Guided Exercise: Rootless Podman

Analyze a non-functioning rootless Podman environment.

Outcomes

You should be able to:

- Analyze the symptoms of a Podman environment that lacks group and user ID mapping.
- Provide the group and user ID mapping to fix the environment issues.

As the `student` user on the `workstation` machine, use the `lab` command to prepare your system for this exercise.

```
[student@workstation ~]$ lab start custom-rootless
```

Instructions

1. Explore and build the Gitea container image.

   Change to the `/home/student/DO188/labs/custom-rootless/gitea` directory.

   ```
   [student@workstation ~]$ cd ~/DO188/labs/custom-rootless/gitea
   no output expected
   ```

   Explore the `Containerfile` file. Note that the image creates and uses the `default` user.

   Build the container image with the `localhost/gitea` tag.

   ```
   [student@workstation gitea]$ podman build -t gitea .
   ...output omitted...
   Successfully tagged localhost/gitea:latest
   e92a...390b
   ```

   Repeat the last command for the `root` user. Use the double exclamation mark (`!!`) to refer to the previously executed command.

   ```
   [student@workstation gitea]$ sudo !!
   ...output omitted..
   Successfully tagged localhost/gitea:latest
   a247...2e58
   ```

   This guided exercise requires that you use the `gitea` image to start a container by using the `root` user in a later step. Consequently, because the `gitea` image is local to your environment, you must build the `gitea` image for the `root` user. Users do not share local images by default.

2. As the `root` user, execute the `/home/student/DO188/labs/custom-rootless/ids.sh` script to remove the user and group ID system mapping.

   ```
   [student@workstation ~]$ sudo ~/DO188/labs/custom-rootless/ids.sh
   Backing up /etc/subgid and /etc/subuid
   OK
   ```

3. Start the containerized Gitea process.

   Start a container that uses the `gitea` image in rootless mode.

   ```
   [student@workstation gitea]$ podman run --rm -p 3030:3030 gitea
   ERRO[0000] cannot find UID/GID for user student: cannot read subids - check rootless mode in man pages.
   WARN[0000] Using rootless single mapping into the namespace. This might break some images. Check /etc/subuid and /etc/subg
   id for adding sub*ids if not using a network user
   Error: OCI runtime error: crun: cannot setresuid to 1001: Invalid argument
   ```

   Podman fails to start the container because the image uses multiple users and Podman does not have enough ID mapping to map the user and group IDs inside the container to non root users and group IDs on your system.

   Start a container that uses the `gitea` image as the root user.

   ```
   [student@workstation gitea]$ sudo podman run --name root-gitea \
     -p 3030:3030 --rm gitea
   ...output omitted...
   2022/06/02 09:22:11 ...s/graceful/server.go:61:NewServer() [I] Starting new Web server: tcp:0.0.0.0:3030 on PID: 1
   ```

In a new terminal, verify the user and group ID mapping.

```
[student@workstation ~]$ sudo podman exec root-gitea \
  cat /proc/self/uid_map /proc/self/gid_map
         0          0 4294967295
         0          0 4294967295
```

When you start the container as root, Podman uses your system's root user for the root user inside the container. Consequently, if an attacker gains root permissions in your container, then they can potentially access your host system.

Stop the `root-gitea` container.

```
[student@workstation ~]$ sudo podman stop root-gitea
root-gitea
```

4. Provide the subuid and subguid ID ranges.

   In the Gitea terminal, create the `/etc/subuid` and `/etc/subguid` files.

   ```
   [student@workstation gitea]$ sudo touch /etc/{subuid,subgid}
   no output expected
   ```

   Starting with the ID `100000`, add `65536` IDs to map for the `student` user.

   ```
   [student@workstation gitea]$ sudo usermod --add-subuids 100000-165536 \
     --add-subgids 100000-165536 student
   no output expected
   ```

   Verify the ID ranges.

   ```
   [student@workstation gitea]$ cat /etc/subuid /etc/subgid
   student:100000:65537
   student:100000:65537
   ```

5. Start a container that uses the `gitea` image in a rootless mode.

   Attempt to start the `gitea` container.

   ```
   [student@workstation gitea]$ podman run --rm -p 3030:3030 --name gitea gitea
   Error: OCI runtime error: crun: cannot setresuid to 1001: Invalid argument
   ```

   The error occurs because you did not inform the Podman runtime about the new ID ranges.

   Migrate the Podman ID ranges.

   ```
   [student@workstation gitea]$ podman system migrate
   no output expected
   ```

   Start a container that uses the `gitea` image. Expose port `3030` to access the application.

   ```
   [student@workstation gitea]$ podman run --name gitea --rm -p 3030:3030 gitea
   ...output omitted...
   2022/06/03 11:29:49 cmd/web.go:212:listen() [I] AppURL(ROOT_URL): http://localhost:3030/
   2022/06/03 11:29:49 ...s/graceful/server.go:61:NewServer() [I] Starting new Web server: tcp:0.0.0.0:3030 on PID: 1
   ```

   Go to `localhost:3030` in a web browser to verify the application functionality.

   In the second terminal, terminate the `gitea` container.

   ```
   [student@workstation ~]$ podman stop gitea
   gitea
   ```

6. Restore the original user and group IDs by using the `/home/student/DO188/labs/custom-rootless/ids.sh` script.

   ```
   [student@workstation ~]$ sudo ~/DO188/labs/custom-rootless/ids.sh
   Restoring /etc/subgid and /etc/subuid
   OK
   ```

Finish

On the `workstation` machine, use the `lab` command to complete this exercise. This is important to ensure that resources from previous exercises do not impact upcoming exercises.

```
[student@workstation ~]$ lab finish custom-rootless
```