KubeCon | CloudNativeCon

North America 2017

Compliance and Identity Management in k8s

Marc Boorshtein, CTO, *Tremolo Security, Inc.*

What Will We Be Talking About?

- Why are identity management and compliance important to you?
- What is “Compliance”?
- How does identity management apply to compliance?
- How does k8s handle identity management?
  - Authentication
  - Authorization
- Demo!

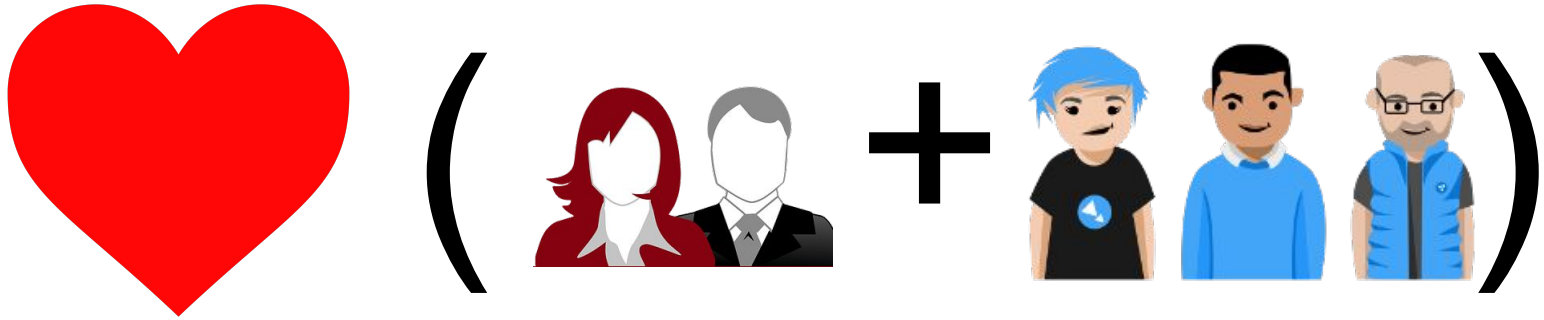
Who Am I?

- Fifteen Years of Identity Management Experience
- Deployments across multiple vendors and industries
- Managed multiple civilian agency's "ICAM" deployments
- Contributed documentation to k8s for OpenID Connect

Why Is Compliance Important?

It’s not just for meetings and auditors…

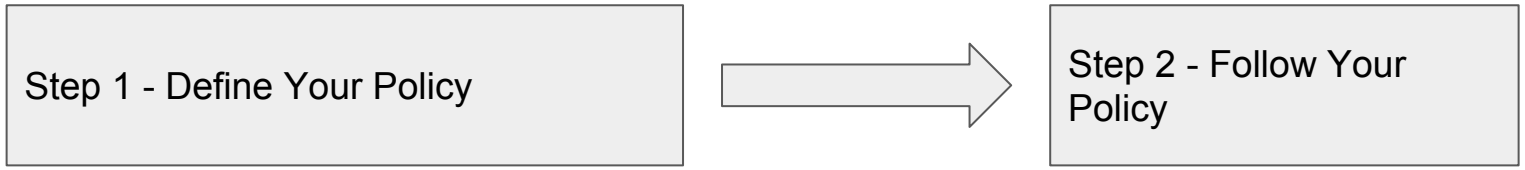
DevOps + Identity Management =



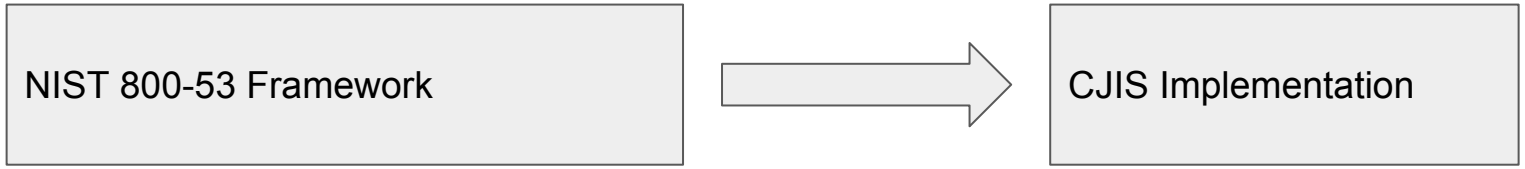
What Is Compliance?

When someone asks if you're compliant...

NIST 800-53

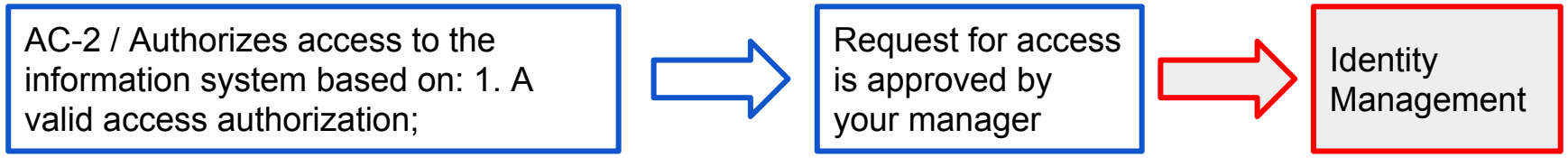


Criminal Justice Information Systems (CJIS)

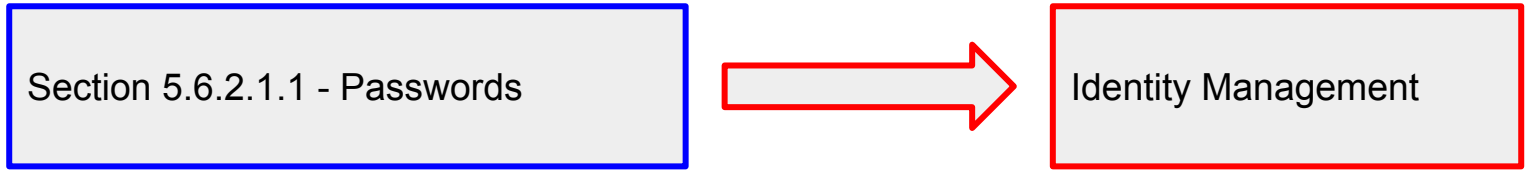


Where Does IDM Fit?

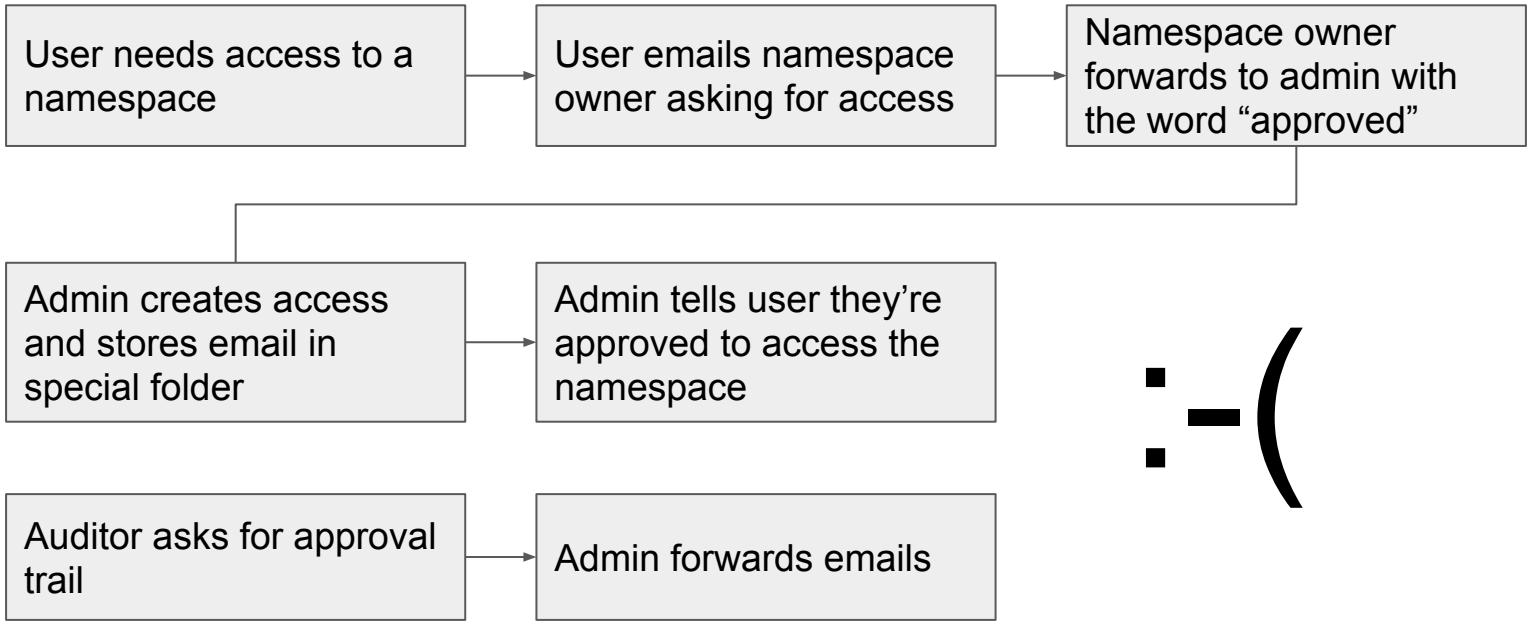
NIST 800-53



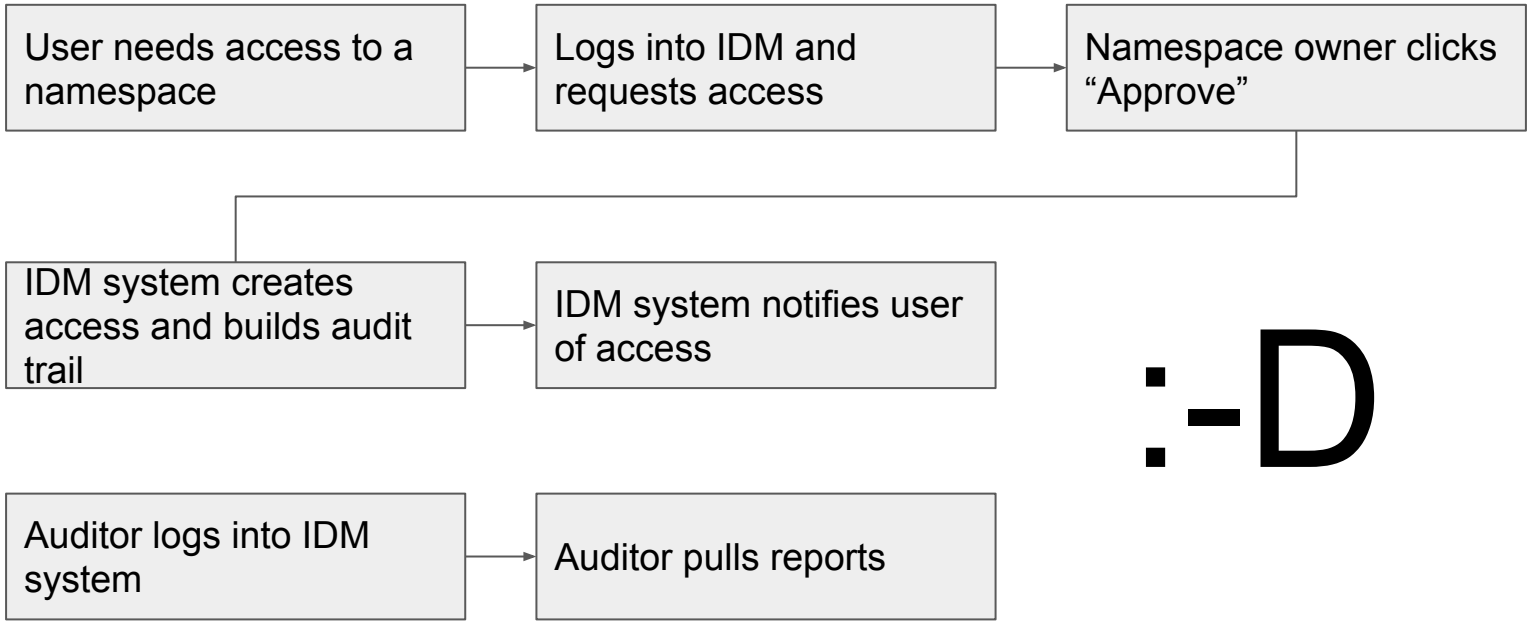
Criminal Justice Information Systems (CJIS)



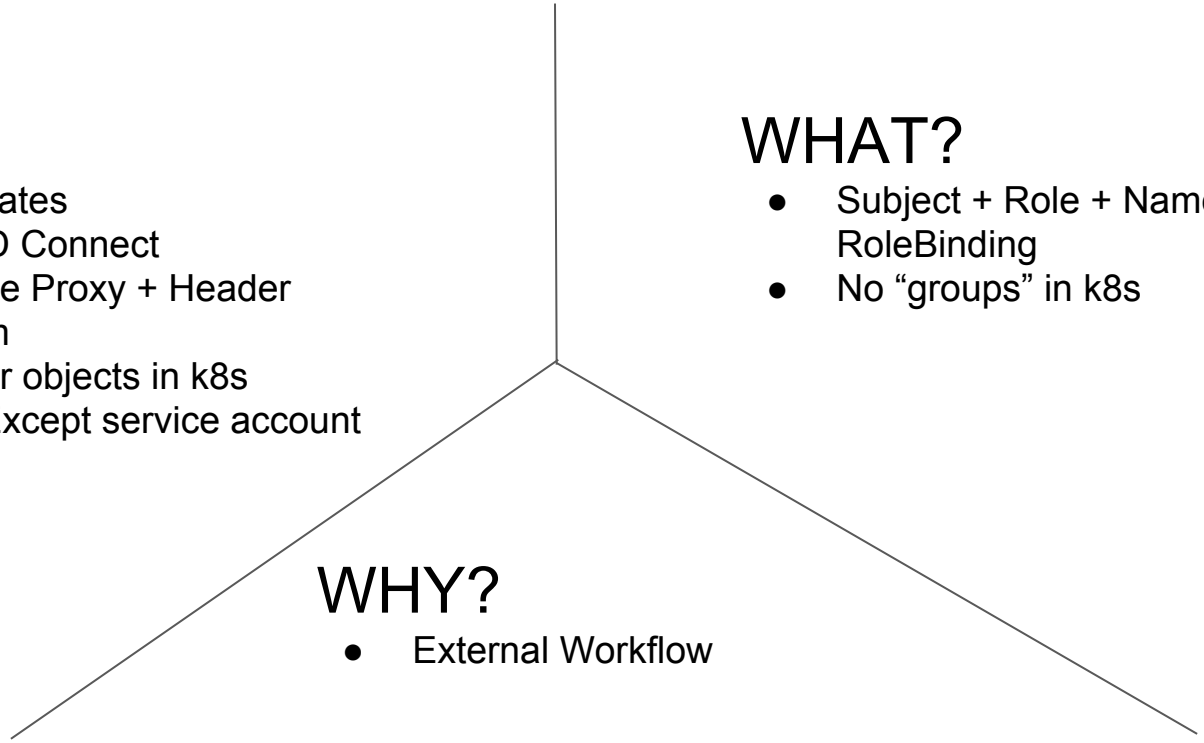
IDM Compliance Without DevOps



IDM Compliance With DevOps



How This Applies to k8s?



WHO?

- Certificates
- OpenID Connect
- Reverse Proxy + Header
- Custom
- No user objects in k8s
  - Except service account

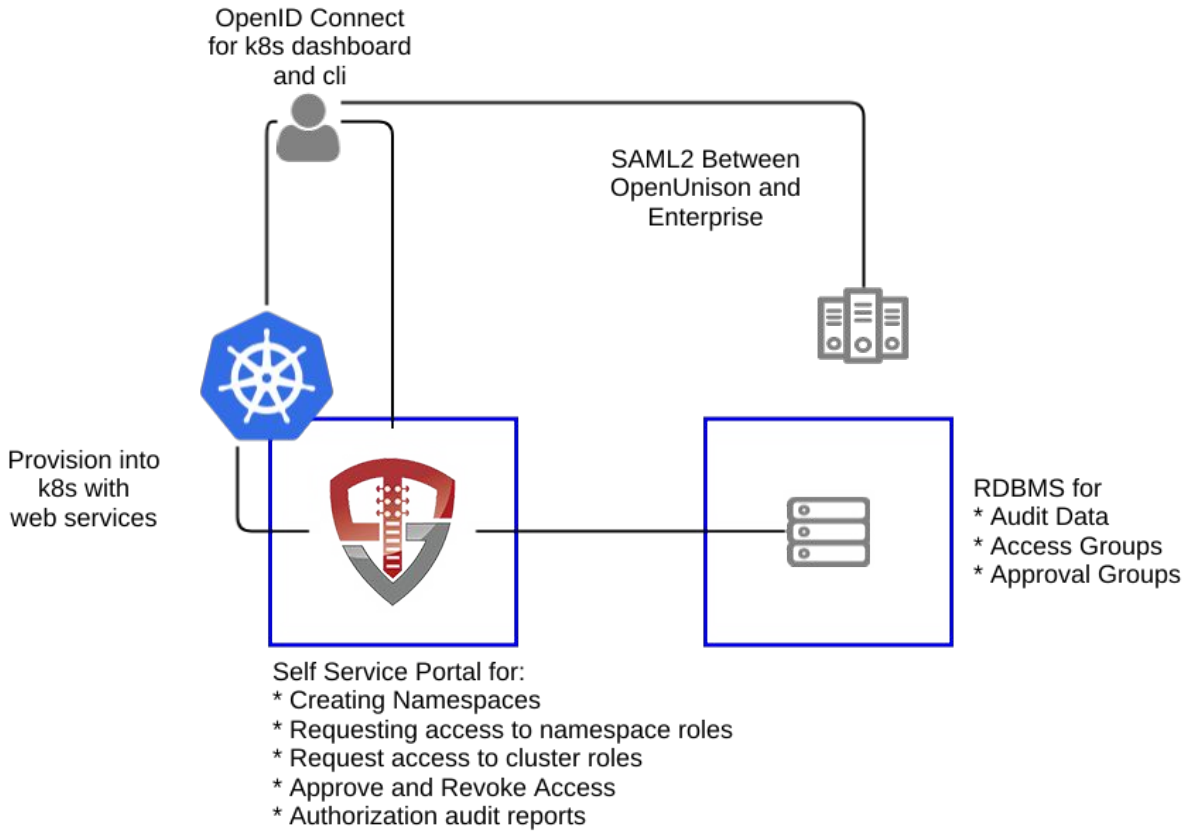
WHAT?

- Subject + Role + Namespace = RoleBinding
- No “groups” in k8s

WHY?

- External Workflow

Demo Environment



Demo!

Useful Resources

- Podctl Episode 15 - https://blog.openshift.com/podcast-podctl-15-identity-management-authentication-and-authorization/
- Kubernetes Authentication - https://kubernetes.io/docs/admin/authentication
- Overview of Kubernetes certificate authorities - https://jvns.ca/blog/2017/08/05/how-kubernetes-certificates-work/
- OpenShift, Identity Management & Compliance - https://www.tremolosecurity.com/openshift-compliance-and-identity-management/

Shameless Self Promotion

- Web - https://www.tremolosecurity.com/kubernetes
- Twitter - @tremolosecurity / @mlbiam
- Kubernetes Identity Manager - https://github.com/TremoloSecurity/openunison-qs-kubernetes
- OpenShift Identity Manager - https://github.com/TremoloSecurity/openunison-qs-openshift
- Kubernetes Identity Manager with U2F and Banner Acknowledgement - https://github.com/mlbiam/openunison-qs-kubernetes/tree/1.0.12-u2f