Kubernetes in Restrictive Environments

Oleg Chunikhin | CTO, Kublr
Introductions

Oleg Chunikhin
CTO, Kublr

- 20+ years in software architecture & development
- Working w/ Kubernetes since its release in 2015
- CTO at Kublr—an enterprise ready container management platform
- Twitter @olgch; @kublr

Like what you hear? Tweet at us!
Kubernetes & Cloud Native in Restrictive/Enterprise Environment

@olgch; @kublr
Cloud Native Attributes

- Lightweight containers
- Language agnostic
- Microservices
- API
- Stateless/stateful separation
- Self-service infrastructure
- Isolated from OS/server deps
- Agile DevOps processes
- Highly automated
- Declarative resource management

@olgch; @kublr
Applications and Architecture

Applications
- Digital Transformation and App Modernization
- Digital – Web/Mobile
- Data Science & Machine Learning
- Video Streaming
- Internet of Things

Architecture
- SDN + NFV
- Hybrid Cloud
- Multi-Cloud
- Private Cloud
- Edge Computing

@olgch; @kublr
# Cloud Native

- Cloud Native Precursors
  - SRE, DevOps, 12factor app
  - SOA / Microservices, API (management)
  - Containers, Cloud, Virtualization

- Empower IT teams to respond to business requirements quickly, reliably, and predictably

- Larger Enterprises can benefit most, but adoption is lagging behind

@olgch; @kublr
“Restrictive” environment

Due to scale and/or nature of business:

- requires governance
- limits access and options
Enterprise Requirements

- Multiple/complex environments (On-prem, Clouds, Hybrid)
- Centralized/unified management and governance
  - Provisioning, Monitoring, Log Collection, IdM/AAA, Cost
- Integration with existing, often legacy, components
- Security (Infrastructure, OS, IdM/AAA)
- Software management (Patches, Packages, Images)

@olgch; @kublr
Enterprise Challenges and Constraints

✓ Separation of Responsibilities
  Infrastructure, Operations, Security, Legal

✓ Network Access (white/black-listing, air gap)

✓ Security Tools and Processes (infra, OS, platform, apps)

✓ OS, Platform, and Software Practices and Standards
  Vendor and version certification; configuration practices; custom package repositories; etc

✓ Regulations

✓ Complexity

@olgch; @kublr
What is Kubernetes?

• Container orchestrator?
• A step in the evolution from mainframes to serverless?
• Microservices platform?

✓ Infrastructure/cloud abstraction and platform
Enterprise Cloud Native

 OPERATIONS

 Automation Infrastructure

 Logging Monitoring

 Observability Custom Cfg Self-service

 API Usage Reporting

 MANAGED SERVICES

 API Mgmt Data Backup & DR

 Ingress Storage Networking

 Service Mesh Repost & Registries CI / CD App Mgmt

 APPLICATION LIFECYCLE

 Container Runtime

 Kubernetes

 Infrastructure

 SECURITY & GOVERNANCE

 RBAC IAM

 Air Gap TLS

 Secret Management Audit

 Scanning Network Policies

 @olgch; @kublr
Kubernetes Management Platform

@olgch; @kublr
Kubernetes Management

K8S Clusters

Data center
- Prod

Cloud(s)
- PoC
- Dev

K8S API
Cloud/Infra API

API
Log collection
IAM, RBAC, SSO, Federation
DR
Binary Repos
Image Mgmt
Operations
UI
Monitoring
Infrastructure management

@olgch; @kublr
Identity Broker: AAA, SSO, Federation

K8S Clusters

Data center
- Prod

Cloud(s)
- PoC
- Dev

Enterprise IdM

API
UI
Operations

Log collection
Monitoring

IAM, RBAC, SSO, Federation

DR
Binary Repos
Image Mgmt

Infrastructure management

@olgch; @kublr
Kubernetes Services

K8S Clusters

Data center
- Prod
- PoC
- Dev

Cloud(s)
- K8S API
- Cloud/Infra API

API
UI
Operations
Log collection
Monitoring
IAM, RBAC, SSO, Federation
DR
Binary Repos
Image Mgmt
Infrastructure management

@olgch; @kublr
Cluster Architecture

Infrastructure Automation

**MASTER**

- **KUBELET**
- **OPS AGENT**

**NODE**

- **KUBELET**
- **OPS AGENT**

Docker

- overlay network, discovery, connectivity
- K8s Master Components: etcd, scheduler, API, controller

**Orchestration Store**

Discovery & orchestration

Orchestration and configuration agent

Control Center

@olgch; @kublr
K8S Monitoring with Prometheus

- Discover nodes, services, pods via K8S API
- Query metrics from discovered endpoints
- Endpoint are accessed directly via internal cluster addresses

@olgch; @kUBLr
Centralized Monitoring

Control plane

- Cluster registry
- Configurator
- Grafana

PROMETHEUS

- Prometheus config
- Prometheus data

KUBERNETES CLUSTER

- Prometheus (collector)

- K8S Proxy API
  - nodes, pods, service endpoints

Ship externally

@olgch; @kublr
K8S Logging with Elasticsearch

- Fluentd runs on nodes
- OS, K8S, and container logs collected and shipped to Elasticsearch
- Kibana for visualization
Centralized Log Collection

Control Plane

- Cluster registry
- Configurator
- Messaging config

- RabbitMQ
  - Shovel
- MQTT Forwarder

- Logstash
- Elasticsearch

KUBERNETES CLUSTER

- RabbitMQ
- Fluentd

K8S Proxy API
Port forwarding MQTT

Ship externally

@olgch; @kublr
Take Kublr for a test drive!
kublr.com/deploy

@olgch; @kublr
Stay in touch! Signup for our newsletter at kublr.com

Oleg Chunikhin
CTO, Kublr
oleg@kublr.com
@olgch

Kublr | kublr.com
@kublr