Step 2: Apply the Seccomp Profile to a Pod

Create a Pod named `seccomp-pod` in the namespace `seccomp` using `alpine/curl:3.14` as the container image. Add a command to the container to do a single `ping` to `kubernetes.io` indefinitely and add delay `5s`. Apply the seccomp profile `seccomp-audit.json` to the pod.

Get the last 50 lines of related logs from `/var/log/syslog` and save to `/opt/seccomp/answer` (save the answer in the controlplane or the default terminal session)

▶ Solution

- Create the Pod manifest using the seccomp profile:

```
kubectl apply -f - <<EOF
apiVersion: v1
kind: Pod
metadata:
  name: seccomp-pod
  namespace: seccomp
spec:
  securityContext:
    seccompProfile:
      type: Localhost
      localhostProfile: profiles/seccomp-audit.json
  containers:
  - name: secure-container
    image: alpine/curl:3.14
    command: ["sh", "-c", "while true; do ping -c 1 kubernetes.io; sleep 5;
done"]
EOF
```{{exec}}

* Get the last related 50 lines of logs: `grep syscall /var/log/syslog | tail
-50 > /opt/seccomp/answer`

* Aware that the syscall number are changing. When you run an infinite loop
with sh, every iteration of the loop will execute the ping command and then
sleep for 5 seconds. This activity will generate syscalls logged by seccomp.

</details>