Hack-proofing Your Kubernetes Clusters

Prachi Damle

https://slack.rancher.io (prachi)
https://github.com/prachidamle
https://twitter.com/prachiSdamle
https://www.linkedin.com/in/prachidamle

Murali Paluru

https://slack.rancher.io (leodotcloud)
https://github.com/leodotcloud
https://twitter.com/leodotcloud
https://linkedin.com/in/leodotcloud

RANCHER LABS

Containers, Kubernetes and...

- Rapid adoption of containers and container orchestrators

- Containerized deployments
  - Consistent and resource efficient
  - Robust and Scalable deployments
  - Flexible, run anywhere

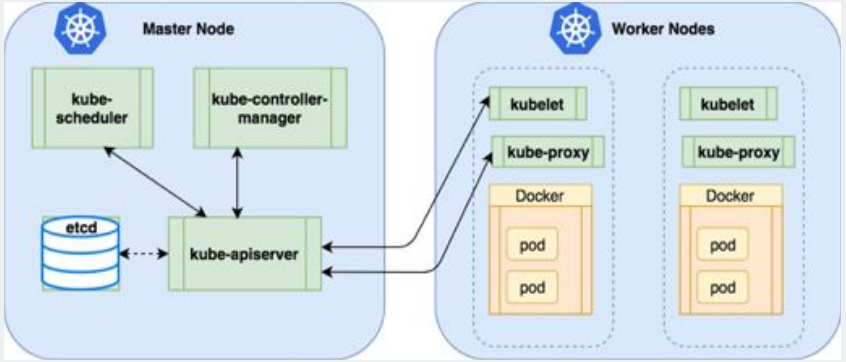
- Rise of Kubernetes: the de facto container orchestration platform

- **Next Challenge: Secure Kubernetes.**

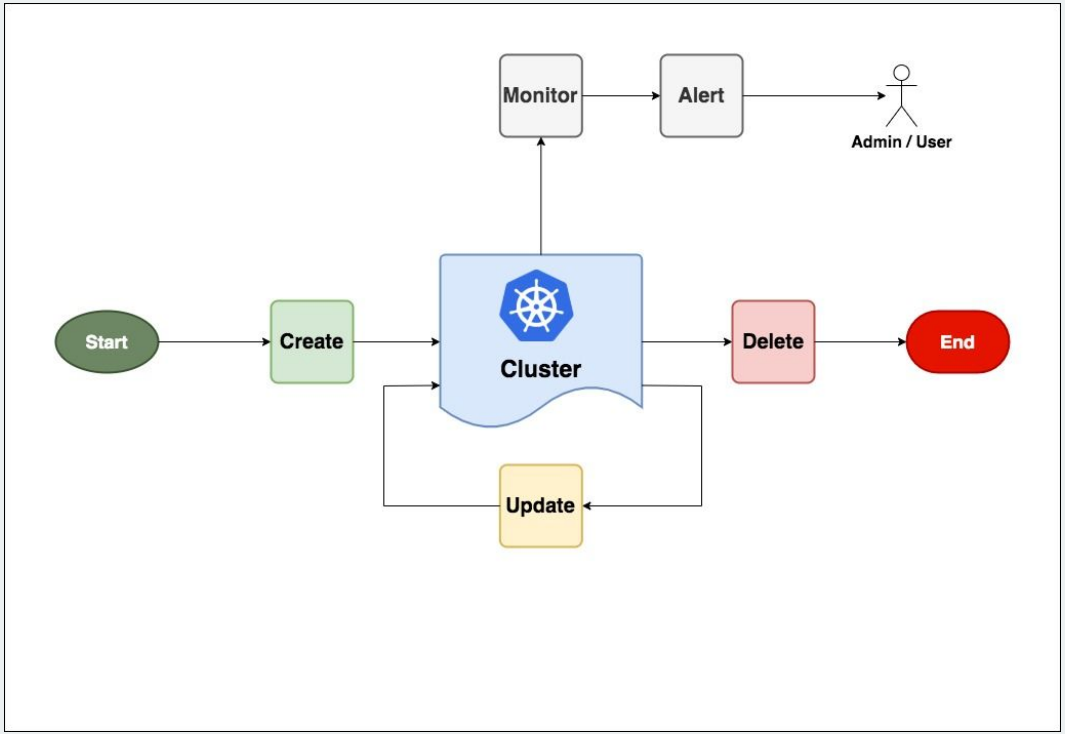
Secure Containerized Deployments

- Container Security
  - Image Scanning in dev/build cycle
  - Private registries
  - Runtime security policies and alerting

- Cluster Security
  - Secure the platform hosting containers
  - Wide scope for security threats due to microservice architecture
  - Recent Security breaches
    - CVE-2018-1002105 – enables attackers to compromise clusters via the Kubernetes API server
    - Cryptocurrency mining malware infection



Kubernetes Cluster Lifecycle



Kubernetes Cluster Security

- How to build and manage secure clusters?
  - Follow the Kubernetes Security Best Practices and CIS Benchmarks
  - Cluster Templates
  - Scan Tool for ongoing compliance monitoring

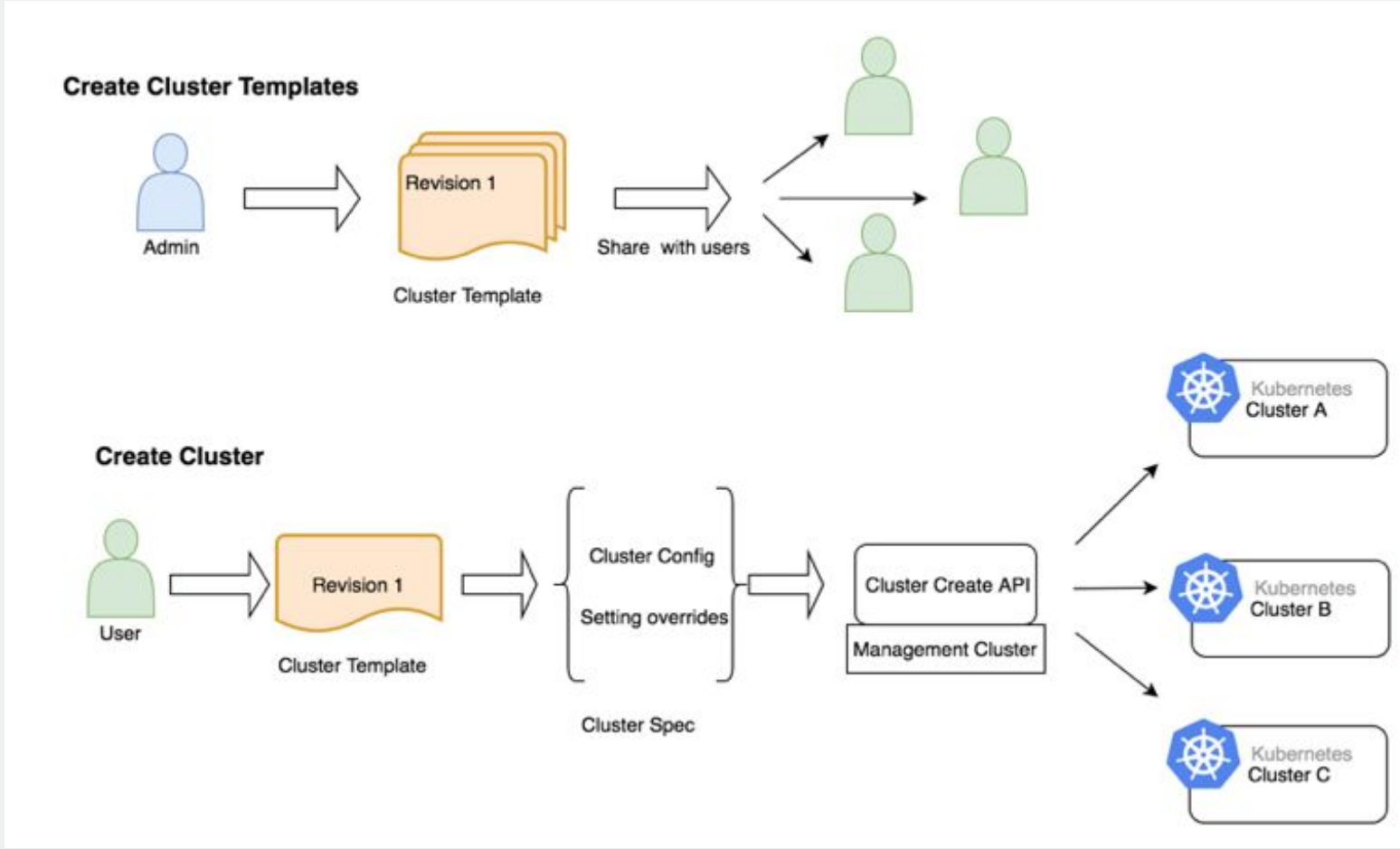
Best Practices for compliant Kubernetes clusters

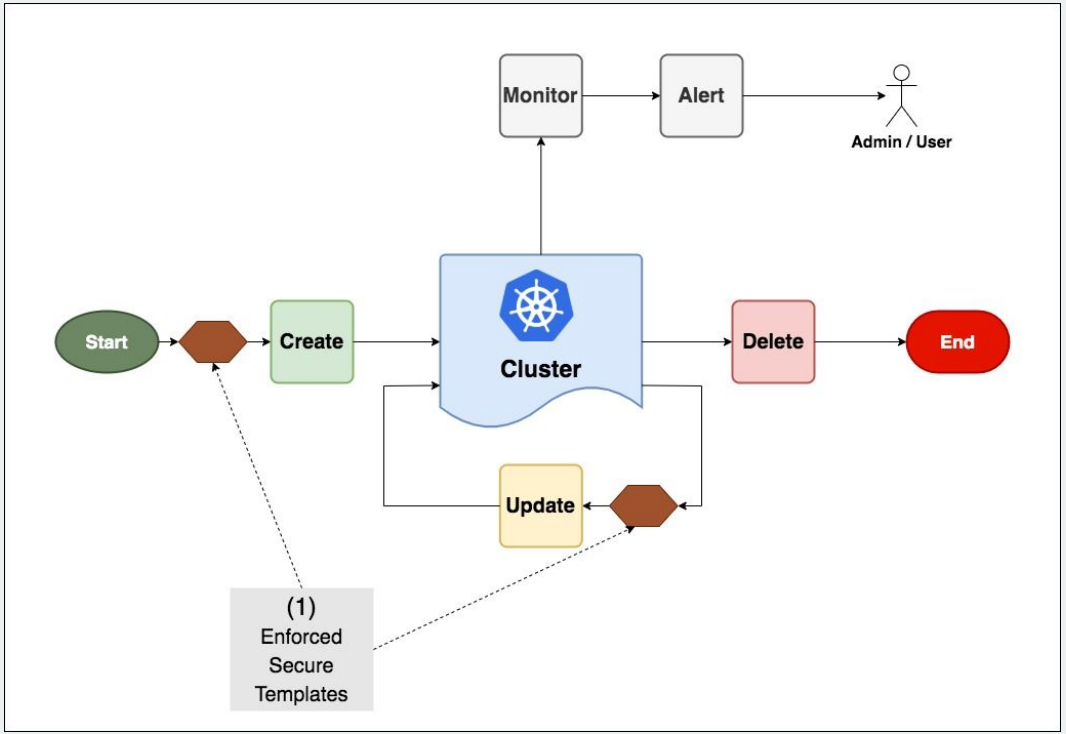
- **CNCF 9 Best Practises**
  - Stay up to date with latest versions
  - Enable RBAC
  - Namespaces – security boundaries
  - Separate Sensitive Workloads
  - Secure Cloud Metadata
  - Cluster Network Policies
  - Pod Security Policies
  - Node Security Benchmarks
  - Audit Logging

- **CIS Benchmarks**
  - Security Configuration per Kubernetes component
  - Published with every Kubernetes release
  - Separate guidelines to configure master nodes and worker nodes
  - Scoring assigned to assess the compliance of the cluster

Cluster Templates

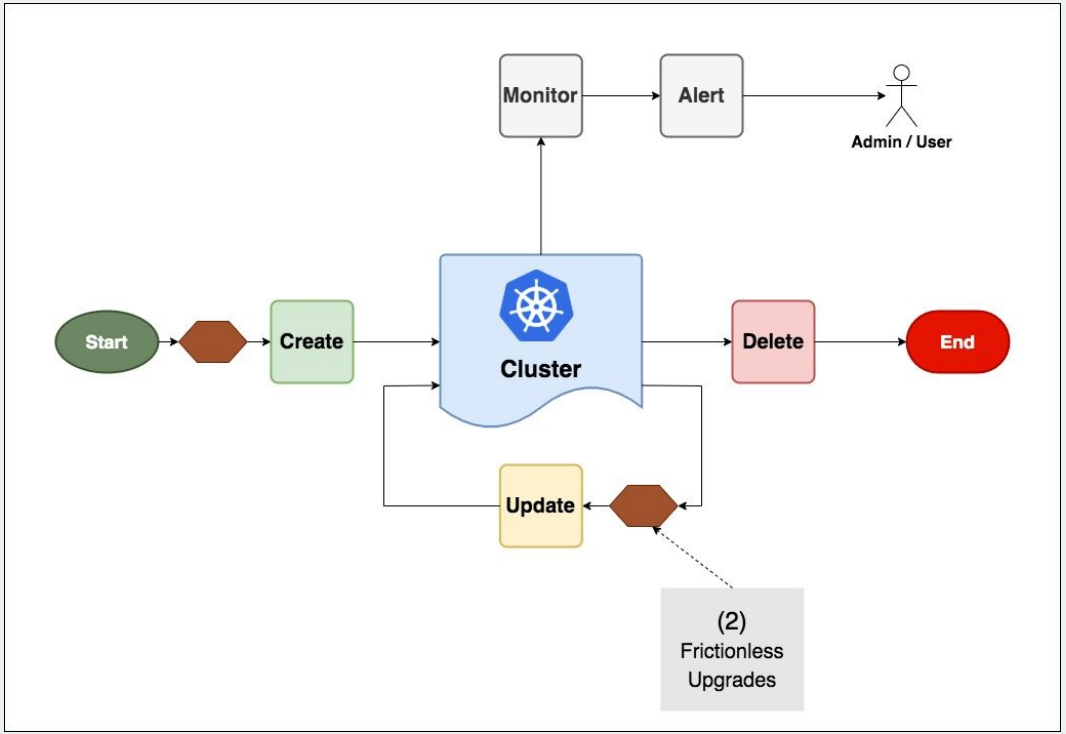
- Pre-define cluster configuration compliant to security benchmarks
- Bake in CIS recommended Kubernetes settings to be applied to a cluster during creation
  - Kubernetes settings per component (Kubernetes API server, Kubelet, etcd)
  - Default Cluster Options
  - Kubernetes version
  - Cloud Provider options
  - Pod Security Policy, Network Security Policy
  - Add-ons
- Facilitates Ease of operations
  - One time cluster definition, reduces complexity
  - Ensures consistent and error free cluster deployments
  - Template versioning can support cluster updates
- Security Policy Enforcement
  - Enables Admins to push policies via cluster template enforcement
  - Helps ensuring compliance


Create Cluster Templates
Admin
Revision 1
Cluster Template
Share with users
Create Cluster
User
Revision 1
Cluster Template
Cluster Config
Setting overrides
Cluster Spec
Cluster Create API
Management Cluster
Kubernetes
Cluster A
Kubernetes
Cluster B
Kubernetes
Cluster C


Monitor
Alert
Admin / User
Start
Create
Cluster
Delete
End
Update
(1)
Enforced
Secure
Templates

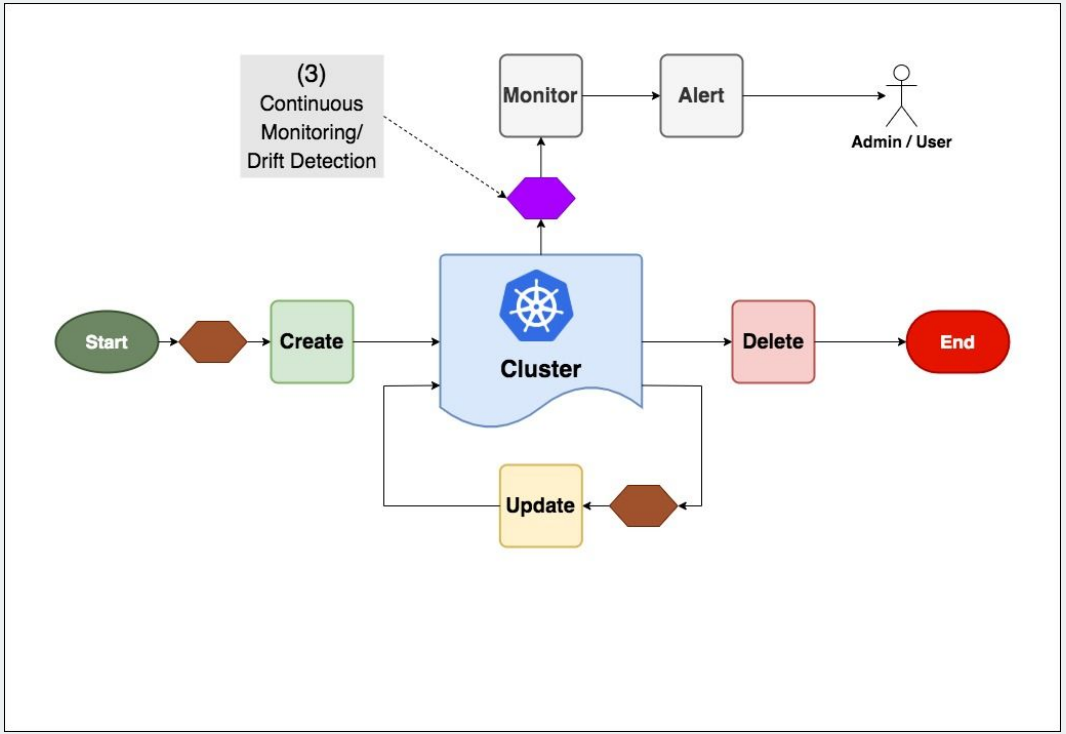
Seamless Kubernetes Upgrades

- Important to keep clusters updated as soon as patches are released to mitigate CVE's
- Keep information on k8s versions and their dependencies like k8s component flags and system addon images separate from your software code.
- Sync this Kubernetes information as metadata periodically to pull updates without requiring releases of your software

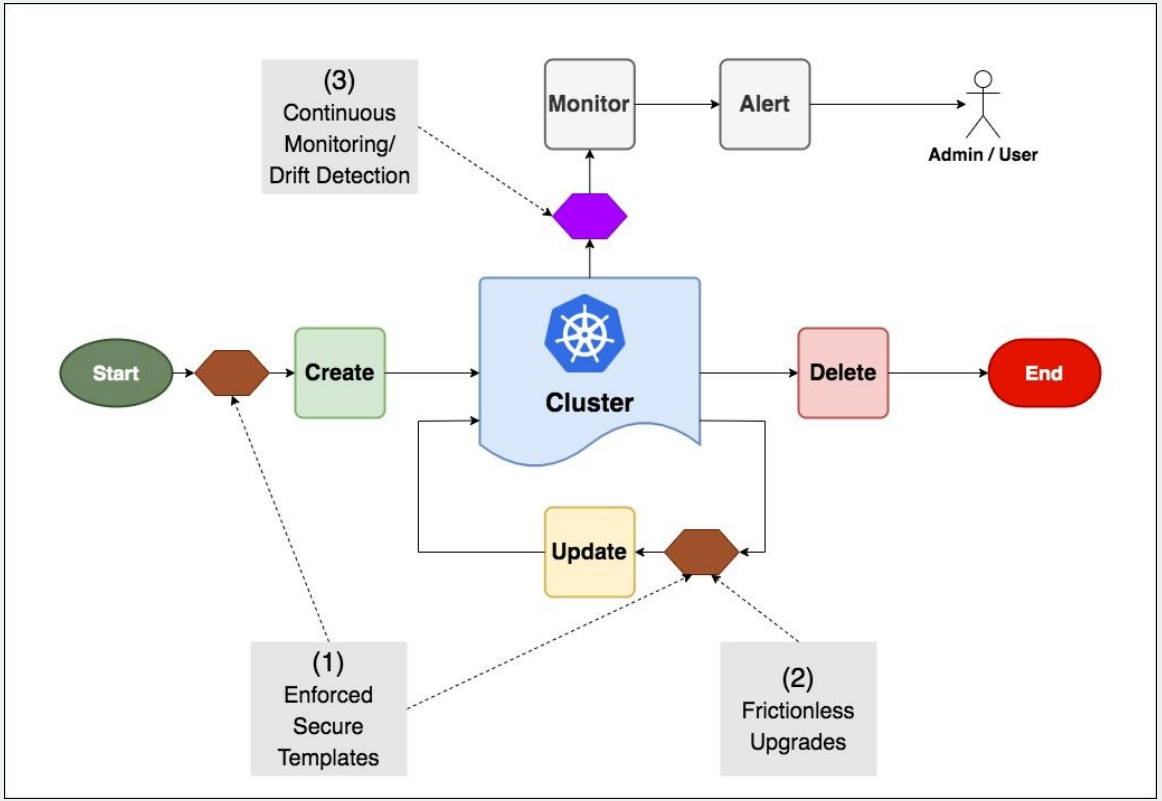

Monitor
Alert
Admin / User
Start
Create
Cluster
Delete
End
Update
(2)
Frictionless
Upgrades

Continuous Scan and Monitor

- Automated Tool to run on-demand CIS compliance check for the entire Kubernetes Cluster
- Deploys **kube-bench** to master node and on every worker node of the cluster
- Collects the results from all nodes to **publish a overall cluster report**
- Helps ensuring ongoing compliance, not just at cluster creation
- Generates compliance report for the entire cluster per node
- Can be integrated with tools to generate automated alerts notifying the stakeholders


(3)
Continuous
Monitoring/
Drift Detection
Monitor
Alert
Admin / User
Start
Create
Cluster
Delete
End
Update

Summary


(3)
Continuous
Monitoring/
Drift Detection
Monitor
Alert
Admin / User
Start
Create
Cluster
Delete
End
Update
(1)
Enforced
Secure
Templates
(2)
Frictionless
Upgrades

Demo

Questions?

Thank You!