Exercise: Kubernetes OPA - Gatekeeper

Steps

1. Let's try another defense on the first cluster takeover scenario: "OPA Gatekeeper" in place of the pod security policy admission controller. We can use OPA Gatekeeper to prevent any account from deploying a host volume-mounting pod.
2. SSH into the Kubernetes control-plane node, using the `bustakube` user's password, `bustakube`:

   ```
   ssh bustakube@bustakube-controlplane
   ```

3. `sudo` to root

   ```
   sudo su -
   ```

4. If the Bustakube cluster isn't in the first scenario, use `scenariochooser` to put the cluster in the first scenario.

   ```
   echo "No action required unless we skipped the Own the Nodes exercise"
   ```

5. Deactivate the Pod Security Policy admission controller:

   ```
   /usr/local/bin/toggle-psp-controller.sh deactivate
   ```

6. Install gatekeeper, using the GitHub-hosted manifest file:

   ```
   kubectl apply -f https://raw.githubusercontent.com/open-policy-agent/gatekeeper/release
   ```

7. Confirm that Gatekeeper is running:

   ```
   kubectl wait -n gatekeeper-system deployment --all --for=condition=Available --timeout=
   ```

8. Now clone the OPA Gatekeeper Library, to get constraints:

   ```
   git clone https://github.com/open-policy-agent/gatekeeper-library.git
   ```

9. Change directory into the set of templates corresponding to the pod security policies:

   ```
   cd gatekeeper-library/library/pod-security-policy
   ```

10. Now apply the template for host-filesystem use, comparable to the `hostPath` pod security policy:

```
kubectl apply -f host-filesystem/template.yaml
```

11. Confirm that the template is loaded:

    ```
    kubectl wait crd --all --for=condition=Established k8spsphostfilesystem.constraints.gat
    ```

12. Now apply the pod security policy-equivalent `hostPath` restriction constraint:

    ```
    kubectl apply -f host-filesystem/samples/psp-host-filesystem/constraint.yaml
    ```

13. Now, let's see that we can't stage a pod that mounts the host filesystem:

    ```
    kubectl apply -f /usr/share/bustakube/Scenario1-OwnTheNodes/Attack/attack-pod.yaml
    ```

14. Observe the error message that says our attack pod was blocked. This means OPA Gatekeeper has blocked our attack.