ALL DAY DEVOPS

caffeinated by sonatype

NOVEMBER 10, 2022

I am Cluster Admin, Destroyer of Everything You Hold Dear

SITE RELIABILITY ENGINEERING

Matt Williams, Evangelist @ Infra
TW: @technovangelist - Mast: @technovangelist@fosstodon.org

Least Privilege

According to Cybersecurity & Infrastructure Security Agency (CISA):

Only the **minimum necessary rights** should be **assigned to a subject** that requests **access to a resource** and should be **in effect for the shortest duration necessary** … careful delegation of access rights can limit attackers from damaging a system.

What happens when we skip Least Privilege

Target - 2013

- HVAC on main network
- Useful for monitoring energy consumption at various stores

Target - 2013

- HVAC on main network
- Useful for monitoring energy consumption at various stores
- Technician compromised

Target - 2013

- HVAC on main network
- Useful for monitoring energy consumption at various stores
- Technician compromised

Attackers stole 40 million debit and credit cards

GitLab - 2017

- SRE responding to incident
- Intended to drop replica database

GitLab - 2017

- SRE responding to incident
- Intended to drop replica database
- Fat fingered the production database and had excessive privileges to do it

GitLab - 2017

- SRE responding to incident
- Intended to drop replica database
- Fat fingered the production database and had excessive privileges to do it

GitLab went down for 6 hours, 5k projects lost (issues, etc), comments, users

Marriott - 2018

User compromised

Had admin access for everything

Ran some database queries

Marriott - 2018

User compromised

Had admin access for everything

Ran some database queries

Hundreds of millions of customer records lost

Capital One - 2019

- Misconfigured firewall
- Generated temp account creds via SSRF exploit
- Had excessive privileges to sync S3 buckets

Capital One - 2019

- Misconfigured firewall
- Generated temp account creds via SSRF exploit
- Had excessive privileges to sync S3 buckets

30GB of credit application data, affecting 100 million in US, 6 million in Canada

Verkada - 2021

- Credentials found for user
- Had excessive privileges

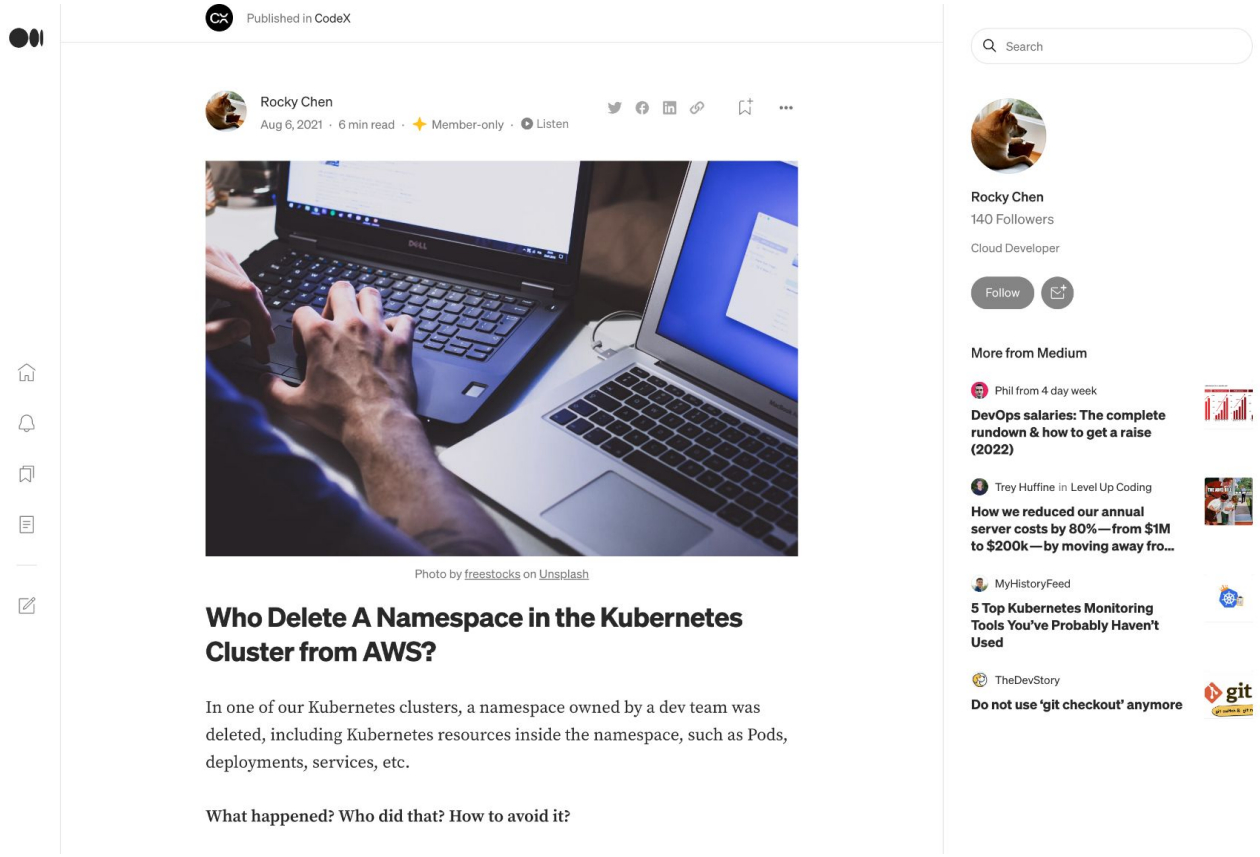
Verkada - 2021

- Credentials found for user
- Had excessive privileges

Accessed 150k live camera feeds in schools, prisons, and hospitals

Reported by Rocky Chen? - 2021

- User accidentally deleted a namespace
- Recreated it - but did it wrong
- He thought he was in his test cluster
- Assumed AWS role made it difficult to troubleshoot



Published in CodeX

Rocky Chen
Aug 6, 2021 · 6 min read · Member-only · Listen

Photo by freestocks on Unsplash

Who Delete A Namespace in the Kubernetes Cluster from AWS?

In one of our Kubernetes clusters, a namespace owned by a dev team was deleted, including Kubernetes resources inside the namespace, such as Pods, deployments, services, etc.

What happened? Who did that? How to avoid it?

Search

Rocky Chen
140 Followers
Cloud Developer
Follow

More from Medium

Phil from 4 day week
DevOps salaries: The complete rundown & how to get a raise (2022)

Trey Huffine in Level Up Coding
How we reduced our annual server costs by 80%—from $1M to $200k—by moving away fro...

MyHistoryFeed
5 Top Kubernetes Monitoring Tools You've Probably Haven't Used

TheDevStory
Do not use 'git checkout' anymore

SW company with tools used by law enforcement and sec teams

- One of the devs ran kubectl command
- Thought he was in test, was actually in prod
- Assumed roles, never figured out who did it

All access to Kubernetes removed and start over

What is the cost of breaches?

- Avg cost: $4.24 million in 2021
- Avg time to identify: 212 days.
- Avg lifecycle: 286 days from identification to containment.
- The likelihood detected and prosecuted 0.05%.
- Personal data involved in 45%.

https://www.securitymagazine.com/articles/93990-a-cluster-without-rbac-is-an-insecure-cluster

How is this relevant to this talk?

Let’s talk about Kubernetes & Cluster Admin

How is this relevant to this talk?

Let’s talk about Kubernetes & Cluster Admin

Cluster Admin is wonderful because you can do anything you want!!

How is this relevant to this talk?

Let's talk about Kubernetes & Cluster Admin

Cluster Admin is wonderful because you can do anything you want!!
Cluster Admin is scary because you can do anything you want!!

How is this relevant to this talk?

Let's talk about Kubernetes & Cluster Admin

Cluster Admin is wonderful because you can do anything you want!!

Cluster Admin is scary because you can do anything you want!!

Cluster Admin is the worst thing ever because you can do anything you want!!

so the answer is
don’t give cluster admin
to everyone, right??

But creating users in k8s is HARD

Users don’t actually exist in kubernetes

But creating users in k8s is HARD

Users don’t actually exist in kubernetes

Everything in k8s is a resource.

But creating users in k8s is HARD

Users don't actually exist in kubernetes

Everything in k8s is a resource.

But there is no user resource

But creating users in k8s is HARD

Users don't actually exist in kubernetes

Everything in k8s is a resource.
But there is no user resource

Its All About the Certs

But creating users in k8s is HARD

Users don’t actually exist in kubernetes

Everything in k8s is a resource.
But there is no user resource

Its All About the Certs in your .kubeconfig

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: certgoeshere
    server: https://clusterendpoint.k8s.ondigitalocean.com
  name: mycluster
contexts:
- context:
    cluster: mycluster
    user: do-sfo3-matt-primary-admin
  name: mycontext
current-context: mycontext
kind: Config
preferences: {}
users:
- name: do-sfo3-matt-primary-admin
  user:
    token: dop_v1_dea9d7ff2b8eb092f53ffebogus31d2bd4602a62a19b5ac4
```

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: certgoeshere
    server: https://clusterendpoint.k8s.ondigitalocean.com
  name: mycluster
contexts:
- context:
    cluster: mycluster
    user: do-sfo3-matt-primary-admin
  name: mycontext
current-context: mycontext
kind: Config
preferences: {}
users:
- name: do-sfo3-matt-primary-admin
  user:
    token: dop_v1_dea9d7ff2b8eb092f53ffebogus31d2bd4602a62a19b5ac4
```

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: certgoeshere
    server: https://clusterendpoint.k8s.ondigitalocean.com
  name: mycluster
contexts:
- context:
    cluster: mycluster
    user: do-sfo3-matt-primary-admin
  name: mycontext
current-context: mycontext
kind: Config
preferences: {}
users:
- name: do-sfo3-matt-primary-admin
  user:
    token: dop_v1_dea9d7ff2b8eb092f53ffebogus31d2bd4602a62a19b5ac4
```

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: certgoeshere
    server: https://clusterendpoint.k8s.ondigitalocean.com
  name: mycluster
contexts:
- context:
    cluster: mycluster
    user: do-sfo3-matt-primary-admin
  name: mycontext
current-context: mycontext
kind: Config
preferences: {}
users:
- name: do-sfo3-matt-primary-admin
  user:
    token: dop_v1_dea9d7ff2b8eb092f53ffebogus31d2bd4602a62a19b5ac4
```

What is a Role?

- Defines the level of access a ‘user’ has to the cluster
  - Resource
  - Verb

What is a Role?

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: marketing-dev
  labels:
    app.infrahq.com/include-role: "true"
rules:
  - apiGroups: [""] # "" indicates the core API group
    resources: ["pods"]
    verbs: ["get", "watch", "list"]
```

What is a Role?

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: marketing-dev
  labels:
    app.infrahq.com/include-role: "true"
rules:
  - apiGroups: [""] # "" indicates the core API group
    resources: ["pods"]
    verbs: ["get", "watch", "list"]
```

What is a Role?

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: marketing-dev
  labels:
    app.infrahq.com/include-role: "true"
rules:
  - apiGroups: [""] # "" indicates the core API group
    resources: ["pods"]
    verbs: ["get", "watch", "list"]
```

What is a Role?

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: marketing-dev
  labels:
    app.infrahq.com/include-role: "true"
rules:
  - apiGroups: [""] # "" indicates the core API group
    resources: ["pods"]
    verbs: ["get", "watch", "list"]
```

How to create a User

- Create the user key (openssl genpkey…)
- Create the CSR (openssl req –new)
- Submit the CSR to the cluster (yaml)
- Approve the request (kubectl certificate approve…)

How to create a User

- Get the approved request (kubectl get csr…)
- Build the kubeconfig (kubectl --kubeconfig myuserconfig config set-credentials, kubectl --kubeconfig myuserconfig configset-context)
- Then distribute the file

https://infrahq.com/blog/how-to-create-users

How to create a User

- And then repeat often
  - Ensure bad parties can’t access
  - You can’t revoke a cert

- And redistribute

that's a lot of steps
can we automate it?

master kubernetes-adduser / add-user.sh

Go to file ...

brendanburns Updates. Latest commit 6d53ffe on Nov 2, 2021 History

1 contributor

Executable File | 63 lines (51 sloc) | 1.41 KB

Raw Blame

```
#!/bin/bash

csr_name="my-client-csr"
name="${1:-my-user}"
cert_name="${name}-client"

if ! which cfssl; then
  echo "Can't find the cfssl tool, please install from https://pkg.cfssl.org/"
  exit 1
fi

if ! which cfssljson; then
  echo "Can't find the cfssljson tool, please install from https://pkg.cfssl.org/"
  exit 1
fi

echo "Generating signing request."
perl -p -e "s/%USER%/${name}/" cfssl.json.tmpl > cfssl.json

cfssl genkey cfssl.json | \
    cfssljson -bare ${cert_name}

```

but…

He doesn’t deal with file distribution

Is there something easier??

main | 68 branches | 89 tags | Go to file | Add file | Code

pdevine Require oldpassword (#3434) 05f7c58 3 hours ago 3,602 commits

.github	fix: postgres-dev to only listen on localhost	6 days ago
api	Require oldpassword (#3434)	3 hours ago
blog	improve: add blog post for creating users video (#30...	last month
docs	maintain: cli docgen fixes to clean up the resulting fil...	10 hours ago
helm	improve: add backwards compat for connector acces...	9 days ago
internal	Require oldpassword (#3434)	3 hours ago
metrics	maintain: update gofmt for go1.19	2 months ago
pki	improve: return our own type from NewDB	2 months ago
ui	Require oldpassword (#3434)	3 hours ago
uid	feat: add sql functions uidStrToInt and uidIntToStr (#...	last month

About

Infra manages access to infrastructure such as Kubernetes, with support for more connectors coming soon.

infrahq.com

go | kubernetes | infrastructure | golang | security | identity | login | iam | access | infra | oidc

Readme

View license

985 stars

16 watching

38 forks

Releases 89

Infra

- Two deployment options
  - Self Hosted
  - Use Infra Cloud (coming soon)

DEMO


ADDO
ALL DAY DEVOPS
caffeinated by sonatype


SITE RELIABILTY
ENGINEERING

Summary

- Least Privilege is important
- but... complicated on Kubernetes
- RBAC
- You can automate...
- Infra makes it easier

ALL DAY DEVOPS

caffeinated by sonatype

NOVEMBER 10, 2022

I am Cluster Admin, Destroyer of Everything You Hold Dear

SITE RELIABILITY ENGINEERING

Matt Williams, Evangelist @ Infra
@technovangelist


ADDO
ALL DAY DEVOPS
caffeinated by sonatype