

# Admission Controller Demo

June 30, 2021

David Shepard

[djshepard@sei.cmu.edu](mailto:djshepard@sei.cmu.edu)

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

Copyright 2021 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM21-0608

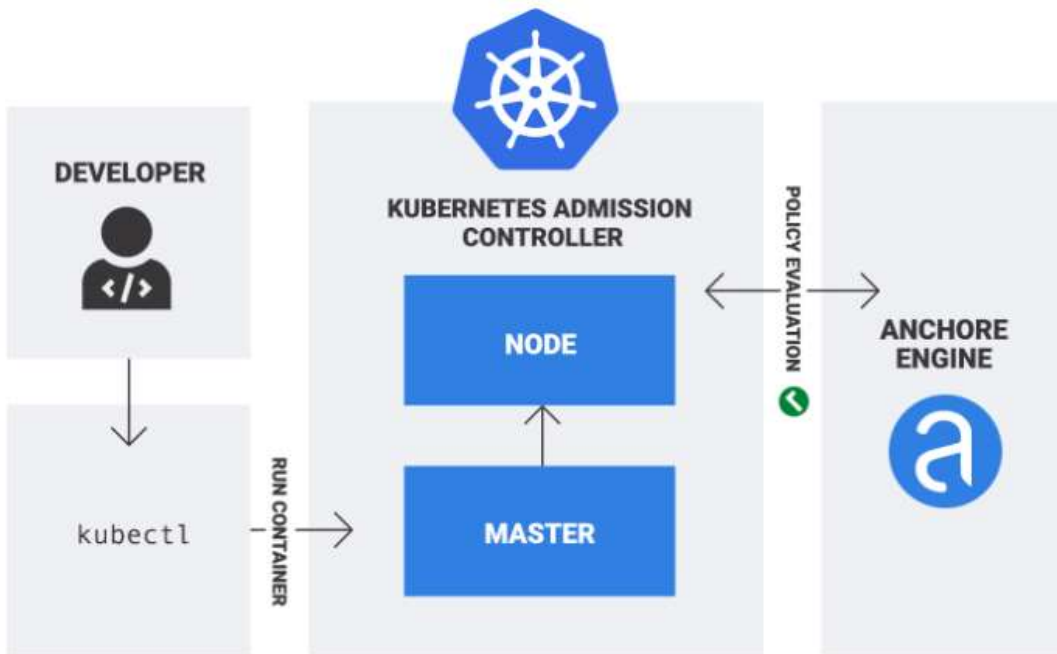
# BLUF

Develop a prototype implementation of a policy-based admission controller for Kubernetes, using technologies such as Open Policy Agent, Sysdig, and Anchore Gatekeeper as needed, and a prototype policy to demonstrate compliance with Anchore scan results for cluster admission. Must have the ability to allow administrative override of scan decisions.

- Multiple possible solutions to the problem
- Demonstration of the following:
  - How to configure Anchore Admission Controller
  - How to write a basic Anchore policy bundle
  - A basic demonstration of an image denial by policy, followed by an exemption

# Filtering Vulnerable Images Using an Admission Controller

## Basic Architecture



# Step One: Deploy a Cluster in Azure and Deploy Anchore

```
I $ ~/D/p/l/admission_controller azure/opa-demo helm upgrade --install anchr-adm-ctrlr a
26:26 2021
W0629 20:26:37.087298 35452 warnings.go:70] admissionregistration.k8s.io/v1beta1 ValidatingWebhookConf
W0629 20:26:37.109378 35452 warnings.go:70] admissionregistration.k8s.io/v1beta1 ValidatingWebhookConf
W0629 20:26:37.137290 35452 warnings.go:70] admissionregistration.k8s.io/v1beta1 ValidatingWebhookConf
Release "anchr-adm-ctrlr" has been upgraded. Happy Helming!
NAME: anchr-adm-ctrlr
LAST DEPLOYED: Tue Jun 29 20:26:36 2021
NAMESPACE: anchore
STATUS: deployed
REVISION: 5
TEST SUITE: None
NOTES:
Anchore admission controller is now installed.
```

# Step Two: Configure Helm Chart For Policy Bundles

The values provided during chart deployment provide Selectors for Policy Bundles. They're in an order of precedence.

```
existingCredentialsSecret: anchore-credentials
anchoreEndpoint: https://anchore-opa-demo.eastus.cloudapp.azure.com/v1/
policySelectors:
  - Selector:
      ResourceType: namespace
      SelectorKeyRegex: name
      SelectorValueRegex: ^emoji$
    PolicyReference:
      Username: admin
      PolicyBundleId: allowlist001
    Mode: policy
  - Selector:
      ResourceType: "image"
      SelectorKeyRegex: ".*"
      SelectorValueRegex: ".*"
    PolicyReference:
      Username: "admin"
      # This is the default bundle id in anchore engine
      PolicyBundleId: "2c53a13c-1765-11e8-82ef-23527761d060"
      # Mode is one of: "policy", "analysis", or "breakglass".
      # policy=>require policy pass, analysis=>require image analyzed,
      # breakglass=>do nothing
    Mode: policy
```

# Configure a Policy Bundle (Anchore Admission Controller)

Default policy is to fail any “high” vulns. This policy bundle allows a whitelist exemption for an image deployed to a specific namespace. This is a version-controlled artifact.

```
{
  "id": "allowlist001",
  "version": "1_0",
  "name": "Allow emoji for emoji ns",
  "comment": "Allowlist for emoji when deployed to emoji ns",
  "whitelisted_images": [
    {
      "name": "AllowlistEmoji",
      "registry": "docker.l5d.io",
      "repository": "buoyantio/emoji-emoji-svc",
      "image": { "type": "tag", "value": "v11" }
    }
  ],
  "blacklisted_images": [],
  "mappings": [],
  "whitelists": [],
  "policies": []
}
```

# Policy Bundles Can Be Changed, Based on Environment

Test –VS– Prod

Example:

- List Available Policies
- Activate a Policy, based on the deployment target

```
I 1 $ ~/D/p/l/admission_controller azure/opa-demo anchore-cli policy list
26:58 2021
Policy ID      Active      Created      Updated
allowlist001  True       2021-06-29T20:11:29Z  2021-06-29T20:24:30Z
2c53a13c-1765-11e8-82ef-23527761d060  False      2021-06-29T16:11:21Z  2021-06-29T20:24:30Z
```

```
I $ ~/D/p/l/admission_controller azure/opa-demo anchore-cli policy activate 2c53a13c-1765-11e8-82ef-23527761d060
27:09 2021
Success: 2c53a13c-1765-11e8-82ef-23527761d060 activated
```

# This Image Will Fail Policy, Based on High Vulns

```
1 1 S -/D/p/l/admission_controller 4/? azure/opa-deno anchore-cli image vuln docker.l5d.io/buoyantio/enojivoto-emoji-svc:v11 all
```

Vulnerability ID	Package	Severity	Fix	CVE Refs	Vulnerability URL
CVE-2020-10878	perl-base-5.28.1-6	High	5.28.1-6+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2020-10878">https://security-tracker.debian.org/tracker/CVE-2020-10878</a>
CVE-2021-20231	libgnutls30-3.6.7-4+deb10u3	High	3.6.7-4+deb10u7		<a href="https://security-tracker.debian.org/tracker/CVE-2021-20231">https://security-tracker.debian.org/tracker/CVE-2021-20231</a>
CVE-2021-20232	libgnutls30-3.6.7-4+deb10u3	High	3.6.7-4+deb10u7		<a href="https://security-tracker.debian.org/tracker/CVE-2021-20232">https://security-tracker.debian.org/tracker/CVE-2021-20232</a>
CVE-2021-3177	libpython3.7-minimal-3.7.3-2+deb10u2	High	3.7.3-2+deb10u3		<a href="https://security-tracker.debian.org/tracker/CVE-2021-3177">https://security-tracker.debian.org/tracker/CVE-2021-3177</a>
CVE-2021-3177	libpython3.7-stdlib-3.7.3-2+deb10u2	High	3.7.3-2+deb10u3		<a href="https://security-tracker.debian.org/tracker/CVE-2021-3177">https://security-tracker.debian.org/tracker/CVE-2021-3177</a>
CVE-2021-3177	python3.7-3.7.3-2+deb10u2	High	3.7.3-2+deb10u3		<a href="https://security-tracker.debian.org/tracker/CVE-2021-3177">https://security-tracker.debian.org/tracker/CVE-2021-3177</a>
CVE-2021-3177	python3.7-minimal-3.7.3-2+deb10u2	High	3.7.3-2+deb10u3		<a href="https://security-tracker.debian.org/tracker/CVE-2021-3177">https://security-tracker.debian.org/tracker/CVE-2021-3177</a>
CVE-2021-3517	libxml2-2.9.4+dfsg1-7+b3	High	2.9.4+dfsg1-7+deb10u2		<a href="https://security-tracker.debian.org/tracker/CVE-2021-3517">https://security-tracker.debian.org/tracker/CVE-2021-3517</a>
CVE-2021-3520	liblz4-1-1.8.3-1	High	1.8.3-1+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2021-3520">https://security-tracker.debian.org/tracker/CVE-2021-3520</a>
CVE-2020-13434	libsqlite3-0-3.27.2-3	Low	3.27.2-3+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2020-13434">https://security-tracker.debian.org/tracker/CVE-2020-13434</a>
CVE-2020-13435	libsqlite3-0-3.27.2-3	Low	3.27.2-3+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2020-13435">https://security-tracker.debian.org/tracker/CVE-2020-13435</a>
CVE-2020-13632	libsqlite3-0-3.27.2-3	Low	3.27.2-3+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2020-13632">https://security-tracker.debian.org/tracker/CVE-2020-13632</a>
CVE-2020-15358	libsqlite3-0-3.27.2-3	Low	3.27.2-3+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2020-15358">https://security-tracker.debian.org/tracker/CVE-2020-15358</a>
CVE-2021-24031	libzstd1-1.3.8+dfsg-3	Low	1.3.8+dfsg-3+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2021-24031">https://security-tracker.debian.org/tracker/CVE-2021-24031</a>
CVE-2021-24032	libzstd1-1.3.8+dfsg-3	Low	1.3.8+dfsg-3+deb10u2		<a href="https://security-tracker.debian.org/tracker/CVE-2021-24032">https://security-tracker.debian.org/tracker/CVE-2021-24032</a>
CVE-2011-3389	libgnutls30-3.6.7-4+deb10u3	Medium	None		<a href="https://security-tracker.debian.org/tracker/CVE-2011-3389">https://security-tracker.debian.org/tracker/CVE-2011-3389</a>
CVE-2017-18258	libxml2-2.9.4+dfsg1-7+b3	Medium	2.9.4+dfsg1-7+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2017-18258">https://security-tracker.debian.org/tracker/CVE-2017-18258</a>
CVE-2018-14404	libxml2-2.9.4+dfsg1-7+b3	Medium	2.9.4+dfsg1-7+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2018-14404">https://security-tracker.debian.org/tracker/CVE-2018-14404</a>
CVE-2018-14567	libxml2-2.9.4+dfsg1-7+b3	Medium	2.9.4+dfsg1-7+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2018-14567">https://security-tracker.debian.org/tracker/CVE-2018-14567</a>
CVE-2019-1551	libssl1.1-1.1.1d-0+deb10u3	Medium	1.1.1d-0+deb10u5		<a href="https://security-tracker.debian.org/tracker/CVE-2019-1551">https://security-tracker.debian.org/tracker/CVE-2019-1551</a>
CVE-2019-1551	openssl-1.1.1d-0+deb10u3	Medium	1.1.1d-0+deb10u5		<a href="https://security-tracker.debian.org/tracker/CVE-2019-1551">https://security-tracker.debian.org/tracker/CVE-2019-1551</a>
CVE-2019-16168	libsqlite3-0-3.27.2-3	Medium	3.27.2-3+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2019-16168">https://security-tracker.debian.org/tracker/CVE-2019-16168</a>
CVE-2019-19923	libsqlite3-0-3.27.2-3	Medium	3.27.2-3+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2019-19923">https://security-tracker.debian.org/tracker/CVE-2019-19923</a>
CVE-2019-19925	libsqlite3-0-3.27.2-3	Medium	3.27.2-3+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2019-19925">https://security-tracker.debian.org/tracker/CVE-2019-19925</a>
CVE-2019-19956	libxml2-2.9.4+dfsg1-7+b3	Medium	2.9.4+dfsg1-7+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2019-19956">https://security-tracker.debian.org/tracker/CVE-2019-19956</a>
CVE-2019-19959	libsqlite3-0-3.27.2-3	Medium	3.27.2-3+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2019-19959">https://security-tracker.debian.org/tracker/CVE-2019-19959</a>
CVE-2019-20218	libsqlite3-0-3.27.2-3	Medium	3.27.2-3+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2019-20218">https://security-tracker.debian.org/tracker/CVE-2019-20218</a>
CVE-2019-20388	libxml2-2.9.4+dfsg1-7+b3	Medium	2.9.4+dfsg1-7+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2019-20388">https://security-tracker.debian.org/tracker/CVE-2019-20388</a>
CVE-2020-10543	perl-base-5.28.1-6	Medium	5.28.1-6+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2020-10543">https://security-tracker.debian.org/tracker/CVE-2020-10543</a>
CVE-2020-12723	perl-base-5.28.1-6	Medium	5.28.1-6+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2020-12723">https://security-tracker.debian.org/tracker/CVE-2020-12723</a>
CVE-2020-13630	libsqlite3-0-3.27.2-3	Medium	3.27.2-3+deb10u1		<a href="https://security-tracker.debian.org/tracker/CVE-2020-13630">https://security-tracker.debian.org/tracker/CVE-2020-13630</a>
CVE-2020-13777	libgnutls30-3.6.7-4+deb10u3	Medium	3.6.7-4+deb10u4		<a href="https://security-tracker.debian.org/tracker/CVE-2020-13777">https://security-tracker.debian.org/tracker/CVE-2020-13777</a>

# Deployment Fails to Default Namespace

```
I $ -/D/p/l/admission_controller azure/opa-demo kubectl --kubeconfig $KUBECONFIG --namespace default apply
31:43 2021
Error from server: error when creating "emojivoto_in_the_cloud.yaml": admission webhook "anchore-admission-controller-admiss
af3b56f958fe48e99a84bbfc15a768e15546" FAILED policy checks for policy bundle "2c53a13c-1765-11e8-82ef-23527761d060"
```

Decision time:

- Determine how to handle the failure. By default, items simply do not deploy.
- If it must be deployed, a policy exemption must be written.

# Deployment Succeeds to Targeted Namespace

```
I $ ~/D/p/l/admission_controller azure/opa-demo kubectl --kubeconfig $KUBECONFIG --namespace emoji apply
31:32 2021
pod/emojivoto created
```

- A determination was made to deploy this container anyway.
- The policy bundle from slide seven allows this to deploy to the custom namespace.
- The policy bundles are placed into version control and applied using automation.

# Questions?