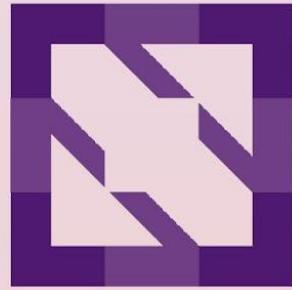




KubeCon

— North America 2023 —



CloudNativeCon





KubeCon



CloudNativeCon

North America 2023

How Intuit Built a Paved Road for Debuggability!

Anusha Ragunathan & Kevin Downey, Intuit Inc

Agenda

- 01 Background
- 02 Problem
- 03 Interactive debugging using Ephemeral Containers
- 04 1-click debugging using Argo Workflows
- 05 Takeaways



KubeCon



CloudNativeCon

North America 2023

Background

AI-driven expert platform



KubeCon



CloudNativeCon

North America 2023

Modern Dev Experience

Enables Intuit engineers to develop code in a fast, secure, and compliant fashion; from app experiences to runtime and traffic management to smart operations.



2500+
services

9x
Increase in dev productivity since 2019

~1M
Active CPU cores

40M+
AIOps inference/day

315
Kubernetes clusters

28k+
namespaces

1k+
teams



KubeCon

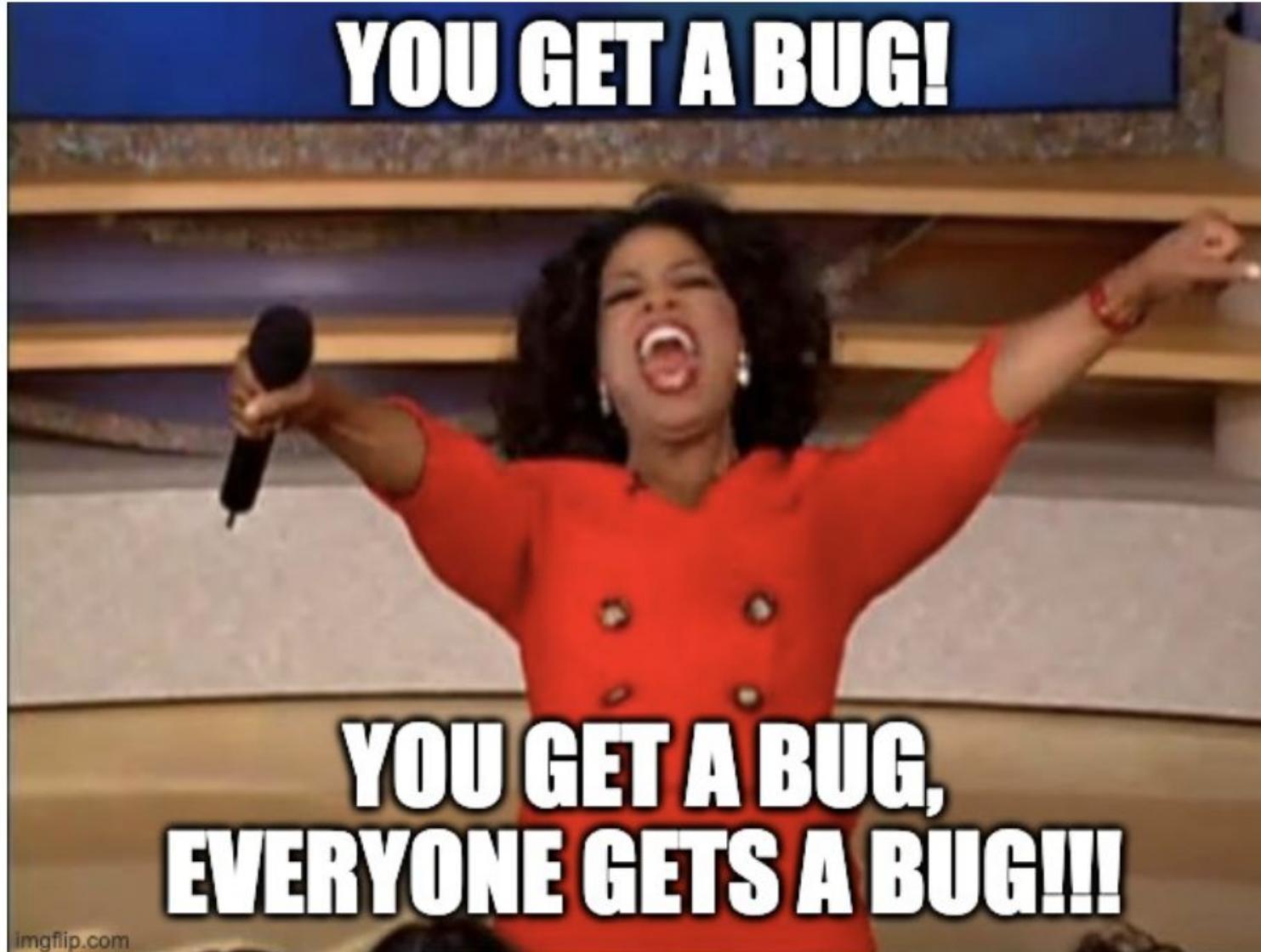


CloudNativeCon

North America 2023

Problem

Bugs! Bugs! Bugs!



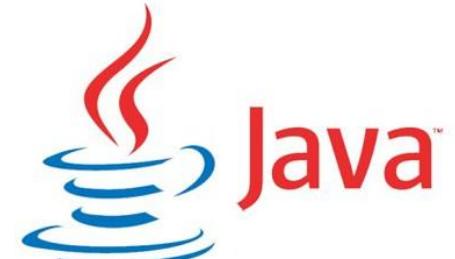
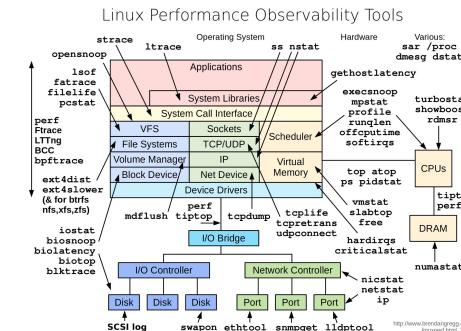
Problem 1: Debug Tooling Setup



```
kubectl exec <pod> -c <app-ctr>
```



```
> cat /etc/issue 66 uname -r  
Debian GNU/Linux wheezy/sid \n \l  
3.2.0-2-amd64  
:  
=> echo $SHELL 66 echo $SSH_VERSION  
/usr/bin/zsh  
4.3.17  
:  
> cd Documents  
>Documents  
=> mkdir Wikipedia  
>Documents  
=> Wikipedia  
>Documents/Wikipedia  
>> ..  
>Documents  
> cd /boot/1  
Compli: directory  
bin/ boot/ home/ [root@] root/ var/  
etc/ conf/ init/ lib/ run/ sys/  
dev/ lib64/ apt/ skin/ [root@] root/  
etc/ test@found/ proc/ selinux/ root/
```



Problem 2: Abstractions & Debugging



Application Intent



```
1 apiVersion: iks.intuit.com/v1beta1
2 kind: ExpressApplication
3 metadata:
4   name: kubecon2023-java
5 spec:
6   components:
7     - type: webservice
8       name: arag-java
9       image: docker.intuit.com/sandbox-sandbox/arag-java/service/arag-java:0.0.3
10      traits:
11        - type: sizing
12          properties:
13            vertical:
14              size: small
15            horizontal:
16              size: small
```

Platform Abstraction



Kubernetes

Problem 2: Abstractions & Debugging

Before Platform Abstraction



I have access to my namespace

kubectl
events

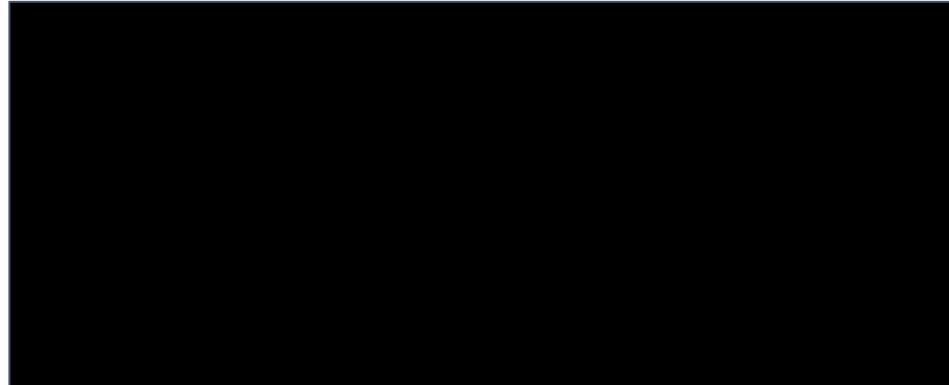
kubectl
exec

kubectl
debug

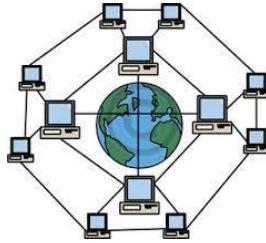
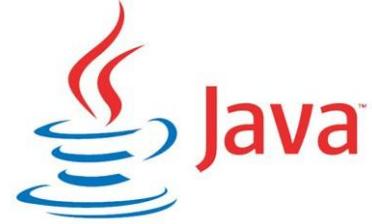
After Platform Abstraction



I don't have access to my namespace



Problem 3: Fragmented Expertise



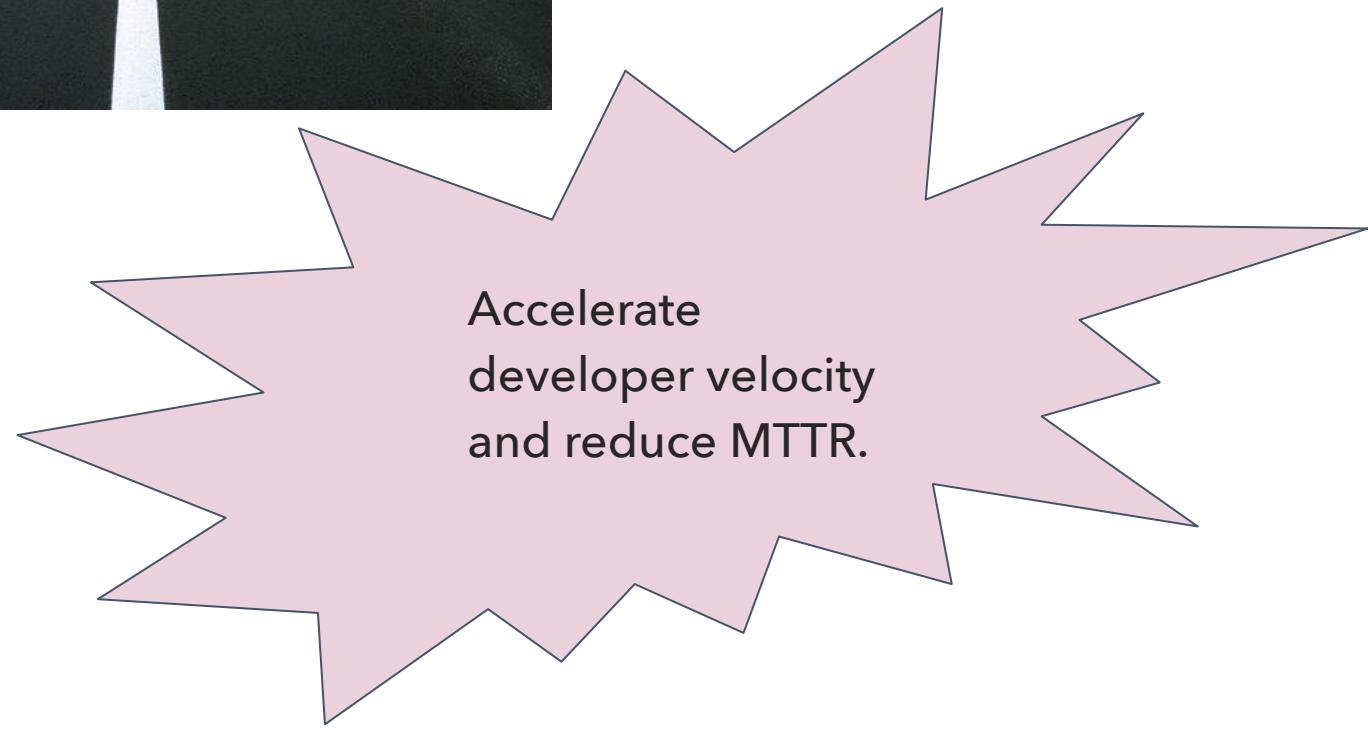
Fragmented Debug Expertise;

Takes longer for incident debugging, root cause and resolve.

Solution: Debuggability Paved Road



Debugging super powers offered through a Debuggability Paved Road.





KubeCon



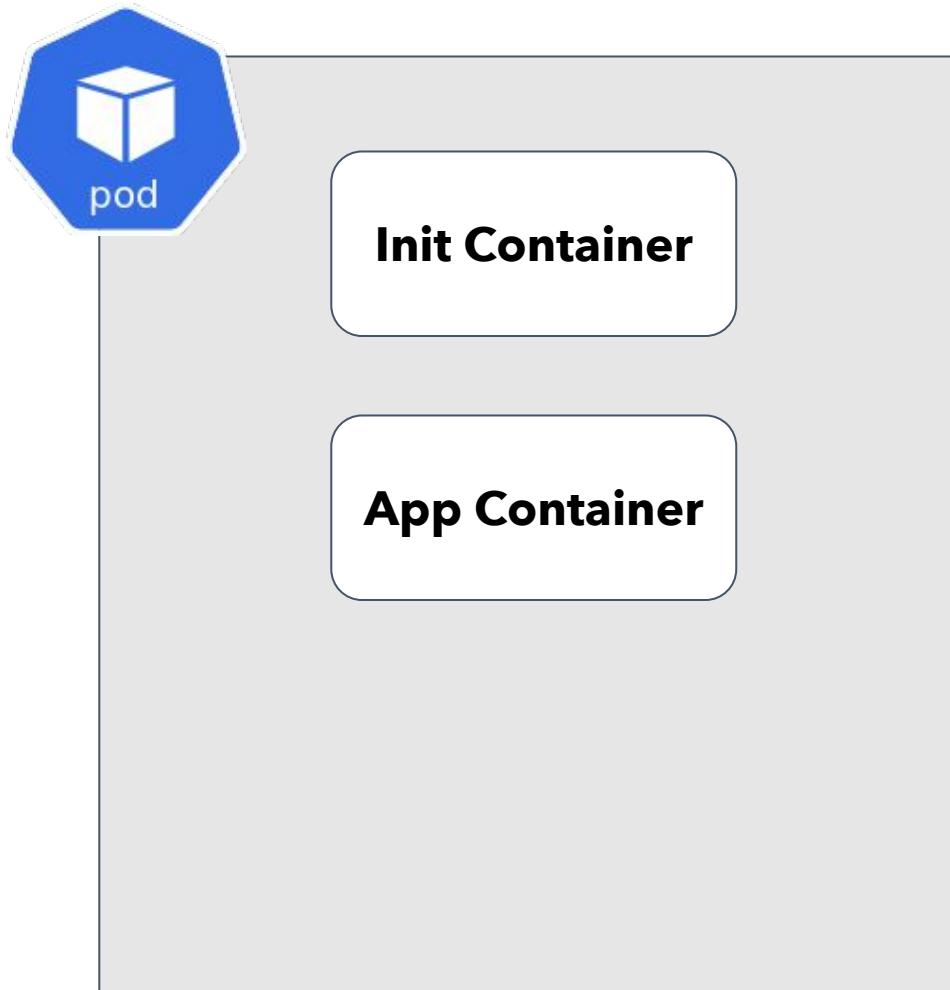
CloudNativeCon

North America 2023

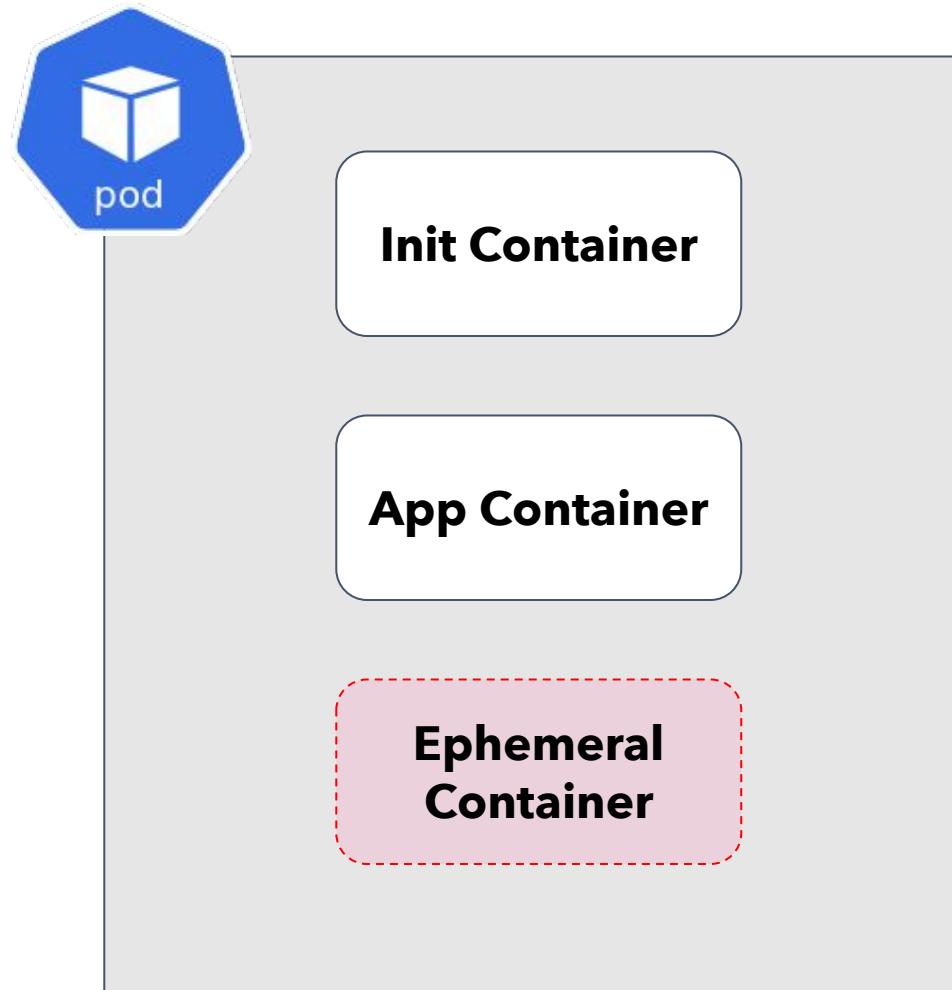
Interactive Debugging Using Ephemeral Containers

Ephemeral Containers

Before Kubernetes 1.23



Kubernetes 1.23 - Ephemeral Ctrs Beta
Kubernetes 1.25 - Ephemeral Ctrs GA



Debug Shell UI Access



KubeCon



CloudNativeCon

North America 2023

INTUIT Development Portal

All Search for assets, accounts, projects or documents

Home > Playground-btzeng > Btzeng031023

Btzeng031023 ★
Asset ID: 8680864205712305
Asset Alias: Intuit.l1name.l2na

Debug

Debug List Logging Levels Debug Shell

Workspace: sandbox-sandbox-btzeng031023-e2e

Max number of connection is 3 per host.
Session expires in 8 hours.

Select hosts to connect

Select a host

Search or select

Connect

Overview API Document Service Configuration Additional Configuration Downstream Services Credentials Upstream Clients Realtime Analytics Compliance Report

E2E Work Region IAM Role Service Heal Links External



KubeCon

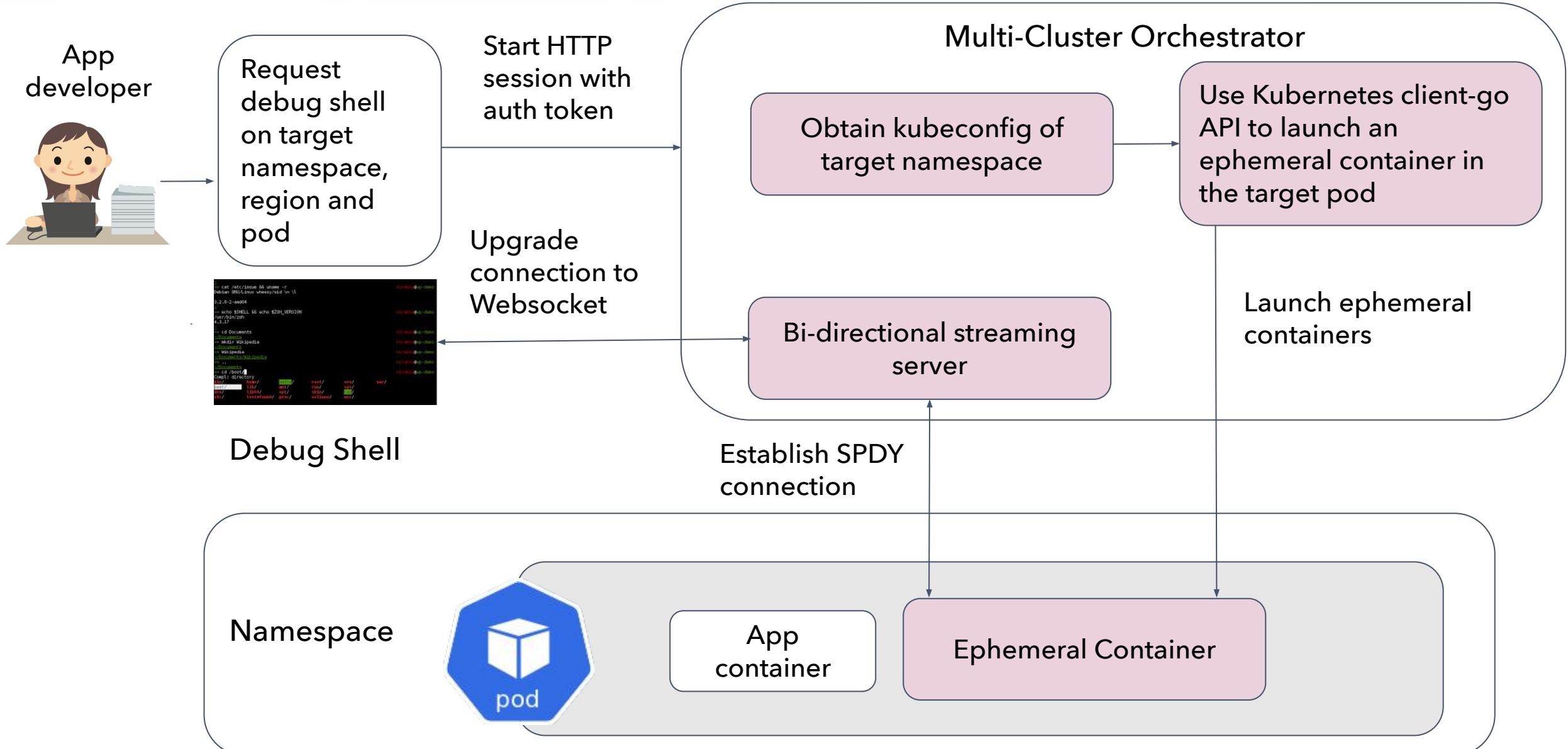


CloudNativeCon

North America 2023

Debug Shell Demo

Interactive Debugging Using Ephemeral Containers



What's in the debug container image ?

- Shell
- Package manager
- General purpose Linux debugging tools (eg, strace, lsof)
- Language specific debugging tools (eg, jmx for Java)
- Cloud provider tools (eg, aws cli)
- Network debugging tools (eg, tcpdump, netstat, arp, nslookup)
- Storage debugging tools (eg, fdisk)
- Misc

Ephemeral Containers: Security

- Session termination after an inactive interval of 30 minutes.
- **RBAC** controlled.
- OPA **policies** extend to debug container as well
- **Audit** records
- **Throttling** limits on:
 - per pod
 - per user
 - number of concurrent debug sessions per cluster
 - number of concurrent debug sessions across all clusters.



KubeCon



CloudNativeCon

North America 2023



1-Click Debugging Using Argo Workflows

1-Click Debugging Using Argo Workflows: Intro

- Argo is a [Cloud Native Computing Foundation \(CNCF\)](#) graduated project.
- Open Source with an Active Community

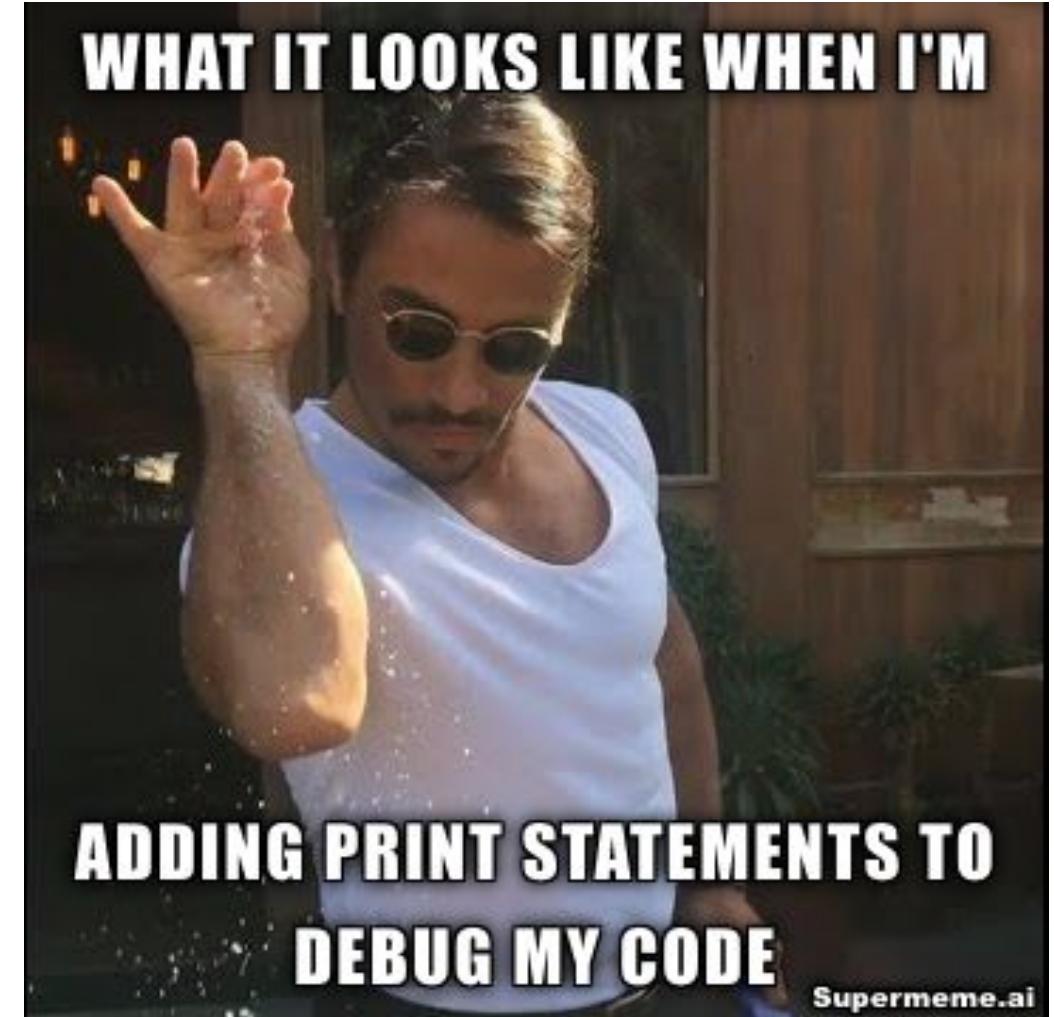
```
apiVersion: argoproj.io/v1alpha1
kind: Workflow
metadata:
  generateName: whalesay-
spec:
  entrypoint: whalesay
  templates:
  - name: whalesay
    container:
      image: docker/whalesay:latest
      command: [cowsay]
      args: ["Hello, Argo!"]
```

Argo Workflows
Kubernetes-native workflow engine supporting DAG and step-based workflows.



1-Click Debugging Using Argo Workflows: Problem

- Developers will need to occasionally debug **running code**.
- Specific debugging techniques are required based on the the **language** and **framework**.
- Preserving application **context** when debugging is important.
- Having the right **tools** or **access** can be a challenge.

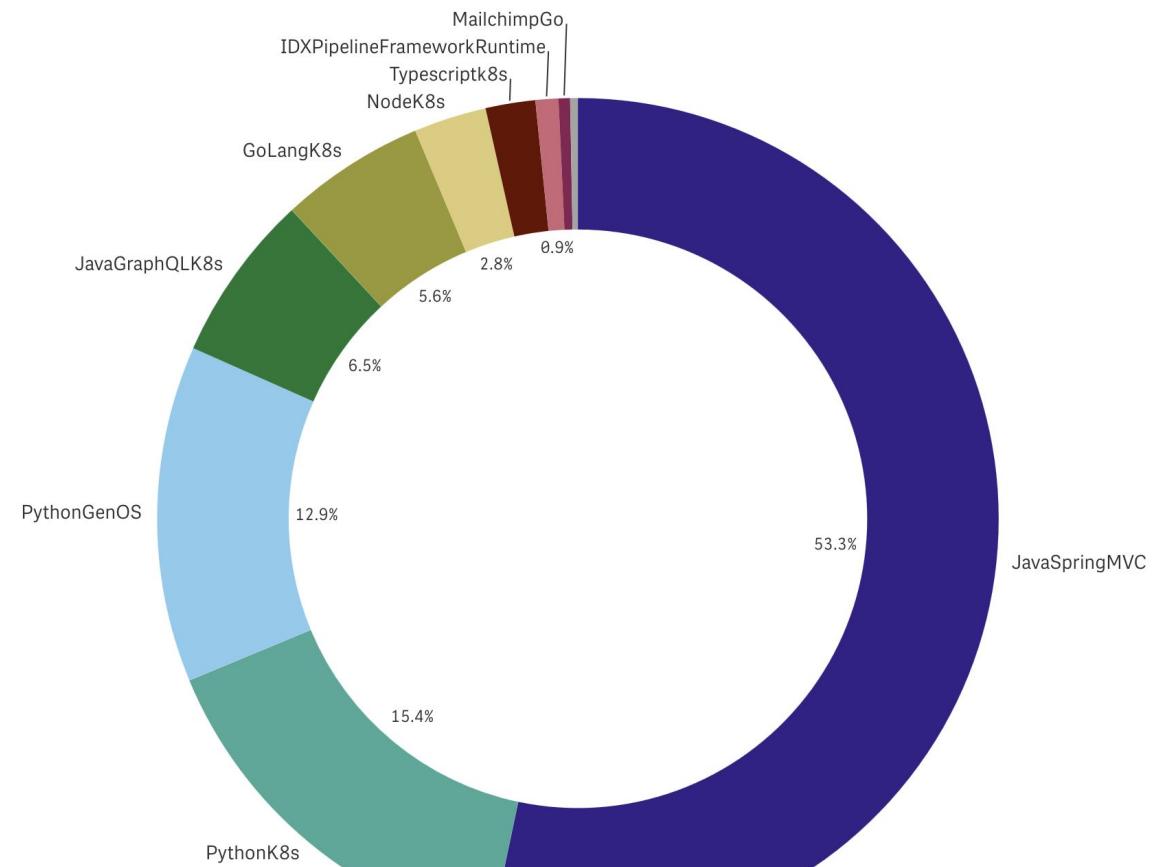


1-Click Debugging Using Argo Workflows: Language and Frameworks

- **Intuit** primarily uses **Java Spring** for web services, though we support multiple languages and frameworks.
- We currently support debugging tools for **Java, Golang** and soon **Python**.



- JavaSpringMVC
- PythonK8s
- PythonGenOS
- JavaGraphQLK8s
- GoLangK8s
- NodeK8s
- Typescriptk8s
- IDXPipelineFrameworkRuntime
- MailchimpGo
- Others



1-Click Debugging Using Argo Workflows: Application Context

Spring Boot

Actuator is a sub-project of Spring Boot. It adds several production grade services to your application with little effort on your part.



application-debug.yml

```
---  
management :  
  endpoints :  
    web :  
      exposure :  
        include :  
          [ "prometheus" , "threaddump" , "heapdump" ]  
      endpoint :  
        prometheus :  
          enabled : true  
        threaddump :  
          enabled : true  
        heapdump :  
          enabled : true
```

manifest.yaml

```
containers:  
- env:  
  - name: SPRING_ACTIVE_PROFILES  
    value: e2e,debug
```

Exposes the following endpoints:

- /actuator/prometheus
- /actuator/threaddump
- /actuator/heapdump

Debugging using Argo Workflows: Thread & Heap Dumps

The diagram illustrates a workflow for debugging a problematic pod. On the left, a cartoon character of a woman sitting at a desk with a laptop and a stack of papers is shown. A large blue arrow points from her towards a central interface. The interface features a hexagonal icon with a cube inside, representing a pod. Below it is a callout box titled "Troubled Pod?" containing a bulleted list of issues: 100% CPU, Memory Leaks, Garbage Collection, Deadlocks, and Performance Bottlenecks. To the left of the interface is a screenshot of a developer portal. It shows a "Debug List" section with a table of results. One row is highlighted, showing a timestamp of Friday, November 3rd, 4:09:36 pm, an operation type of "threaddump", a host name of "kubecon23-java-air-demo-rollout-7dd77848bb-4dmpr", and an expiration time of Saturday, November 4th, 4:09:36 pm. A "Download" button is visible next to the host name. Below the table, there's a "Debug Action" section with instructions for adding a thread/heap dump by selecting a host and type. It includes radio buttons for "Thread Dump" (selected) and "Heap Dump". A dropdown menu for "Select Host(s)" is shown, along with an "Add to Debug List" button and a "Done" button at the bottom right.

- User interacts with **Developer portal UI** to take a thread or heap dump against a target Pod.
- Developer can later download the artifact for analysis using their favorite tools.
- These downloads are available only for 24hrs.



KubeCon



CloudNativeCon

North America 2023

Demo

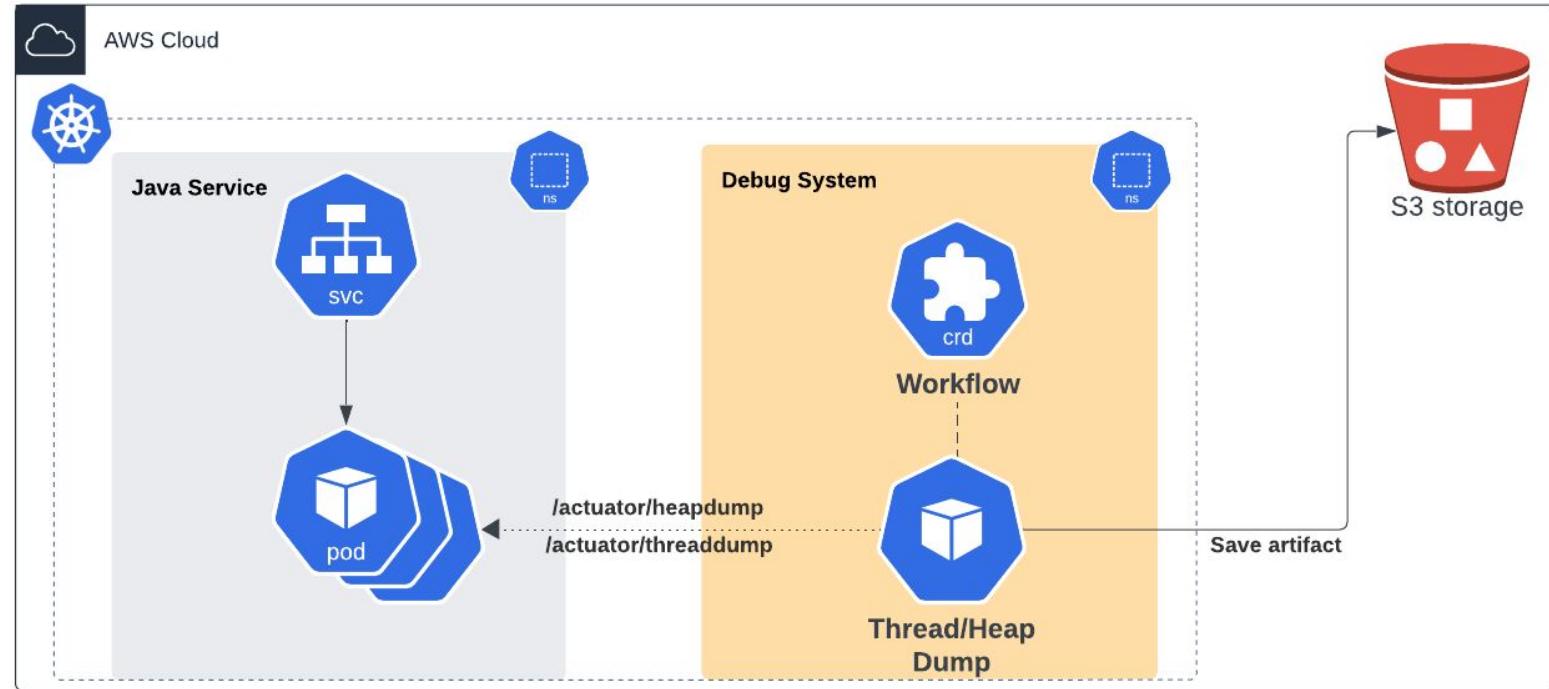
1-Click Debugging Using Argo Workflows: How it works



KubeCon



CloudNativeCon
North America 2023



```
k get wf -n debug-system
NAME                           STATUS        AGE
ws-d-sandbox-sandbox-kubecon23javaairdem-74da5-n2s5s  Succeeded   64m
ws-d-sandbox-sandbox-kubecon23javaairdem-a4a9b-l8fdq  Succeeded   4m19s
ws-d-sandbox-sandbox-kubecon23javaairdem-d751a-v2kxp  Succeeded   85m
```

- The workflow will execute a **Thread/Heap dump** based on the request against the target Pod.
- The result is sanitized and packaged up to **S3** for later download.
- Audit events are recorded at each step.

Debugging using Argo Workflows: Security & AuthZ

- **Auditing** metadata is collected at every step.
- Downloads/Upserts use **RBAC** and IAM **authorization**.
- AWS **pre-signed** urls are generated to encapsulate the expire time.
- Protecting the management endpoints we use via **NetworkPolicy**.

```
io.k8s.api.networking.v1.NetworkPolicy (v1@networkpolicy.json)
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-ingress-debug
spec:
  ingress:
  - from:
    - ipBlock:
      cidr: 0.0.0.0/0
    ports:
    - port: 3000
      endPort: 8489
      protocol: TCP
    - port: 8500
      endPort: 65536
      protocol: TCP
  - from:
    - namespaceSelector:
      matchLabels:
        name: kubecon-debug-java-demo
  - from:
    - namespaceSelector:
      matchLabels:
        iks.intuit.com/debug: "true"
    ports:
    - port: 8490
      protocol: TCP
  - from:
    - namespaceSelector:
      matchExpressions:
      - { key: kubernetes.io/metadata.name, operator: In, values: [metrics-system] }
    ports:
    - port: 8490
      protocol: TCP
  podSelector: {}
  policyTypes:
  - Ingress
```

Excludes 8490-8499

Allows debug port to specific namespaces



KubeCon



CloudNativeCon

North America 2023

Takeaways

Takeaways

- Enhance developer velocity & improve MTTR by reducing friction to take debugging actions.
- Automate and secure access to sensitive data during the debugging process.
- Facilitate seamless collaboration among developers through auditable, downloadable artifacts.
- Democratize debugging tools.



Session QR Codes will be
sent via email before the event

**Please scan the QR Code above
to leave feedback on this session**

We believe in open source and open collaboration



KubeCon

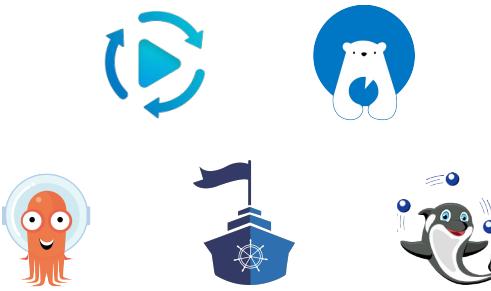


CloudNativeCon

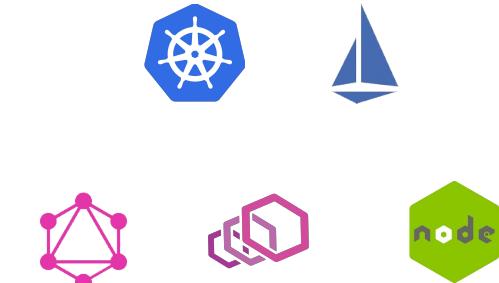
North America 2023



Recipient of the
End User Award
in 2019 & 2022



Created, **open-sourced**,
used, and maintained
by Intuit



End user of Cloud
Native and mobile
open source tech

bit.ly/intuit-oss