1. Package Repository Security Mechanisms
Package repositories use:
- Digital signatures: Packages are signed with GPG keys. The system verifies signatures against trusted keys.
- Checksums: Hashes (SHA-256) ensure package integrity.
- HTTPS: Encrypted connections prevent MITM attacks.
- Key rotation: Expired/compromised keys are revoked.

2. Ubuntu Repository Components

Component	Description
`main`	Officially supported, open-source software.
`restricted`	Proprietary drivers (e.g., GPU).
`universe`	Community-maintained open-source software.
`multiverse`	Non-free software with legal restrictions.
`updates`	Stable updates for `main`/`restricted`.
`security`	Critical security patches.
`backports`	Newer software versions (not officially supported).

3. KVM vs QEMU
- KVM: Kernel module that turns Linux into a hypervisor (requires CPU virtualization support).
- QEMU: Emulates hardware (slower, works without virtualization).
- qemu-kvm: QEMU with KVM acceleration for near-native performance.

4. VM vs Container Recommendations

Scenario	Recommendation	Why
Database with heavy disk writes	VM	Better I/O isolation and direct disk access.
Stateless web app	Container	Lightweight, fast scaling.
Monolithic app with high resources	VM	Dedicated resources.
Hardware driver needed	VM	Direct hardware access.
GUI applications	VM	Better GPU passthrough.
Boot-dependent services	VM	Full OS initialization.
Custom kernel modules	VM	Kernel-level access.

| Lightweight programs | Container | Low overhead.
|
| Process interaction | VM | Stronger isolation between processes.
|

5. Hashing vs Encryption
- Hashing: One-way function (e.g., SHA-256). Used for integrity checks (cannot reverse).
- Encryption: Two-way function (e.g., AES). Secures data (can decrypt with key).

6. Detect File Changes with Checksums
Run this in the directory:
sha256sum *.conf > checksums.txt # Generate checksums
sha256sum -c checksums.txt # Verify later

- Single-character changes will alter the hash and trigger warnings.