CONTINO

Kubernetes Is Hard, But Worth It.
Here's How To Get Started.

Today's Hosts:

James Strong - Cloud Native Director
Gregory Patmore - Technical Principal
Kurt Karpov - Solutions Principal

About Contino

We work with the World's Leading Brands to help them with measurable transformation, through the adoption of Enterprise DevOps, Cloud Native Computing and Data Platforms.

We help our clients build their own innovation engine which allows them deliver better software faster and more efficiently as part of their digital transformation ambitions.

400+
People

The deepest pool of DevOps & cloud transformation talent in the industry

5
Global offices

We can scale rapidly to support diverse client requirements across the globe

500+
Engagements

More DevOps transformation executed than any other professional services firm

250+
Customers

Specialising in helping the world's leading brands accelerate digital transformation

Ministry of Justice · Allianz · vodafone · BARCLAYS · adidas · HSBC · verizon · NSW Government Transport for NSW

Kurt Karpov

Solutions Principal

kurtkarpov

CONTINO

James Strong

Cloud Native Director

@strongjz

strongjz

CONTINO

Gregory Patmore

Technical Principal

gregory-patmore

CONTINO

Ground Rules

How We'll Proceed:

- Go with the flow
- Chat is live and useful for communicating with the group
  - Audience is Muted
- Questions will be captured in the "Questions" block.
  - Questions may be answered in line during the event through the "Questions" block
  - Questions will be reviewed live at the end

Getting Started

This webinar will cover:

- **Getting started with Kubernetes** - laying the foundations for success
- Clusters: **Set up, security and operations**
- **Best practices** for container and Kubernetes adoption
- **Securing** containers
- **Optimising application development** in Kubernetes environments

Why Kubernetes?

- What problem are you solving?
- How variant is your traffic?
- Is your team familiar with containerized applications?
- Do you have a good release process?
- Do you want to separate the management of the infrastructure from the applications?
- Do you frequently have too much or not enough compute power for your applications and deployment processes?

Agenda

01 | Containers

- Architecture
- Builds

02 | Workloads

- Workload basics
- Sidecars

03 | Logistics

- Build Pipelines
- Change Control
- Deployment

04 | Clusters

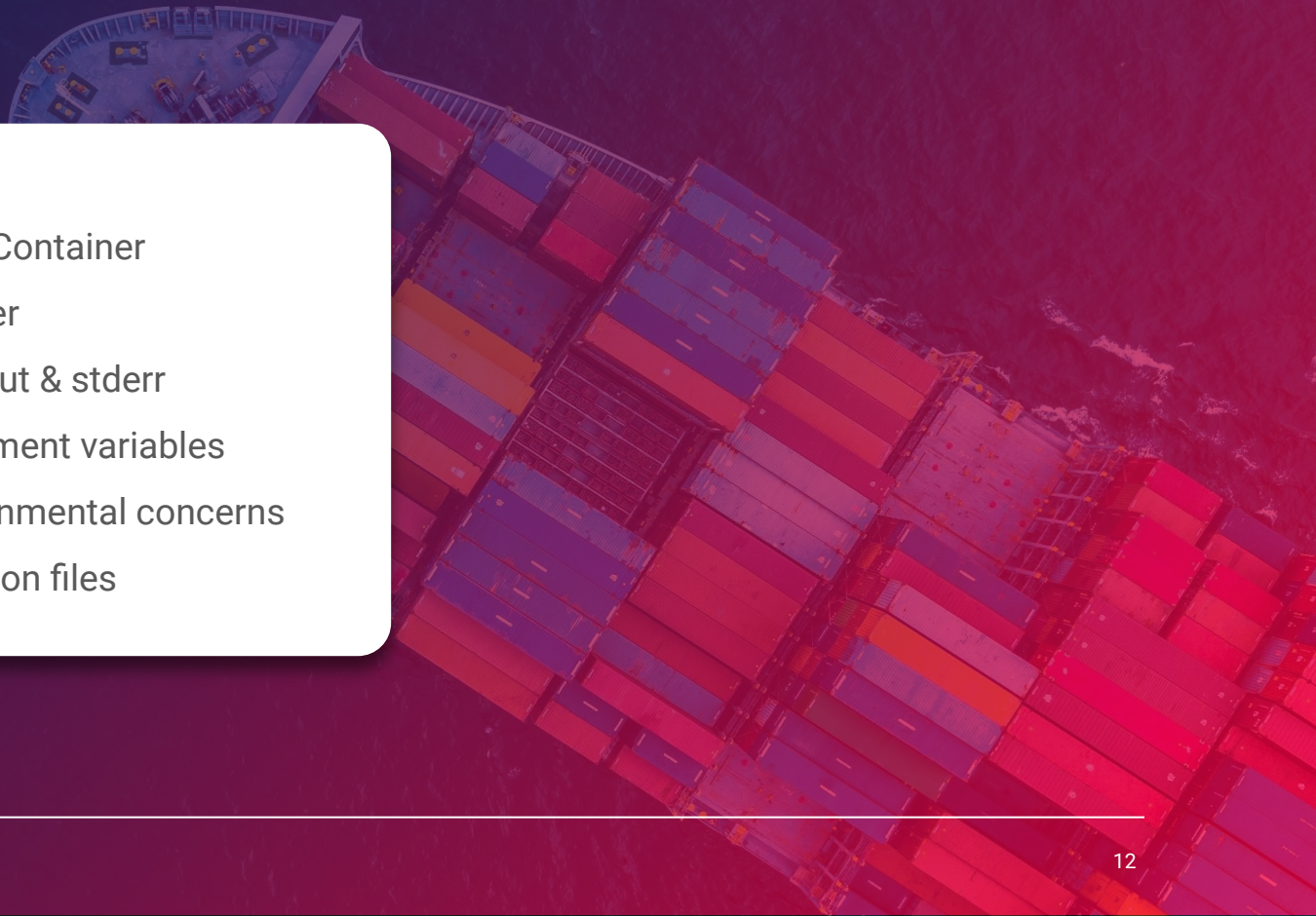
- Cluster Setup
- Cluster Admin

05 | Security

- Pipeline
- Operating Environments

06 | Developer Experience

Containers



- Minimal OS
- One Process per Container
- Run with local user
- Write logs to stdout & stderr
- Leverage environment variables
- Separating environmental concerns
- Mount configuration files

Minimal Container OS

Alpine

Debian Slim

AWS BottleRocket

Custom

Minimal Host OS

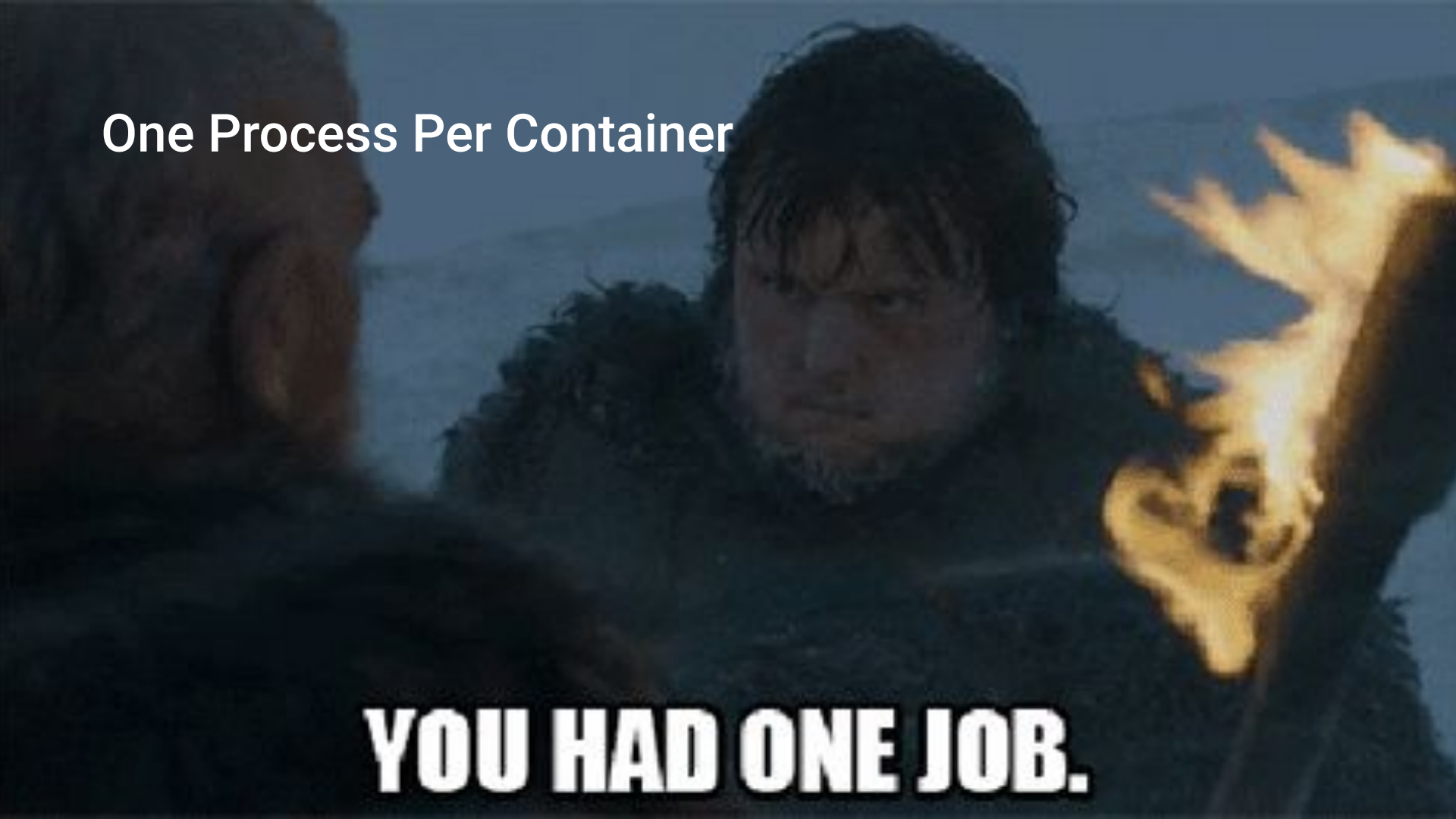
Redhat CoreOS

RancherOS

Ubuntu Core OS

Vmware Photon OS

One Process Per Container

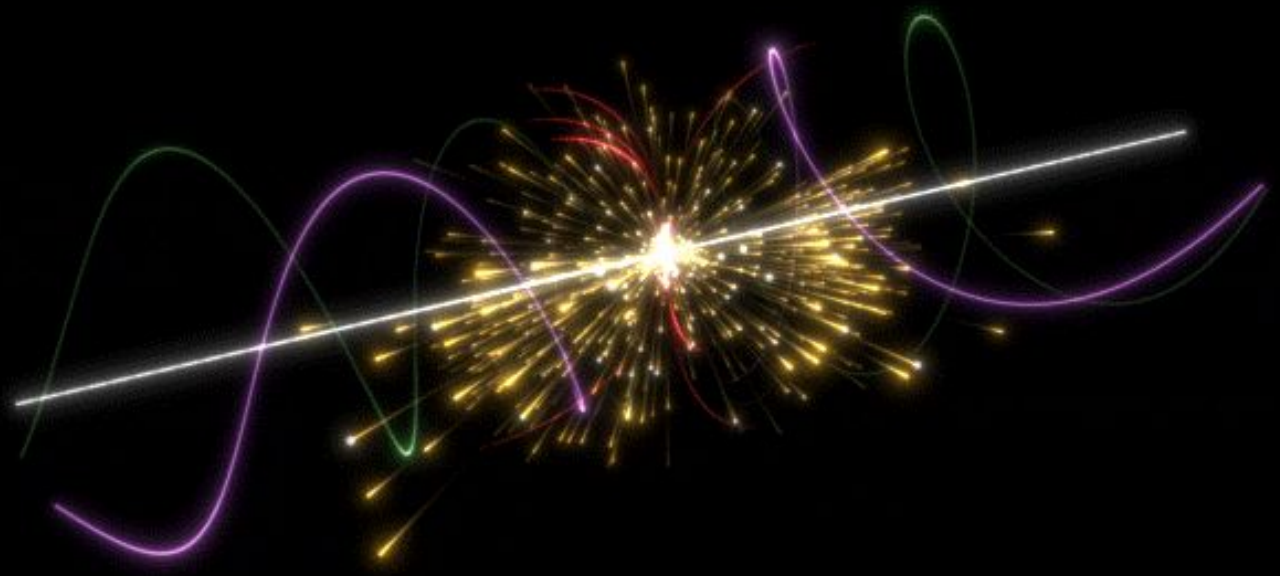


Run With Local User

- Don’t run as root
- Run with local user
- Docker File
- RBAC

Write logs to stdout & stderr

Environment Variables



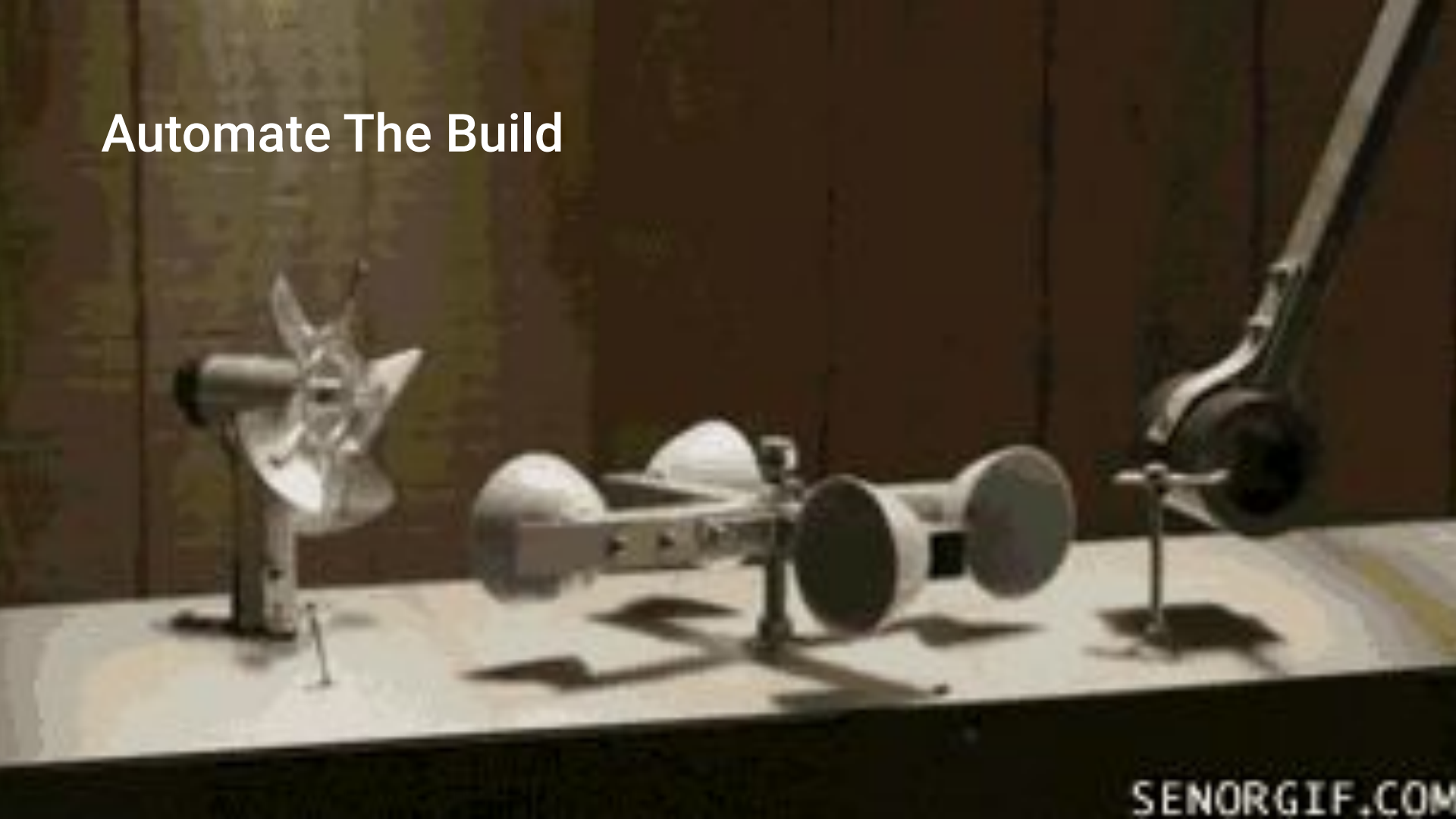
Configuration

- Database endpoints vs. Feature Flags
- App config where?
- Separate env config

Container Builds

- Automate the build process
- Avoid using :latest tags
- Establish a base container to reduce build times
- Test early, test often and track measurable differences
- Invest in implementing a solid versioning strategy right away

Automate The Build



Versioning

- Invest in Strategy
- Containers follow build Versions of Software
- Metadata

Latest Tag

- Avoid using :latest tags
  - Unable to control
  - Unknown updates
- Versions the way to go
- Container digest

Base Container

- Reduce Build Times
- Scratch Container

Testing

- Early & Often
- Track Differences
- Points of Measure

Workloads

- Workload basics
- Sidecars
- Periodic Jobs

Workload Basics

- Higher Level Objects
- Deployments & StatefulSets
- Not Replica Sets or Bare Pods

Sidecars

- The Fun Stuff
- You need it? I can get it.
- Think like Dr Frankenstein

Jobs

- “Cronjobs as a service”
- Make sure to account for the resources it will use.
- Consider using a proper deployment for frequent jobs

Logistics

- Build Pipelines
- Change Control
- Deployment

Build Pipeline

- Automating your build pipelines
  - Visibility
  - Troubleshooting
  - Defect Remediation
- Build small autonomous pieces

Change Control

- Easy as long as nothing changes
- Practice Practice Practice
- Automation pays dividends, got the hint yet?

Deployment

- Checklist
- Resources
- Automation

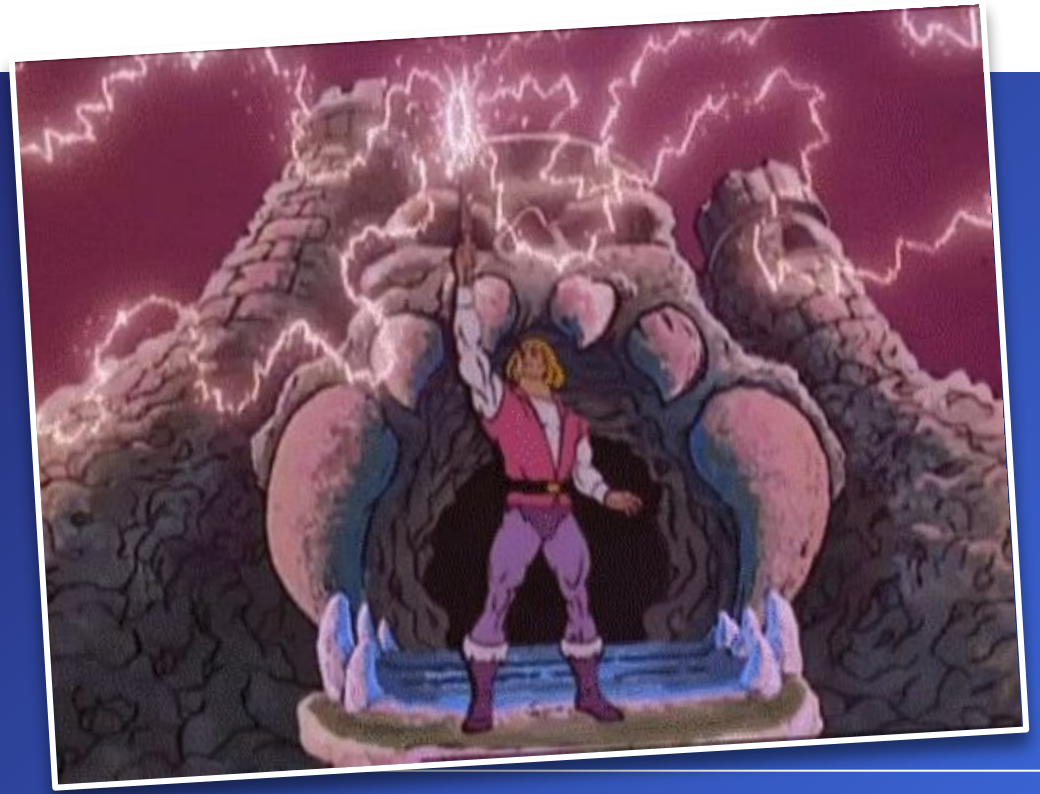
Clusters

- Cluster Setup
  - Nodes
  - Network isolation
  - Storage
  - Application programming interface (API) management

Nodes

- Auto-Upgrades
- Liveness-monitoring
- Validation of setup

Master Nodes



- Load Balanced
- HA
- Updates

Network Isolation

- Per Namespace
- Default Deny

Storage

- Make sure it's flexible
- Make sure you know what your storage engines will do
-

Application Programming Interface (API) Management

- Critical to Cluster Operations
- Authentication Use
- TLS
- Admission Control

Cluster Admin

- Cluster Admin
  - Namespaces
  - **Namespace Quotas**
  - Resources
  - Monitoring
  - **Backup**
  - **Auto-scaling groups**

Namespaces

- Organize
- Privileges
- Isolation

Namespaces Quotas

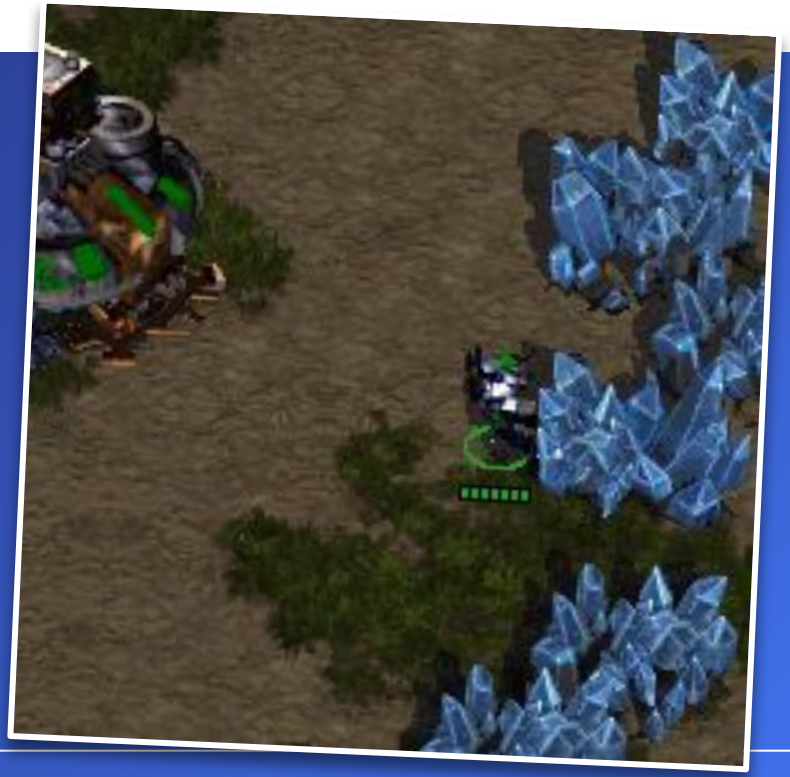
- Noisy neighbors
- Understanding application requirements
- Limits and Requests

Monitoring

- What to look at?
- What to use?

Resources

- Upgrading
- CPU/Memory
- Limits/Requests
- OOM



Autoscaling

Security

- Containers
- Kubernetes
- Pipeline
- Operating Environments
- Network policies
- Container Runtime Security
- RBAC

Secure Containers

- DISABLE ROOT
- Least Privilege
- Run time, Pipeline & Network practices
- DISABLE ROOT

Secure Pipelines

- Signed Images
- Verify Trusted Images
- Kickoff Security Assessment

Operating Environment

- Dev, Test, Prod, Others
- Shared Kernel
- Kube-bench

Network Policies

- Per Namespace
- Per application
- Examples

Container Runtime Security

- Pipeline
- Run time
- Registry

RBAC

- Avoid default service accounts
- Cluster or Role
- Grouping as appropriate

Developer Experience

- Lorem Ipsum
- Lorem Ipsum
- Lorem Ipsum

Adopting Containers

- Make it easy!
- Set up a base container with common tools/technologies.
- Enable local development
- Automate, automate, automate.

Adopting Kubernetes

- Working Group
- Enable local development (kind, minikube)
- Create a reference application and good docs
- Workshops and user groups.

CONTINO
CLOUDFEST

Join us **Wednesday 22 April** for the next webinar:

Boost Your Applications With an SRE Approach to Development

VIEW UPCOMING WEBINARS

Introduction to Kubernetes

Thursday 7 May | 9:00am - 5:00pm BST

REGISTER HERE

Useful References

https://github.com/contino/kubernetes-best-practices

james.strong@contino.io

greg.patmore@contino.io

CONTINO

Thank You.

London
london@contino.io

New York
newyork@contino.io

Melbourne
melbourne@contino.io

Sydney
sydney@contino.io

Atlanta
atlanta@contino.io

www **contino.io** **continohq** **contino**