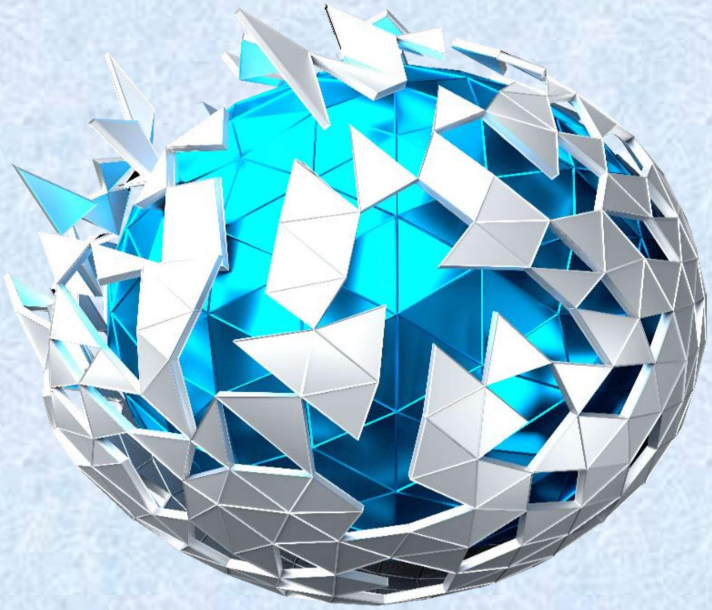
118699 Cloud Admin Knowledge EISA



118699 Cloud Admin Knowledge A

Question 1: Implement the Cloud Management Service (Marks 12)

1.1 Cloud Infrastructure and Cloud-Related Services (Marks 3)

StreamMedia Inc. is launching a video streaming platform (similar to YouTube) and expects 100,000 concurrent users immediately. They have identified four specific technical bottlenecks that standard web hosting cannot handle:

1. **Uploads:** Users upload raw 4K video files (up to 50GB each) which must be converted into 5 different formats (4K down to 360p). This process currently crashes their standard web servers.
2. **Global Latency:** Users in Asia and Europe report buffering because the servers are located in the US.
3. **Database Scale:** They expect millions of user comments and "likes" per hour, which is overwhelming their traditional SQL database.
4. **Recommendations:** They need to suggest new videos based on viewing history, which requires heavy mathematical processing.

Identify the specific infrastructure components required, focusing on the **Compute** types needed for video conversion vs. recommendations, and the **Network** components to solve the buffering issues.

1.2 Implementation of a Cloud Management Service (Marks 3)

MultiCloud Enterprises has acquired three smaller companies, resulting in a messy environment where they use three different cloud providers (Cloud A, Cloud B, and Cloud C). The CIO is facing a crisis:

- **Shadow IT:** Developers are using personal credit cards to spin up servers without permission.
- **Waste:** An audit found 50 servers that have been running for months with 0% CPU usage (orphan resources).
- **Security:** There is no central way to see which servers have open ports to the internet.

The CIO(Chief Technical Officer) wants to implement a **Cloud Management Platform (CMP)**. Explain how this platform would solve the specific problems of **Cost Visibility**, **Governance**, and **Provisioning**.

1.3 Resources (Marks 3)

GameDev Studios is launching a competitive multiplayer shooter game. The technical requirements are strict:

1. **The Match:** 100 players interact in a shared virtual world. If a player shoots, the server must calculate the physics in **less than 50ms**.
2. **The Lobby:** Players sit here while waiting for a match. Latency doesn't matter, but the system must handle thousands of idle connections cheaply.
3. **Matchmaking:** A background process that scans the player list to find players of similar skill levels. It runs sporadically (only when players join).
4. **Replays:** After a match, a video file is saved for players to watch later.

Determine the resources for these three distinct workloads. Specifically, justify why you would use **High-Performance Compute** for the Match but different resources for the Lobby and Replay storage.

1.4 Containerisation and Orchestration (Marks 3)

FinTech Solutions runs a mobile banking app. It is currently a **Monolithic Application** running on large Virtual Machines. They face two major operational issues:

1. **"The Update Nightmare":** To update just the "Login" feature, they have to restart the entire banking system, causing downtime for logged-in users.
2. **"It Works on My Machine":** Developers write code on Windows laptops, but the servers run Linux. Code often breaks in production because libraries are missing or different.

They want to move to **Containers** and **Orchestration (e.g., Kubernetes)**. Explain how this move solves these two specific problems.

Question 2. Monitor and Maintain Specific Elements of the Cloud (Marks 36)

2.1 Effective Server Maintenance and Optimisation (Marks 10)

GlobalLogistics runs a fleet of 200 Virtual Machines (VMs) that manage their trucking routes. They are facing a crisis because they have neglected maintenance for two years.

- **The Security Issue:** The VMs are running an operating system version that reached "End of Life" six months ago. They have not been patched because the Operations Manager is terrified that "rebooting for updates might crash the application."
- **The Performance Issue:** Drivers are complaining that the route app is crashing. An analysis shows the servers are constantly running at **99% RAM usage**, even though the CPU is only at 10%.
- **The Process Issue:** Currently, the team manually logs into each of the 200 servers once a month to clear out temporary files. This takes 40 hours of staff time.

The CTO(Chief Technical Officer) has tasked you with formulating a new strategy that handles **Patching**, **Right-Sizing**, and **Automation** without causing downtime.

2.2 Effective Storage Management Policies (Marks 10)

MediaArchive Corp stores 2 Petabytes (PB) of news footage. They pay a flat rate for "Standard Storage" (R0.30 per GB), resulting in a massive monthly bill. An analysis of their access logs shows a clear lifecycle:

1. **Breaking News (Days 0-30):** Footage is accessed constantly by editors. Speed is critical.
2. **Recent History (Days 31-90):** Footage is used occasionally for documentaries.
3. **Deep Archive (Day 90+):** Footage is almost never watched (maybe once a year) but must be kept for legal reasons.

Design a **Storage Lifecycle Policy** that moves data between specific tiers (Hot, Cool, Cold/Archive) based on these three timeframes to reduce the monthly bill by 65%.

2.3 Performance Characteristics of Storage (Marks 8)

ShopFast Inc. is experiencing website slowdowns. The DevOps team suspects the storage attached to the database is the bottleneck. Users report two different symptoms:

1. **Symptom A:** "The daily backup job takes 6 hours instead of 1, slowing down the whole system." (This job reads massive sequential files).
2. **Symptom B:** "During the Black Friday sale, the checkout page froze." (This involves thousands of tiny, random database writes per second).

Describe a monitoring strategy. Which specific metric would you track to diagnose Symptom A (**Throughput/Bandwidth**) versus Symptom B (**IOPS**)?

2.4 Cost Implications Related to Storage and Database Management (Marks 4)

StartupTech provides a SaaS platform. Their monthly bill is **R35,000**. The CFO wants to reduce this. The infrastructure audit reveals:

- **Storage Waste:** They host a 4K video background (200MB) on their homepage. 10,000 daily visitors download this file directly from the main server (High Egress Cost: R2.00/GB).
- **Database Waste:** They run a massive "Production-Size" database for their "Test" environment, which is only used by developers from 9 AM to 5 PM.

Calculate the current daily Data Transfer cost. Then, explain how implementing a **Content Delivery Network (CDN)**, **Auto-Scheduling** and **Caching policies** would drastically reduce this specific line items.

2.5 User Activity Through the Use of Logs (Marks 4)

SecureBank has a security policy that forbids "Shared Root Accounts," yet a recent incident revealed a database was deleted at 3 AM using the "root" login. There is no way to know *which* of the 5 admins did it.

Design a logging framework to ensure **Non-Repudiation** (proof of who did what) for future incidents.

Question 3. Maintain Security Protocols (Marks 12)

3.1 Compliance and Governance (Marks 3)

GlobalHealthcare is expanding to Europe. They collect patient data. A former patient, "Mr. Smith," has formally exercised his **GDPR "Right to be Forgotten."**

- **The Conflict:** Mr. Smith's data is in the active database, but also on 500 backup tapes stored in a vault. You cannot edit a backup tape without destroying it.
- **The Question:** How do you comply with the deletion request without destroying your disaster recovery backups?

Discuss the governance and technical challenges here. How do you ensure you are compliant with his deletion request without destroying the integrity of your backup?

3.2 Data Life Cycle Management (Marks 3)

InvestCorp is under investigation. Regulators demand all emails from 2020. The IT Manager worries that a rogue employee might have altered old emails to hide illegal activity.

Explain how using **WORM (Write Once, Read Many)** storage technology would have protected the company from this risk.

3.3 Security Vulnerabilities and Mitigation Strategies (Marks 3)

SaaS-App Inc. had a security audit that found three critical flaws:

1. **Vulnerability A:** The login page allows users to type code into the username box to bypass passwords (SQL Injection).
2. **Vulnerability B:** Database backups are stored in a public storage bucket.
3. **Vulnerability C:** Developers left "Secret Access Keys" hardcoded in the application text files.

For each flaw, provide the specific **Mitigation Strategy** (e.g., Input Validation/WAF, Encryption, Secrets Management).

3.4 Recovery Methods and Business Continuity (Marks 3)

GlobalFactory produces 500 cars a day.

- **The Constraint:** Downtime costs R100,000 per minute. They require **Zero Downtime**.
- **Current State:** They have a Disaster Recovery site that is "Active-Passive" (it sits cold and takes 4 hours to turn on).
- **The Problem:** A 4-hour recovery time costs R24 Million.

Explain the architecture required to achieve the Zero Downtime goal.

118699 Cloud Admin Practical A

Task 1

Section outline

- MetroTraffic Control is deploying a new traffic monitoring system for the city. They need a "Fog Node" (a compute instance) set up to collect data from street cameras. This node must be properly configured with network connectivity, storage partitions, and the ability to receive data feeds.

1.1: System & Network Setup

The Job: Deploy the primary data collection node for the traffic monitoring system.

Specifications Required:

- **Instance Name:** Traffic-Node-1
- **vCPU:** 1 core
- **Memory:** 2GB RAM
- **Boot Disk:** 15GB
- **Network:** Bridged Mode (or equivalent cloud networking that simulates connection to street sensor grid)

Your Tasks:

1. Create a compute instance/VM meeting the above specifications
2. Configure network adapter appropriately
3. Ensure the instance is running and accessible

Evidence to Submit:

- Screenshot from hypervisor/cloud console showing:
    - VM/instance name
    - Hardware specifications (CPU, RAM, Disk)
    - Network device configuration
    - Instance status (running)

1.2: Connectivity & Integration

The Job: The camera sensors require a fixed IP address to send data to. You must configure static networking and deploy a control panel interface.

Your Tasks:

1. Configure a static IP address inside the VM (use appropriate subnet: 10.0.0.50 or 192.168.x.50)
2. Install a lightweight web server (nginx or lighttpd) to act as the control panel

3. Verify the web server is accessible

Evidence to Submit:

- Screenshot of terminal showing static IP configuration (use ip addr or equivalent)

1.3: Storage Configuration

The Job: Video logs must be stored on a separate partition for performance and organisation reasons.

Your Tasks:

1. Add a second virtual disk (8GB) to your instance
2. Create a partition on the new disk
3. Format the partition as ext4
4. Mount it permanently to /var/traffic_logs

Evidence to Submit:

- Screenshot of df -h command showing:
    - The new mount point /var/traffic_logs
    - Approximately 8GB available space
    - Filesystem type

1.4: Functional Testing

The Job: Verify the node can accept data by creating test user accounts and log files.

Your Tasks:

1. Create a system user named camera_bot
2. Create a "dummy" log file named cam_feed_01.log inside /var/traffic_logs
3. Verify file permissions and ownership

Evidence to Submit:

- Screenshot of ls -l /var/traffic_logs showing:

    - The file cam_feed_01.log exists
    - File ownership and permissions visible

Task 2

Background

FragFest E-Sports is hosting a live online gaming tournament. The game server is experiencing performance issues (lag/rubber-banding) and storage problems due to massive replay files being saved from every match. Players are complaining and the tournament is at risk.

2.1: Resource Monitoring

The Job: Players are reporting "rubber-banding" (lag) during matches. You must identify whether the bottleneck is CPU, RAM, or Disk I/O.

Your Tasks:

1. Simulate system stress (use stress tools or I/O commands to generate load)
2. Use real-time monitoring tools to identify the bottleneck
3. Capture evidence of high resource utilization (>90% or equivalent)

Tools You May Use:

- Command-line: top, htop, iostat, vmstat, iotop
- Cloud console: CloudWatch, Azure Monitor, Cloud Monitoring
- Hypervisor: Built-in performance graphs

Evidence to Submit:

- Screenshot of monitoring tool showing high resource usage
- Metric clearly visible (e.g., "CPU Load: 98%" or "Disk I/O: 95%")
- Timestamp or duration visible

2.2: OS Maintenance

The Job: Tournament rules require the server to run the latest kernel patches to prevent known cheating exploits.

Your Tasks:

1. Check for available operating system updates
2. Identify kernel or security updates specifically
3. Document what needs updating (do NOT perform the actual upgrade during exam)

Evidence to Submit:

- Screenshot of command checking for updates

- Screenshot of apt list --upgradable (or equivalent) showing available kernel or security updates
- Output clearly shows package names and versions

2.3: Emergency Storage Expansion

The Job: CRITICAL: The "Replays" disk is at 99% capacity. If it reaches 100%, the tournament will stop automatically and FragFest will face penalties.

Current State:

- Replays disk: 12GB (99% full)
- Target: Expand to 25GB

Your Tasks:

1. Document current storage state
2. Increase virtual disk size to 25GB (using hypervisor or cloud console)
3. Expand the partition and resize the filesystem online
4. Verify expansion without data loss

Evidence to Submit:

- "BEFORE" screenshot: `df -h` showing 12GB limit and high usage
- Screenshot from hypervisor/cloud console showing disk resize operation
- "AFTER" screenshot: `df -h` showing 25GB capacity
- Command output showing partition/filesystem expansion steps

Task 3

Background:

Barrister & Associates, a prestigious law firm, stores sensitive client evidence on their server. They recently failed a security audit because their "Evidence Server" has multiple security vulnerabilities including weak file permissions, outdated software with known exploits, and open insecure ports.

3.1: Access Control Lists (ACLs)

The Job: The directory /home/evidence/case_files currently allows "read" access to the group "others" (everyone on the system). This violates attorney-client privilege and legal confidentiality requirements.

Current Permissions: rwxr-xr-x (755) **Required Permissions:** rwx------ (700)

Your Tasks:

1. Create the directory structure /home/evidence/case_files
2. Set initial permissions to demonstrate the violation
3. Change permissions so ONLY the root user can read/write/execute
4. Revoke ALL rights for "group" and "others"

Evidence to Submit:

- "BEFORE" screenshot: ls -l showing rwxr-xr-x permissions
- "AFTER" screenshot: ls -l showing rwx------ permissions
- Command history or terminal showing permission change command

3.2: Vulnerability Detection

The Job: The law firm uses an FTP server to transfer case files between attorneys and the office.

Simulated Environment Data:

- Service: ProFTPD
- Version: 1.3.3c

Your Tasks:

1. Search public vulnerability databases for "ProFTPD 1.3.3c"
2. Identify the critical vulnerability associated with this version
3. Note the CVE ID (if applicable) and severity

Resources You May Use:

- https://nvd.nist.gov (National Vulnerability Database)
- https://www.exploit-db.com
- https://cve.mitre.org

Evidence to Submit:

- Screenshot of vulnerability database search results
- The vulnerability name clearly visible (e.g., "ProFTPD 1.3.3c Backdoor Command Execution")
- CVE ID or severity rating visible
- URL visible in browser

3.3: Remediation Recommendations

The Job: The law firm partners need professional advice on how to secure their file transfer method immediately.

Your Tasks: Create a security memorandum that includes:

1. Brief description of the vulnerability and its risk
2. Immediate remediation action (within 24 hours)
3. Long-term security recommendation
4. Verification steps

Evidence to Submit:

- Text file named security_memo.txt
- Screenshot of file contents using cat security_memo.txt or text editor
- Memo must include all required sections

3.4: Port Hardening

The Job: The vulnerable FTP service is currently accessible from the internet on its standard port. You must close this attack vector.

Your Tasks:

1. Identify the standard FTP port number
2. Configure the system firewall to DENY all traffic on the FTP port
3. Verify the firewall rule is active and enforced
4. Ensure other essential services (like SSH) remain accessible

Evidence to Submit:

- Screenshot showing open ports BEFORE firewall configuration
- Screenshot of firewall status showing the DENY rule for Port 21
- Command output showing rule number and status (e.g., ufw status numbered)

- Verification that SSH (Port 22) remains accessible

MICTSETA | Media, Information And Communication Technologies Sector Education And Training Authority

SHAPING SKILLS, PIONEERING INDUSTRIES, EMPOWERING FUTURES