MICTSETA

118699 CLOUD ADMINISTRATOR

EISA - MEMO

PRACTICAL

Cloud Administration Practical Exam - Student Scenarios

Scenario 1: The Smart City Project (Cloud Implementation & Deployment)
Marks: 20 points | Time Allocation: 60 minutes

Background
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.

Reference
Table Section 1.1 (Build & Deploy)

1.1: System & Network Setup
Scenario: 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)

Assessment Criteria:

- Instance created with correct specifications
- Network properly configured
- Evidence is clear and complete

1.2: Connectivity & Integration
Scenario: 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)
- Screenshot of web browser showing the default web server page (e.g., "Welcome to Nginx")

Assessment Criteria:

- Static IP correctly configured
- Web server installed and running
- Both pieces of evidence clear

1.3: Storage Configuration
Scenario: Video logs must be stored on a separate partition for performance and organization 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

Assessment Criteria:

- Disk added and partitioned correctly
- Formatted as ext4
- Mounted to correct location
- Evidence shows all requirements

1.4: Functional Testing
Scenario: 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

Assessment Criteria:

- User camera_bot created correctly
- Log file created in correct location
- Evidence is clear

Scenario 2: The Gaming Tournament (Cloud Maintenance & Monitoring)
Marks: 60 points | Time Allocation: 60 minutes

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.

Reference
Table Section 2.1 - 2.2 (Monitor, Update, Expand)

2.1: Resource Monitoring
Scenario: 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

Assessment Criteria:

- Stress/load successfully generated
- Appropriate monitoring tool used
- Bottleneck clearly identified
- Evidence quality

2.2: OS Maintenance
Scenario: 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

Assessment Criteria:

- Update check performed correctly
- Kernel/security updates identified
- Evidence is complete and readable

2.3: Emergency Storage Expansion
Scenario: 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

Assessment Criteria:

- Initial state documented
- Disk resized in hypervisor/cloud
- Filesystem expanded within OS
- No data loss, evidence sequential

Scenario 3: The Law Firm (Cloud Security & Compliance)
Marks: 20 points | Time Allocation: 60 minutes

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.

Reference
Table Section 3.1 (Security & Vulnerabilities)

3.1: Access Control Lists (ACLs)
Scenario: 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

Assessment Criteria:

- Before state properly demonstrated
- Permissions correctly changed to 700
- Evidence clearly shows both states

3.2: Vulnerability Detection
Scenario: 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

Assessment Criteria:

- Correct vulnerability identified
- Appropriate database used
- Screenshot quality and completeness

3.3: Remediation Recommendations
Scenario: 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

Assessment Criteria:

- Vulnerability risk properly explained

- Immediate actions are practical
- Long-term recommendations sound
- Professional presentation

3.4: Port Hardening
Scenario: 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

Assessment Criteria:

- FTP port correctly identified
- Firewall rule configured correctly
- Rule verification shown
- SSH access maintained

General Submission Requirements

File Naming Convention
[StudentID]_Scenario1_Task1.1.1_SystemSetup.png
[StudentID]_Scenario1_Task1.1.2_StaticIP.png
[StudentID]_Scenario1_Task1.1.2_WebServer.png
[StudentID]_Scenario1_Task1.1.3_Storage.png
[StudentID]_Scenario1_Task1.1.4_Testing.png
[StudentID]_Scenario2_Task2.1.1_Monitoring.png
[StudentID]_Scenario2_Task2.2.2_Updates.png
[StudentID]_Scenario2_Task2.2.3_Storage_Before.png
[StudentID]_Scenario2_Task2.2.3_Storage_After.png
[StudentID]_Scenario3_Task3.1.1_Permissions_Before.png
[StudentID]_Scenario3_Task3.1.1_Permissions_After.png

[StudentID]_Scenario3_Task3.1.2_Vulnerability.png
[StudentID]_Scenario3_Task3.1.3_Memo.txt
[StudentID]_Scenario3_Task3.1.4_Firewall.png

Screenshot Requirements
All screenshots must include:

- Visible timestamp or date
- Your username or session identifier
- Full command output (not truncated)
- Clear, readable text (minimum 12pt equivalent)
- Terminal prompt visible (showing working directory when relevant)

Text File Requirements

- Plain text format (.txt)
- UTF-8 encoding
- Professional formatting
- Include your student ID in the header

Post-Exam Cleanup

If Using Cloud Resources:
MANDATORY - Delete all resources to avoid ongoing charges:

- Terminate/delete all compute instances
- Delete unattached storage volumes/disks
- Remove cloud storage buckets (if created)
- Verify in billing dashboard: $0.00 ongoing costs

If Using Local Hypervisor:

- Shut down VMs (optional: delete if instructed)
- Note: You may keep VMs for practice if using personal equipment

Grading Rubric Summary

Time Management Recommendation

Scenario	Recommended Time	Buffer
Scenario 1 (Implementation)	40 minutes	+5 min
Scenario 2 (Maintenance)	40 minutes	+5 min
Scenario 3 (Security)	40 minutes	+5 min
Documentation & Review	15 minutes	Buffer

Cloud Administration Practical Exam Rubric	VM created with exact specs (1 vCPU, 2GB RAM, 15GB disk); network in Bridged Mode; instance running; all evidence clear.	VM created but with minor spec deviations; network active; evidence provided but slightly unclear.	Failed to meet hardware specs or network requirements; insufficient evidence of running state.
	Static IP (10.0.0.50 or 192.168.x.50) correctly set; Nginx/Lighttpd running and accessible via browser.	Static IP set but in wrong subnet; web server running but browser verification missing.	Networking remains dynamic; web server not installed or failing to serve pages.
Total Marks: 20 | Focus: VM Deployment, Networking, and Storage	8GB disk added, partitioned, formatted as ext4, and permanently mounted to /var/traffic_logs.	Disk added and mounted, but missing permanent configuration or incorrect filesystem type.	Secondary disk not detected or mounted to the wrong directory.
	camera_bot user created; cam_feed_01.log exists in the new mount with correct ownership/permissions.	Log file created but in the root partition; user created but permissions are incorrect.	Failed to create system user or generate test log files.
Task	Exemplary (Full Marks)	Proficient	Beginning
1.1.1 System Setup	VM created with exact specs (1 vCPU, 2GB RAM, 15GB disk); network in Bridged Mode; instance running; all evidence clear.	VM created but with minor spec deviations; network active; evidence provided but slightly unclear.	Failed to meet hardware specs or network requirements; insufficient evidence of running state.
1.1.2 Connectivity	Static IP (10.0.0.50 or 192.168.x.50) correctly set; Nginx/Lighttpd running and accessible via browser.	Static IP set but in wrong subnet; web server running but browser verification missing.	Networking remains dynamic; web server not installed or failing to serve pages.
1.1.3 Storage	8GB disk added, partitioned, formatted as ext4, and permanently mounted to /var/traffic_logs.	Disk added and mounted, but missing permanent configuration or incorrect filesystem type.	Secondary disk not detected or mounted to the wrong directory.
1.1.4 Testing	camera_bot user created; cam_feed_01.log exists in the new mount with correct ownership/permissions.	Log file created but in the root partition; user created but permissions are incorrect.	Failed to create system user or generate test log files.

Cloud Administration Practical Exam Rubric	VM created with exact specs (1 vCPU, 2GB RAM, 15GB disk); network in Bridged Mode; instance running; all evidence clear.	VM created but with minor spec deviations; network active; evidence provided but slightly unclear.	Failed to meet hardware specs or network requirements; insufficient evidence of running state.
Scenario 2: The Gaming Tournament (Maintenance & Monitoring)			
Total Marks: 60 | Focus: Performance Diagnosis and Resource Scaling			
Task	Exemplary (Full Marks)	Proficient	Beginning
2.1.1 Monitoring	Stress successfully generated; bottleneck correctly identified using tools like htop or iostat (>90% load shown).	System stress attempted but load is low; tool used but bottleneck identification is vague.	Monitoring tool used incorrectly; no evidence of high resource utilization captured.
2.2.2 Maintenance	OS update check performed; specifically identified kernel or security patches; detailed documentation provided.	General update check performed but failed to highlight critical security or kernel packages.	Failed to check for updates or provide a list of upgradable packages.
2.2.3 Storage Expansion	Sequential evidence showing 12GB (Before) -> Resize in Hypervisor -> Resize in OS -> 25GB (After) with no data loss.	Disk resized in hypervisor but student struggled to expand the partition/filesystem within the OS.	No "Before" documentation; failed to expand filesystem; evidence is non-sequential or missing.
Scenario 3: The Law Firm (Security & Compliance)			
Total Marks: 20 | Focus: Hardening, Vulnerability Research, and Firewalls			
Task	Exemplary (Full Marks)	Proficient	Beginning

Cloud Administration Practical Exam Rubric	VM created with exact specs (1 vCPU, 2GB RAM, 15GB disk); network in Bridged Mode; instance running; all evidence clear.	VM created but with minor spec deviations; network active; evidence provided but slightly unclear.	Failed to meet hardware specs or network requirements; insufficient evidence of running state.
3.1.1 Access Control	Permissions explicitly changed from 755 to 700; verified that only root has access; before/after evidence clear.	Permissions changed but not to the exact 700 requirement; evidence only shows final state.	Directory permissions remain insecure (others still have read/execute access).
3.1.2 Vulnerability	Correctly identified ProFTPD 1.3.3c Backdoor; cited CVE ID and severity from an appropriate database.	Identified a vulnerability for ProFTPD but not the specific version-related exploit.	Search results are irrelevant or for the wrong software version.
3.1.3 Remediation	Professional memo includes risk description, 24-hour action, long-term fix, and verification steps.	Remediation plan provided but lacks professional formatting or misses long-term recommendations.	Memo is incomplete or provides technically unsound security advice.
3.1.4 Port Hardening	Port 21 correctly identified and blocked via firewall; SSH (Port 22) remains active; rule verified via status command.	Port 21 blocked but student inadvertently blocked SSH access or failed to verify the rule.	Wrong port identified; firewall remains inactive or open to the internet.

General Submission & Professionalism (Deduction Criteria)

File Naming: Files must follow the [StudentID]_Scenario_Task convention.

Screenshot Quality: Must include timestamps, visible usernames, and full command prompts.

Cloud Hygiene: Failure to terminate resources after the exam may result in administrative penalties.

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

SHAPING SKILLS, PIONEERING INDUSTRIES, EMPOWERING FUTURES