KubeCon | CloudNativeCon

Europe 2021

Virtual

Forward Together »

KubeCon | CloudNativeCon

Europe 2021

Virtual

Making dynamic admission control even more dynamic using WebAssembly

Flavio Castelli – SUSE
Rafael Fernández López - SUSE

The $1m question

How do you handle security?

Security is hard

- 66% of respondents are worried about unaddressed security needs
- DevSecOps is growing, but only 16% are implementing security policies as code
- Biggest hurdles to Kubernetes adoption:
  - 36% internal skills shortage
  - 34% steep learning curve

Source: StackRox state of containers and Kubernetes security – fall 2020

We feel the pain

- Steep learning curve
- Doing non-trivial policies is hard
- Frustration: "it would take me X minutes to write this check using Y"
- How to distribute the policy across clusters in a safe way

Our Wishlist

- Reuse existing knowledge, tooling, best practices, infrastructure,…
- Have a framework to write policies and a platform to run them
- Really treat policies as code
- Have a curated index of policies

Our take on the problem

- Kubernetes Policy Engine
- Manage all Kubernetes paperwork
- Policies are WebAssembly Modules

WebAssembly is fantastic

- Not just a "browser thing"
- Many programming languages support it, more are coming
- It's portable
- It's secure

More info about WebAssembly

Cluster admins: we have you!

- Policies are distributed using container registries
- It's easy to test a policy using different settings and input
- Policies run in a safe Wasm environment
- The policy server is written in Rust

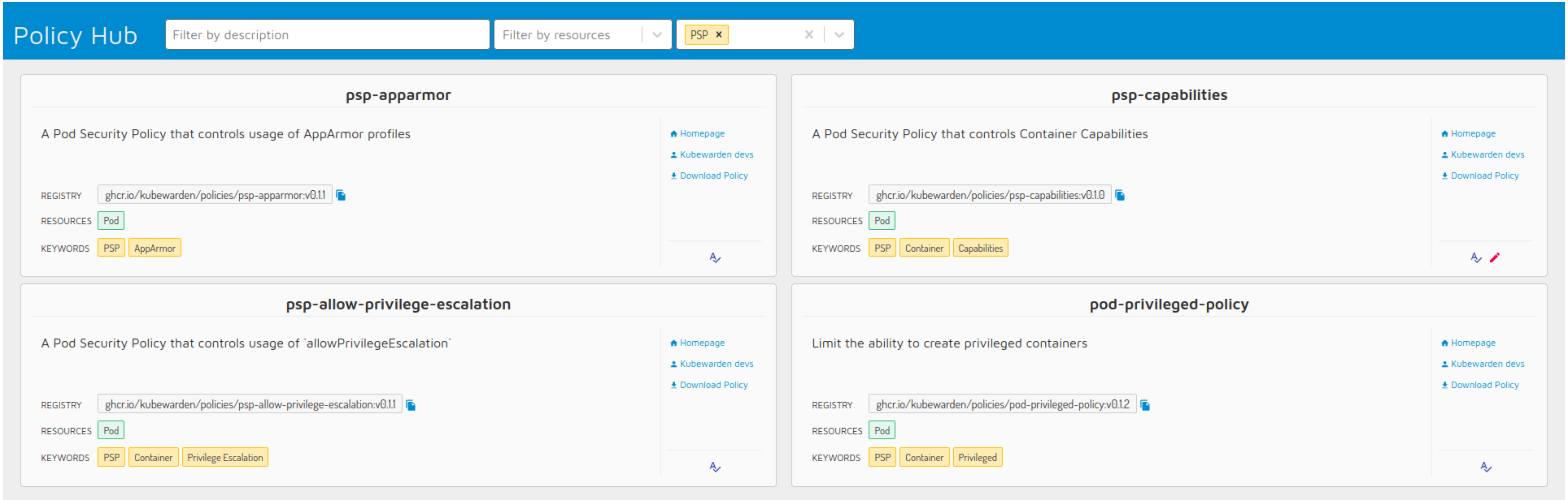
Policy authors: feel productive

- Use your favorite programming language
- Build once, run everywhere! -- for real
- Simple way to write mutation policies
- Reuse your knowledge: libraries, TDD, code linting, CI/CD systems,…

Current status

- Alpha quality and stability
- Kubernetes Custom Resources and controller to manage policies
- Validation and Mutation policies
- Prototype of context-aware policy
- Policy SDK
- Policy Hub

Policy Hub



Policy Hub

Filter by description

Filter by resources

PSP ×

psp-apparmor

A Pod Security Policy that controls usage of AppArmor profiles

Homepage
Kubewarden devs
Download Policy

REGISTRY ghcr.io/kubewarden/policies/psp-apparmor:v0.1.1

RESOURCES Pod

KEYWORDS PSP AppArmor

psp-capabilities

A Pod Security Policy that controls Container Capabilities

Homepage
Kubewarden devs
Download Policy

REGISTRY ghcr.io/kubewarden/policies/psp-capabilities:v0.1.0

RESOURCES Pod

KEYWORDS PSP Container Capabilities

psp-allow-privilege-escalation

A Pod Security Policy that controls usage of `allowPrivilegeEscalation`

Homepage
Kubewarden devs
Download Policy

REGISTRY ghcr.io/kubewarden/policies/psp-allow-privilege-escalation:v0.1.1

RESOURCES Pod

KEYWORDS PSP Container Privilege Escalation

pod-privileged-policy

Limit the ability to create privileged containers

Homepage
Kubewarden devs
Download Policy

REGISTRY ghcr.io/kubewarden/policies/pod-privileged-policy:v0.1.2

RESOURCES Pod

KEYWORDS PSP Container Privileged

Let's build something together

- Kubewarden is a fresh project, there's plenty to do!
- Feedback about design, architecture,…
- Help shape Policy SDKs
- Come back, share your achievements with us!

Where to find us

- GitHub: https://github.com/kubewarden
- Main website: https://kubewarden.io
- Policy Hub: https://hub.kubewarden.io