Everything git
A practical approach to GitOps on AKS

Christoph Burmeister
Principal Solutions Architect, Microsoft MVP

Sponsors

Agenda

- Intro
- What is GitOps
- Why use it to bootstrap AKS?
- Demo (maybe?)
- Q&A

Christoph Burmeister

Principal Solutions Architect, MVP

- @chrburmeister
- /in/chrburmeister
- chrburmeister
- itinsights.org
- berlin-bytes.de

Why all this?

Running Kubernetes

- can be hard
- processes need to change
- tooling is different
- so many apps to run
  - operator applications <- **we will focus on this part**
- security
- compliance
- backup / recovery / disaster recovery

Kubernetes Ecosystem

- Deployments - Helm / Kustomize
- Ingress Controller
- Certificate Management for TLS termination
- Observability
- Networking Requirements – Service Mesh
- Secret Management
- Custom Scaler
- Policies
- …

How to manage all this?

The default approach

- CD pipelines to connect to your cluster and deploy on demand
- A lot of pipelines – one per:
  - operator application
  - cluster config
  - custom application
- Security concerns
  - admin overhead
  - pipeline needs write access to k8s cluster
  - hyper-scaler move away from using k8s local accounts – disabled by default – used extern identity for human interaction

Lets do this better:

GitOps!

GitOps

- method to manage your entire application lifecycle from a git repository
- for
  - Infrastructure (kind of)
  - Application <- **we will focus on this**
- part of continuous deployment
- the repository represents the current state at all times!
  - single source of truth
  - (reconciliation loop)

GitOps

- we will have a look at GitOps on Kubernetes
- Tools:

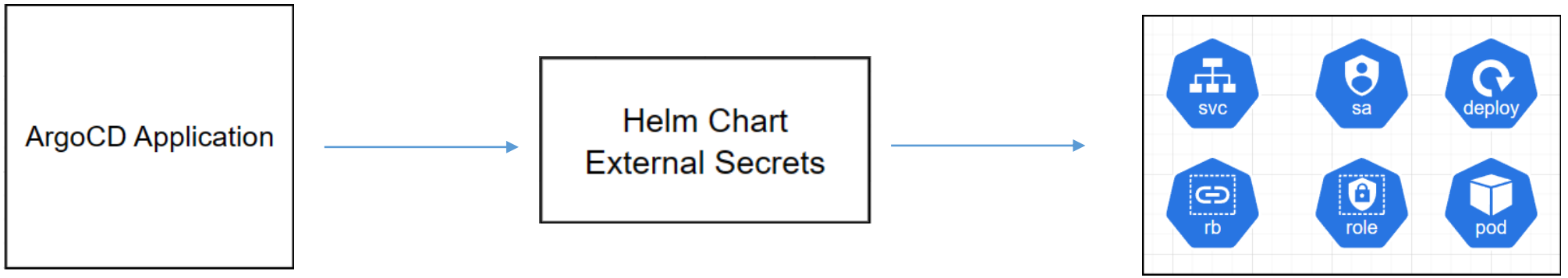
argo

flux

argo

- listens to git repo for changes -> (applies them)
- clean set of permissions
  - no local accounts in k8s necessary
  - read permissions to the repo is enough
  - only read permissions required on k8s
  - login possible by Entra ID
- agent running inside the cluster
  - pull instead of push
  - (can run outside, this defeats the purpose of a minimal set of permissions and local accounts)

- use ArgoCD – similar to Flux
- connect to git repository
- based on repo, create applications (crd) - k8s operator
  - helm / k8s native manifest / kustomize

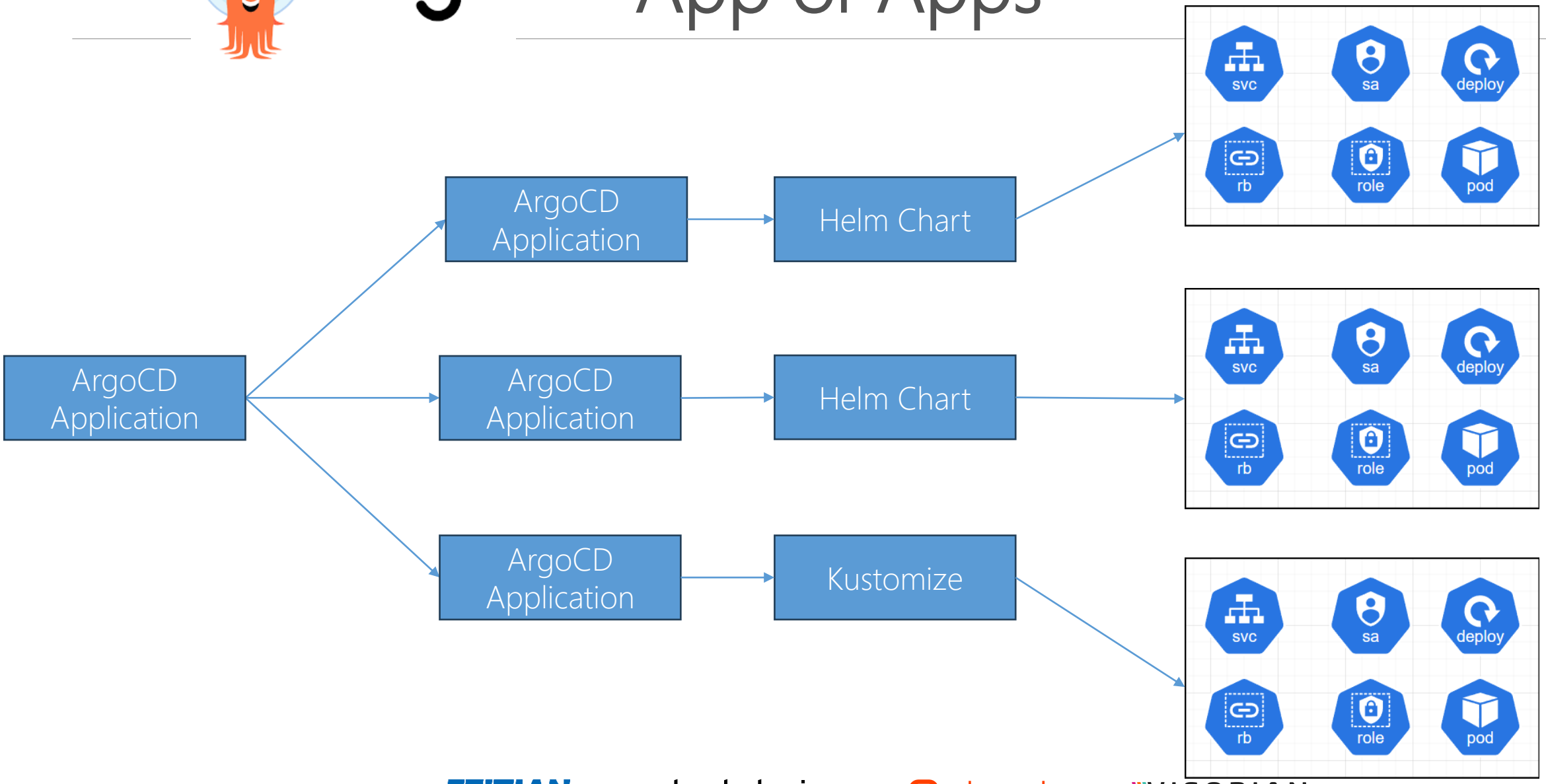


Demo

argo

- since ArgoCD applications are crds, we can deploy applications with one application
- App of Apps pattern -> bootstrap the entire setup/management

App of Apps


ArgoCD Application
ArgoCD Application
Helm Chart
ArgoCD Application
Helm Chart
ArgoCD Application
Kustomize
svc
sa
deploy
rb
role
pod
svc
sa
deploy
rb
role
pod
svc
sa
deploy
rb
role
pod

Demo

- update helm versions
  - renovate bot
  - creates PRs in your repo to update operator applications
  - like depandabot on GitHub
- very fast setup and
- recovery / disaster recovery
- least privilege for all people
- multi-tenant setup with ArgoCD
- find the code here: https://gitlab.com/chrburmeister/app-of-apps

Questions?

Azure Saturday Hamburg 2024

9:30 AM	Keynote
10:05 AM	Mastering Your Logging Ninja Skills with LogAnalytics
10:05 AM	Empowering Cloud security with Microsoft Sentinel, Defender for Cloud and Defender XDR
1:00 PM	Lightning Sessions
2:00 PM	Hybrid- and Multi- Cloud Server Management mit Azure Arc
3:00 PM	1st AID for EID - how to prevent lateral movement to Entra ID when your Active Directory has fallen
4:00 PM	Microsoft Fabric, how to keep your items and data safe
5:00 PM	Gewinnspiel & Hang Out