cc lab https://github.com/rvit-user/cloud

✅ Answers to Today’s Viva Questions

1. What are Cloud Service Providers (CSP)?
Cloud Service Providers are companies that offer cloud computing services such as infrastructure (IaaS), platform (PaaS), or software (SaaS) to users over the internet. Examples: AWS, Google Cloud, Microsoft Azure.

2. What is Docker?
Docker is a platform used to develop, ship, and run applications inside containers. Containers are lightweight, portable, and include everything needed to run the application, ensuring it works consistently across different environments.

3. What is ElastiCache?
ElastiCache is an AWS service that provides in-memory caching using Redis or Memcached. It helps reduce latency and improve performance for web applications by storing frequently accessed data closer to the application.

4. What is a VPN (Virtual Private Network)?
A VPN creates a secure, encrypted connection over the internet between your device and a private network. It is often used to access restricted resources securely and anonymously.

5. What is a Virtual Machine (VM)?
A Virtual Machine is a software emulation of a physical computer. It runs an operating system and applications just like a physical machine, but it's hosted on a physical server using a hypervisor.

6. How is VPN different from CloudShell?

- **VPN** is a secure tunnel to access private networks remotely.
- **CloudShell** is a browser-based command-line tool provided by cloud platforms (like Google Cloud or AWS) that allows you to manage cloud resources without installing anything locally.
  Key difference: VPN is for secure access to private networks; CloudShell is for managing cloud services through terminal access.

✅ Theory-Based Viva Questions & Answers

---

1. What are the different types of cloud deployment models?
There are **four main deployment models**:

- **Public Cloud**: Services are provided over the internet to multiple users. Example: AWS, Azure, GCP.
- **Private Cloud**: Used by a single organization, either hosted on-premises or by a third party.

- **Hybrid Cloud**: Combines public and private clouds, allowing data and apps to move between them.
- **Community Cloud**: Shared by several organizations with common goals or concerns (e.g., compliance, security).

---

2. What is a hypervisor? Explain its types.
A **hypervisor** is software that enables virtualization—it allows multiple virtual machines (VMs) to run on a single physical machine.

Types:

- **Type 1 (Bare Metal)**: Runs directly on the hardware. Example: VMware ESXi, Microsoft Hyper-V.
- **Type 2 (Hosted)**: Runs on a host OS like any other application. Example: VirtualBox, VMware Workstation.

---

3. Differentiate between IaaS, PaaS, and SaaS.

Model	Description	Example
IaaS	Infrastructure as a Service – offers virtual machines, storage, networks.	AWS EC2, GCP Compute Engine
PaaS	Platform as a Service – provides a platform for app development without managing infra.	Google App Engine, Heroku
SaaS	Software as a Service – provides software applications over the internet.	Gmail, Google Docs, Dropbox

---

4. What is virtualization and why is it important in cloud computing?
Virtualization is the creation of virtual versions of physical resources (e.g., VMs, storage, networks).
Importance:

- Efficient resource usage
- Isolation between users
- Scalability and flexibility
- Enables cloud service models (IaaS, PaaS)

---

5. What is the purpose of inter-cloud resource management?
Inter-cloud resource management ensures **efficient sharing and coordination of resources** between different cloud providers or multiple clouds within an organization.
Benefits:

- Avoid vendor lock-in
- Load balancing across clouds
- Cost optimization
- High availability and fault tolerance

---

6. Explain security risks associated with shared images in the cloud.
Shared VM images may contain:

- **Hardcoded credentials**
- **Sensitive data (e.g., API keys, passwords)**
- **Malware or vulnerabilities**
  These risks can lead to **data breaches** and **unauthorized access** if not properly cleaned before sharing.

---

7. What is XOAR and its relevance in cloud security?
XOAR (eXecutable Only Access Region) is a security mechanism that **restricts code execution to specific memory regions**, making it difficult for attackers to inject or modify code.
Used in **trusted hypervisors** to ensure VM isolation and OS-level protection.

---

8. Describe the architectural design of compute and storage clouds.

- **Compute Cloud**: Provides processing power using virtual machines, containers, etc. Managed by orchestration tools like Kubernetes or autoscaling engines.
- **Storage Cloud**: Provides scalable storage like object (e.g., S3), block (e.g., EBS), and file storage (e.g., NFS).
- **Design Considerations**:
  - Redundancy
  - Load balancing
  - Scalability
  - Security
  - APIs for access and automation