**Project Title: Linux Admin Toolkit CLI**

**Description:**

A powerful Bash-based toolkit designed for Linux system administrators to manage daily tasks such as health checks, backups, package updates, and service restarts. It supports GitOps-style version control and runs in both native and containerized environments.

**Goal**

To develop a modular, powerful, and extensible command-line toolkit for Linux system administration. It should automate tasks like health monitoring, auditing, compliance tracking, system optimization, backup, and logging, with support for GitOps-style logging and optional TUI (Text-based User Interface).

**In Scope**

* System monitoring and reporting (CPU, memory, disk, network)
* User and group audits
* Log rotation and cleanup
* Docker container inspection
* Firewall and network diagnostics
* GitOps-style audit logging
* JSON-based config handling
* Optional TUI frontend for ease of use

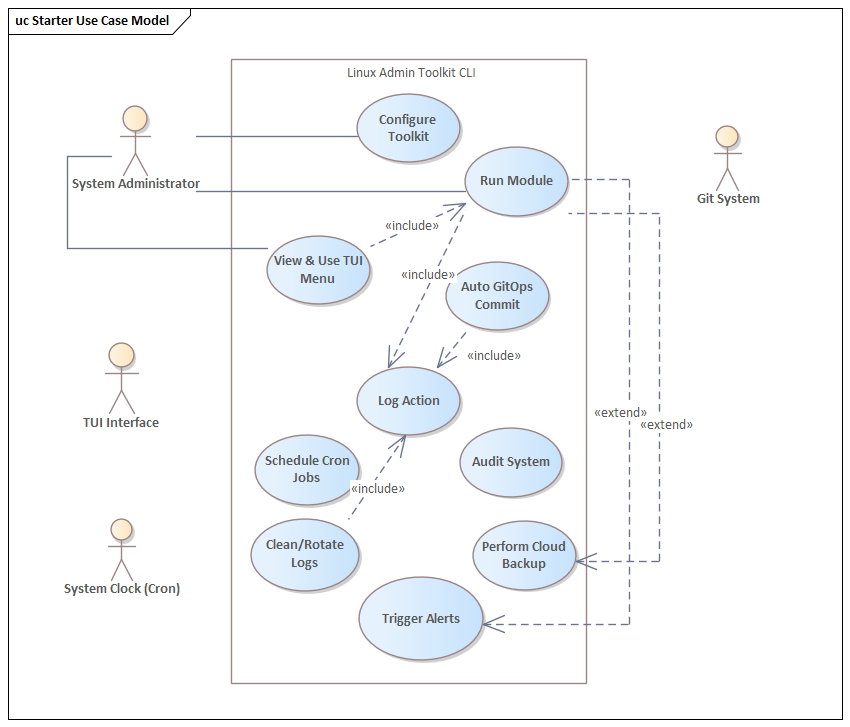
**Functional Features**

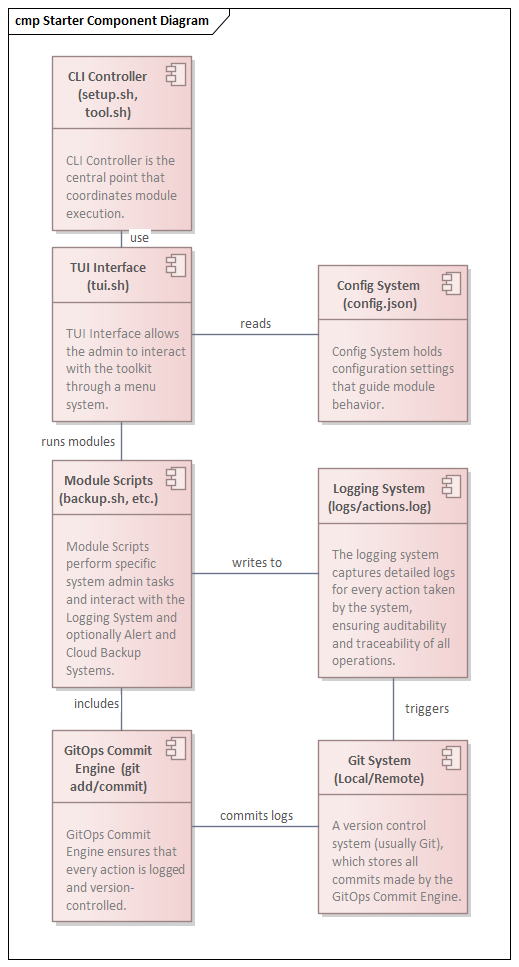
|  |  |
| --- | --- |
| Feature | Description |
| Modular Scripts | Scripts perform specific tasks independently (e.g., backups, audits). |
| GitOps Logging | Logs every action using git add and git commit for tracking changes. |
| System Monitoring | Monitors system health, uptime, CPU load, memory usage, disk usage, and more. |
| User Audits | Analyzes users, groups, sudo access, and file permissions. |
| Firewall Audit | Displays and verifies current firewall settings. |
| Package Manager Integration | Supports various Linux package managers (apt, yum, dnf, zypper). |
| Log Cleaner | Removes old logs based on age or pattern for efficient log management. |
| Configurable Expiry Checks | Monitors expiry dates for SSL certificates, licenses, and important documents. |
| Docker Monitoring | Monitors Docker container resource usage (CPU, memory, network). |
| Network Diagnostics | Runs diagnostics like ping, traceroute, and DNS tests. |
| Optional TUI | Provides an interactive terminal UI for users using dialog, whiptail, or fzf. |

**Non-Functional Requirements (NFR)**

|  |  |
| --- | --- |
| NFR | Description |
| Performance | Modules should execute within 1 second for small tasks. |
| Portability | Works across major Linux distros (Ubuntu, CentOS, Debian, etc.). |
| Testability | Each module should be testable in isolation for unit testing. |
| Security | Sensitive information (e.g., passwords, tokens) should never be logged. |
| Maintainability | Code should be clean and easy to extend with new features. |
| Minimal Dependencies | The toolkit should rely on native bash and core utils (no external dependencies). |
| Logging | All actions performed by the toolkit should be logged for audit purposes. |
| Extensibility | New modules should be easy to add to the system. |
| CI-Friendly | Designed to integrate with CI pipelines for automation. |

**Use Case Model for Linux Admin Toolkit CLI**

****

****