Page No.
Date

Cloud Applications

25/04/23

Virtualization Types

① Hardware Virtualization
② Network Virtualization
③ Storage Virtualization
④ Data Virt.
⑤ Application Virt.
⑥ Desktop virtualization
⑦ Memory Virtualization

Server Virtualization

1. Hardware Virtualization :- It is creating a logical pool of physical resources and alloting it to a machine.

→ It is a process that partition a physical server in multiple virtual servers.

① → Hardware - Assisted Virtualization (Specialised H/w is dedicated for this)
② → Full Virtualization
③ → Partial Virtualization
④ → Para Virtualization

④ All the physical resources will be virtualized
③ Some of
Some features will not be available in partial.

#1 Hardware - Assisted Virtualization :- The H/w provide architectural support for building a VM manager (VMM) able to run a guest OS system in complete isolation. Ex :- Intel VT → Virtualization Technology.

#2 Full Virt :- It refers to ability of running a program on top of VM without any modification & provide a complete emulation of the underlying H/w.

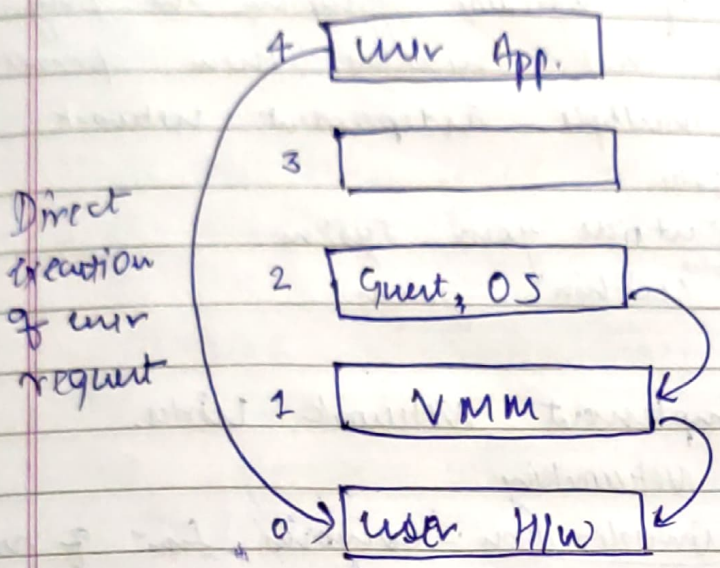
#3 Partial Vir :- It provides a partial emulation of the underlying H/w resources.

#4 Para Vir :- It expose a software interface to the VM i.e modified from the host and guest OS needs to be modified.

Full	Para
• They are in isolation to one-another	• Any virtual machine is aware that it is sharing their resources
• It supports all guest OS without modification.	• The guest OS has to be modified and only a few OS support it.
• It provides the best isolation	• It provides less isolation compare to full virt.
• The guest OS will issue H/w call	• Using the drivers the guest OS will directly communicate with the hypervisor.

Ques. Which among the full Vir, and Para virt. is secure and why.

Full Virtualization

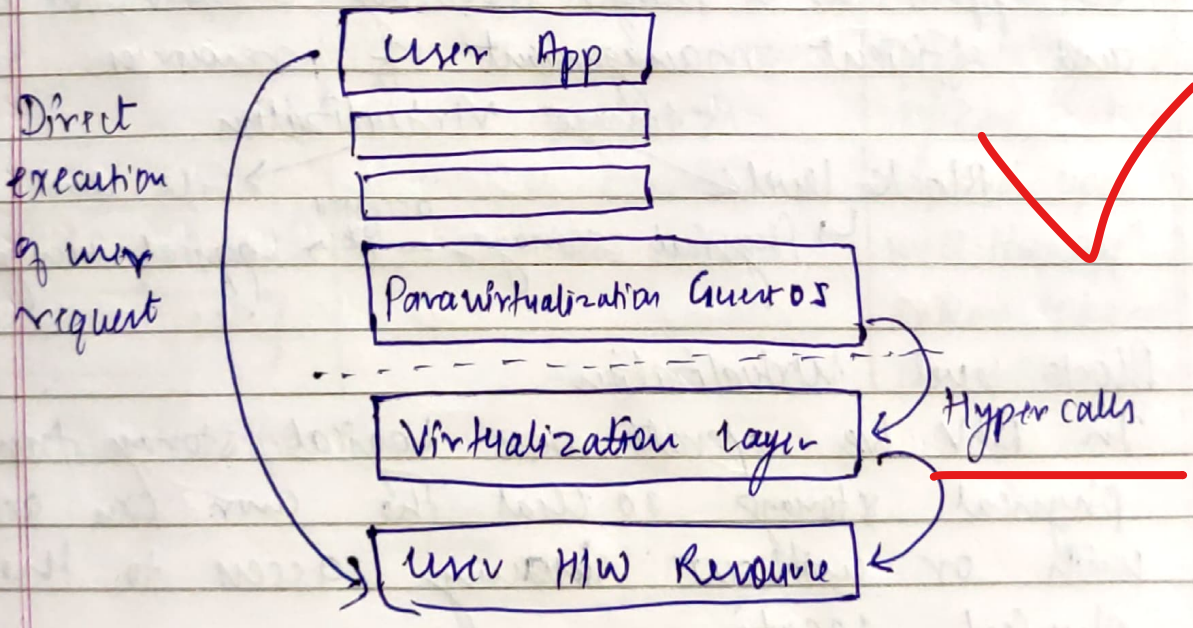


Direct execution of user request

Binary Translation of OS request

Ex:- VMware

Para Virtualization



Direct execution of user request

Ex:- VMware, Parallel system, Xen

Network Virtualization

It is a process of logically grouping the physical network resources and making them operate as a single or multiple independent network.

Ex:- Virtual LAN (VLAN)

Types
External LAN → Outside your system
Internal LAN → Within system

Approaches to Implement Network Virtu.

1. Software Defined Networking
2. Network function virtualization :- combines func" of network appliances to improve the network performance.
3. Storage Virtualization —

Multiple physical storage devices are grouped together to appear as a single storage device for easier and efficient management of resources.

Storage Virtualization
- Block level
  - ↳ Physical storage → accessed by → Logical unity
- File level

Block level virtualization

In BLV we seperate our logical storage from the physical storage so that the user can access with or without knowing :access to the physical location.

File level Virtualization —

It removes the dependency caused for accessing the data at file level of that of location where they are actually present.

Page No.
Date

Memory Virtualization — H/w Assisted / Software Assisted

Physical memory across the different server are aggregated in a virtualization memory pool.

H/w Assisted — Intel Xeon 5500 (Page table)

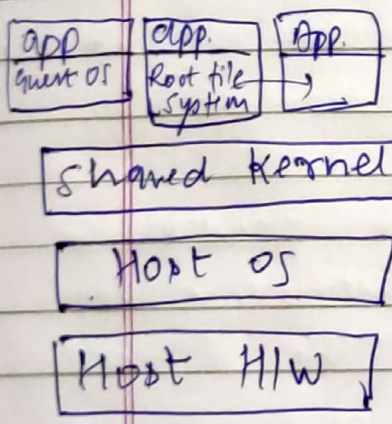
S/w Assisted — ESXi - Elastic Sky X integrated.

Software Virtualization -

The main fun is to develop a virtual env. in the system where software, application and OS is installed.

Software Virtualization

OS Virtualization



Application Virtualization

It helps a user to have a remote access to an application from a server

Eg :- Wine s/w

Service Virtualization

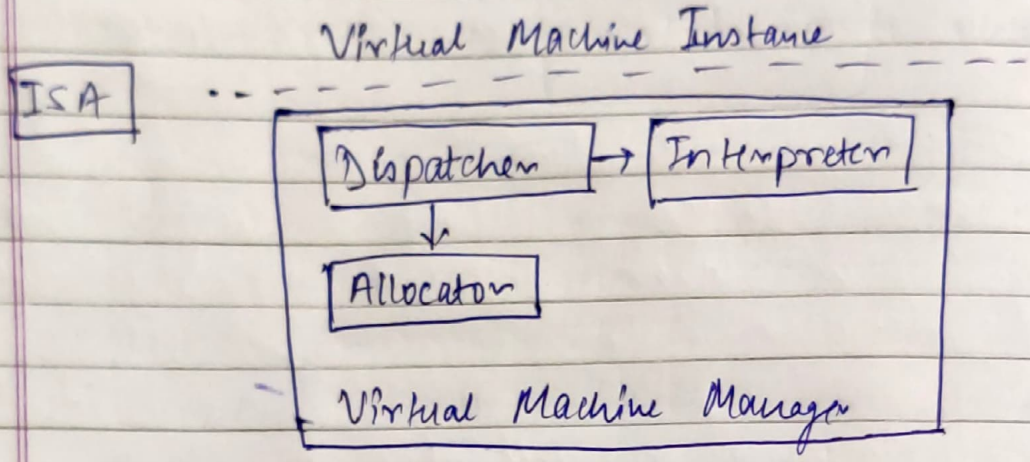
Service virtu. is a proces of creating replicas of systems that new appln depend upon to test how well the app" and systems integrate. Eg- (Salesforce service cloud)

Page No.
Date

Hypervisor Architecture

It has 3 components

1. Dispatcher 2. Allocator 3. Interpreter



There are 3 main modules that ~~coordinate~~ coordinate its activity in order to emulate the underlying H/w

* Dispatcher – constitute the entry point of the monitor and re-route the instruction issued by VM instance to one of the 2 modules.
* Allocator – is responsible for deciding the system resources to be provided to VM
* Interpreter consist of interpreter routines. These are executed whenever a VM execute a privileged instruction

vmware

Page No.
Date

Goldberg & Popek Essential criteria to be met by VM manager to efficiently support Virtualization.

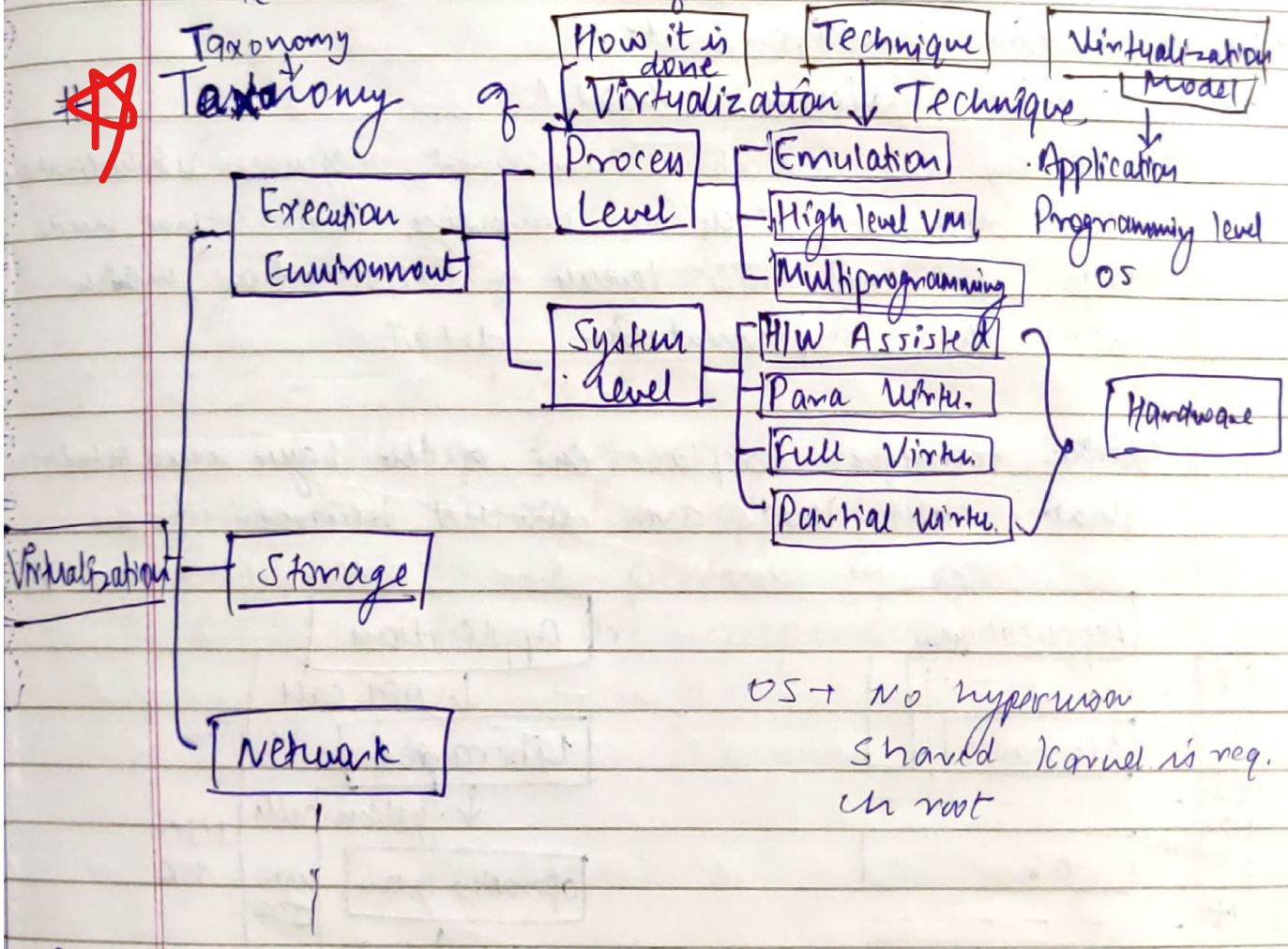
Characteristics of Hypervisor

1. Equivalence - A guest running under the control of VMM should exhibit the same behaviour as when executed directly on physical host.
2. Resource Control:- VMM should be able to completely control the virtualized resources.
3. Efficiency - Machine Inst. should be executed without the intervention of VMM.

Taxonomy of Virtualization Technique

Taxonomy

How it is done | Technique | Virtualization Model



Ques What is the diff. virtualization technology that can be used to implement virtualization. Mention the current publications in upto. Briefly exp. the involved existing virtn. technique and technology.

Page No.
Date

Ans = Virtualization is the technology that enables the creation of multiple instances or environments on a single physical machine, resource utilization etc

1. Full Virtualization :- In full virtu. a hypervisor is installed on the host machine, and virtual machines (VMs) are created, each running

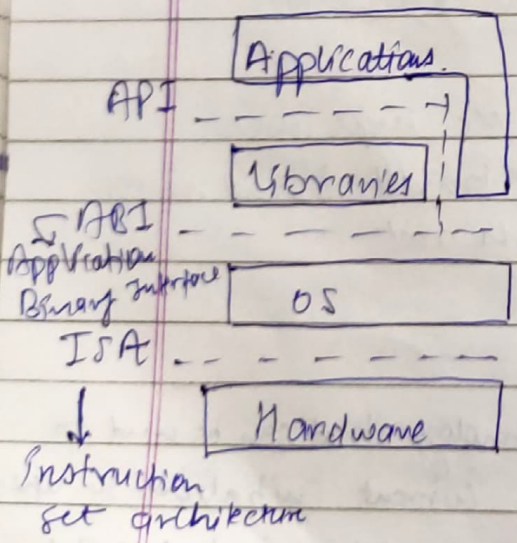
Virtualization

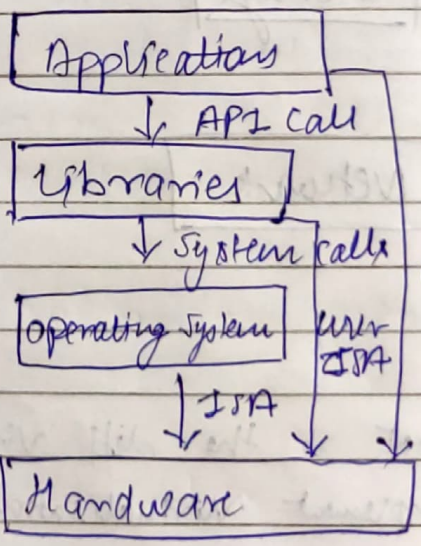
Execution ~~Environment~~

Machine Reference Model

Virtualizing an execution environment requires virtualization at different levels of computing stack that needs diff. interfaces b/w levels of abstraction which hide the implementation detail.

Virtu. technique replace one of the layer and intercept that calls that are directed towards it.





ISA

At the bottom layer the model of H/w is expressed in terms of ISA defining the instruction set for processor, register, memory & interrupts management.

System ISA	User ISA
• It is use for OS developers.	• It is more for developer of applications that directly manage the H/w.

ABI represents the application Binary Interface that seprates the OS layer from application and libraries. It covers details such as low level data types, alignments, defines a format for executable programs.

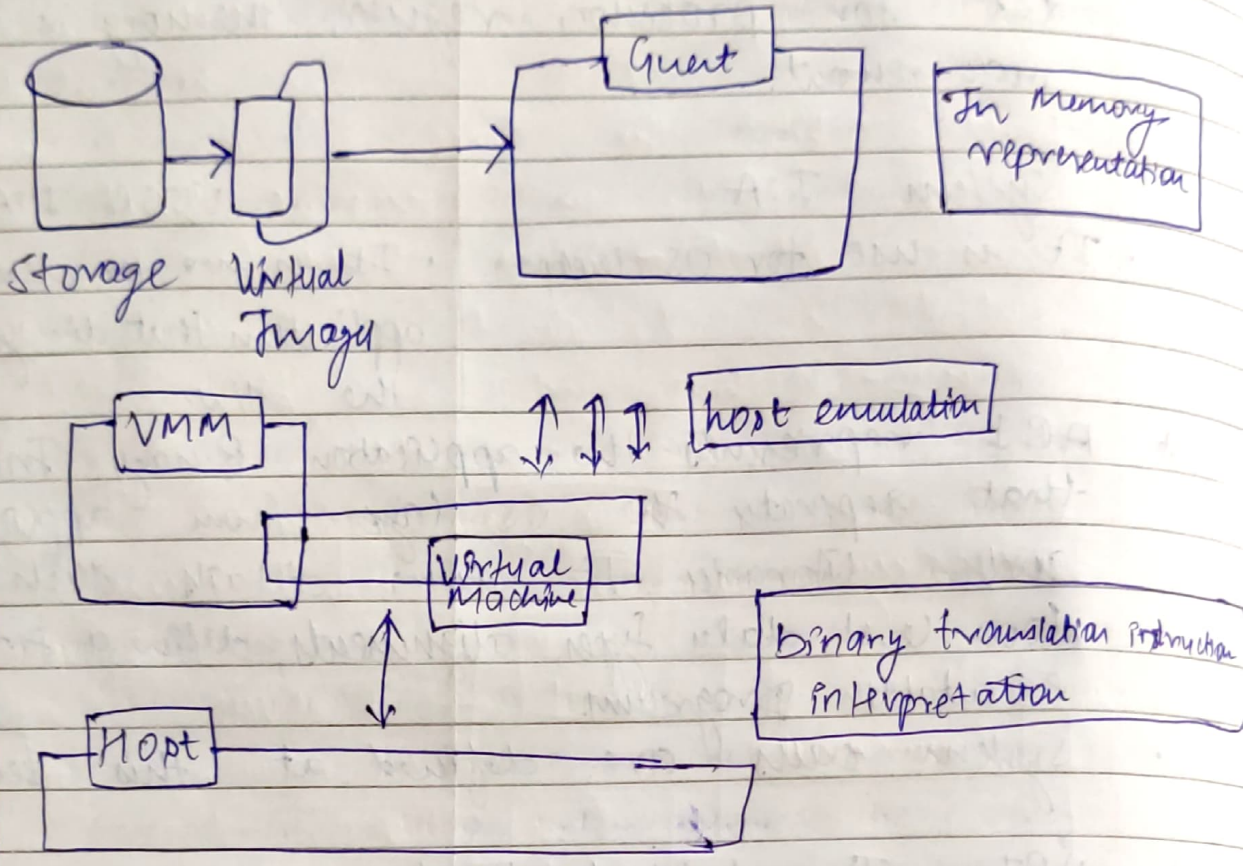
- System calls are defined at this level.

API - The highest level of abstraction is rep. by Application Programming Interface which interfaces app. to library & app. to OS.

- Any op^n to be perform in app. level API, ABI & ISA are responsible to make it happen

Page No.
Date

Hardware Virtualization Reference Model



→ Guest is rep. by the OS, Host by the physical computer H/W. Virtual machine by the emulation of physical hardware. VMM by the hypervisor

→ It is use for achieving ease of deployment of app. managed execution & portability.

→ It consist of a VM executing the bytecode of a program.

→ Compilers produce a binary format for an abstract architecture.

Eg:- Small talk, Java, BCPL

Page No.
Date

Operating System Virtualization

- OS level virt. do not use the hypervisor and don't apply a host-guest mechanism. Instead it utilized a process called containerisation which creates multiple user instances called containers through a kernel in OS.
- → Ch root to achieve OS level partition / virtual.

Ques. Write down the benefits and drawbacks of virtualization.

Virtual Infrastructure Environment

1. Appropriate plan, business development, market volatility, technological advancement will influence the H/w req. and dependence on computing resources.
2. Suitability Assessment
   The greater utilization of physical server resources must not be at the cost of service to the business
3. Prepare for failure
   By taking the adv. of monitoring software buying extra H/w & depending on clustering worst case scenario should be avoided

3.1 Detailed Report

- security and administration model
- Backup methodology
- Host Physical and Virtual disk layout.
- Virtual n/w topology
- Virtualization service console config.
- Virtualization kernel Device
  → Shared factor config.
- Config. of Virtual machine server with req. db.

- VM distribution among the host.
- Process for the ongoing management.
- Host server H/W specification etc.

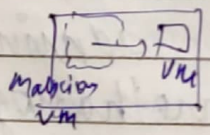
Cloud Security ☆

1. Authentication
2. Confidentiality
3. Integrity – It means the data or info. in our system is maintained so that it is not modified or deleted by unauthorized parties.
4. Availability
5. Data privacy - It means the ability to determine for themself (individual) the extent of what, how and when of the personal info to be shared or communicated with others.
6. Non-Repudiation – It is a method of establishing the user action accountability.

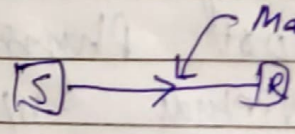
Types of Attacks: [Internal (within the org)
External (outside the org).

Security Thread in Cloud Computing

1. Denial of Service (DoS) - Resource overloading
2. Side channel Attack



3. Authentication Attack
4. Man-in-the-Middle-Attack



5. Insider & Organised Crime Threat
6. Social Networking Attack

Page No.
Date

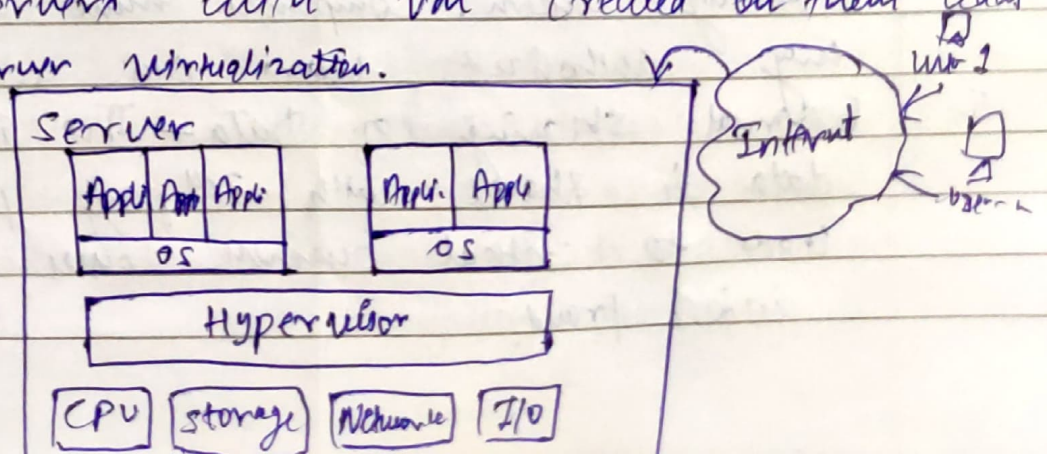
7 Attack ~~to the~~ through Mobile Device

Virtualization : [Benefits]
1. Cost effective / cheap
2. Proper utilization of resources
3. Environment friendly / save energy.
4. Carbon footprint will reduced due to less server.
5. Uptime will be more (due to replica of servers)
6. Availability
7. Easy Recovery it will take less time (Snapshots)
8. Efficient
9. Faster and Easy disaster recovery.
10

[Demerits]
1. Security (Side channel attacks)
2. High Initial investment (at supplier end)
3. Scalability is dependent upon the service provider
4. Data Risk (Virtual Machine specific attacks)
5. Performance degradation (Creating multiple VM on a single machine)
6. Unintended server sprawl (not manage effectively)

Server Virtualization

The servers with VM created on them leads to server virtualization.



Page No.
Date

Advantages	Disadvantages
1. Isolation	1. If server is down all the hosted websites will cease to exist
2. Easier database & recovery.	2. It consume significant amount of ram.
3. High availability	3. Efficiency for server usage is difficult to measure
4 Inc. Efficiency	4. Managing and its setting is difficult
	5. Virtualization may not be supported by all databases, H/w or apps.

Que 2 Current Virtualization Initiatives.

Cloud Security challenges

1. Misconfiguration (Loopholes in system where attackers will attack)
2. Unauthorized access - This include unauthorized access to user data, theft of data & malware attacks.
3. Hijacking of user accounts - users can protect themselves using strong passwords security question and multifactor authentication
4. Data Privacy & confidentiality - Business can access the data from anywhere which leads to security concern. Companies must ensure that only authorized users can access it.
5. External sharing of Data - The issue arises where data is shared with 3rd party providers which can leads to critical business losses and theft of info., fraud.

Cloud security Alliance

6. Legal & Regulatory compliance – There includes the local policies of the customer which the customer should follow & there might be the constitutional requirements.
7. Unsecured Third Party Resources – External 3rd party resource may be an appli. or a software which is external to the cloud and is compromised by the attackers.

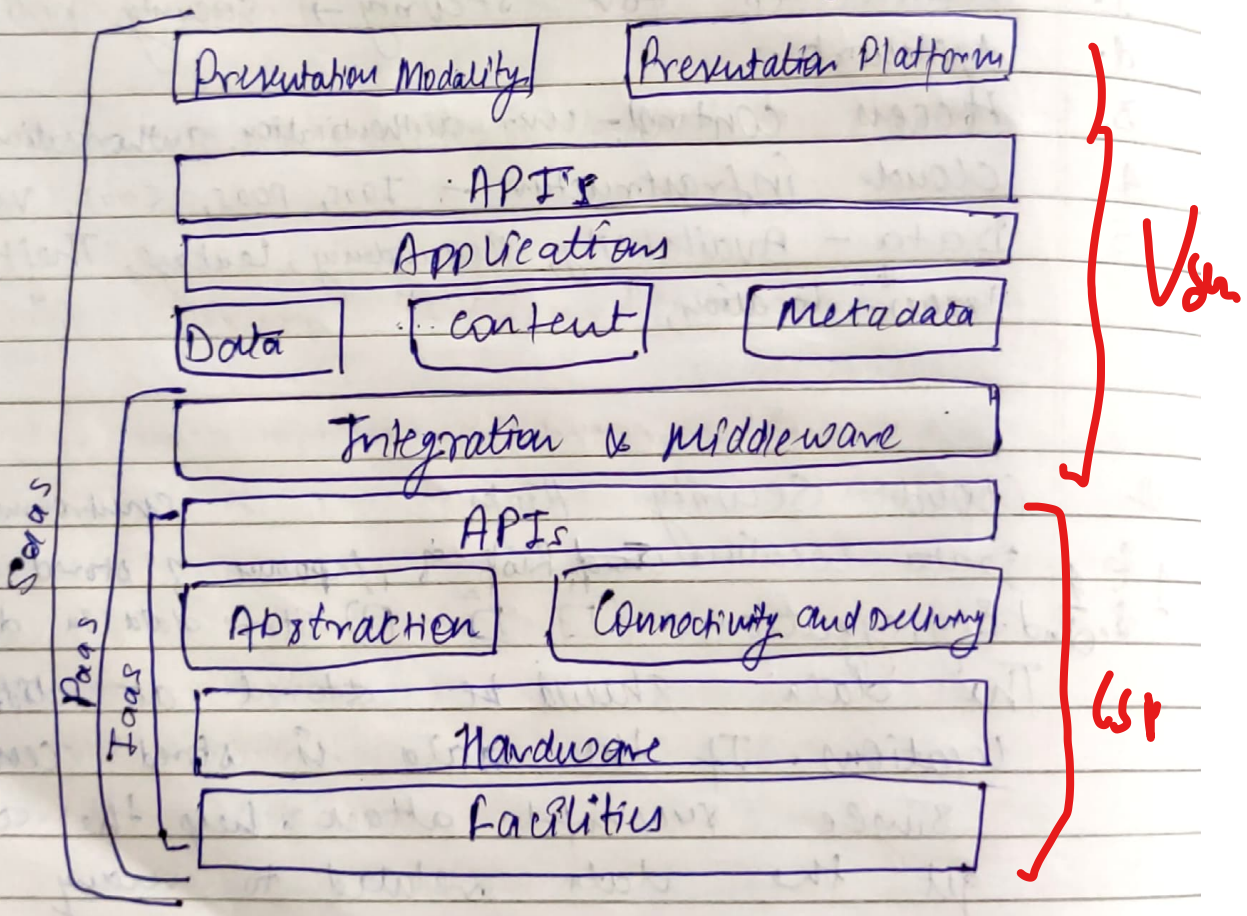
Challenges are divided in 5 broad categories
1. Standards for security → security policies
2. Network.
3. Access control – user authentication, authorization & Identification
4. Cloud infrastructure – IaaS, PaaS, SaaS, VM attacks.
5. Data – Availability, Redundancy, Leakage, Theft, Privacy etc
Issues → location,

Cloud Security Risks
1. Data location – Risk of exposure of stored data, environmental disaster leads to data loss
2. Segregation – Store data in diff locations.
The data should be stored at different locations. If the data is stored centrally a single successful attack, help the attacker to get the data related to many org.
3. e-Investigations & Protective monitoring
4. Previlged user Access → location & Provider
5. Data disposal → Deletion of data, due to high availability.
6. Cloud security Assurance – No standard rules for security of cloud computing, users have concern over
1. Defining security needs
2. Due Deligence on cloud Service Providers.

Page No.
Date

CSA Cloud computing security Architecture Reference Model

1. Each service inherit the capability and security concern of the model below it.
2. IAAS has the lowest integrated functionality and security level while SAAS has the highest.
3. This model describes the security boundary at which cloud service provider responsibility and and customer responsibility begin.



Saas Security—

The set of best practices and policies implemented by saas provider to ensure the privacy & security of customer data is referred to as saas security

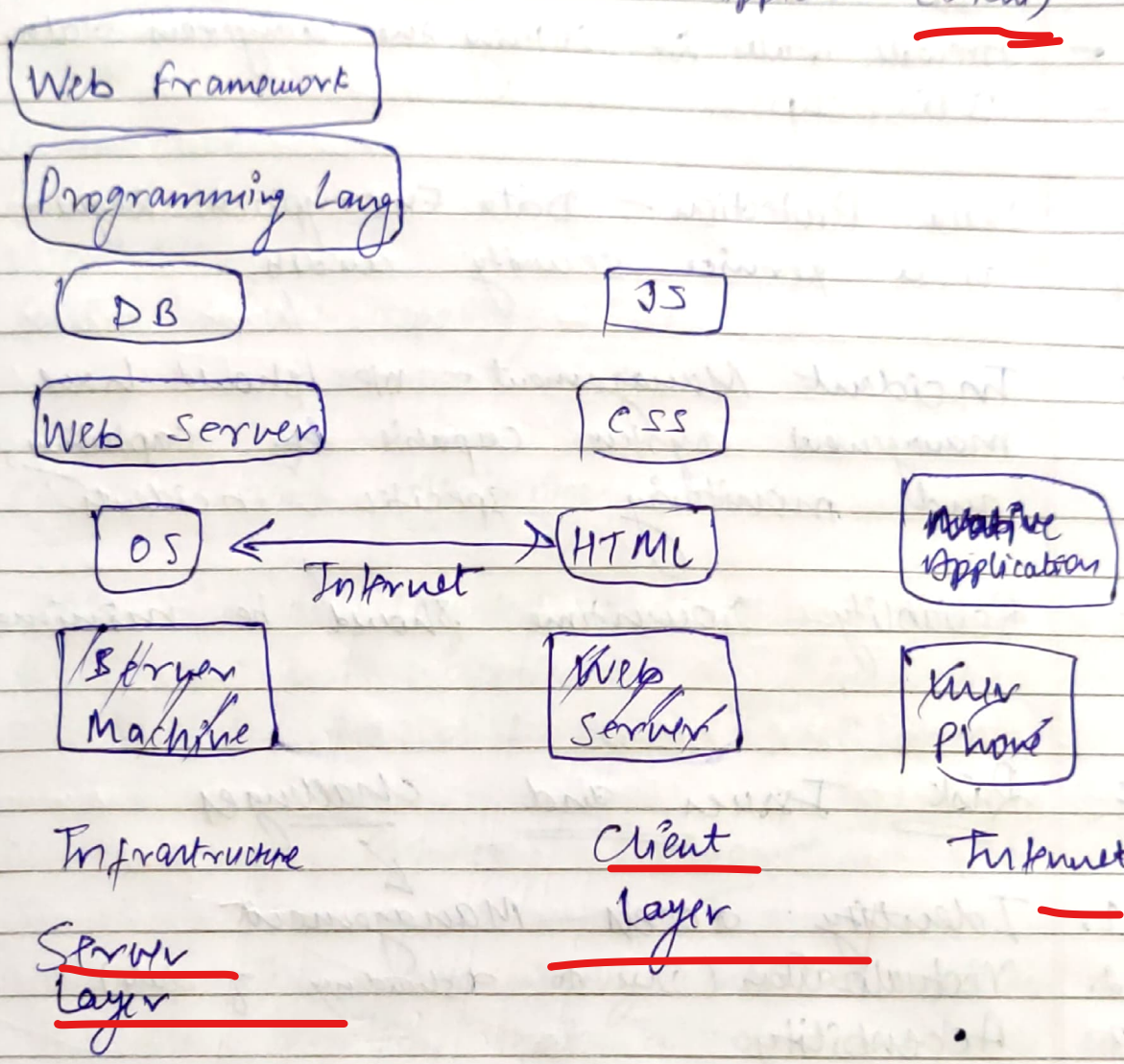
Page No.
Date

Saas security

Infrastructure (server)

3- Layers of Saas security ← Internet

Application (client)



Key Principles of Saas security

1. Access Management - Role based access
   Admin → All access, others → Read only
   - system access control
   - workflow management
2. VM Management - Continuous updation of VM's
   - Implementation of security patches
3. Network Control - It could be implemented by - Network access control list and VPN

4. Perimeter Network control – Config. in the rules of the Firewall
- firewall rules for filtering the dangerous data.
- IDs, IPs

5 Data Protection – Data Encryption, Regular Software security as a service security audits.

6 Incident Management – We should have incident management system capable of capturing, tracking and monitoring specific incidents

7 Reliability – Downtime should be minimal.

Risk Issues and challenges

1. Identity access Management
2. Virtualization (Due to redundancy of data)
3. Accessibility
4. Hidden Backend Details
5. Data control
6. Misconfiguration
7. Regulatory Compliance
8. Data disaster recovery

Best Practices

1. Vulnerability Monitoring and Testing
2. End-to-end encryption
3. Enforcing data security – Multifactor authentication, role based access control

RBA → Risk Based Authentication

4. Virtual Private Network Implementation and TLS
5. Discovery and Invent.

IAM
1. Authentication
2. Authorization
3. User Management
4. Central user repository

Cloud Security Monitoring

CSM supervises physical and virtual servers to asses the data, application or infrastructure. Infra behaviour for the diff. potential cloud risk / threat

Cloud security Monitoring software → Tools must be able to monitor large volume of data across distributed loc.

(ii) Scalability

(iii) Visibility – The more visibility into the app, user, and the file behaviour that a cloud monitoring sol. provide the better it can identify potential risk

(iii) Timeliness – It should ensure that new or modified files are scanned in real time

(iv) Integration – It should provide well integration for diff storage sol or network sol

(v) Auditing and Reporting –

Benefits of cloud security Monitor

1. Maintain Compliance
2. Identify Vulnerability in systems and resolve it.
3. Preventing the business loss.

Challenges of CSM

1. Lack of cloud security strategy – Most org. migrate to the cloud to support remote work without developing the cloud security strategy.
2. Alert fatigue – ~~Lto~~ ~~CSM~~ cloud monitoring sol. are noisy which can result in IT and security teams lacking insight into what's important to focus.
3. Lack of context – Security team should understand what they want to monitor and why and once they receive the alert they should know what actions to take.

Best Practices –

1. Careful evaluation of CSP.
2. Perform a cloud infrastructure inventory. (Shadow IT)
3. Layered approach of IT security (AWS Guard Duty)

Cloud Security Tools

1. Amazon Cloudwatch
2. Jupiter One
3. Datadog.

Cloud Data Security

→ CDS protects the data i.e stored or moving in and out of cloud from security threats, unauthorized access, theft and corruption.

Need

Companies must solve how to protect the data and manage access to data as it move across multiple environments.

* CIA Triad

Challenges

1. Lack of visibility (where data is stored)
2. Lack of control
3. Confusion over shared responsibility.
4. Inconsistent coverage
5. Growing Cyber Security Threats
6. Strict compliance Requirements
7. Distributed data storage

Benefits of cloud Data security

1. Greater visibility
2. Easy Backup and recovery.
3. Cloud data compliance (cloud data loss prevention) DLP
   It can help us to discover, classify & deidentify the sensitive data to reduce the risk of policy violation
4. Data encryption.
5. Lower cost

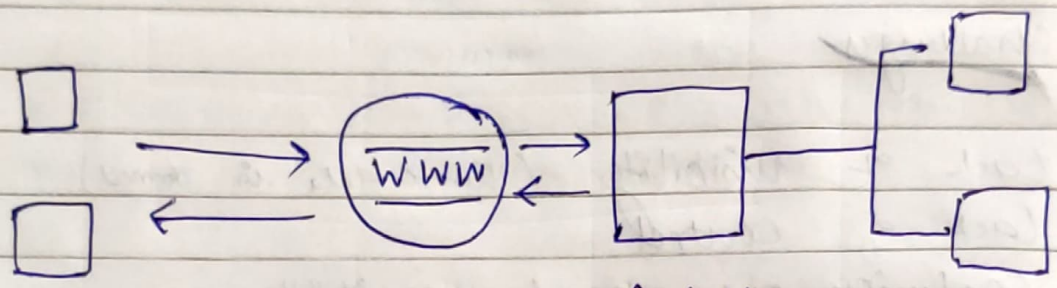
Ques. Who/which Party is responsible for securing the data?

Products of CDS (Google) Security Tools)

1. Identity and Access Management.
2. Cloud key Management
3. Cloud Data Loss prevention

Application Security (AppSec)

It refers to security precautions used at the application level to prevent theft of data or code within the application. It covers the entire application life cycle including requirement analysis, design, testing and maintenance.



Application security can be implemented at → [H/w, S/w, procedures]

Types of application Security

1. ~~Validation → Username & password~~
2. Authentication
3. Authorization
4. Encryption
5. Logging
6. App. Security Testing - It ensures that all of the security control are functioning effectively.

~~Tools~~ Approaches

1. Design Review - The architecture & design of the app. can be examined for security flaws before the creation of code.
2. White box security Review - App. is examined by manually inspecting the source code and looking for security issues

Page No.
Date

③ Blackbox security Audit – It is accomplished through use of app. to test it for the security flaws

④ Automated Tooling – ~~Dif~~ out security tools can be automated by including them in development or testing process.

⑤ Coordinated Vulnerability Platform – It offer hacker powered app. security solutions where individual can be identified and compensated for reporting defects

Tools for application security

① (SAST) Static app. Security Testing – Source code are examined.

② (DAST) Dynamic " " " – Simulate false attack during Compilation

③ Interactive " " " SAST + DAST → It is in real time.

④ Runtime application Security Protection – It is more concerned with security than with testing. It provides continuous security checks and automated responses for the possible threats which includes informing the IT team or terminate the session.

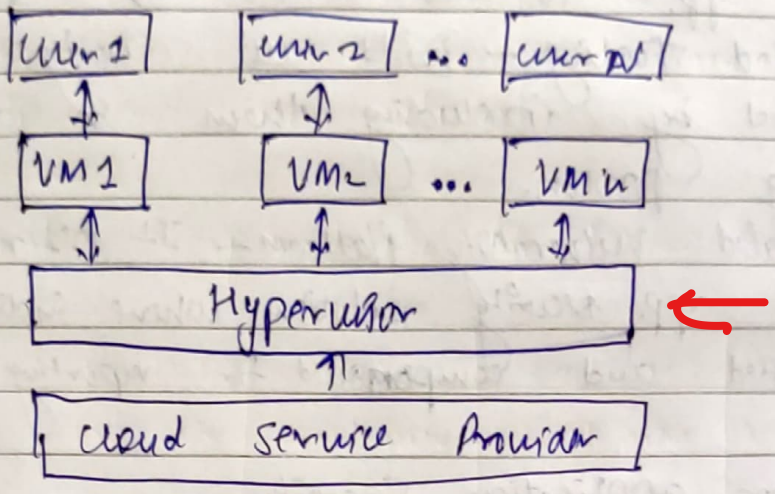
Application Security Risks

1. Cross site Scripting – (XSS) – It allows an attacker to insert client side code into webpage and obtain user sensitive information.
2. DoS
3. SQL Injections – It is a technique used by hackers to exploit the db flaws and these attacks in particular reveal user identity, user id, password.

Virtual Machine Security (Virtualized security)

→ It describes security sol. that are software based and created to operate in virtualized IT environment.

VM security



Resources: H/w & S/w

* Some attacks
# Hyperjacking – Hacker is controlling Hypervisor.
2 DOS Attack
3 Coresidential attack (side attack) avg. between b/w VMs
4 Network config Attacks.
5 Virtualized rootkit → software to gain root access. They operate as a malware that executed as a hypervisor controlling one or many VMs

VM security Implementation
(1) Service Provider security – the system virtualization H/w should not be physically accessable to unauthorized persons.
(2) Hypervisor security – the code integrity is protected via a technology called hypervisafe.
(3) VM security – Administrator must setup a program that prevents VM from consuming additional resources without permission.
→ It also includ logging, firewalls, Antivirus, Host intrusion prevention system.

(4) Guest Image security — A policy to control creation use storage and deletion of images should be implemented at this level.

Benefits

(1) cost effectiveness.
(2) Regulatory compliance.
(3) Operational efficiency. (Scaling)
(4) flexibility
(5)

Essential steps to secure a VM

(1) Keep connection secure & private
(2) Seperate management API to secure the network.
(3) Ensure that all components have been tested and verified.
(4) Protect the hosted elements by isolating them. — We can isolate by hosting & feature connection withing a private subnetwork.

Security Architecture Design

A cloud security architecture is defined by security layer Design and Structure of platform tools, software infrastructure and best practices that exist within a cloud security solutions.

Key Elements of cloud security Architecture

1. Security at each level
2. Robust Design

3. Centralized Management.
4. Scalability and Elasticity.
5. Appropriate storage for deployment.
6. Alerts and notifications

Shared Responsibility Model for Security in Cloud

	On-Premises	IaaS	PaaS	SaaS
User Access	Customer	Customer	Customer	CSP
Data	"	"	"	"
Applications	"	"	"	"
OS	"	"	CSP	"
Network Traffic	"	"	"	"
Hypervisor	"	CSP	"	"
Infrastructure	"	CSP	"	"

IaaS cloud security model includes
(i) Audit and monitor resources for misconfig.
(ii) Prevent data loss with data loss prevention (DLP)

PaaS cloud security features include :-
(i) Cloud access security brokers,
(ii) Cloud workload protection platform,
(iii) Business Intelligence
(iv) IP restrictions.

SaaS security restrictions includes
1 Prevent ~~personal~~ unauthorized sharing of data to wrong data.
2 Block personal data to corporative devices
3 Detect compromised accounts.

Page No.
Date

Working with different cloud Platforms :-

* AWS compute Services (IaaS)
It is a means to provision and manage infra. (Virtual machines and containers)

* features
1 Scalability,
Vertical — Increase in computational capacity
Horizontal — Increase in the no. of resources.

2. Multi-utility - Resources can be provisioned and run for years as long as users pay for it

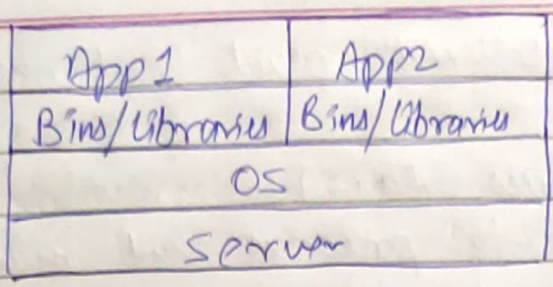
3 Ethernet

4 Regions and availability zones.

Instances — Server environment.
AMI — Amazon Machine + Image (OS + Tools)

Compare AWS compute Services

Category	Services
1. Instance	1. AWS EC2
	AWS Lightsail - less config. than EC2
2. Containers - provide a standard way to package application code, configuration and dependencies in a single object.	2. AWS Batch



AWS Elastic Compute Cloud

3. Serverless — 3. AWS Lamda

4. Edge and Hybrid — 4. AWS Outpost
AWS local zones

5. Cost and Capacity Management — 5. AWS Elastic Beanstalk
AWS saving Plan
EC2 Image Builder

AWS compute

#1 EC2 (Instance (Types))

1. On-Demand (Pay-per-usage) (created when required)
2. Reserved (Taken for 1,2.. years) (Not pay as you go)
3. On-Spot (On req. AWS can take it back), it is borrowed.

* On-Demand Instances
  - → These are the instances that we pay for as and when we need them.
  - → These are charged by (Pay by second/hour)

* Reserved Instances
  - Instead of requesting Instance as and when we need we reserve Instances either for 1 year or 3 year....

* Spot-Instance
  - It uses spare EC2 capacity i.e available & is provided for less than on demand price.
  - → It is similar to borrowing concept where if the demand goes up & the cloud provider needs extra capacity they will take it back.

4. C7g (compute) Instances - AWS Graviton3 processors Compute intensive.
5. Inf2 (inference) Instances - It is used for deep learning inference.
6. M7g Instances - General purpose workloads & applications built on open source softwares. Such as gaming, app. servers etc.
7. R7g Instances - It is used for Memory Intensive workloads.
8. Trn1 Instance - Deep learning training.
9. Dedicated Host - Servers

2 Storage Services

1. Amazon simple storage service (S3) →
   → It is a kind of object storage

2. Amazon Glacier
   → object storage → archive storage
   A service that provides low cost highly durable archive storage.

3. Amazon EBS (Elastic Block store)
   → It provides Block storage for EC2 instances

4. Amazon EFS (Elastic File ~~Stor~~ System)
   → It provides scalable network file storage for EC2 instances.

5. Amazon EC2 Instance storage. (Block storage) ↘ temporary data.
   → It provides a temporary block storage volume for EC2 instances.

6 AWS storage Gateway –
   → It is a On-premises storage appliance that integrate with cloud storage.

7 AWS Snowball – It is a service that transport large amount of data to and from the cloud.

8. AWS Cloud Front – It is a service that provides content delivery frameworks.

Page No.
Date

#3 Network & connectivity services

Broad Categories ← N/w Architecture
N/w connectivity
Application delivery

* N/w Architecture –

* Route 53 – It is a highly scalable on demand DNS web service.

#4 Communication Developer services
How you interact with customers

1. Amazon Simple Email Service (SES)
→ use for bulk email sending.
It is a cloud email service provider that can integrate into an application for bulk email sending transactional / marketing.

2. Amazon Pin Point
→ It offers developers and marketing people to develop customized tool for delivering customer communication across channels and campaigns at scale, to deliver.
→ OTP is delivered through Pin Point

3. Amazon chime SDK
Builders can easily add real time video, voice and messaging powered by ML into the application.

Google App Engine → Platform as Service
↳ App development and deployment

→ Google Distributed Infra. is used.
→ Local machine (SDK)

Architecture

① Infrastructure ② Runtime ③ Application Services ④ Storage

Sandbox → for storage and isolation of app. / apps are separated by sandbox

Infrastructure
→ Load balancing, Redirecting, Monitoring, Billing Statistics

Runtime Environment
→ The env. during the starting and ending of execution of app.
2 - Types ← Standard → Fixed instances, You can choose any, Pay/hour
Flexible → Create an instance acc to your req.

→ Sandboxing → Isolate the app. from each other. And it can't make any changes to the servers.
↳ Temporarily created

Storage - 3 Types
- Memcache (In-memory cache)
- Datastore (Storage for semi-structured data)
- Static file servers (Long term storage for static data)

Application Services
Access to data, Account Management,

Page No.
Date

MS Azure → PaaS + IaaS + SaaS Manage portal

* Services
  PaaS + IaaS
* Accessing
  Azure Platform/Portal
* Services Provided
  → Compute, Storage, Network, IoT, DB, Container, Business Intelligence
  → All the services are tied together with a middleware called Appfabric.
  → The services compute, storage, Networking, IAM are tied together by a middleware called Appfabric it was renamed to Service Fabric.

Compute (creating VM)
↳ are offered with Roles < Web Roles (Http)
Worker Roles
VM Roles

* Role is a run time env. customized for a specific compute task.

1. Web Role - It is designed to run scalable web app. (IIS 7 server)
2. Worker Role - These are designed to host general purpose compute services or the services that do not communicate via HTTP.
   → Used to perform background processing for web app.
3. VM Role - Windows Hyper-V Technology.
   Custom images of windows servers 2008 R2 are used

Storage service -

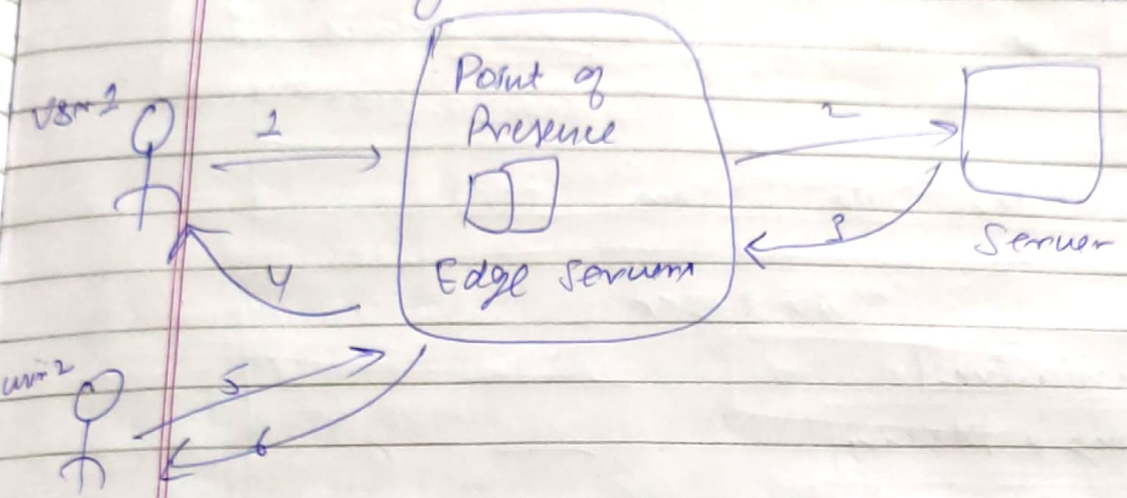
1. Azure BLOB → Binary data
   Text and binary data
   ↳ Objects storing data

2 Azure Files - Managed file share service.
3 Azure Elastic SAN - It is used for deploying, scaling, managing and config. storage area network
4 Azure Queues - It is used for reliable messaging b/w the app components.
5 Azure Tables - NoSQL storage
6 Azure Managed Disk → Block level storage volumes for Azure VM.
7 Azure NetApp Files - It is a Azure native highperformance, file storage service. -
• It is powered by NetApp.

Networking Services -
1 Azure Virtual Network - It is a logical rep. of network in cloud. We can define our private IP add. range on Azure.
* Features —
1. Isolation
2. Communication with internet - by default the outbound traffic to internet is there, but we need to establish the inbound connection.
3. Communication with onpremise resources →
4 Network traffic filtering
4.1 Azure Firewall 4.2 Network security groups.
5 Route Network traffic
6 Monitor Network traffic.

2 Azure Traffic Manager → Load balancing
3 Azure AD Connect (Active directory) - It is a tool for connecting Onpremises identity info. to MS Azure AD.
4 Azure CDN (Content Delivery Network)

It is a distributed network of servers that can efficiently deliver web content to users.



Azure web app, Azure storage account or any ~~Origin~~ publically accessable servers.

Saas

Outlook, Office 365

~~Σ~~ # Azure SQL is a relational ~~db~~ hosted on Azure cloud & it is built upon SQL server technology

We can have scalable, highly available and fault tolerant db using Azure SQL.

→ It is a Paas database engine.

→ The db can be communicated and managed by using Rest API.

→ Protocol → Tabular data stream protocol. Access to SQL Azure is based on Tabular data stream protocol.

AppFabric → Middleware

Page Service Fabric

Date

Client layer

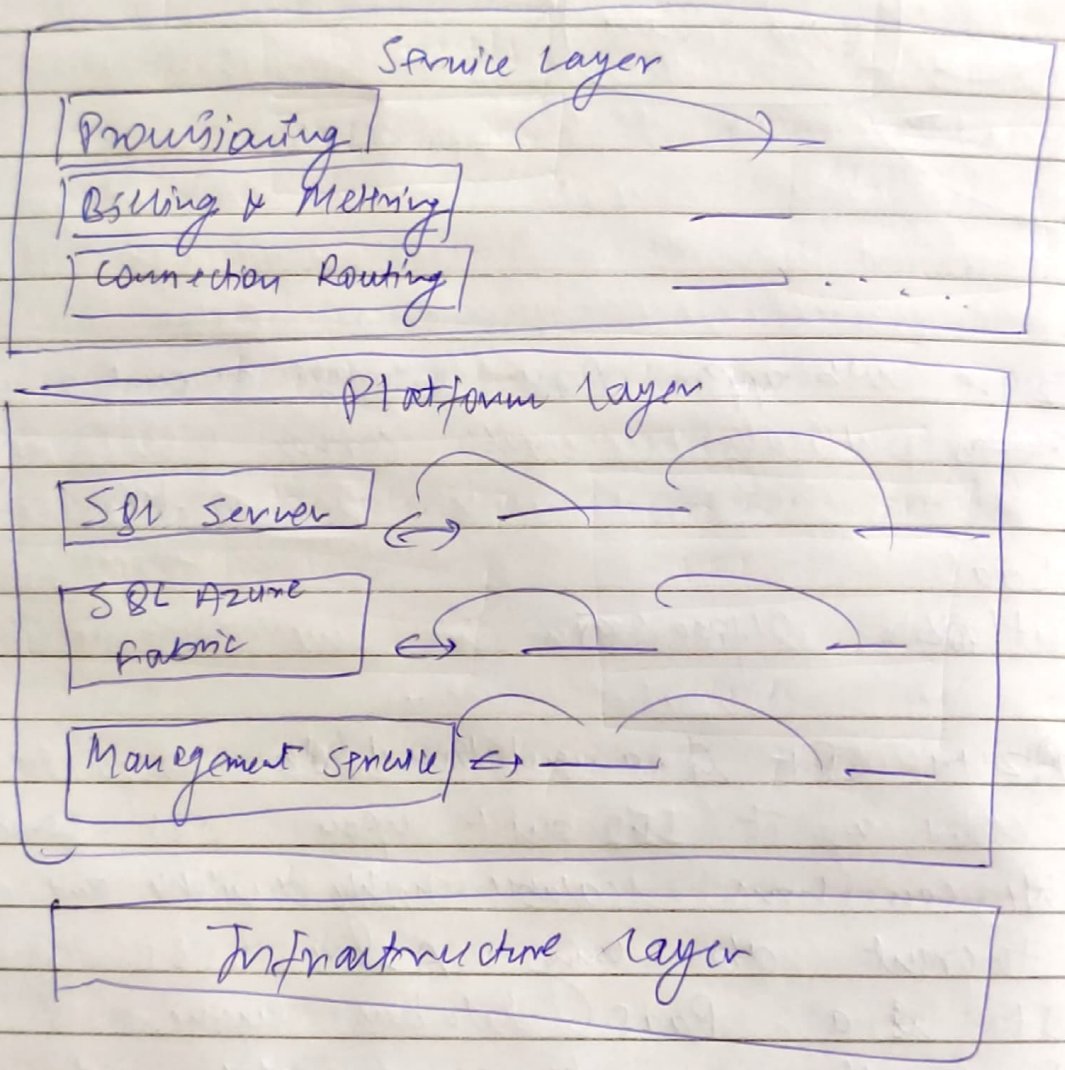
Client Premises or Azure Platform

HTTP/REST

PHP | SQL server Application & Tools | WCF Data Services

ODBC | ADO.NET

Tabular Data Stream (TDS)



Azure SQL

Domain Name

Server Name → server

`server.database.windows.net`

Pricing → per hour and unit that you as using.

Page No.
Date

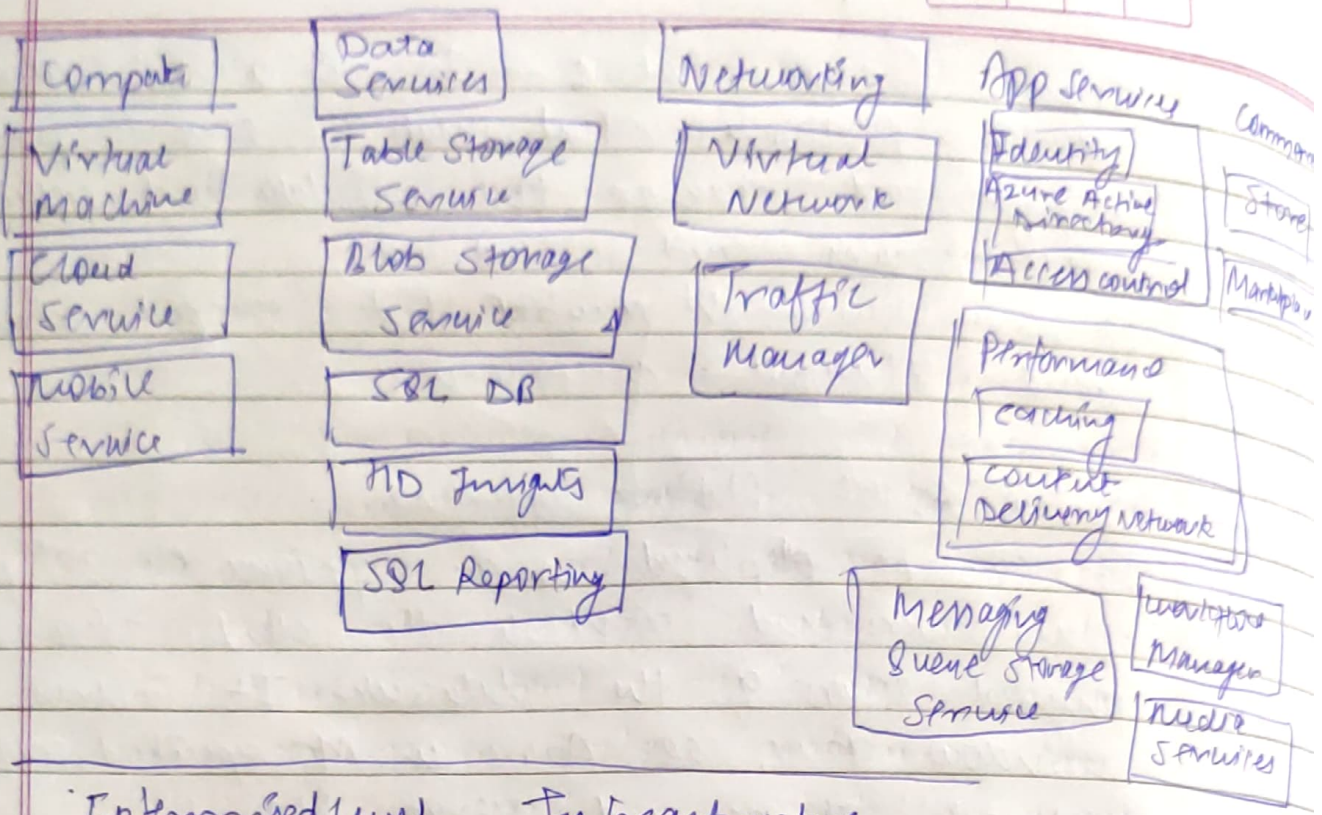
* Azure Service Fabric – It is a distributed system platform that make it easy to package deploy and manage the scalable and reliable microservices and containers.
→ It is a light weight runtime that support stateless and stateful microservices

* Window Azure Platform appliance
It can be deployed as an appliance on 3rd party data centers and contribute the cloud infra. running physical servers of the data center. It includes window azure, SQL Azure & MS specified config of Network storage and server H/W.

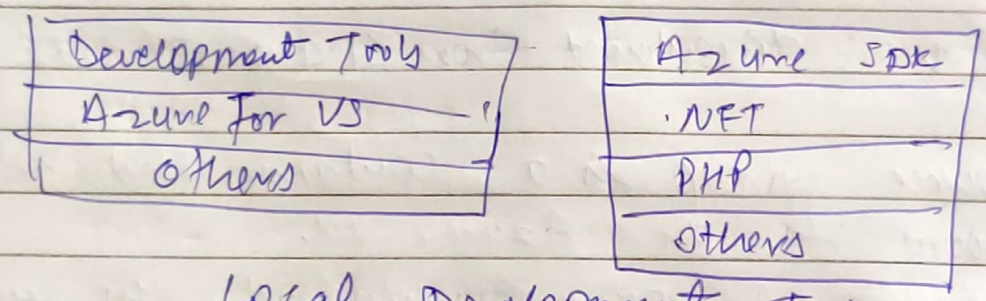
They we discontinued from 31 August 2018

Resource Group is a container that hold related resource for an Azure sol.
- Resource group can include all the resources that we want to manage as a group and sharing the same life cycle.

Local Deployment
→ Developer tools
→ VS Team service
→ Azure Dev Test Labs



Enterprised level Infrastructure.



Local Development Tools

1) 5 Real world applications
2) MS Azure 3) G.cloud Platform 3) Google App Engine
4) Aneka 5) AWS

Applications

MS Azure
AI, Ecommerce, Data Analytics, ~~Backup~~, IOT
Web & Mobile development, ML

Aneka

Page No.
Date

~~Aneka~~

Google cloud Platform
- Data Analytics and Machine learning, cloud Storage and data, IoT, App. development & deployment

Gaogle App Engine
- Web Application Hosting
- Mobile Backend as a Service
- Microservices Architecture
- Data Procesing and Analytics
- IoT

Aneka
- Scientific Research
- Financial Analysis
- Healthcare and Bioinformatics
- E-commerce and recommendation system.
- IoT

AWS
- E-commerce and Retail
- Media and Entertainment
- Healthcare and Life Science
- FinTech and Banking
- IoT

Applications of Diff cloud Platforms

Scientific Applications

→1 Healthcare → ECG analysis in cloud

→2 Biology → Protein structure Prediction, Gene. explanation
It is computationally intensive task and requires massive no. of states acc cloud Sol are used.
Ex:- ~~Giva~~ Jeeva → ~~Bard~~ It is an integrated web portal that enable scientist to offload the prediction to cloud band on aneka.

* Gene Expression Data Analysis → Gene Exp. profiling is used to provide a more accurate classification of tumors.
* Learning classifiers – It started with XCS (extended classifier system)
* coXCS
* cloud - coXCS → It is cloud band imp. of coXCS that uses aneka to solve the classification problem in parallel and determine the output.

→3 Satellite Image Procesing (Geo Science)
Geographic info. system capture, store, manipulate & manage all type of geo. reference data.

A workflow has been developed by GOI where at the SaaS level app. provide collection of services such as data visualization at paas level aneka is controls import of the data in Virtualized Infra.
↳ Execution of image procesing task. The Infra. is utilizing Xen private cloud along with Aneka.

Page No.
Date

Business & Consumers

VVD

→ Applications

1. CRM → Salesforce.com, MS-Dynamic CRM
App. provide user with facilities for marketing, sales and advanced CRM.
2. Net suite → Net suite Global ERP, Net suit global CRM plus, " " " E-Commerce, Net suit Business OS → It consist of complete stack of tech. for building SaaS Business App.

Productivity Applications

1. Dropbox → Doc. storage service / folders based concept
2. iCloud → only sync with apple devices
3. Google Drive
4. Google Docs
5. Cloud Desktops → EyeOS, Xcerion XML Internet OS/3
6. Social Networking → Social graph of user is created where collection of interlinked interest is created.

Media Applications

1. Animoto → It creates videos out of images, music and video fragments submitted by user. Core func is imp. on top of Aws. S3 → storing pictures, videos
EC2 → webfront & workhorses
SQS → Connecting all the components

2. Maya Rendering with Arnold
Visualization of mechanical models is not used only at the end of the design but is used in a iterative way.
A private cloud is for rendering the 3rd design has been imp. by go front where the dept. is imp for designing decorations etc.

Page No.
Date

3. Video Encoding.

Encoding.com is a software sol. for video transcoding resources. (AWS and Rackspace)

transcoding

Multiplayer Online Game Playing

→ Prototype imp. of cloud based game log processing has been built by Xfire with using game log processing using Apache.