PAGE NO.

Unit - IV

Service Level Agreement -

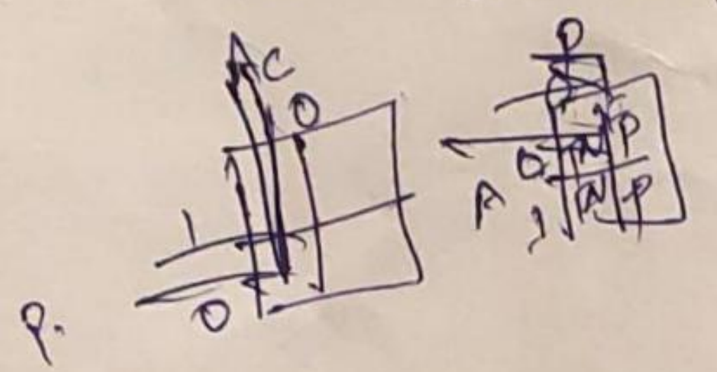
A formal contract between a service Provider and a service Consumer.

→ SLA is a foundation of the consumer's trust in the provider.

→ SLA contains service level Objectives (SLOs)

SLA Contents -

- A set of services which the provider will deliver.
- A complete, specific definition of each service.
- A responsibilities of the provider and consumer.
- A set of metrics to measure whether the provider is offering the services as guaranteed.
- An auditing mechanism to monitor the services.
- The remedies available to the consumer and the provider if the terms are not satisfied.
- How the SLA will change overtime.



PAGE NO.

Types of SLA -

There are two types of SLA -

— Off the shelf SLA or Non-negotiable SLA or Direct SLA

- Non conducive for mission critical data or applications.
- Provider creates the SLA template and define all criteria viz. Contract period, billing, response time, availability etc.
- Followed by the present day state-of-the-art clouds.

Negotiable SLA.

→ Negotiation via external agent.
→ Negotiation via multiple external agents.

Service Level Objective -

- Objectively measurable conditions for the service.
- Encomposes multiple QoS parameters viz. availability, serviceability, billing, penalties, throughput, response time or quality.

Example-

→ Availability of a service X is 99.9%.

→ Response time of a database query Q is between 3 to 5 seconds

⇒ Throughput of a server S at peak load time is 0.875.

7 fundamentals of cloud Security-

1. Understand what you are responsible for
2. Control user access
3. Data Protection
4. Secure Credentials
5. Implement multifactor authentication.
6. Increase Visibility
7. Adopt a shift-left approach.

↓

Shift left means is to take a task that's traditionally done at a later stage of the process and ~~for~~ perform that task at earlier stages.

Shift left is a practice intended to find and prevent defects early in the software delivery process.

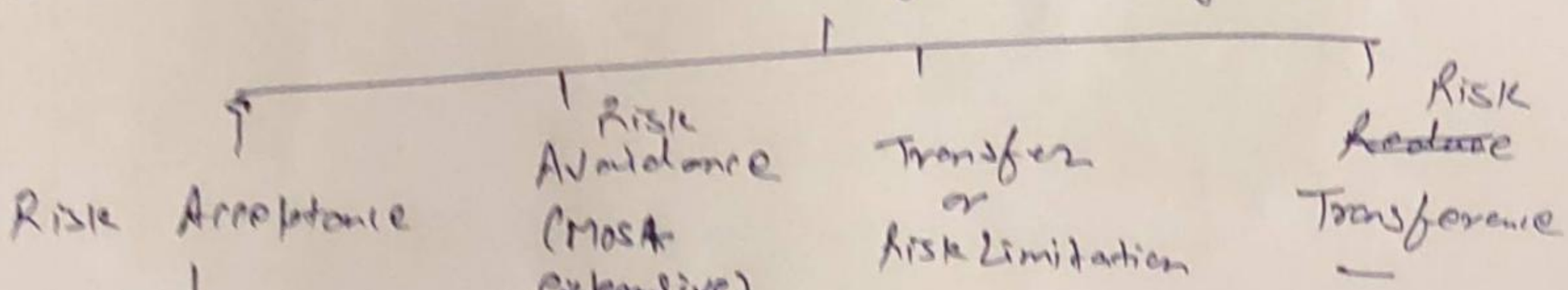
PAGE NO.

Risk Mitigation- It is a approach to mitigate cloud security threats and protect user data.
Risk Mitigation can be defined as taking steps to reduce adverse effects.
→ Limit user access to cloud security
→ set up multifactor authentication
→ Regularly back up company data
→ Conduct employee training workshops on cloud security.
→ Increase network bandwidth to prevent DDos attacks.
→ Businesses can also benefit from having a backup internet connection. If all else fails that would let users connect to the cloud through different IP addresses.

Stratagies to Mitigate cloud Risk-
(1) Data Encryption at Rest- Encryption at rest protects data that is not in use or in transit.
(2) ~~Two~~ Two factor authentication.
(3) Eliminate shared Accounts
(4) Insist on a well defined shared responsibility model.
(5) use standardized cloud Assesment Questions.

~~Types of Security policies for cloud computing -~~

For Four Types of Risk Mitigation



Types of Security policies for cloud computing -

(1) Secure cloud accounts and create groups.
→ Ensure that the root account is secure.
(2) Check for free security upgrades.
(3) Restrict Infrastructure access via firewalls.
(4) Tether the cloud.
(5) Replace ~~pass~~. passwords with keys.
(6) Turn on auditing and system monitoring.

Cloud Security Challenges -

(1) Distributed Denial of Service and Denial of Service attacks.
(2) Data ~~breached~~. breaches.
(3) Data loss
(4) Insecure access control points.
(5) Notifications and alerts

PAGE NO. ...

Trust Managment In cloud-computing —

A system proposed that implements the trust managment system for cloud computing, that assures secure data access through trustworthy cloud service provider.

Trust Creation
- Create trust functions
- Define policies
↑
Group Creation

→ Trust Negotiation
- Exchange credentials
- Map policies
↑
New node joins the System

→ Trust Managment
→ Trust calculation
→ Trust distribution
- Trust update
- Trust storage
↑
transaction

Business Continuity Plan- (BCP)

Adapt and respond to risks with a business Continuity plan.

A business continuity plan is a document that outlines how a business will continue ~~operations~~ operating during an ~~unplanned~~ unplanned distruption in service. It contains contingencies for business processes, assets, human resources and business partners. - every aspect of the business that might be affected.

A key component of BCP is a disaster recovery plan that contains strategies for handling IT disruptions to networks, servers, personal computers, and mobile devices.

Key features of an effective BCP-

(1) strategy- objects that are related to the Stradagies used by the business to complete day to day activities while ensuring continuous operations.

(2) organization - objects that are related to the structure, skills, communication and responsibilities of its employees.

(3) Applications and data - objects that are related to the software necessary to enable business operations, as well as the method to provide hight availability that is used to implement that software.

(4) Processes - objects that are related to the critical business process necessary to run the business as well as the IT processes used to ensure smooth operations.

(5) Technology - objects that are related to the systems, network and industry specific technology necessary to enable continuous operations and backups for applications and data

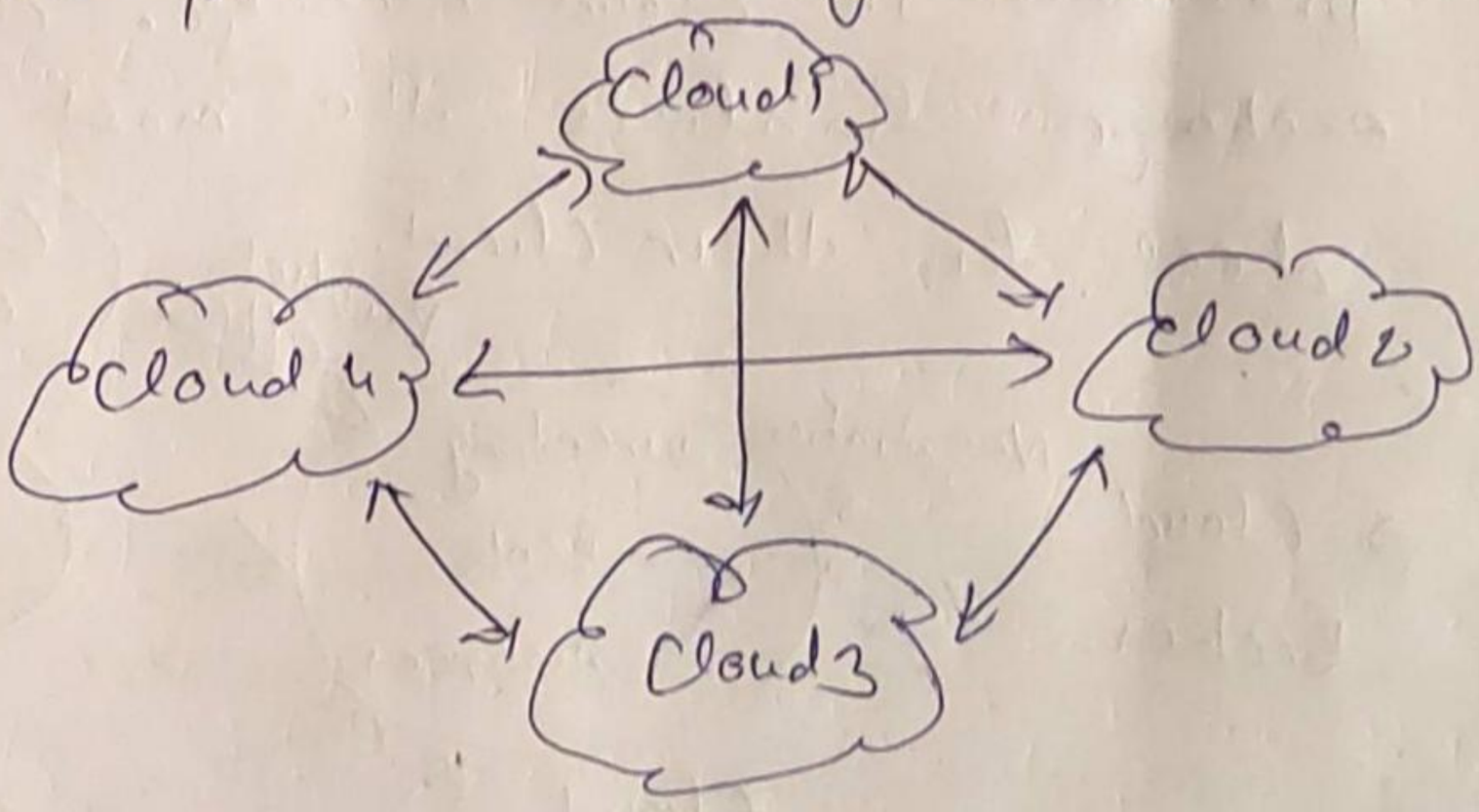
(6) Facilities - objects that are related to providing a disaster recovery site if the primary site is destroyed..

Unit - V

PAGE NO.

Cloud Federation - Is the deployment and management of several external and internal cloud computing services to match business needs. It is a multinational cloud system that integrates private, community and public clouds into scalable computing platforms.

Federated clouds is created by connecting the cloud environment of different cloud providers using a common standard.



The architecture of Federated cloud -

1. Cloud Exchange - The cloud exchange acts as a mediator between cloud coordinater and cloud broker.

2. Cloud Coordinater - The ~~Cloud~~ Cloud Coordinater assigns the resources of the cloud to the remote users based on the quality of service they demand and the credits they have in the cloud bank.

3. Cloud Broker - The cloud broker interacts with the cloud coordinator, analyzes the the service level agreement and the resources offered by several cloud providers. in cloud exchange. cloud broker ~~exchange~~ finalizes the most suitable deal for their client.

PAGE NO. .....

Unit-V

Google app engine is a platform as a service, product that provides web app developers and enterprises with access to google's scable hosting and tier 1 internet service. GAE requires that applications must be written in Java or python, store data in google bigtable and use the Google query language.

GAE's key features -

API selection - GAE has several built in API's including the following five -

→ Blobstore for serving large data objects.
→ GAE cloud storage for storing data objects.
→ Page speed service for automatically speeding up webpage load times.
→ URL fetch service to issue HTTP requests and receive responses for efficiency and scaling
→ Mem cache - for a fully managed in memory data store.

Managed infrastructure - Google manages the back ~~end~~ end infrastructure for users. This ~~approach~~ approach makes GAE a serverless platform and simplifies API management.

Several programming languages - GAE supports Go, PHP, Java, Python, NodeJS, .NET and Ruby.

It also supports custom runtimes.

Support for legacy runtimes - GAE supports legacy runtimes, which are versions of programming languages no longer maintained. For ex. Python 2.7, Java 8 and Go 1.11.

Application diagnostics - GAE lets users record data and run diagnostics on applications to gauge performance.

Security features - GAE enables users to define access policies with the GAE firewall and managed Secure Sockets Layer/ Transport Layer Security certificates for free.

Traffic Splitting - GAE lets users route requests to different application versions.

Versioning - Applications in google app engine function as a set of microservices that refer back to the main source code.

PAGE NO. 5

Benefits of fedrated Cloud-

1. It minimized the consumption of energy.
2. It increases reliability.
3. It minimizes the time and cost of providers due to dynamic scalibility.
4. It provides easy scaling up of resources.
5. It connects various cloud service providers globally. The providers may ~~buy~~ buy and sells services on demand.

~~Challe~~. Challenges in fedrated Cloud-

1. In cloud fedration it is common to have more than one provider for processing the incoming demands. In such cases there must be scheme needed to distribute the incoming demands equally among the cloud service providers.

2. The increasing requests in cloud fedration have resulted in more heterogenrous infrastructure, making interoperability an area of concern. It becomes a challenge for cloud users to select relevant cloud service providers and therefore it ties them to a particular service provider.

3. A fedrated cloud means constructing a seamless cloud environment that can interact with people, different devices, several applications interfaces and other entities.

Fedrated Cloud technologies-

1- openNebula 2. Aneka coordinator

3. Eucalyptus.