

	behaviors are identified through monitoring tools. 5.4 Alerts and notifications are configured to respond to security incidents in real time. 5.5 Security performance metrics (failed login attempts, privilege escalations, access trends) are analyzed regularly. 5.6 Incident response procedures are followed to mitigate identified threats and vulnerabilities. 5.7 Monitoring reports are generated and documented in line with organizational and regulatory compliance requirements.
6. Manage database backups	6.1 Backup requirements (frequency, type, retention period) are determined according to organizational and regulatory policies. 6.2 Appropriate backup methods (full, incremental, differential, snapshot) are selected based on database size and criticality. 6.3 Automated backup schedules are configured using DBMS tools or third-party software. 6.4 Backup files are secured through encryption and access controls to prevent unauthorized access. 6.5 Backup storage locations (onsite, offsite, cloud) are managed to ensure data availability and disaster recovery readiness. 6.6 Test restorations are performed periodically to validate the integrity and reliability of backup data. 6.7 Backup and recovery procedures are documented and updated in accordance with organizational standards.

RANGE

This section provides work environments and conditions to which the performance criteria apply. It allows for different work environments and situations that will affect performance.

Variable	Range
Database management system may include but not limited to:	• MySQL workbench CE, MS SQL server, • MySQL Database
Database Monitoring tools may include but not limited to:	• Nagios • Solar winds Database Performance analyzer • Amason cloud watch • Azure Monitor

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Analytical skills
- Requirements analysis
- Data modeling
- Database Schema implementation
- SQL Programming skills
- Security configuration
- System administration
- Disaster recovery
- Monitoring and auditing
- Incident response

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:

- Communications (verbal and written);
- Proficient in digital literacy
- Time management;
- Analytical
- Faults troubleshooting
- Problem solving;
- Planning;
- Decision making;
- Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects of Competency	1.1 Document for database needs was outlined as per organizational requirements for data storage, access, and security. 1.2 Evaluation matrix of DBMS options such as MySQL, Oracle
-----------------------------------	--

	was mapped against organizational/security needs. 1.3 Requirements document from user interviews, surveys, or organizational was established as per policy analysis. 1.4 ERDs are outlined according to identifying entities, attributes, and relationships. 1.5 SQL scripts or schema files outlined based on definition of tables, fields, and relationships. 1.6 SQL code showing primary keys, foreign keys, and constraints outlined as per organizational/security needs. 1.7 Document for authentication configuration were outlined in line with organizational requirements (password policies, MFA). 1.8 Roles and access privileges were assigned and documented according to the principle of least privilege. 1.9 Security patches and updates were applied and recorded in accordance with vendor and organizational policies. 1.10 Backup files were secured with encryption and access controls, and the measures were documented. 1.11 Backup storage management (onsite, offsite, cloud) was outlined to ensure disaster recovery readiness.
2. Resource Implications for competent certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Practical demonstration 3.3 Projects 3.4 Observation
4. Context of Assessment	Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

assessment	
------------	--

INSTALL AND CONFIGURE LINUX

TVET CDACC UNIT CODE: SEC/OS/CS/CR/05/5/MA

UNIT DESCRIPTION

This unit covers the competencies required for installing, configuring, and administering a Linux operating system. It entails mastering the Linux command line, managing file systems and storage, and handling software package management. Additionally, it includes managing system services, users, and groups to ensure efficient system operation. Trainees will also gain expertise in network management, configuring critical server roles, and implementing security measures to safeguard the Linux operating while reinforcing best practices in system administration.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT	PERFORMANCE CRITERIA
These describe the key outcomes which make up workplace function.	These are assessable statements which specify the required level of performance for each of the elements <i>(Bold and italicised terms are elaborated in the Range)</i>
1. Install and configure Linux Operating System	1.1 The Linux OS is installed successfully on the target machine with no critical installation errors. 1.2 System settings (hostname, timezone, locale, keyboard layout) are configured according to project specifications within upon completion of installation 1.3 The system boots correctly into the login screen without requiring reinstallation.
2. Execute Linux Commands in the terminal	2.1 At least basic and advanced Linux commands for concepts such as file navigation, search, permissions, process control, network configuration) are executed successfully without syntax errors. 2.2 Command output matches the expected result 100% of the time during assessment. 2.3 Terminal commands are executed using shortest valid syntax where possible, demonstrating efficiency.

3. Manage File Systems and Storage	3.1 Disk partitions are created, mounted, with no mounting errors. 3.2 File systems for example ext4, XFS are formatted and verified using fsck or equivalent tools. 3.3 Storage space usage is monitored and reported, with alerts configured when usage exceeds 90% capacity.
4. Administer Users and Groups	4.1 New user and group accounts are created with correct home directories, default shells, and permissions on the first attempt. 4.2 User passwords are set to meet defined security policies (minimum length, complexity, expiry). 4.3 Group memberships are correctly assigned and verified using id or equivalent commands.
5. Manage System Services and Software Packages	5.1 Services are enabled, started, stopped, and restarted using systemctl with no service failures. 5.2 Software packages are installed, updated, and removed using the distribution's package manager without dependency errors. 5.3 Service startup behavior is configured correctly (enabled or disabled) according to project requirements.
6. Configure Network Settings and Server Roles	6.1 IP addresses (static or DHCP) are configured and verified with successful ping tests to local and external hosts. 6.2 Hostname resolution and DNS settings are tested and confirmed to work. 6.3 At least one server role (e.g., web server, file server, SSH) is configured and verified as operational from a remote client.
7. Implement Linux Security Measures	7.1 File and directory permissions are set according to the principle of least privilege. 7.2 Firewall rules are configured to allow only approved services, verified by appropriate scanning tools.

	7.3 Security updates and patches are applied within 24 hours of availability.
8. Apply Best Practices in Linux System Administration	8.1 System logs are monitored, rotated, and stored according to retention policies. 8.2 Resource usage (CPU, memory, disk, network) is monitored using tools like top, htop, or vmstat, with reports generated weekly. 8.3 Documentation of system configuration changes is updated immediately after each change.

RANGE

This section provides work environment and conditions to which the performance criteria apply. It allows for different work environment and situations that will affect performance.

Variable	Range
Linux distributions include but not limited to:	• Ubuntu • CentOS • Debian • Fedora • Mint
Platform usage includes but not limited to:	• Oracle Virtual Box • VMware Workstation. • Bare Metal

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Installing Linux on VMware, VirtualBox, or bare metal
- Configuring partitions and mounting points during installation
- Applying updates and initial configurations after installation
- Managing permissions and ownership with chmod, chown, and usermod
- Implementing SSH key-based authentication
- Removing software packages
- Applying firewall configurations

- Installing and configuring IDS/IPS tools
- Monitoring logs for suspicious activity
- Applying security updates automatically

FOUNDATION SKILLS

The individual needs to demonstrate the following foundation skills:

- Communications (verbal and written);
- Time management;
- Problem solving;
- Planning;
- Decision making;
- Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1 Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Installed the Linux operating system successfully on the target machine without critical installation errors. 1.2 Executed Linux commands for file navigation, search, permissions, process control, and network configuration without syntax errors. 1.3 Monitored and configured alerts for reported storage usage. 1.4 Created user and group accounts with correct home directories, default shells, and permissions on the first attempt. 1.5 Configured service startup behaviour according to project requirements. 1.6 Tested and confirmed hostname resolution and other settings such as DHCP and DNS 1.7 Applied security updates and patches. 1.8 Monitored CPU, memory, disk, and network usage using tools like top, htop, or vmstat, generating weekly reports.
---	--