NCR ICI

NATIONAL CAPITAL REGION
INTEROPERABLE COMMUNICATIONS INFRASTRUCTURE

9-1-1: Cloud Native Kubernetes for Public Safety Systems

Who Am I

- CTO Tremolo Security
- 20+ Years in Identity Management
- Kubernetes since 2016
- Co-Author Kubernetes: An Enterprise Guide, 2nd Ed
- Contributor to multiple projects

What is NCR IAMS?

- Identity as a Service for 22+ jurisdictions in the Washington, DC region
- Users from local jurisdictions, state, partners, and US Federal Government
- Authentication & Authorization
- Applications include emergency response and collaboration
- Production since 2013
- Built on OpenUnison from Tremolo Security

Where IAMS Began…

September 11, 2001

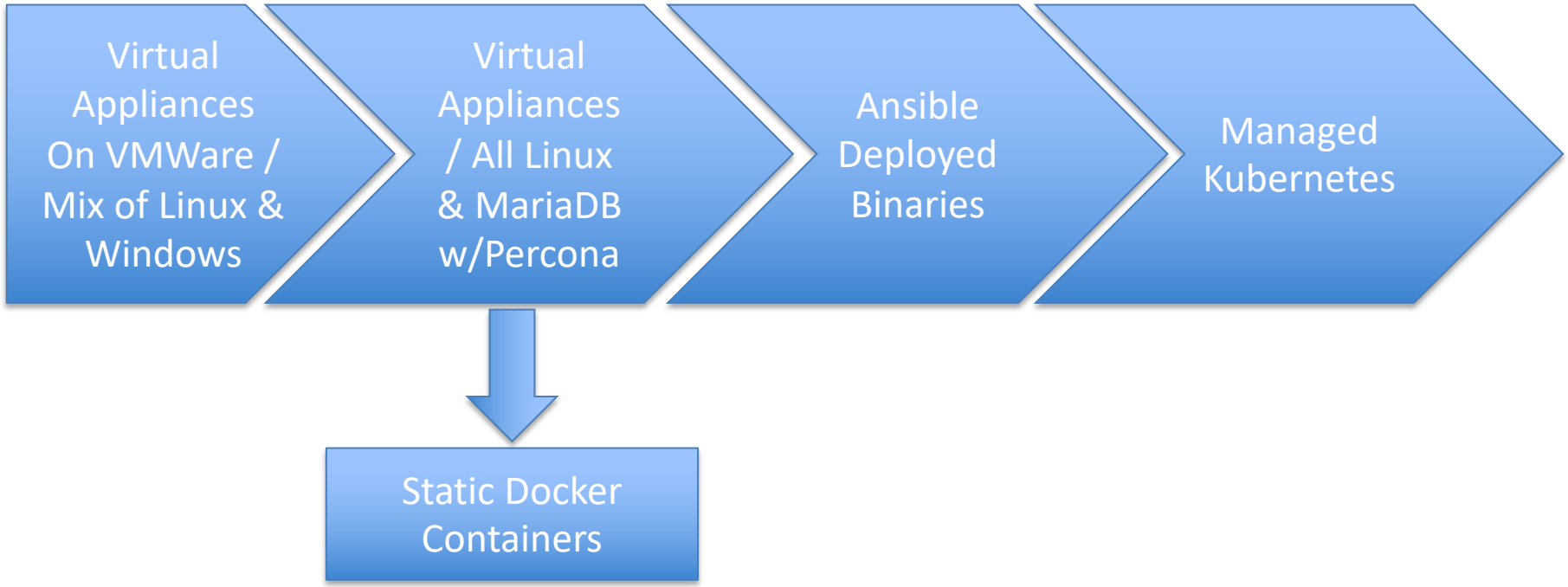
Priorities

- Availability
- Privacy
- Security
- Performance

Challenges

- Legacy systems
- Exceptions to “The Rule”
- Silos of Silos
- Technology
- Regulations

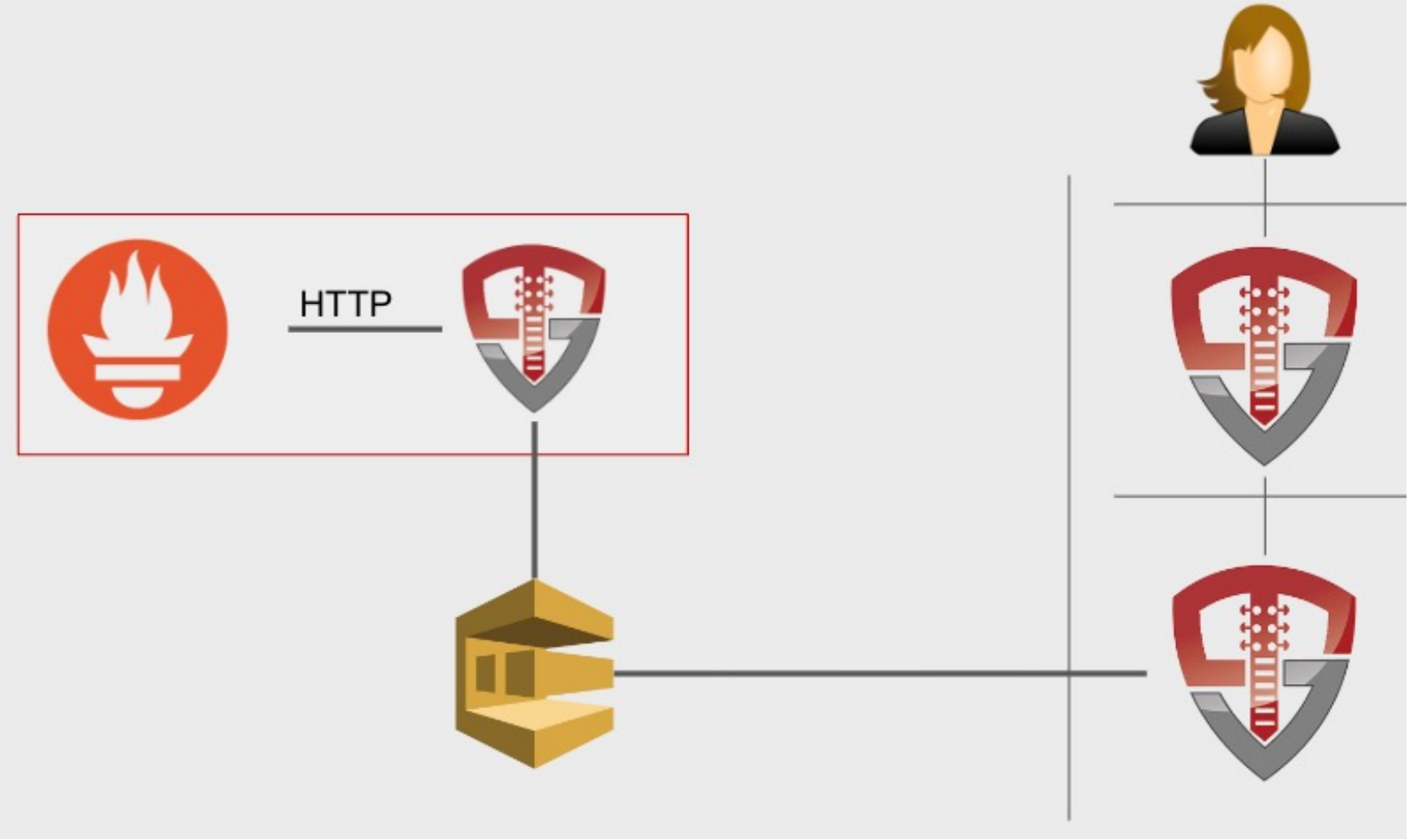
Journey to Kubernetes



Virtual Appliance → Ansible

- Unison → OpenUnison
  - Eliminate GUIs
  - Externalized environment specific configuration
- Emulate containers with Ansible
- Monitoring changed from legacy to Prometheus
- Updated via Ansible

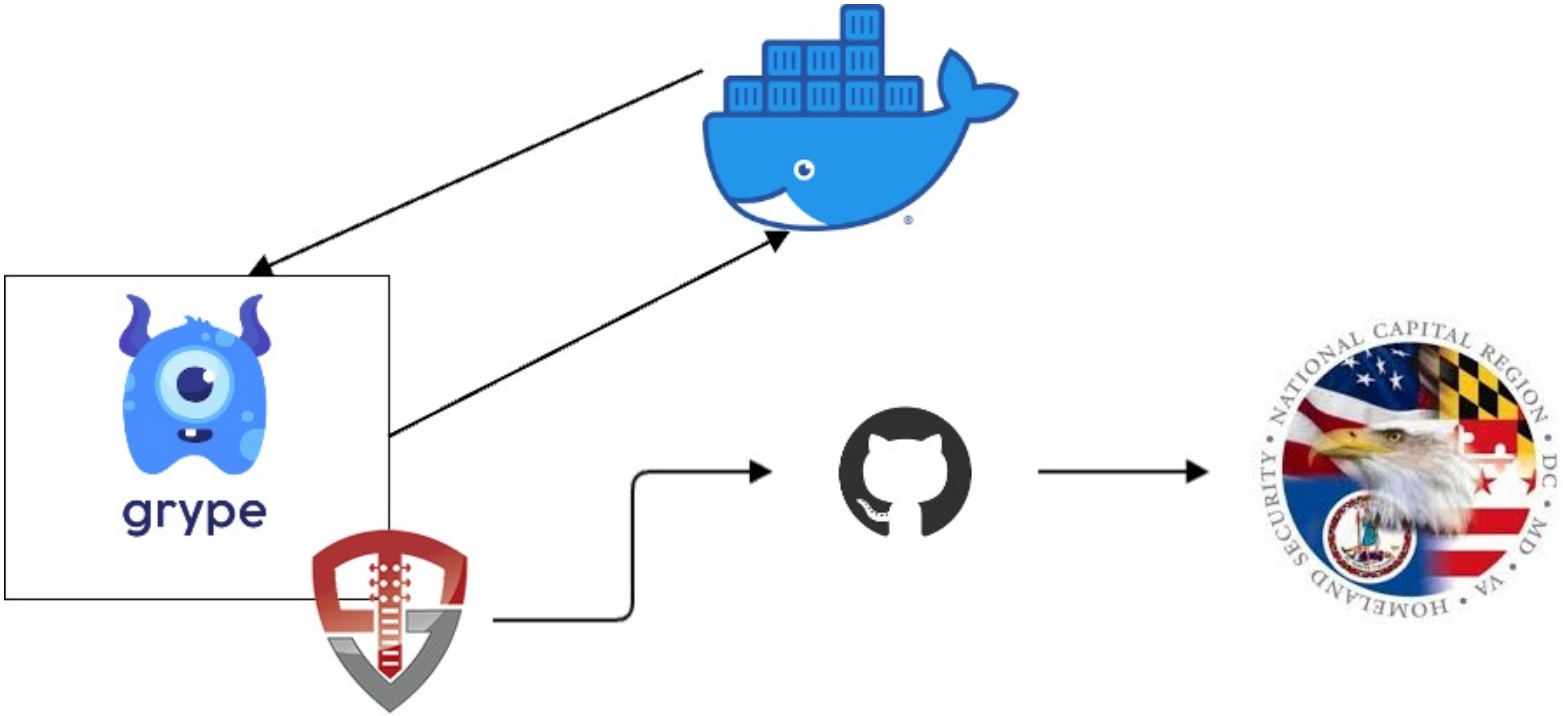
Prometheus Monitoring



VMs → Kubernetes

- Challenges:
  - Networking
  - Legacy Security
  - CI/CD
  - Logging
  - Monitoring

CI/CD



To Kubernetes, AND BEYOND!

Secrets Management

- Needed for GitOps
- No Secrets in Git
- Goal on externalization, not “lockdown”
  - Plain Kubernetes Secrets are Fine https://www.macchaffee.com/blog/2022/k8s-secrets/
- CSI Secret Store Driver - https://secrets-store-csi-driver.sigs.k8s.io/

Secrets Management (Cont.)

- Step 1 – Convert existing Secrets into vault
- Step 2 – Connect CSI to vault
- Step 3 – Synchronize into Secrets

GitOps

- Eventual Consistency is a lie
- Combination of Helm charts and static manifests
- Environment specific repos
  - Dev has to emulate customer environments
- ArgoCD with “App of Apps” pattern

GitOps (Cont.)

- How to export existing configuration?
  - Organize manifests by object type
  - Remove cluster specific data
  - Skip intermediate object types
  - Namespace Export Tool
    - https://github.com/TremoloSecurity/k8s-export

Challenges for GitOps

- CI/CD – Committing to git instead of making API calls
- Monitoring – Making maintainable changes to the Prometheus Stack
- Leveraging “waves” in ArgoCD
- Synchronizing ArgoCD Application objects in order

Thank You

- Twitter - @mlbiam / @tremolosecurity
- OpenUnison – https://openunison.github.io/
- NCRNet – https://ncrnet.us/
- Kubernetes: An Enterprise Guide 2nd Ed 20% Discount on Amazon - **20KAEG**