1. Resource Monitoring Techniques

Resource monitoring is used to track performance, usage, and health of cloud resources.

Common Monitoring Techniques

1. **CPU Monitoring**
   - Tracks CPU utilization and load
   - Helps detect performance bottlenecks
2. **Memory Monitoring**
   - Monitors RAM usage
   - Prevents application crashes
3. **Disk Monitoring**
   - Tracks disk usage, IOPS, and latency
   - Helps avoid storage overflow
4. **Network Monitoring**
   - Monitors bandwidth, latency, and packet loss
5. **Log Monitoring**
   - Collects system and application logs
   - Helps in troubleshooting and auditing
6. **Alerting and Notifications**
   - Sends alerts when thresholds are exceeded

Tools

- AWS CloudWatch
- Azure Monitor
- Google Cloud Monitoring

---

2. How to Access Compute (Windows and Linux) from the Internet – Tools and Security

Accessing Linux Compute

Tool: SSH (Secure Shell)

- Default Port: **22**
- Used for secure remote command-line access

Security Measures:

- Use key-based authentication
- Disable root login
- Restrict access using security groups/firewalls
- Use VPN where possible

Accessing Windows Compute

Tool: RDP (Remote Desktop Protocol)

- Default Port: **3389**
- Used for graphical remote access

Security Measures:

- Enable Network Level Authentication (NLA)
- Use strong passwords and MFA
- Restrict IP access
- Use VPN or Bastion host

Other Access Tools

- Bastion Host (Jump Server)
- Cloud Shell
- Web-based Console Access

---

3. Encryption Technologies and Methods

Encryption protects data by converting it into unreadable form.

Types of Encryption

Data at Rest

- Encrypts stored data (disk, database, backups)
- Technologies:
  - AES (Advanced Encryption Standard)
  - Disk encryption

Data in Transit

- Encrypts data during transmission

- Technologies:
    - SSL/TLS
    - HTTPS
    - VPN

Data in Use

- Encrypts data while being processed
- Uses secure enclaves and confidential computing

Encryption Methods

1. **Symmetric Encryption**
    - Same key for encryption and decryption
    - Fast and efficient
      Example: AES
2. **Asymmetric Encryption**
    - Uses public and private keys
      Example: RSA
3. **Hashing**
    - One-way encryption
    - Used for password storage
      Example: SHA-256

---

4. Cloud Security: Network, Compute, and Storage Security

A. Network Security in Cloud

Protects cloud networks from unauthorized access.

Techniques:

- Virtual Private Cloud (VPC)
- Firewalls / Security Groups
- Network ACLs
- VPN and Private Connectivity
- DDoS Protection

B. Compute Security

Protects virtual machines and workloads.

Techniques:

- OS hardening
- Patch management
- IAM and RBAC
- Anti-malware software
- MFA and secure login
- Regular vulnerability scanning

C. Storage Security

Protects stored data in the cloud.

Techniques:

- Encryption at rest
- Access control using IAM
- Backup and snapshots
- Versioning
- Secure deletion

Summary Table (For Exams)

Security Type	Key Techniques
Network	VPC, Firewall, VPN
Compute	OS hardening, IAM
Storage	Encryption, Backup