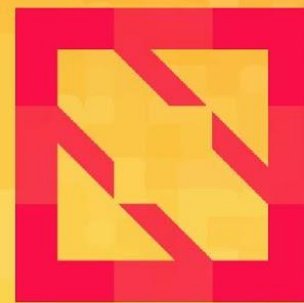




KubeCon



CloudNativeCon

North America 2019

Moving from Legacy Infrastructure to the Cloud in a Government Organization

Chris Carty, CKA, Senior Developer / Integrator, City of Ottawa

Capital of Canada



KubeCon



CloudNativeCon

North America 2019



I live here

Temperature



KubeCon



CloudNativeCon

North America 2019

- Record low with windchill -47.8C (-54F)
- Record high with humidex +47.2 (+117F)

-47C --> +47C

Size

- Population just hit 1 million
- In 2001, 11 cities and townships amalgamated
- Ottawa is big: 2,796km² (1737mi²)



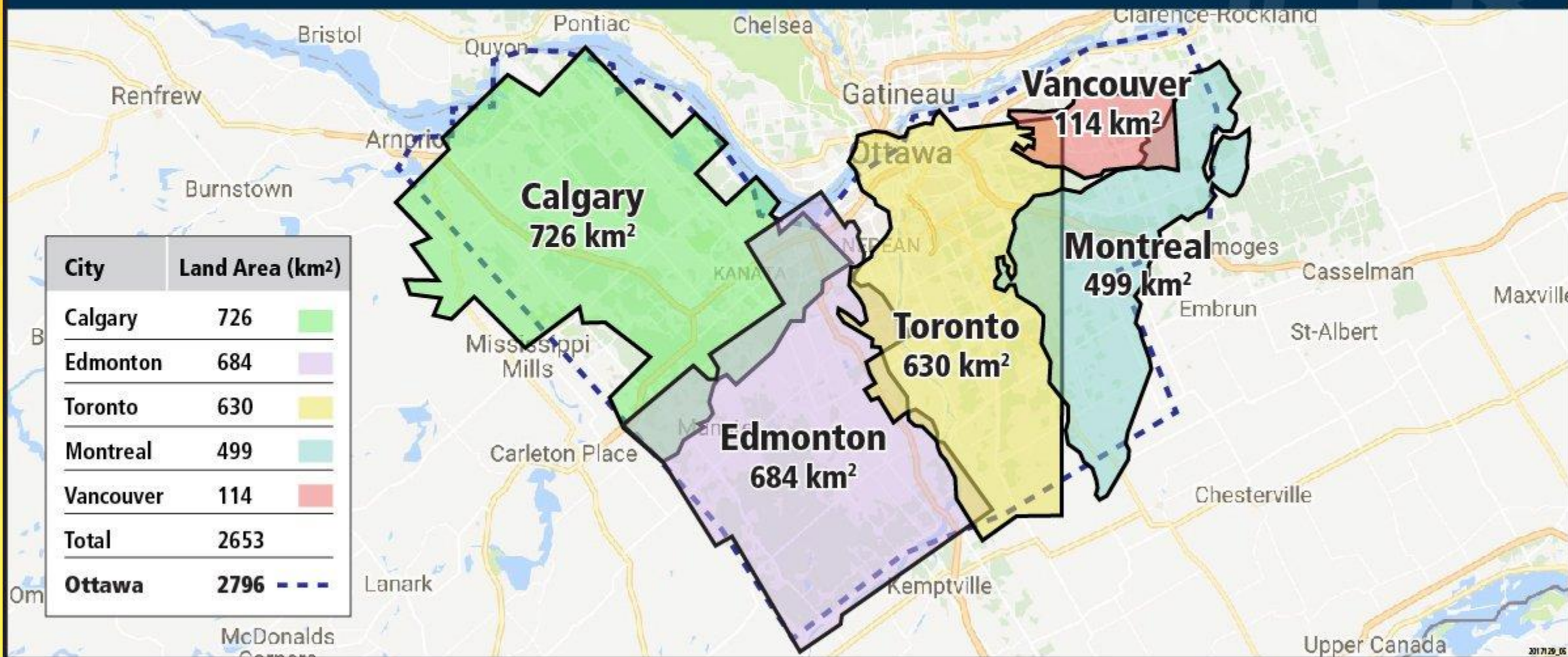
KubeCon



CloudNativeCon

North America 2019

Ottawa's scale in perspective



City of Ottawa Complexity



KubeCon



CloudNativeCon

North America 2019

Supports for federal government workers, addresses urban and rural concerns, and maintains infrastructure through temperature extremes

- 17,000+ employees (300+ IT)
- 120+ different lines of business
- 400+ Applications (CoTs, Java, dotNet, Perl)

Part 1:

How to Do Kubernetes Stuff

Who, Where, How to Deploy



CNCF Landscape



KubeCon



CloudNativeCon

North America 2019

CNCF Cloud Native Landscape
2019-11-02T13:33:39Z fa1e71d

Overwhelmed? Please see the CNCF Trail Map. That and the interactive landscape are at l.cncf.io

Database Streaming & Messaging Application Definition & Image Build Continuous Integration & Delivery Platform Observability and Analysis

App Definition and Development Scheduling & Orchestration Coordination & Service Discovery Remote Procedure Call Service Proxy API Gateway Service Mesh

Cloud Native Storage Container Runtime Cloud Native Network

Automation & Configuration Container Registry Security & Compliance Key Management

Provisioning

Platform

Observability and Analysis

Monitoring Logging Tracing Chaos Engineering

Serverless

Members

Special

Kubernetes Certified Service Provider

Kubernetes Training Partner

Cloud Native Landscape
CLOUD NATIVE COMPUTING FOUNDATION
Redpoint Amplify

This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path.

l.cncf.io

Break Things Down

1. K8s Distribution (Cluster Management)
2. Security
3. Storage
4. CI/CD
5. Container Registry
6. Monitoring
7. Key Management
8. Ingress



KubeCon



CloudNativeCon

North America 2019

CLOUD NATIVE TRAIL MAP

The Cloud Native Landscape [Landscape](https://landscape.cncf.io) has a large number of options. This Cloud Native Trail Map is a recommended process for leveraging open source, cloud native technologies. At each step, you can choose a vendor-supported offering or do it yourself, and everything after step #3 is optional based on your circumstances.

HELP ALONG THE WAY

A. Training and Certification

Consider training offerings from CNCF and then take the exam to become a Certified Kubernetes Administrator or a Certified Kubernetes Application Developer

cncf.io/training

B. Consulting Help

If you want assistance with Kubernetes and the surrounding ecosystem, consider leveraging a Kubernetes Certified Service Provider

cncf.io/kcsp

C. Join CNCF's End User Community

For companies that don't offer cloud native services externally

cncf.io/enduser

WHAT IS CLOUD NATIVE?

Cloud native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach.

These techniques enable loosely coupled systems that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil.

The Cloud Native Computing Foundation seeks to drive adoption of this paradigm by fostering and sustaining an ecosystem of open source, vendor-neutral projects. We democratize state-of-the-art patterns to make these innovations accessible for everyone.



1. CONTAINERIZATION

- Commonly done with Docker containers
- Any size application and dependencies (even PDP-11 code running on an emulator) can be containerized
- Over time, you should aspire towards splitting suitable applications and writing future functionality as microservices

3. ORCHESTRATION & APPLICATION DEFINITION

- Kubernetes is the market-leading orchestration solution
- You should select a Certified Kubernetes Distribution, Hosted Platform, or Installer: cncf.io/ck
- Helm Charts help you define, install, and upgrade even the most complex Kubernetes application

5. SERVICE PROXY, DISCOVERY, & MESH

- CoreDNS is a fast and flexible tool that is useful for service discovery
- Envoy and Linkerd each enable service mesh architectures
- They offer health checking, routing, and load balancing

7. DISTRIBUTED DATABASE & STORAGE

When you need more resiliency and scalability than you can get from a single database, Vitess is a good option for running MySQL at scale through sharding. Rook is a storage orchestrator that integrates a diverse set of storage solutions into Kubernetes. Serving as the "brain" of Kubernetes, etcd provides a reliable way to store data across a cluster of machines. TiKV is a high performance distributed transactional key-value store written in Rust.



9. CONTAINER REGISTRY & RUNTIME

Harbor is a registry that stores, signs, and scans content. You can use alternative container runtimes. The most common, both of which are OCI-compliant, are containerd and CRI-O.

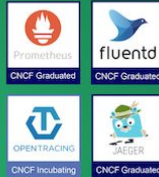


2. CI/CD

- Setup Continuous Integration/Continuous Delivery (CI/CD) so that changes to your source code automatically result in a new container being built, tested, and deployed to staging and eventually, perhaps, to production
- Setup automated rollouts, roll backs and testing

4. OBSERVABILITY & ANALYSIS

- Pick solutions for monitoring, logging and tracing
- Consider CNCF projects Prometheus for monitoring, Fluentd for logging and Jaeger for Tracing
- For tracing, look for an Open Tracing-compatible implementation like Jaeger



6. NETWORKING & POLICY

To enable more flexible networking, use a CNI-compliant network project like Calico, Flannel, or Weave Net. Open Policy Agent (OPA) is a general-purpose policy engine with uses ranging from authorization and admission control to data filtering.



8. STREAMING & MESSAGING

When you need higher performance than JSON-Rest, consider using gRPC or NATS. gRPC is a universal RPC framework. NATS is a multi-modal messaging system that includes request/reply, pub/sub and load balanced queues. CloudEvents is a specification for describing event data in common ways.



10. SOFTWARE DISTRIBUTION

If you need to do secure software distribution, evaluate Notary, an implementation of The Update Framework.



KubeCon



CloudNativeCon

North America 2019

1. Containerization
2. CI/CD
3. Orchestration & Application Definition
4. Observability & Analysis
5. Service Proxy, Discovery, & Mesh
6. Networking & Policy
7. Distributed Database & Storage
8. Streaming & Messaging
9. Container Registry & Runtime
10. Software Distribution

Selecting a Distribution

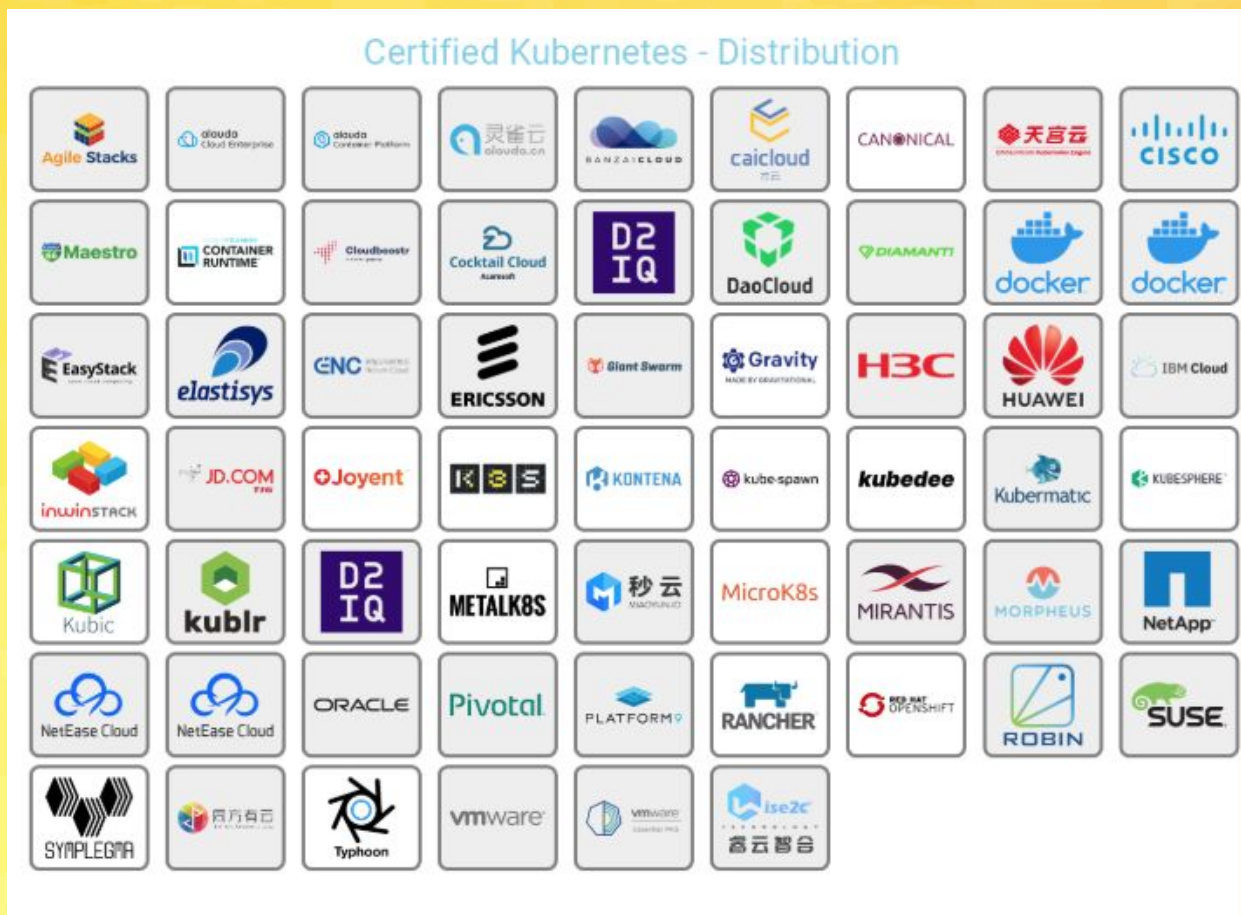


KubeCon



CloudNativeCon

North America 2019



Setting Objectives



KubeCon



CloudNativeCon

North America 2019

- **Vendor Agnostic** - keep options open for evolving technology
- **Open Source Kubernetes**
- **On-Prem and Public Cloud** - sensitive workloads on-prem
- **Multiple Clusters** - security blast radius
- **Enterprise Level Support** - no team with knowledge onsite
- **Future Support for Windows Containers**
- **Role Based Access Controls** - granular security controls

Try Things Out



KubeCon



CloudNativeCon

North America 2019

- Use open source software to test before commitment
- Leverage the tools you already have
- Try trial demos (Vendor Hall)

Allows for a detailed Request For Proposal or Sole Source

Patterns Over Tools



KubeCon



CloudNativeCon

North America 2019

Tools should be swappable to give the flexibility to meet the changing needs of various teams and new tools available

People → Process → Technology

Our Stack



KubeCon



CloudNativeCon

North America 2019

- **Orchestration:** Kubernetes, Rancher, Azure Kubernetes Service
- **Observability:** Prometheus/Grafana, ELK Stack
- **Security:** Open Policy Agent, Network Policies, Kube-Bench/Hunter
- **Service Mesh:** Linkerd
- **CI/CD:** Fluxcd, GitLab, Azure DevOps
- **Registry:** Harbor
- **Storage:** NetApp Trident, Longhorn
- **Ingress:** ingress-nginx



Part 2:

How to Get People to Use It

The Hard Part

Growing Awareness



KubeCon



CloudNativeCon

North America 2019

- Lunch presentations
- Senior management presentations
- Team presentations
- One-on-one sessions
- Phippy and Friends



Full adoptions requires massive cultural shifts in legacy organizations.
Go slow, be patient, and get it right.

Finding Pain Points



KubeCon



CloudNativeCon

North America 2019

Meet with project teams to discover specific pain points

Offer carrots not sticks

- Scalability - ability to spin up new instances without pre-provisioning servers
- Self healing - reduced on call



Automate All of the Things



KubeCon



CloudNativeCon

North America 2019

Automate where possible to minimize knowledge needed to deploy to Kubernetes. Not all users need to be experts.

- Create starter templates that follow best practices
- Continuously iterate for easier adoption as issues are identified

Migrating Applications

- Legacy Perl and Java apps
- Migrating from Unix To Kubernetes
- Similar Build/Deploy Process



KubeCon



CloudNativeCon

North America 2019

Drag and Drop Deploy



KubeCon



CloudNativeCon

North America 2019

 CI/CD configuration

Auto DevOps enabled

 Add Kubernetes cluster

Name	Last commit	Last update
 .gitlab-ci.yml	updated project name	2 days ago
 Dockerfile	first commit	2 months ago
 graffiti.war	Replace graffiti.war	1 month ago

Added Metrics

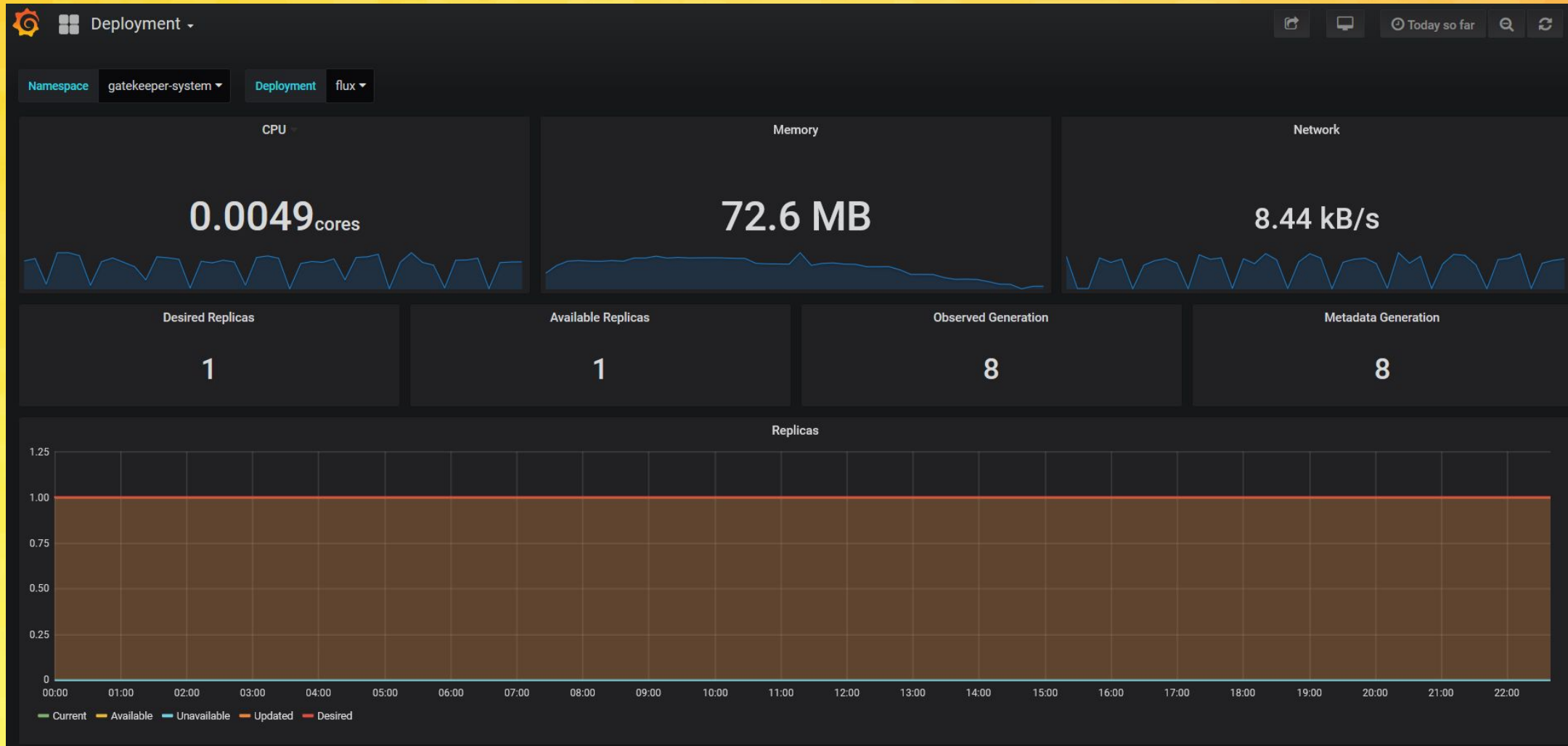


KubeCon



CloudNativeCon

North America 2019



Traffic

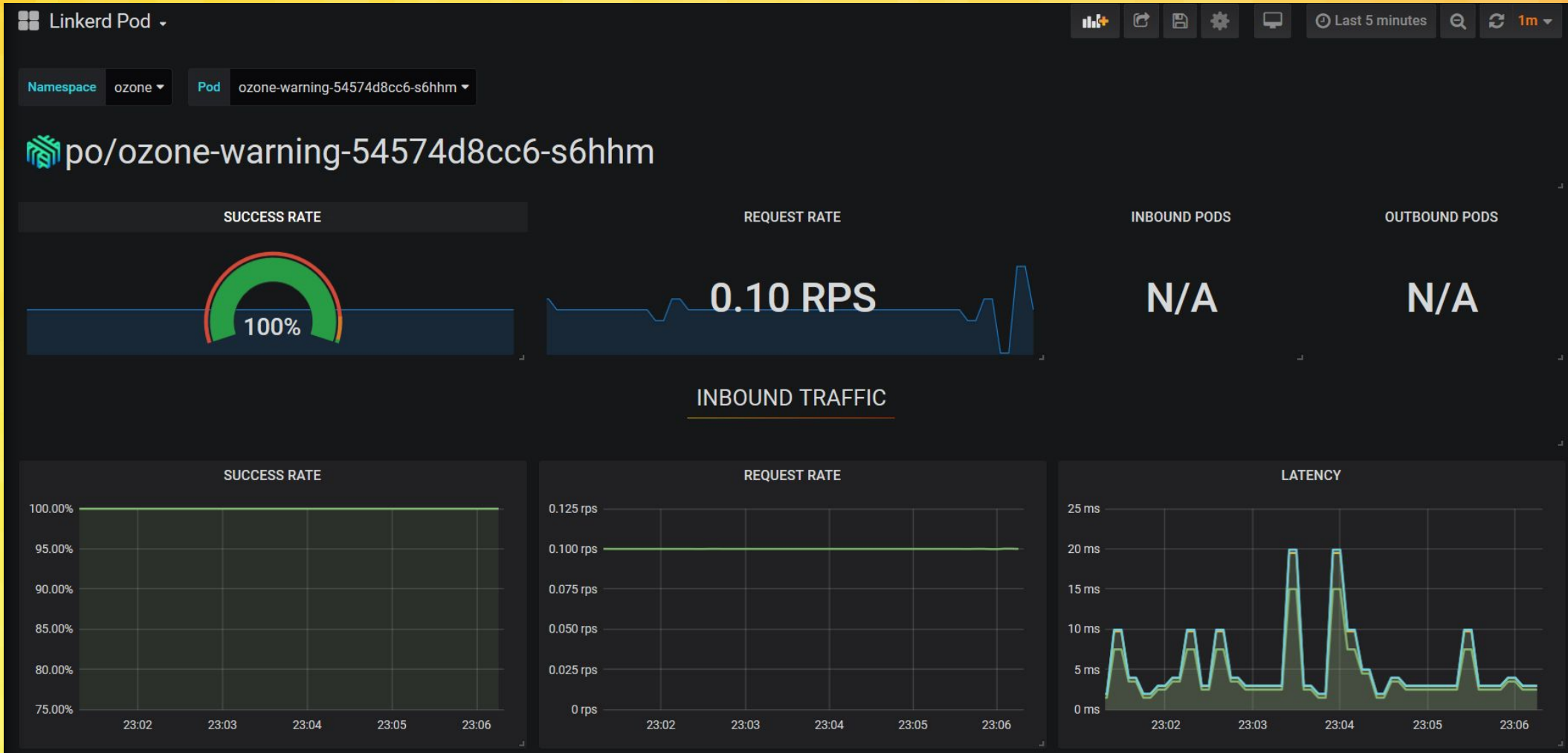


KubeCon



CloudNativeCon

North America 2019



Linkerd



KubeCon



CloudNativeCon

North America 2019

deployment/ozone-warning meshed

Unmeshed

- po/exporter-node-cluster-monitoring-6v6ls
- po/weave-scope-agent-weave-scope-6qmj5
- po/nginx-ingress-controller-tndc4
- po/canal-44l7t
- po/cattle-node-agent-wg8jl

deploy/ozone-warning

SR	100.00%
RPS	0.1
P99	20 ms

LIVE CALLS ROUTE METRICS

	Name	Method ↑	Path ↑	↓ Count	↑ Best	↓ Worst	↑ Last	↑ Success Rate	Tap
FROM	10.100.48.236 🔗	GET	/	3	4 ms	7 ms	4 ms	100.00% ●	🔗
FROM	10.100.48.236 🔗	GET	/	2	4 ms	15 ms	15 ms	100.00% ●	🔗
FROM	10.100.48.236 🔗	GET	/	2	3 ms	4 ms	4 ms	100.00% ●	🔗
FROM	10.100.48.236 🔗	GET	/	2	3 ms	14 ms	3 ms	100.00% ●	🔗
FROM	10.100.48.236 🔗	GET	/	2	3 ms	4 ms	3 ms	100.00% ●	🔗

Training



KubeCon



CloudNativeCon

North America 2019

Provide tools and guidance for developers to learn at their own pace

- One-on-one and team mentoring
- Pluralsight
- Katacoda
- CNCF Kubernetes Fundamentals
- kubernetes.io/tasks
- Kubernetes the Hard Way

Conclusion

Current State - If You Build It...



KubeCon



CloudNativeCon

North America 2019

- Internal Dev, QA and Prod and External QA and Prod clusters
- 3 Teams are engaged and actively developing + others testing
- First application with public traffic in prod
- Azure App Service and VMs are competing systems in use

Looking Ahead



KubeCon



CloudNativeCon

North America 2019

- First Java Applications will be going live for external traffic
- Internal web forms will be served internally
- Corporate Container Security Standards will be approved
- Service accounts setup and cloud governance
- Increased automation tooling (ie Terraform)

Key Takeaways

1. Set objectives
2. Work through your pathway
3. Develop patterns
4. Patiently spread awareness
5. Dangle “carrots”
6. Automate all the things
7. Come back next year



KubeCon



CloudNativeCon

North America 2019

Resources / Contact

- github.com/cartych/kube-con-resources
- Follow me @macintoshprime
- email: christopher.carty@ottawa.ca



KubeCon



CloudNativeCon

North America 2019

Questions / Discussion