Homework Four

Due Date and Time: 11:55 PM, Sunday, December 08, 2019

The goal of this homework is to gain an understanding of how OS level virtualization tools are built and get some hands-on experience with using Linux cgroups and namespaces.

You may work in teams of size two students.

Implement a system tool that provides support for a scaled down version of Linux containers called capsules. Input to this tool is a zipfile provided by the user. When launched, this tool will create a capsule, which is an isolated virtualized computing environment containing the directory zipped in the input zipfile as well as all files and libraries needed to run a shell (e.g. *bash*) and *ls* command, and start that shell in this capsule. The zipfile provided by the user contains one or more executable binaries along with all the libraries needed to run those binaries. Your tool should enforce the following limits on all process running with in a capsule:

(1) Processes cannot access any files or directories other the ones in the input zipfile and the ls and bash commands.
(2) The total CPU utilization of all processes in a capsule cannot exceed 10% at any point in time.
(3) The total memory usage of all processes in a capsule cannot exceed 2 MB.
(4) The maximum disk read/write rate of processes in a capsule is 1 MB/sec.
(5) All processes in a capsule belong to a single isolated process namespace with process ids starting at 1.
(6) Processes in a capsule have their own mount namespace.
(7) None of the processes with in a capsule have access to any network interface.
(8) Processes in a capsule have their own IPC resources.

To test the system, create a set of test programs to check the limits of a capsule. Include the executable binaries of all these test programs in the input zipfile along with all libraries needed, so that you can run them with in a capsule.