

**Hardware Networking**

**Resource Management and Security**

**SUBMITTED TO**

**KAMLESH SHUKLA SIR**

**SUBMITTED BY**

**MANAV BANDHANIA**

**1. Resource Monitoring Techniques**

Resource monitoring is crucial in cloud computing to track and optimize the performance of various resources like CPU, memory, storage, and network. Below are the main techniques used for resource monitoring:

**a. Agent-Based Monitoring**

* Involves installing a monitoring agent on cloud instances to collect metrics.
* Provides detailed insights into system performance.
* Examples:
  + Amazon CloudWatch Agent
  + Azure Monitor Agent
  + Prometheus (Open-source)

**b. Agentless Monitoring**

* Uses API calls to monitor resources without installing an agent.
* Less detailed but reduces resource overhead.
* Examples:
  + AWS CloudWatch Metrics
  + Azure Monitor

**c. Log-Based Monitoring**

* Analyzes system logs to detect performance issues and security threats.
* Examples:
  + AWS CloudTrail (for security logs)
  + Google Cloud Logging

**d. Network Monitoring**

* Tracks network traffic, latency, and potential security threats.
* Examples:
  + AWS VPC Flow Logs
  + Wireshark (Open-source network analyzer)

**e. Application Performance Monitoring (APM)**

* Focuses on application-level performance, including response times and errors.
* Examples:
  + New Relic
  + Datadog
  + AppDynamics

**f. Infrastructure Monitoring**

* Monitors the health of underlying cloud infrastructure (virtual machines, containers, storage, etc.).
* Examples:
  + Nagios
  + Zabbix

**2. How to Access Compute (Windows and Linux) from the Internet?**

**a. Accessing Windows Compute (VMs) from the Internet**

* **Remote Desktop Protocol (RDP):** Used to connect to Windows virtual machines remotely.
* **Tools:**
  + Microsoft Remote Desktop (Windows)
  + AnyDesk, TeamViewer (Third-party tools)
* **Security Measures:**
  + Use **strong passwords** and **multi-factor authentication (MFA)**.
  + Restrict RDP access using **firewall rules** (allow only specific IPs).
  + Use **RDP over VPN** instead of exposing it directly.
  + Enable **Network Level Authentication (NLA)** for secure login.

**b. Accessing Linux Compute (VMs) from the Internet**

* **Secure Shell (SSH):** Used to connect securely to Linux instances.
* **Tools:**
  + OpenSSH (Linux, macOS)
  + PuTTY (Windows)
  + Termius (Cross-platform)
* **Security Measures:**
  + Use **SSH key-based authentication** instead of passwords.
  + Restrict SSH access to **specific IPs** using security groups.
  + Disable root login (PermitRootLogin no in /etc/ssh/sshd\_config).
  + Change default SSH port (default is **22**) to a non-standard port.
  + Use **fail2ban** to block repeated failed login attempts.

**3. Encryption Technologies and Methods**

Encryption is a fundamental technique used to secure data in transit and at rest.

**a. Types of Encryption**

1. **Symmetric Encryption (Private Key Encryption)**
   * Uses the same key for encryption and decryption.
   * Fast but requires secure key distribution.
   * **Examples:** AES (Advanced Encryption Standard), DES, Blowfish
2. **Asymmetric Encryption (Public Key Encryption)**
   * Uses a public key for encryption and a private key for decryption.
   * More secure but slower than symmetric encryption.
   * **Examples:** RSA, ECC (Elliptic Curve Cryptography)
3. **Hashing**
   * Converts data into a fixed-size hash, which is irreversible.
   * Used for password storage and integrity verification.
   * **Examples:** SHA-256, MD5 (not recommended due to vulnerabilities)

**b. Encryption for Data at Rest**

* **Full Disk Encryption (FDE):** Encrypts the entire storage disk.
  + Examples: BitLocker (Windows), LUKS (Linux)
* **Database Encryption:** Protects sensitive database records.
  + Examples: Transparent Data Encryption (TDE) in SQL Server
* **Cloud Storage Encryption:** Encrypts stored data using AES-256.
  + Examples: AWS S3 Server-Side Encryption, Google Cloud KMS

**c. Encryption for Data in Transit**

* **TLS (Transport Layer Security):** Encrypts data between web servers and clients.
* **VPN (Virtual Private Network):** Encrypts network traffic over the internet.
* **SSH (Secure Shell):** Encrypts remote access connections.

**d. End-to-End Encryption (E2EE)**

* Ensures that only sender and receiver can read messages.
* Examples: Signal, WhatsApp

**4. Security in Cloud Computing**

**a. Network Security in Cloud**

Network security in the cloud protects communication between cloud resources and external networks.

**Techniques for Network Security:**

1. **Firewalls**
   * Control incoming and outgoing traffic.
   * Examples: AWS Security Groups, Azure NSGs
2. **Virtual Private Cloud (VPC)**
   * Creates an isolated network in the cloud.
   * Examples: AWS VPC, Google Cloud VPC
3. **DDoS Protection**
   * Mitigates Distributed Denial of Service (DDoS) attacks.
   * Examples: AWS Shield, Cloudflare
4. **Zero Trust Security**
   * Requires authentication for every request.
   * Example: Google BeyondCorp
5. **Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS)**
   * IDS detects threats; IPS prevents attacks.
   * Examples: Snort, AWS GuardDuty

**b. Compute Security**

Compute security focuses on protecting virtual machines and containers in the cloud.

**Best Practices:**

1. **Patch Management:** Regular updates for OS and applications.
2. **Least Privilege Principle:** Restrict permissions to the minimum necessary.
3. **Use Hardened OS Images:** Pre-secured images reduce vulnerabilities.
4. **Enable Logging & Monitoring:** Tools like AWS CloudTrail, Azure Monitor.
5. **Use Containers for Isolation:** Docker and Kubernetes improve security.

**c. Storage Security in Cloud**

Cloud storage security ensures data is protected from unauthorized access and corruption.

**Security Measures:**

1. **Encryption at Rest and In Transit:**
   * Encrypt stored data using AES-256.
   * Use TLS/SSL for data in transit.
2. **Access Control Policies:**
   * IAM policies to restrict access.
   * Example: AWS IAM, Google Cloud IAM.
3. **Versioning & Immutable Backups:**
   * Prevent accidental deletion or ransomware attacks.
   * Example: AWS S3 Object Versioning.
4. **Data Loss Prevention (DLP):**
   * Detects and prevents sensitive data leaks.
   * Example: Google Cloud DLP.
5. **Secure Erasure & Deletion Policies:**
   * Ensure proper data deletion using cryptographic erasure.