

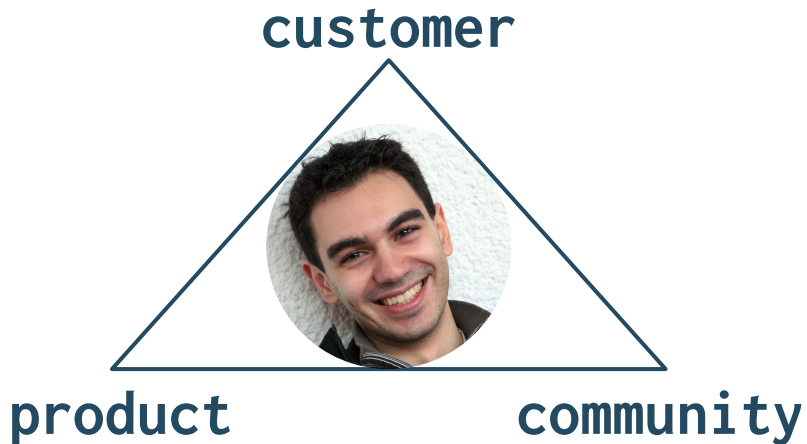
Hardening Kubernetes Setups: War Stories from the Trenches of Production

Puja Abbassi - @puja108

11.12.2018

Puja

@puja108



@puja108

- Developer Advocate / Product Owner @ Giant Swarm
- #CKA #Security #Operators
- Data & Network Science “Almost-PhD”

Agenda

1. On running 100+ clusters
 2. Postmortems - Lots of them!
 3. Hardening and Best-Practices
-

On running 100+
clusters



100+ clusters

- Different Clouds
- Different Regions
- On-Premise
- China

Diversity

- Companies
- Industries
- Users
- Use Cases

Freedom vs. Control

- Opt for Freedom
- Educate Users
- Harden up

Postmortems - Lots of them!



Postmortem Philosophy

“The primary goals of writing a postmortem are to ensure that the **incident is documented**, that **all contributing root cause(s)** are well understood, and, especially, that effective **preventive actions are put in place** to reduce the likelihood and/or impact of recurrence.”

- Google SRE book

Single Product

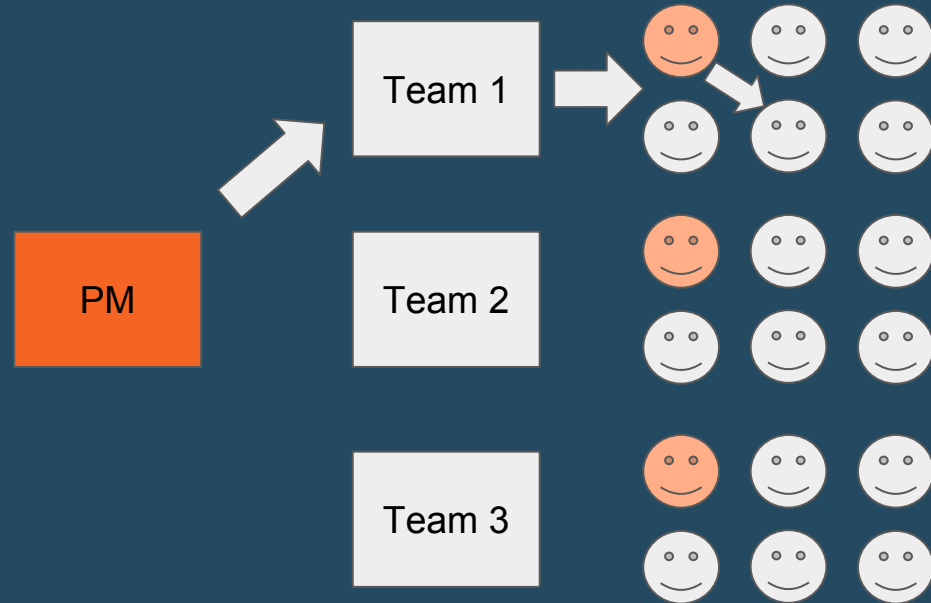


1. Gather Issues
2. Fix in Code
3. Roll out continuously
4. Profit 🐛

Postmortem Practice

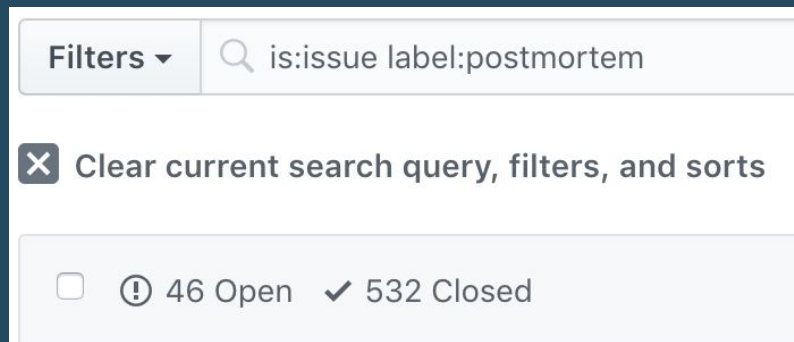
- Issue Template
- High Priority
- Assigned to
x-functional team

Load Balancing Postmortems



500+ Postmortems

@puja108



The screenshot shows a GitHub search interface. At the top, there is a search bar with the query "is:issue label:postmortem". To the left of the search bar is a "Filters" dropdown menu. Below the search bar, there is a button with an "X" icon and the text "Clear current search query, filters, and sorts". At the bottom of the search results area, there is a summary bar showing "46 Open" (with an exclamation mark icon) and "532 Closed" (with a checkmark icon).

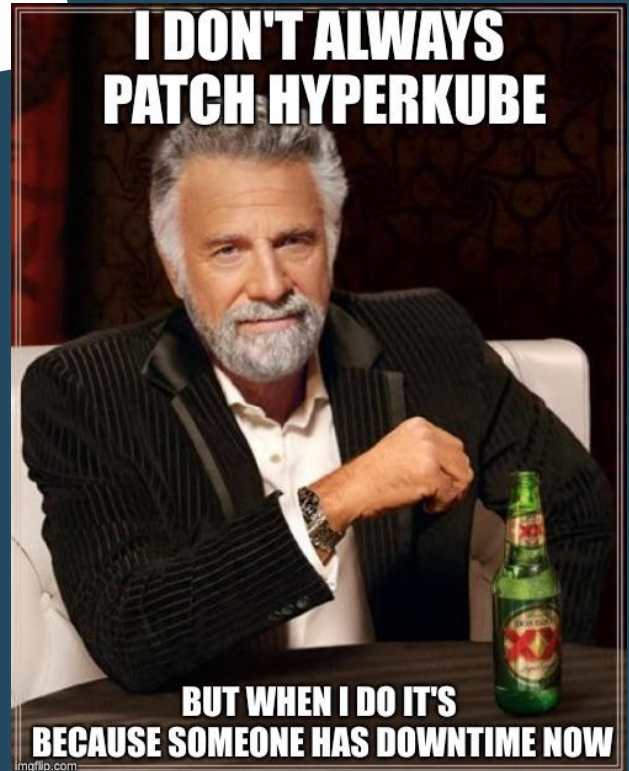
War Stories



Memory leak in k8s-apiserver on asgard - causes tenant cluster k8s API downtime #4187
Closed tuommaki opened this issue on Sep 13 · 20 comments

Kubernetes
upstream issue:
#57992
(fixed in 1.11.4
and 1.12.0)

@puja108



Ingress Controller Misconfiguration

- Faulty ingress objects can break controller
- Lots of teams + lots of freedom
= lots of issues

Ever built a
full-mesh IPIP
tunnels ICMP
pinger?

@puja108



Customer Load Test goes bad?

You take the
blame!

- “Must be Calico, kube-proxy, IC!”
- Turns out EC2 network saturation was the bottleneck
- Solution: More workers!

Hardening and Best-Practices



Postmortem Hotspots

- Old versions
 - Ingress (~15%)
 - Networking & DNS
 - Resource Pressure
 - Multi-tenancy
-

Old versions

- Issues might have been solved already
 - CVEs
 - Test Upgrades extensively
 - Automate Upgrades (or have a process)
-

Ingress

- NGINX IC: Newer versions are less prone to misconfiguration
- Separate controllers
- Load- and failover-testing
- Last resort:
_____ SVC of type LB

Networking & DNS

- Monitor network health
 - Monitor DNS latency
 - Check for known issues
 - Apply best practices
-

Resource Pressure

- Resource Management!
- Include Buffers (lots of them)
- Protect K8s and critical addons (priority)

Multi-tenancy

- Separate and isolate namespaces with RBAC
 - No cluster-admins!
 - Separate clusters if possible
 - Automate with CI/CD
 - Minimize manual ops
-

Best Practices

- Preemptive Monitoring & Alerting are key!
 - Logging (and Tracing) help debugging
 - Fix issues fast
 - Educate users
 - Have a postmortem process
 - Train Recovery
-

Stand on the Shoulders of Giants!

- [Kubernetes the very hard way - Datadog](#)
- [Scaling Kubernetes to 2,500 Nodes - OpenAI](#)
- [5 - 15s DNS lookups on Kubernetes? - BitMEX](#)
- [Scaling CoreDNS in Kubernetes Clusters](#)
- [Inside Kubernetes Resource Management \(QoS\) - Michael Gasch](#)
- [List of Kubernetes Best Practice talks/blogs](#)
- [Kubernetes Office Hours](#)

Thank you!



@puja108

Questions?

Stay in touch

- Twitter: @puja108
- Github: puja108
- Slack/Discuss: puja