SUSE

Up and Running With K3s

Week Two: New Dog, New Tricks

Welcome!

Your Instructor

Adrian Goins

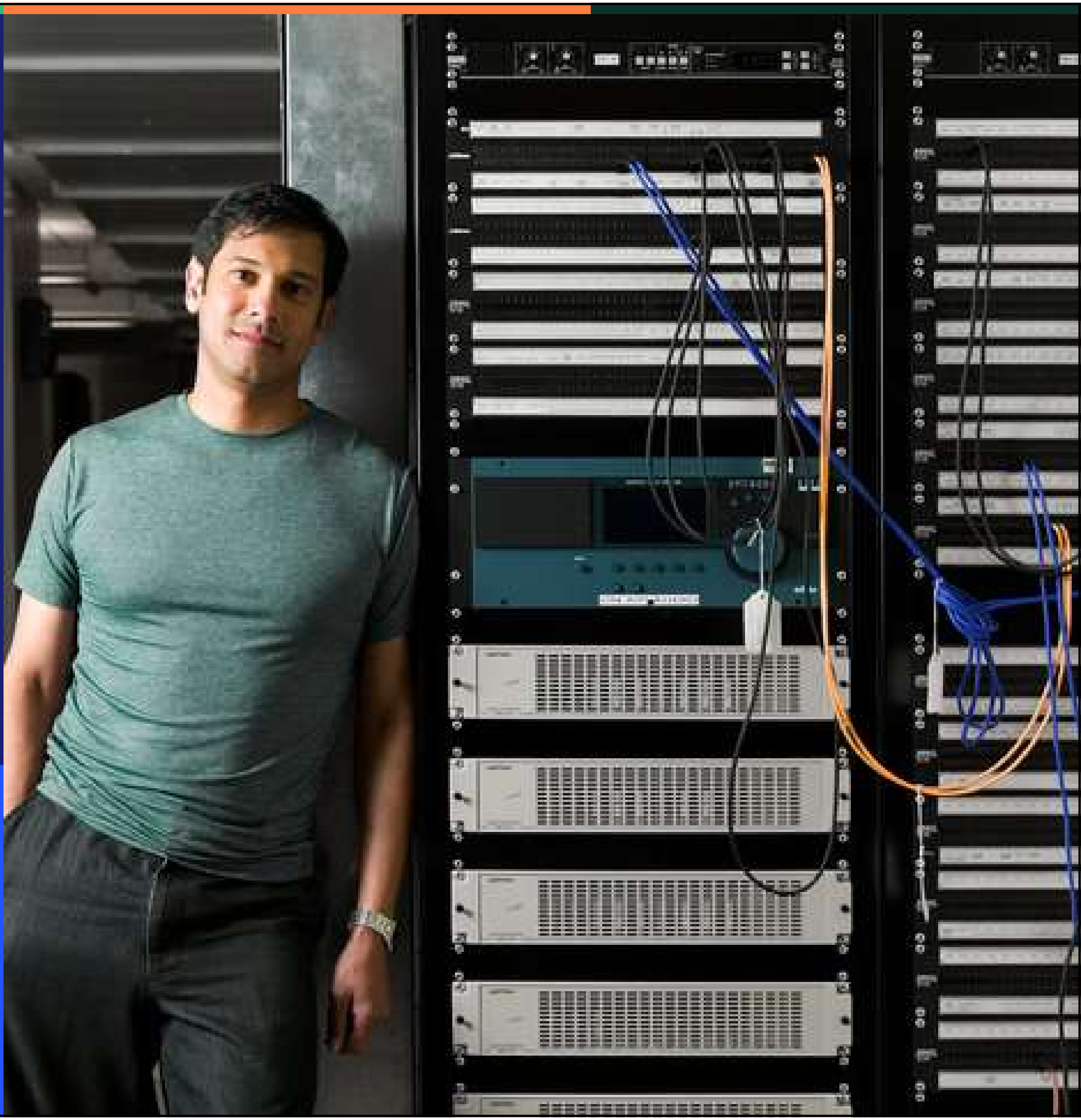
adrian.goins@suse.com

- Host of Coffee and Cloud Native
- 24 years experience in building Internet infrastructure
- 4 years with Rancher in engineering and marketing

Objectives

- Learn how to replace stock K3s networking components like servicelb controller, ingress controller, and the CNI
- Explore how to use out-of-tree drivers for additional functionality
- Learn how to use the HelmChart controller and automatic manifest deployments

Replacing Stock Networking Components



Klipper LB / Service LB

- It’s a controller that listens for LoadBalancer services
- Creates a DaemonSet that connects the listening port to the service
- If the node has an external IP, the service LB will use it
- If another service LB is already using the port, the service will stay in a Pending state

Controlling Service-LB

- Can be selectively included on nodes by adding the label `svccontroller.k3s.cattle.io/enablelb`
- If this label is present, only these hosts will receive the servicelb Pods
- Can be disabled by adding `--disable servicelb` to the installation or execution options

What Can Replace Service-LB?

- MetalLB
- kube-vip
- Porter

Traefik Ingress Controller

- Uses Traefik 1.x for easy operation
- Will be updated to 2.x in a future release
- Auto-deployed by the manifest found at `/var/lib/rancher/k3s/server/manifests/traefik.yaml`
  - Changes to this manifest will be auto-applied to the cluster
- Attaches to a Service-LB listening on 80/443/8080

Disabling and Replacing Traefik

- Traefik can be replaced by passing `--disable traefik` to the install or startup options
- It must be removed before installing another Ingress controller

What Can Replace Traefik?

- ingress-nginx
- Traefik v2
- HA Proxy
- Ambassador
- API Gateways like Gloo Edge or Kong
- Service mesh like Istio, Linkerd, or Kuma

Using a Different CNI

- K3s uses Flannel by default
  - Easy and lightweight
  - Minimal features
  - Defaults to VXLAN (unencrypted)
- Any other CNI can be deployed at install time
  - Calico
  - Canal
  - Cilium

Making Flannel More Secure

- Replace the backend with IPSec or WireGuard
  - https://rancher.com/docs/k3s/latest/en/installation/network-options/
- Replace it with an alternative CNI

Calico

- Robust CNI that uses eBPF and BGP
- Support for Windows and Linux nodes
- Support for non-Kubernetes workloads
- Incorporates multiple layers of security
  - Kubernetes NetworkPolicy support
  - CalicoNetworkPolicy for enhanced security

https://www.projectcalico.org

Canal

- Originally designed to bring NetworkPolicy from Calico into Flannel
- Still available, but superseded by CNI Plugins and the need for enhanced network security beyond NetworkPolicy

https://docs.projectcalico.org/getting-started/kubernetes/flannel/flannel

Cilium

- Built on eBPF
- Replaces kube-proxy load balancer
- Identity-aware network visibility
- API-aware network visibility
- Context-aware network policy support

https://cilium.io/

Replacing the CNI

- Disable Flannel during installation and join
  - Master nodes: `--flannel-backend=none --no-flannel`
  - Agent nodes: `--disable-network-policy --no-flannel`
- Install the alternative CNI
  - Cilium: https://docs.cilium.io/en/v1.9/gettingstarted/k3s/
  - Calico: https://docs.projectcalico.org/getting-started/kubernetes/k3s/

In-Tree and Out-of-Tree Drivers

Definitions

- In-Tree: within the core Kubernetes codebase
  - This was the original location for third-party drivers
  - All drivers are now out-of-tree but bundled with upstream Kubernetes

- Out-of-Tree: not part of the core Kubernetes repository
  - This is the current standard, built around solutions like Container Storage Interface (CSI) and Cloud Provider Interface (CPI)

What K3s Excludes

Anything that isn’t necessary to run Kubernetes.

How to Add Things Back

- Find the out-of-tree driver for the component
  - CSI drivers are at: https://github.com/kubernetes-csi/
- Install it
- Profit!

Should you run K3s in the cloud?

Workload Deployment Magic

Auto-Deployed Workloads

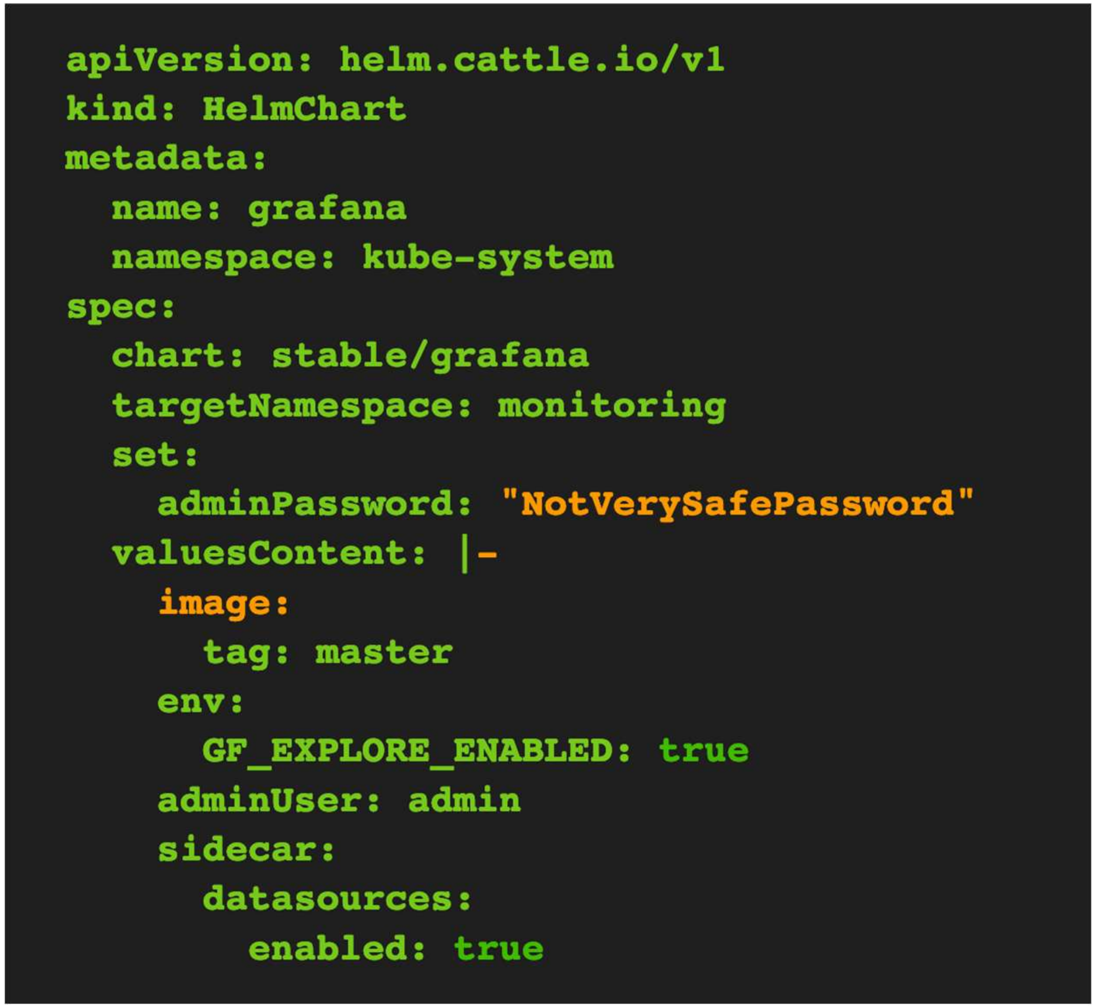
- Anything dropped into `/var/lib/rancher/k3s/server/manifests` will be automatically deployed
- These are registered as addons, which loosely translates to “core components not part of Kubernetes that extend its functionality”
  - CNI / CSI / DNS / Visualization
  - Visible with `kubectl get addon -A`
- Addons take their name from the filename of the manifest

HelmChart Manifests

- K3s includes a Helm controller that manages Helm charts using a HelmChart Custom Resource Definition (CRD)
- HelmChart manifests can be applied via the auto-deploy mechanism discussed earlier

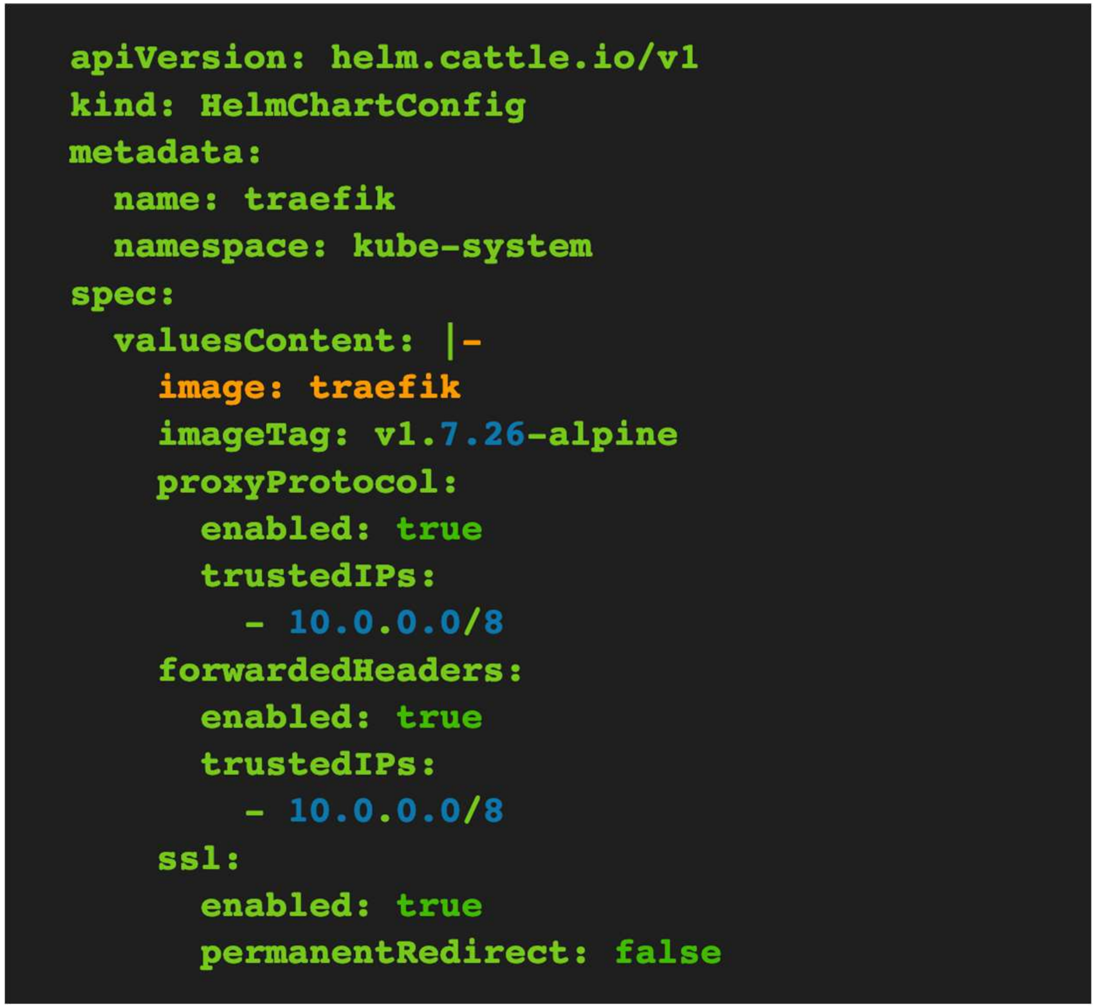
HelmChart CRD

- Represents the commands and flags used to install an app via Helm
- Enables individual values by providing key/value pairs to `set`
- Enables multiple values to be set by passing a block of YAML to `valuesContent`



```yaml
apiVersion: helm.cattle.io/v1
kind: HelmChart
metadata:
  name: grafana
  namespace: kube-system
spec:
  chart: stable/grafana
  targetNamespace: monitoring
  set:
    adminPassword: "NotVerySafePassword"
  valuesContent: |-
    image:
      tag: master
    env:
      GF_EXPLORE_ENABLED: true
    adminUser: admin
    sidecar:
      datasources:
        enabled: true
```

HelmChartConfig CRD



```
apiVersion: helm.cattle.io/v1
kind: HelmChartConfig
metadata:
  name: traefik
  namespace: kube-system
spec:
  valuesContent: |-
    image: traefik
    imageTag: v1.7.26-alpine
    proxyProtocol:
      enabled: true
      trustedIPs:
        - 10.0.0.0/8
    forwardedHeaders:
      enabled: true
      trustedIPs:
        - 10.0.0.0/8
    ssl:
      enabled: true
      permanentRedirect: false
```

- Available from v1.19.0+k3s1
- Enables override of system-level HelmChart resources like Traefik
- Lower priority than any directly-set value in the HelmChart
- Must have the same name and namespace as the HelmChart to which it applies

Next Steps

Where Do I Go Next?

Join the Office Hours Session

Review and start on the Weekly Challenges

Resources

Documentation and Links

- K3s Documentation - https://rancher.com/docs/k3s/latest/en/
- SUSE & Rancher Community - https://community.suse.com
- Rancher Users Slack - https://rancher-users.slack.com
  - Request an invitation from https://slack.rancher.io
- Kubernetes Documentation - https://kubernetes.io
- Comparing Kubernetes Ingress Controllers - https://learnk8s.io/research#ingress-controllers

SUSE

Thank you

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

+49 (0)911-740 53-0 (Worldwide)

Maxfeldstrasse 5
90409 Nuremberg
www.suse.com