Rootless Containers

Unprivileged Container

Advantages:
- Allow code to run inside a rootless container without having to run the container as host machine root user.
- Adds a Security
- Allow multiple unprivileged users to run and maintain containers on the same machine

Disadvantages:
- Dropped Capabilities
- Binding the Ports less than 1024
- Volume Mounting

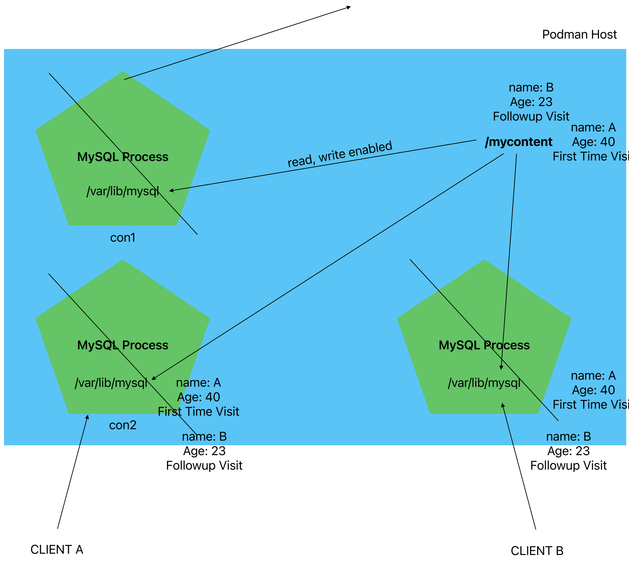
Volume Mounting

COW File System
(Copy-on-Write)

Stored Data, Change made inside a container is ephemeral

Persisting Data

1. Containers are ephemeral, so even if a container is deleted its data should be available.
2. This mounted data can now be shared amongst multiple containers.



Two Ways of Mounting

1. -v, --volume
-v <path_on_host>:<path_in _container>:<OPTIONS>

2. --mount
--mount type=<TYPE_of_Mount>,source=<path_on_host>,destination=<path_in_container>

Types of Mounting

1. bind for bind mounting
2. volume for volume mount (Preferred Method)
3. tmpfs for memory-only

OPTIONS

:Z (Sets a SELinux Context)
:rw (Read-Write Enabled Connection)
:ro (Read-Only Connection)

Podman Compose

Podman Compose is an open source tool that we can use to run Compose files.
A compose file is a YAML file that specifies that containers to manage.

The Compose File is a YAML file that contains the following sections:

Version: (Deprecated)
Specifies the Compose version used.

Services:
Defines the containers to be used.

Networks:
Defines the networks used by the containers.

Volumes:
Defines the volumes used by the containers.