intuit

turbotax quickbooks proconnect mint

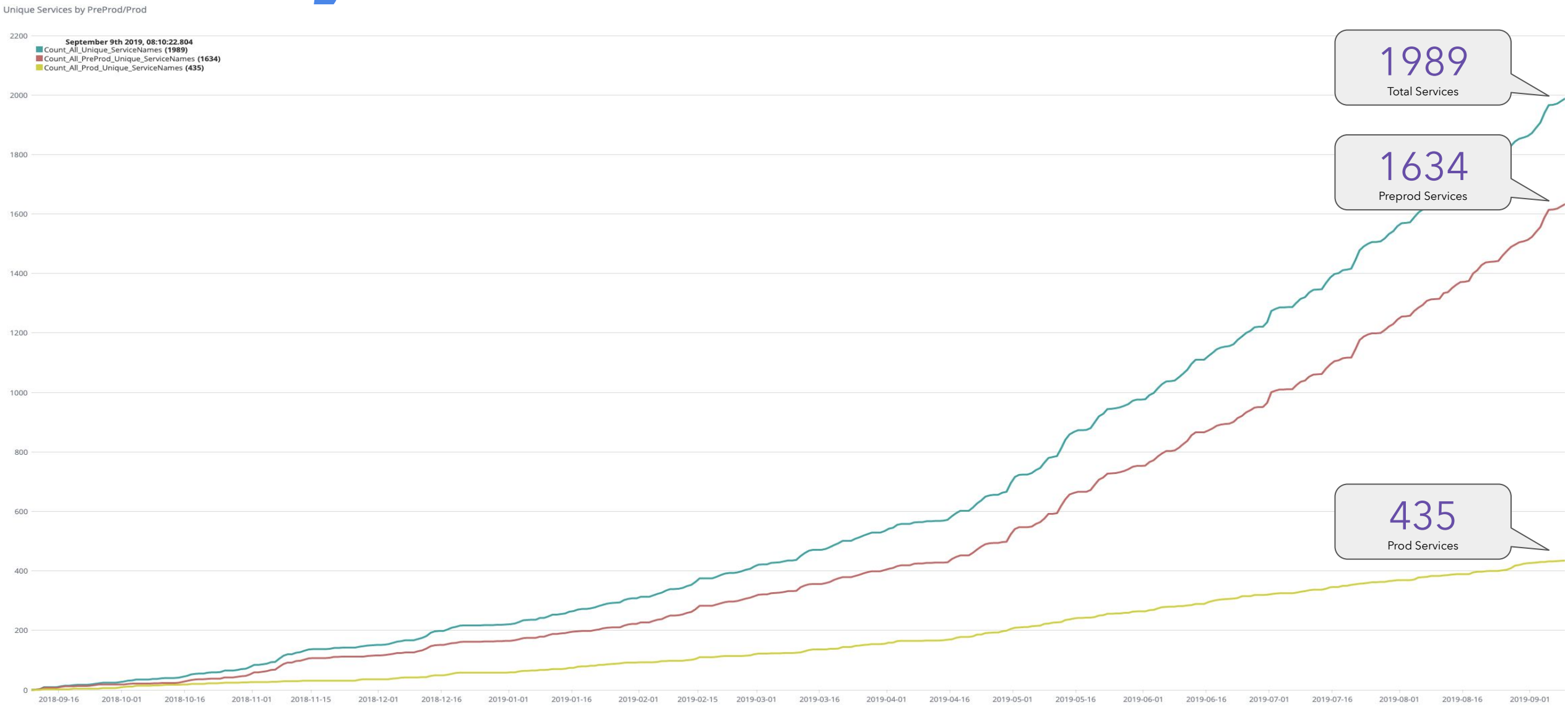
Kubernetes Clusters at scale on AWS @ Intuit

- Shri Javadekar (@shrinandj)

Journey so far ...

- Design and development started in Jan ‘18
- First application was running Kafka on Kubernetes
- Running clusters in dev/test, pre-prod and prod environments since Apr ‘18.
- Over 150 Kubernetes clusters and 3000 namespaces today…

Journey so far ...

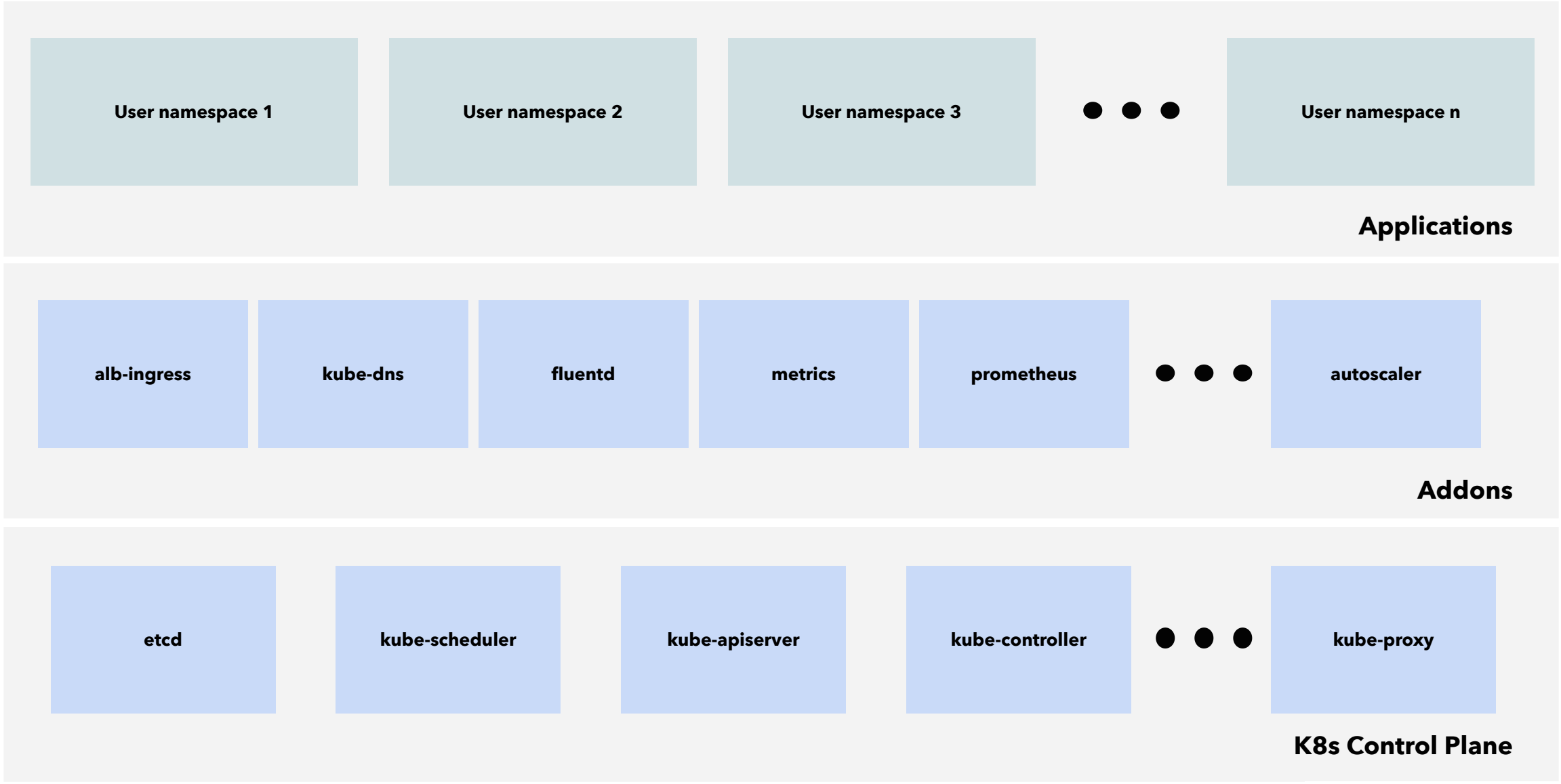


intuit

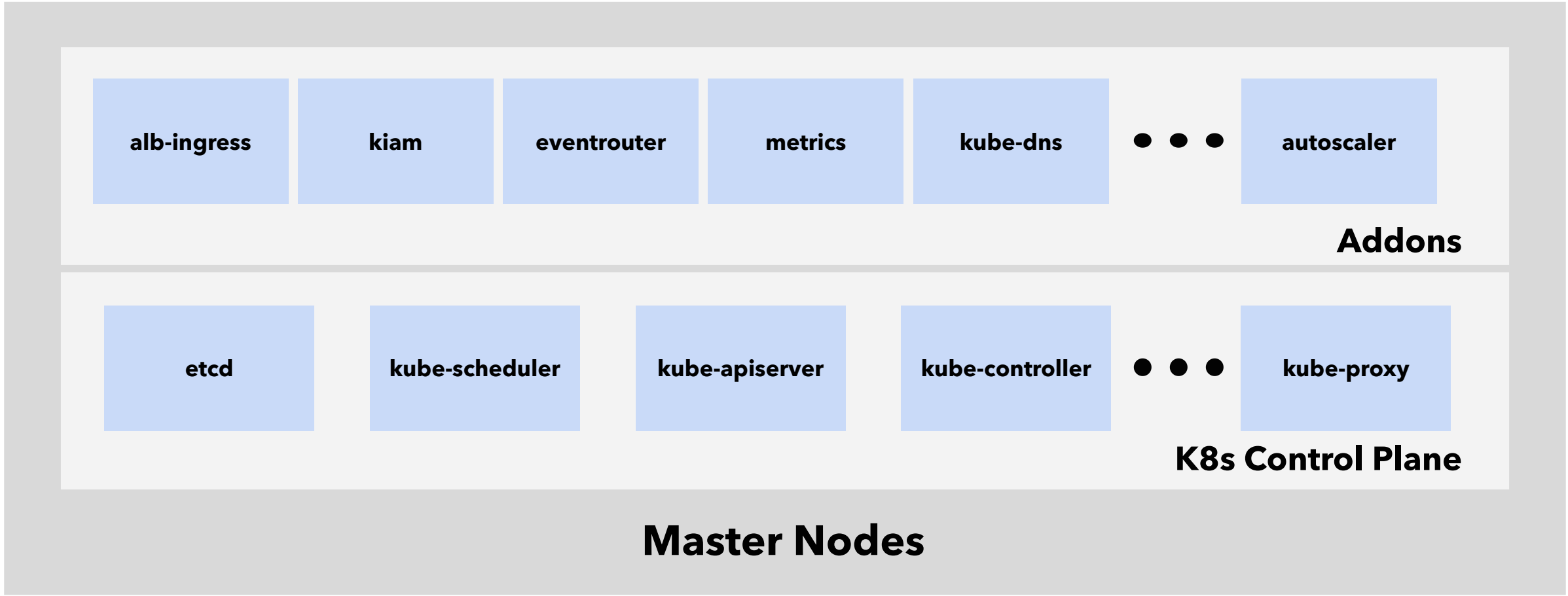
Modern SaaS platform today ...

- Intuit Kubernetes Service
  - Using Kops today
  - Moving to EKS
- Intuit Kubernetes Service Manager (may open source)
- Custom Resources for cluster lifecycle management (aka. Keiko)

Each Kubernetes cluster today ...



Each Kubernetes cluster today ...



The Problems

Addons

- Common functionality needed by all apps on a cluster
- DNS, log forwarding, metrics, identity, etc.
- Integrate with other AWS services such as ALB.

Multi-tenancy

- What does each tenant mean?
- Namespace?
- Kubernetes objects with the same label?
- Some CRD?

We decided to go with Kubernetes Namespaces

Multi-tenancy

- What does each tenant mean?
- Namespace?
- Kubernetes objects with the same label?
- Some CRD?

We decided to go with Kubernetes Namespaces

More Multi-tenancy issues

- Noisy neighbour
- Customized setup
  - Tenant specific AMIs
  - Tenant specific instance types
- Cost accounting

Multi-tenancy solutions

We decided to go with ...

- Instance Group per Namespace
- Customized labels
- Centralized upgrades

Resilience and hardening ...

- Pods stuck in terminating state ...
- EC2 instance networking broken ...

Deep monitoring

- Not enough to simply check if components are “up”
- Deep monitoring
  - Actually exercise the functionality
  - Periodically
  - Preferably automatic remediation

Cost efficiency

- How do we reduce costs?

Keiko

"Keiko provides a set of independent open-source tools for orchestration and management of multi-tenant, reliable, secure and efficient Kubernetes clusters at scale."

github.com/keikoproj

Instance manager	Kube forensics	Upgrade manager	Active monitor	Addon manager	Governor	Minion manager

Keiko

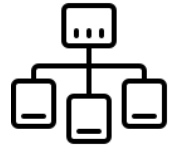
github.com/keikoproj

twitter.com/keikoproj

github.com/keikoproj

Instance manager	Kube forensics	Upgrade manager	Active monitor	Addon manager	Governor	Minion manager

Instance-manager

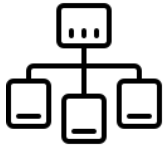


- Declaratively provision and manage ASGs (nodes)
  - Number and type of nodes
  - Labels and taints
  - Subnets and security groups

```
$ kubectl create -f /tmp/hello_world.yaml
instancegroup.instancemgr.keikoproj.io/hello-world created

$ kubectl get igs
NAME          STATE   MIN   MAX      GROUP NAME                                                    PROVISIONER   STRATEGY
AGE
hello-world   Ready   2     3        shri-east-2-instance-manager-hello-world-NodeGroup-16Y8ZA1ZJW8JK  eks-cf        crd           3m
nodes         Ready   2     3        shri-east-2-instance-manager-nodes-NodeGroup-1K1T3YSXCCCK9        eks-cf        crd           1d
```

Upgrade-manager



- Upgrade Manager provides *RollingUpgrade*, a Kubernetes native mechanism for doing rolling-updates of instances in an AutoScaling group using a CRD and a controller.

Addon-Manager

Addons are critical components within a Kubernetes cluster that provide basic services needed by applications like DNS, Ingress, Metrics, Logging, etc. Addon Manager provides a CRD for lifecycle management of such addons using Argo Workflows.

Addon-Manager

```yaml
apiVersion: addonmgr.keikoproj.io/v1alpha1
kind: Addon
metadata:
  name: fluentd-addon
  namespace: addon-manager-system
spec:
  pkgName: core/fluentd
  pkgVersion: v0.0.1
  pkgType: composite
  pkgDescription: Company fluentd addon.
  pkgDeps:
    argoproj/workflows: v2.2.1
  params:
    namespace: mynamespace
    clusterContext:
      clusterName: "my-test-cluster"
      clusterRegion: "us-west-2"
    data:
      hec_splunk_server: hec.splunk.example.com
  selector:
    matchLabels:
      app.kubernetes.io/name: fluentd
      app.kubernetes.io/version: "1.0.0"
  lifecycle:
    prereqs:
      template: |
        apiVersion: argoproj.io/v1alpha1
        kind: Workflow
        ...
    install:
      template: |
        apiVersion: argoproj.io/v1alpha1
        kind: Workflow
        ...
```

Governor

Governor improves the stability of large Kubernetes clusters by proactively terminating failed but stuck pods and misbehaving nodes.

Minion-manager

Minion-manager enables the intelligent use of Spot Instances in Kubernetes clusters on AWS. This is done by factoring in on-demand prices, spot-instance prices and current state of the AutoScalingGroups.

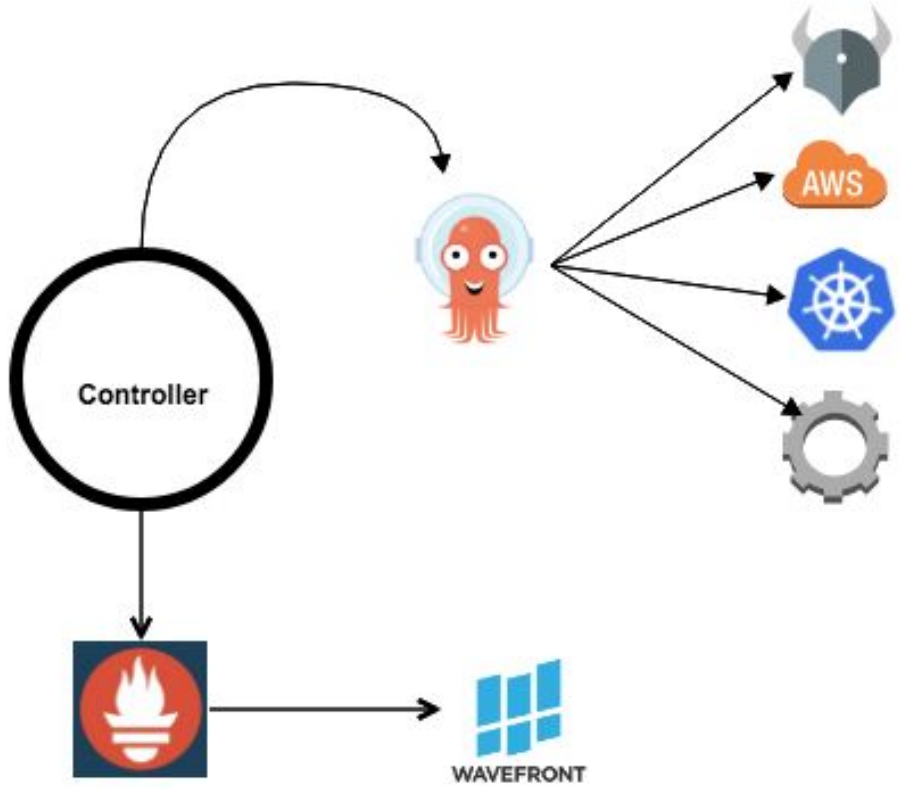
Kube-forensics

Kube-forensics allows a cluster administrator to dump the current state of a running pod and all its containers so that security professionals can perform offline forensic analysis.

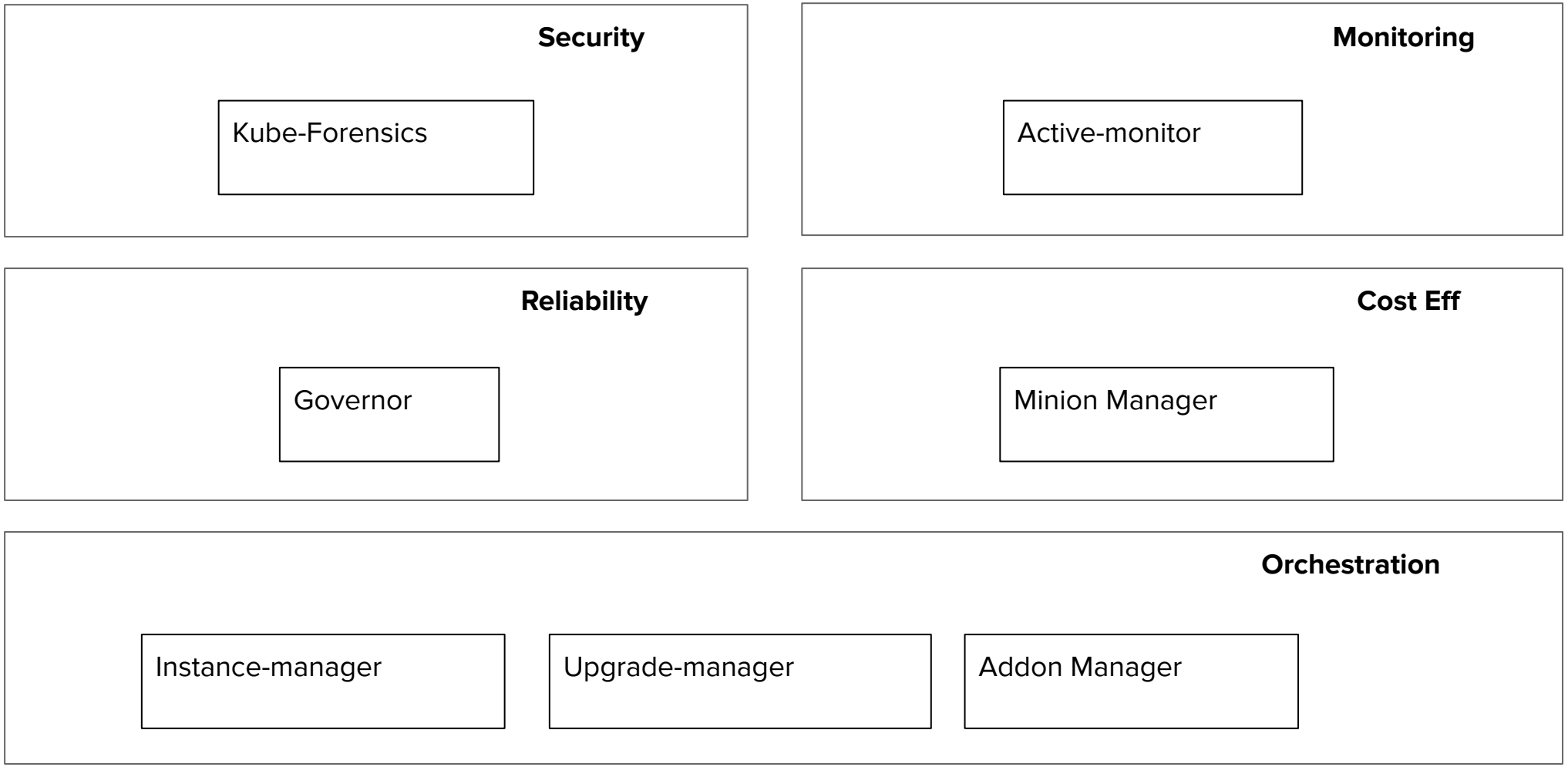
```yaml
apiVersion: forensics.keikoproj.io/v1alpha1
kind: PodCheckpoint
metadata:
  name: podcheckpoint-sample
  namespace: forensics-system
spec:
  destination: s3://my-bucket-123456789000-us-west-2
  subpath: forensics
  pod: bad-pod-1234567890-dead1
  namespace: default
```

Active-monitor

Active-Monitor is a Kubernetes custom resource controller which uses Argo Workflows for deep cluster monitoring.



Keiko


Security
Kube-Forensics
Monitoring
Active-monitor
Reliability
Governor
Cost Eff
Minion Manager
Orchestration
Instance-manager
Upgrade-manager
Addon Manager

Keiko Demo

Coming up ...

- Kubernetes control plane using EKS
- Multi-cluster Service Mesh using Istio
- OpenTelemetry
- GitOps for AWS resources
- Experimentation platform
- And more ...

There’s a lot happening …

<Shameless plug about hiring (referrals) …>

Thank you