Week2

"Provisioning is the process of setting up IT infrastructure. Provisioning is not the same thing as configuration. Once something has been provisioned, the next step is configuration.

A cloud service consumer is Software programs or applications that programmatically interface with a cloud service’s through API. Any app that uses cloud service

Cloud administrator: provision IT resources. responsible for administering a cloud-based IT resource. It can be clous consumer, cloud provider or any 3rd party

Resilient/replication: Redundant resources within the same cloud, but in different physical locations (e.g. ASW or Multiple clouds (e.g. AWS and azure)

Cloud problems

Multitenancy: overlapping trust boundaries and data leaving premises can be a risk

Limited portability: vendor lockin and lack of standards and can bully govt

Difficult to identify where breach happened

A cluster is a collection of desktop computers or servers connected together by a local area network to act as a single larger computer  
A Warehouse Scale Computer (WSC) is a cluster comprised of tens of thousands of servers  
WSCs form the backbone of cloud infrastructure Contains 50,000 – 100,000 processors  
• A hierarchy of network connects, servers, racks and  
cells/arrays  
• A "rack" consists of ~48 servers connected to an ethernet  
switch, the switch connects to a cell  
• A cell/array consists of several racks, the racks in a cell are  
connected by an array switch

Cloud providers invest heavily in software development to automate their data centers. Ex-provisioning of resources, replication and fault recovery.

Network-Attached Storage (NAS) is a dedicated device or storage server that is connected to a computer network/cells/arrays. designed to provide centralized data storage, file sharing,

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Artifact Registry is the recommended service for container image storage and management on Google Cloud. Artifact Registry provides the same container management features as Container Registry and includes additional features and benefits. As a fully-managed service with support for both container images and non-container artifacts, Artifact Registry extends the capabilities of Container Registry.

K8s better because it gives flexibility to add containers in different nodes unlike docker compose.

**Week 5**

Why K8s

Load balancing: automatically route the user request to different nodes when demand is high

scaling

Storage orchestration: manage thousands of containers

Self healing: when pod dies it automatically generate new

Secret mngmt: allows to store secret and config in cluster

Kubernetes objects are persistent entities in the Kubernetes system. Kubernetes uses these entities to represent the state of your cluster. Specifically, they can describe: What containerized applications are running (and on which nodes) and resources available (desired state and its current state)

A diagram of a state

Description automatically generated

Week 6

Kubectl converts commands into api calls that goes to api server. It manipulates object like deleting and view

A screenshot of a computer

Description automatically generated

Current config: kubectl config view.

CrashLoopBackOff is a Kubernetes state representing a restart loop that is happening in a Pod: a container in the Pod is started, but crashes and is then restarted, over and over again

A screenshot of a computer

Description automatically generated

You can scale the Deployment manually

kubectl scale deployment [DEPLOYMENT\_NAME] --replicas=5

auto-sacle

kubectl autoscale deployment [DEPLOYMENT\_NAME] --min=5 --max=1

Session affinity ensures that all client requests are sent to the same Pod

Namespace divide resources of cluster between different users. Ex dev team, production team. Organize pods into groups. Applies at the cluster level

Labels are key/value pairs that are attached to objects such as Pods. Labels are intended to be used to specify identifying attributes of objects. Applies to individual objects, pods, services, etc.

Deployment is a 2 step process

Deployment controller will internally start Replica set controller to make replicas.

Deployment strategies:

Canary is a strategy which includes gradual increase/shift of traffic to newer pods version

Session affinity: when app depends upon a state of certain pod. ensures that requests from the same client are always routed to the same backend server in a load-balanced environment. By using session affinity, you can maintain session state and data consistency for clients.

A/b testing allows some users to use version 2 based on some conditions. After passing test we can route traffic to ver 2.

Shadow testing: use ver 1 prod server to test ver 2 mirrored server using original requests. Once ver 2 ready it can be used

A screenshot of a computer

Description automatically generated

Job unlike deployment will not restart the pod/container if operation is completed

Tag completion:3 means u want jobs to run in parallel

Manually scaling down the cluster will select nodes randomly

Auto scaling by default remove those pods which utilization<50 and move to other nodes

We can have 0 node in node pool but not 0 node pool in cluster. By default it will create 1

Helm is a package manager and management of applications in a Kubernetes cluster. It allows you to define, install, and upgrade even the most complex Kubernetes applications

chart is a collection of files that define a set of Kubernetes resources needed to run an application. It includes YAML files for services, deployments, pods,

ephemeral vol: not durable and depends on pod lifecycle. Pod dies volume dies.

Empty dir: created when a Pod is assigned to a node

pv : opp of ephemeral

**pv benefits:**

promotes microservice archi

gives abstraction b/w provisioned storage and actual storage

A screenshot of a computer

Description automatically generated

Pvc at cluster level while pv at pod level

Access levels of pv:

Readwriteonce: only 1 node

readOnlymany: m nodes

readWriteMany:

**Week 8**

A cloud deployment model represents a specific type of cloud environment, primarily  
distinguished by ownership, size and control access of the infrastructure and its location. The cloud delivery model defines how you will deliver your software, the cloud deployment model defines where you will deliver your software from

Public cloud: advantage: pay per use (low cost), 0 management and hardware

Disadvantages: Security, Organizations must trust cloud provider to deliver on their  
service level agreements

Pvt cloud: centralizing access to IT resources by different parts, locations, or departments of the organization.

Advantages: control, security, legacy systems, customization, data privacy

Disadvantages: cost, maintenance overhead, limited scalability

A VPN, which stands for virtual private network, establishes a digital connection between your computer and a remote server owned by a VPN provider, creating a point-to-point tunnel that encrypts your personal data, masks your IP address

A virtual private cloud is a segment of a public cloud using a secure connection(vpn). V PCs and VPNs are two essential components of cloud-based infrastructure that work together to provide secure and efficient access to resources. While VPCs create a private network within a public cloud environment, VPNs offer secure access to those resources remotely

Advantages: more secure than public,cheaper than pvt, same as public

Disadva: not a pvt cloud, problems of public

**Community cloud:** A community cloud is similar to a public cloud, except that its access is limited to a specific community of cloud consumers. The community cloud may be jointly owned by the community members or by a 3rd. A **community cloud** in [computing](https://en.wikipedia.org/wiki/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.  
party cloud provider that provisions a public cloud with limited access. Usually this means a data center that rents rack space to small companies, data center looks after power/internet availability, community member looks after their own servers/storage

Advantages: choose hardware and less cost than pvt cloud

Cons: sharing , same as public, do not get much advantages from both

Hybrid:   
A cloud consumer chooses to deploy cloud services processing sensitive data to a private cloud, and  
other, less sensitive cloud services to a public cloud

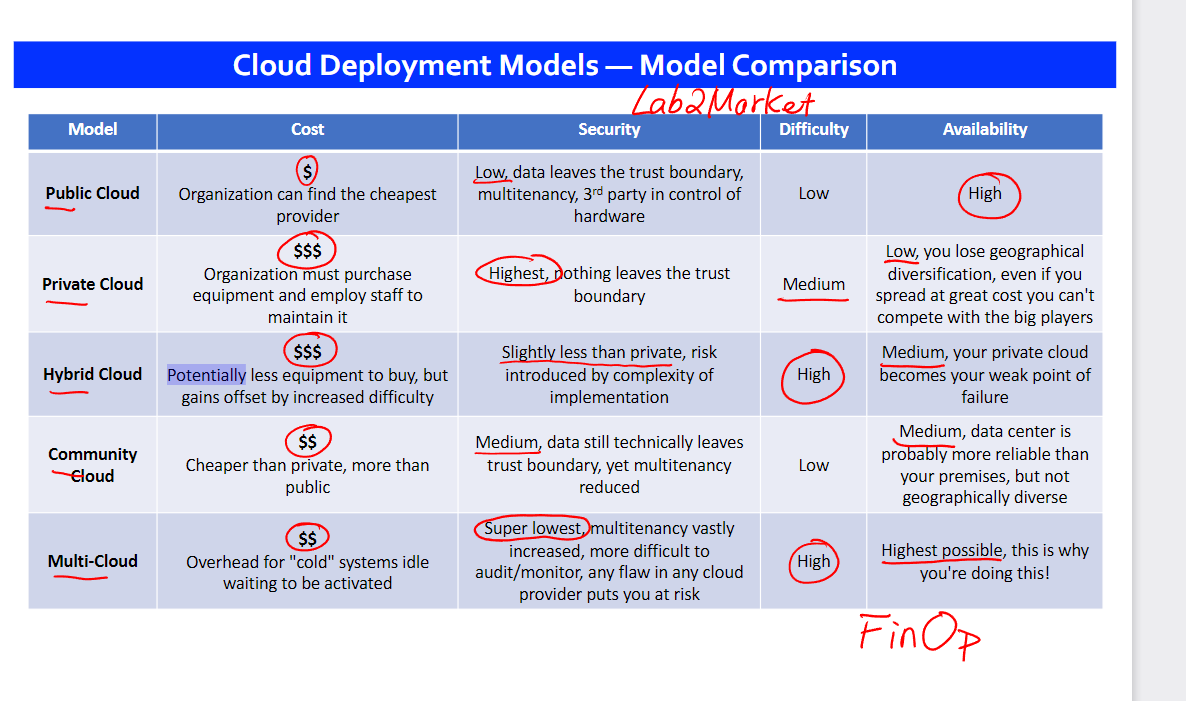
Pros: best of public and pvt

Cons: architecture overhead, complexity, risk of mistakes, expert needed

Multi cloud: more than 1 provider

Pros: highly available, no vendor lockin, best services

Cons: extra cost to store data on multiple provider, difficult to achieve, super lowest security



**Week 9**

release process for web/cloud apps

release planning, sprint begins, testing, staging and release

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

DevOps is important because it's a software development and operations approach that enables faster development of new products and easier maintenance of existing deployments.

Why devops needed?

provisioning  
complex architectures in the cloud adds complexity to our projects, especially in areas that affect deployment lead time. If we do not plan well and use dev ops practices then deployment lead time will grow and non efficiency and operational performance

3 ways of Devops

**A screenshot of a computer

Description automatically generated**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Automation in handoff to avoid dependency. Ex I only have access to prod db

A white paper with black text and red text

Description automatically generated

Week 9b see pdf

Week 10

Confidentiality: The characteristic of something being made accessible only to authorized parties." Within cloud environments, confidentiality primarily pertains to restricting access to  
data in transit and storage.

Integrity: The characteristic of not having been altered by an unauthorized party.” An important issue that concerns data integrity in the cloud is whether a cloud consumer can be guaranteed that the data it transmits to a cloud service matches the data received by that cloud service.

Authenticity: The characteristic of something having been provided by an authorized source. Authentication in non-repudiable interactions provides proof that these interactions are uniquely linked to an authorized source.

Availability: The characteristic of being accessible and usable during a specified time.

Threat: potential risk to harm the system and data privacy. Attack- execution of threat.

Vulnerability: A weakness that can be exploited either because it is protected by insufficient security controls, or because existing security controls are overcome by an attack. IT resource vulnerabilities can have a range of causes, including configuration deficiencies, security policy weaknesses, user errors, hardware or firmware flaws, software bugs, and poor security architecture.

Risk: The possibility of loss or harm arising from performing an activity. Risk is typically measured according to its threat level and the number of possible or known vulnerabilities.

2 metrics:

1. Probability of threat
2. Possibility of loss upon the IT resource being compromised.

Security Controls: Countermeasures used to prevent or respond to security threats and to reduce or avoid risk.

Security mechanism: Countermeasures are typically described in terms of security mechanisms. Defensive framework to protect it resources, data.

Security policies: set of rules and policies. Defines how rules and policies will be implemented. Includes the positioning and usage of security controls and mechanisms.

A diagram of security system

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Threat agents:

An Anonymous Attacker is a "non-trusted cloud service consumer without permissions in the cloud. Typically exists as an external software program that launches network-level attacks through public networks.

A malicious service agent is "able to intercept and forward the network traffic that flows within a cloud.

A trusted attacker "shares IT resources in the same cloud environment as the cloud consumer and  
attempts to exploit legitimate credentials to target cloud providers and the cloud tenants with whom they share IT resources.

Malicious insiders are "human threat agents Typically, current or former employees or third parties  
with access to the cloud provider's premises Carries tremendous damage potential as they may have administrative privileges for accessing cloud consumer IT resources

Week 12

Upfront code:

Up-front costs are associated with the initial investments that organizations need to make in order to fund the IT resources they intend to use. Purchase+deploy+administer cost.

On-going costs

represent the expenses required by an organization to run and maintain the IT resources. Licensing fee, electri, labour,bandwidth, insurance.

Cost of Capital: Making your initial purchase of the hardware required to host a modern webapp on-premise may require a loan, or investment, cost of capital is the cost of raising these funds

Sunk Costs: These are costs already paid for existing IT resources, a strong motivator to remain on-premise for as long as possible

Integration Costs: These are the costs required to transition from on- premise to in the cloud, another motivator to remaining on-premise

Locked-in Costs: Once you transition to the cloud you will build your systems specifically for one provider or another, this cost represents the cost of transferring (altering your architecture, from one cloud provider to another

Network usage: cost of transferring data over network

Separate for inbound and outbound. Different cost for different regions. 1gb, 0.001/gb upto 10 tb, then 0.002/gb

In clude traffic from organization top cloud and cloud service to customer.

A screenshot of a computer screen

Description automatically generated

See pdf