Roberto Myftaraga

Senior project report 5

10/19/2025

Docker Based Container Engine: Process, Resource, and Filesystem Isolation

Week 5, this has been the hardest week so far. I underestimated how hard it would be to connect the code and to refine it the way it handles process and filesystem isolation using Linux namespaces and chroot. After removing cgroup functionality from the previous version, I concentrated on making the program easier to understand, more modular, and user-friendly for future improvements.

I restructured the codebase into three clear files: main.cpp, container.cpp, and namespace_manager.cpp. The main module now handles command-line input and execution flow. The container module manages the setup and teardown of isolated environments, including creating temporary root filesystems (rootfs) under /**containers**/.The namespace manager focuses exclusively on system calls such as unshare, chroot, and mount, ensuring the container process runs in its own UTS, PID, IPC, and mount namespaces.

A major addition this week was the creation of a reusable **base rootfs** built from essential host directories (/bin, /lib, /usr, /etc). Each time a new container runs, the base is copied into a new subdirectory (e.g., /containers/program_1234/), giving every instance a clean filesystem. I also mounted minimal filesystems (/proc, /dev, /tmp) inside the container to allow programs to access process information, temporary files, and device nodes without exposing the host's environment.

The program first checks if the base root filesystem (base_rootfs) already exists. If not, it builds it by copying core system folders like /bin, /lib, and /etc. Then it creates a new run directory for the specific program, copies the base rootfs into it, and places the user's program inside.

As of right now the program is partially functional. I was not able to get it working. I need to lay out the code layout a little better for me to understand how I can get this working in the best way possible. I read a lot of source and most of them guided me on how to structure and use these function and linux namespaces :

https://docs.docker.com/engine/storage/drivers/

https://man7.org/linux/man-pages/man2/unshare.2.html

https://man7.org/linux/man-pages/man2/chroot.2.html

https://man7.org/linux/man-pages/man2/mount.2.html

https://github.com/lizrice/containers-from-scratch/blob/master/main.go