

Security In The Cloud

1-Resource Monitoring Techniques

Ans- **Resource Monitoring Techniques:**

- **Top/htop** – Monitor CPU, memory in real-time.
- **vmstat/iostat** – View system and disk performance.
- **Cloud Tools** – AWS CloudWatch, Azure Monitor, etc.
- **Grafana + Prometheus** – Advanced monitoring dashboards.

2-How to access compute (windows and Linux) from internet?
describe tools and its security

Ans- **Access Compute from Internet (Windows/Linux):**

- **Windows:**
 - Tool: **RDP (Remote Desktop Protocol)**
 - Port: **3389**
 - Secure with: **Strong password, firewall rules, VPN, MFA**
- **Linux:**
 - Tool: **SSH (Secure Shell)**
 - Port: **22**
 - Secure with: **SSH keys, disable root login, firewall, fail2ban**

3-Encryption Technologies and Methods

Ans- **Encryption Technologies and Methods:**

- **At Rest:** Encrypt data stored on disk (e.g., AES-256).

- **In Transit:** Use SSL/TLS for data over network.
- **End-to-End:** Encrypt data from sender to receiver.
- **Tools:** OpenSSL, GPG, BitLocker, LUKS.

4-Describe network security in cloud, compute security and storage security

Ans- **Security Types in Cloud:**

- **Network Security:**
 - Firewalls, VPCs, VPNs, security groups.
- **Compute Security:**
 - OS patching, antivirus, secure access (SSH/RDP), IAM roles.
- **Storage Security:**
 - Data encryption, access control, versioning, backup protection.