network and

gives it preference for load balancing

It requires real time communication with network that can help in increasing traffic of system.

(3)

Robin Round Algorithm

- First, it chooses a node on random basis and assigns the tasks to other nodes in round robin way.

(4)

Weighted Round Robin Load Balancing Algorithm

- It is developed to enhance the most challenging issues of Robin Round.
- There is a designated prescribed weight and jobs which are distributed as per the values of the weight.



(5) Opportunistic Load Balancing Algorithm

→ Regardless of current workload on task of node, OLP distributes all unfinished tasks ~~as~~ to that nodes randomly.

(6) Minimum to Minimum

A minimum is selected among all tasks. As per minimum time, the task is scheduled on machine.

(7) Maximum to Maximum

→ Maximum value → selected after selecting out the minimum completion time.

→ A task is scheduled on machine, all assigned task → removed from list.



PAGE NO.

DATE:

Ug

Cloud Scalability

Cloud Scalability is one of the features of cloud computing.

A scalable cloud can grow and manage the increasing demand of processing, networking, infrastructure and software from industry.

Why is it necessary?

In case there is short demand for you to have more servers and storage space to handle a larger workload, it allows to make new nodes easily.

--> Once work is done, we can revert back to original configuration with same ease.

3 D.Ant Types

(1) Vertical Scaling

Also known as up/down. You can add resources to your existing operations to manage the increasing workload.

A notable flaw with this type of scaling is that once you reach capacity doesn't mean accordingly to size.

(2) Horizontal scaling

- It works by adding nodes to regular infrastructure
- The increase in nodes manages the increased work load volume and latency is reduced.

(2) Diagonal Scaling

This is seen as combination of vertical and horizontal scaling.

With this, you get the flexibility of adding more resources of accounts to the needs in specific time instances.

When traffic goes up, requirements are met, but when traffic goes down, configuration goes back to normal.