



**KubeCon**



**CloudNativeCon**

**North America 2023**





KubeCon



CloudNativeCon

North America 2023

# Streamlining Infrastructure with Crossplane: A Transformation Story

*Clément Blaise*

*Jared Watts*

# Agenda



KubeCon



CloudNativeCon

North America 2023

- Introduction
  - Starting Point
  - The Appeal of Crossplane
- Our Journey
- Deep Dives into Key Features
  - Multi-Tenancy
  - Claim References
  - Cluster Components
- Conclusion
- Q&A



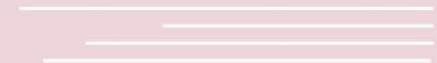
**KubeCon**



**CloudNativeCon**

———— North America 2023 ————

# Introduction





## Clément Blaise

Senior Platform Engineer at Consensys

Passion for creation not confined to work, also revel in photography and music



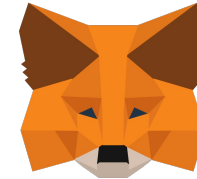
## Jared Watts

Co-Creator of Crossplane, Founding Engineer at Upbound

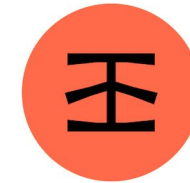
Building open source communities, splitting time in San Diego and Brussels, always hunting good waves 🏄



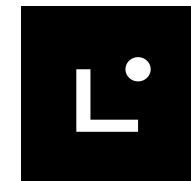
- Founded in 2016
- 800+ employees
- Blockchain technology and web3 software development



**MetaMask**  
Self-Custodial Wallet



**Infura**  
Web3 Development Platform



**Linea**  
zk-EVM L2 Network



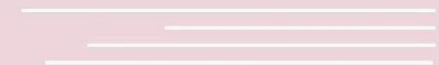
**KubeCon**



**CloudNativeCon**

———— North America 2023 ————

# Our Crossplane Journey



# Starting Point



KubeCon

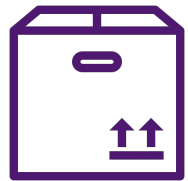


CloudNativeCon

North America 2023

I need to  
scale

*Team A*

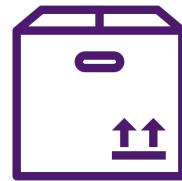


HashiCorp

**Terraform**

I need a  
database

*Team B*

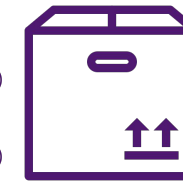


AWS CLOUDFORMATION



ANSIBLE

*Team C*



**Pulumi**

I need to  
patch all of  
them...



*Embedded SREs*



# Inefficiencies



KubeCon



CloudNativeCon

North America 2023

- Requires tool-specific knowledge
  - Learning curve
  - Cognitive Load
- Mostly human interaction
- Reinventing the wheel
- Time to Market
  - Lack of a golden path
  - Lack of reusable automation (Pet vs Cattle)

# Our Plan



KubeCon



CloudNativeCon

North America 2023

## Goals

- Golden Paths
- Self-service

## Who?

- New projects
- Stateless First

## How ?

- Leverage Kubernetes
  - API
  - Isolation
  - RBAC
  - Reconciliation
- Consume via Argo CD

# Before Crossplane



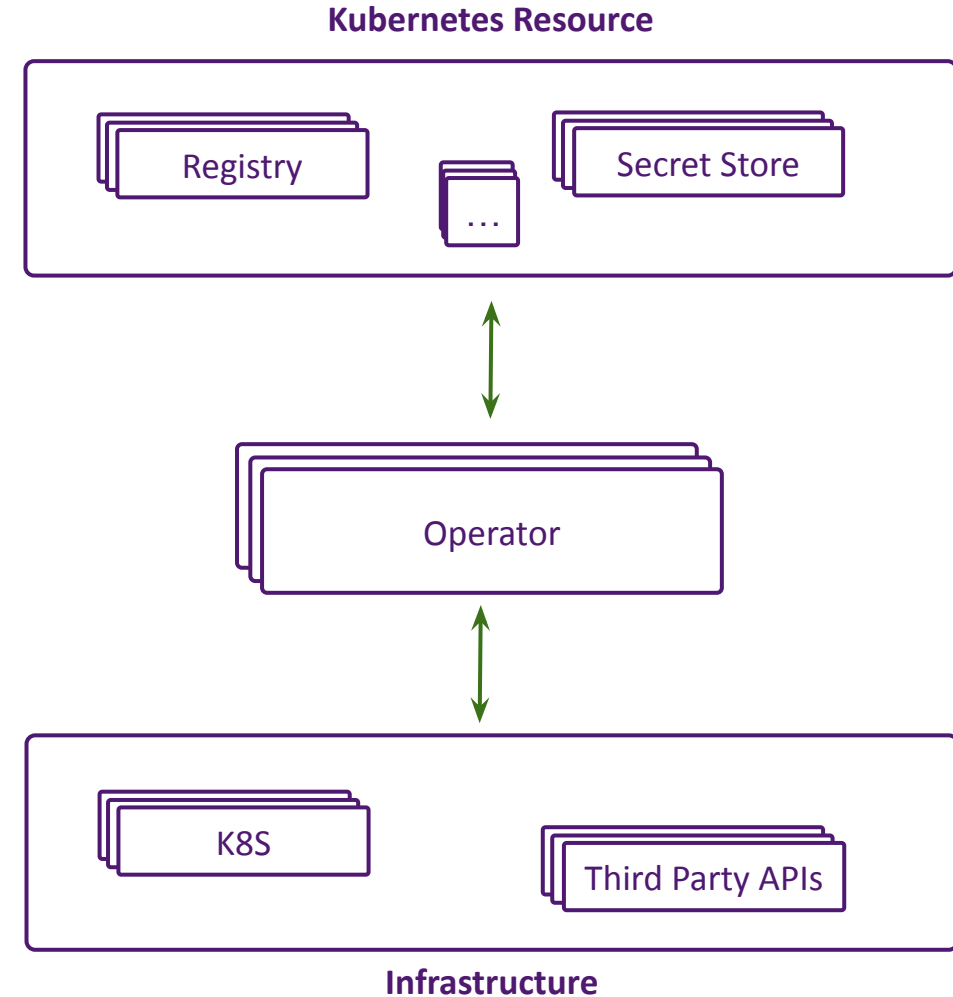
KubeCon



CloudNativeCon

North America 2023

- High learning curve
- Increased cognitive load
- Time-consuming setup and management
- Specific purpose built



# The Appeal of Crossplane



KubeCon



CloudNativeCon

North America 2023

- Build your platform without writing code
  - No custom operators or controllers to write
  - Declaratively describe the resources of your platform - let Crossplane provision, manage, reconcile, etc.
  - Deep customization of the platform's logic possible with Functions (low-code)
- API first design
  - Strong “separation of concerns” between platform and developers
  - Self-service enablement on golden paths
  - Normalize on K8s API for infra and apps, easily integrate rich ecosystem of cloud native tools

# Refresher: Composition API model

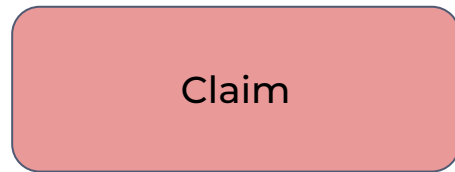


KubeCon

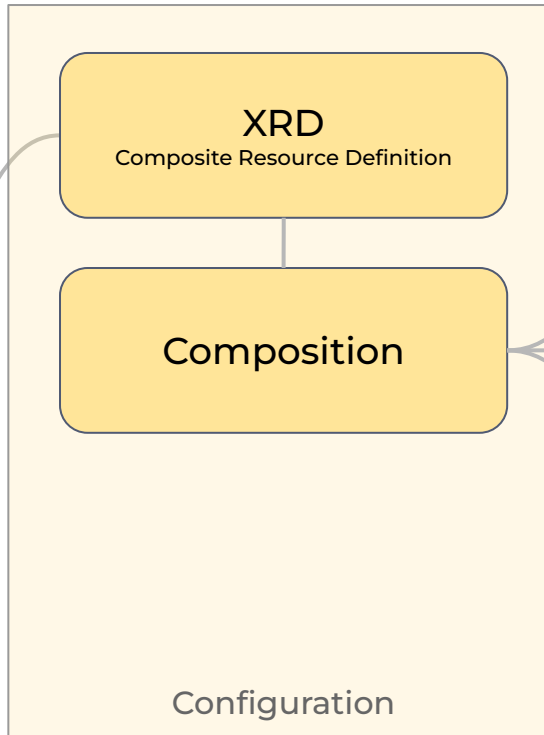


CloudNativeCon

North America 2023



Claim

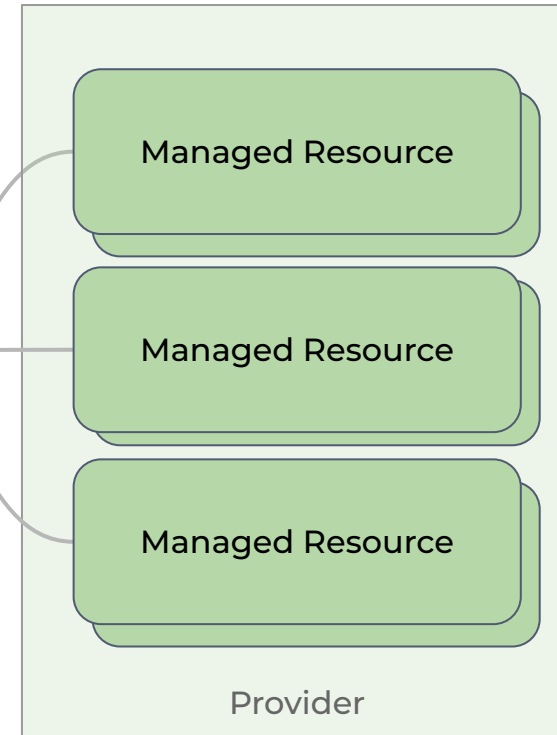


XRD

Composite Resource Definition

Composition

Configuration



Managed Resource

Managed Resource

Managed Resource

Provider

# Refresher: Composition API model

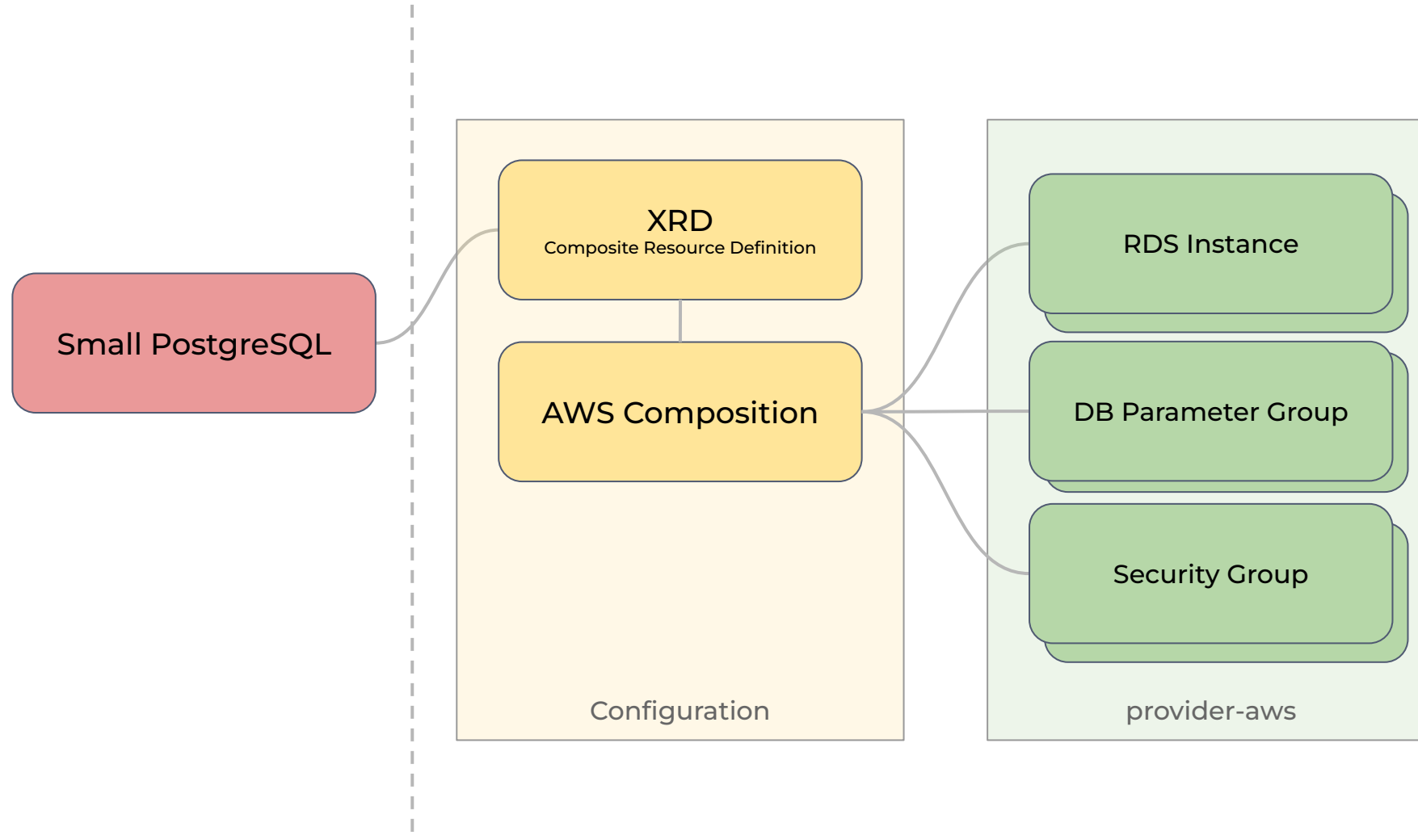


KubeCon



CloudNativeCon

North America 2023



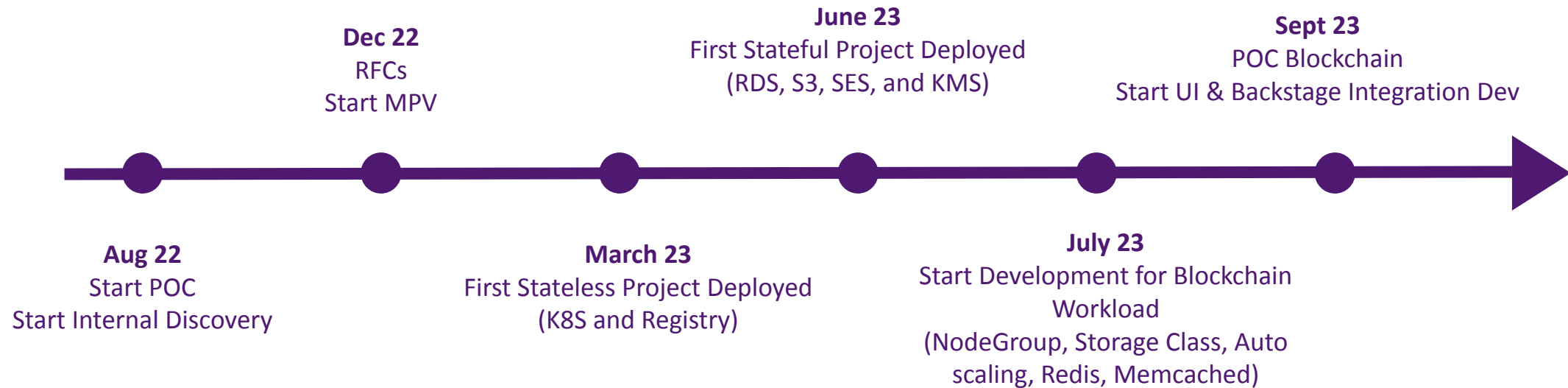
# Timeline



KubeCon  
North America 2023



CloudNativeCon  
North America 2023





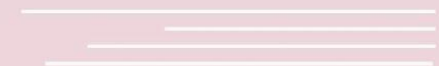
**KubeCon**



**CloudNativeCon**

North America 2023

# Multi-Tenancy





# Namespace Isolation

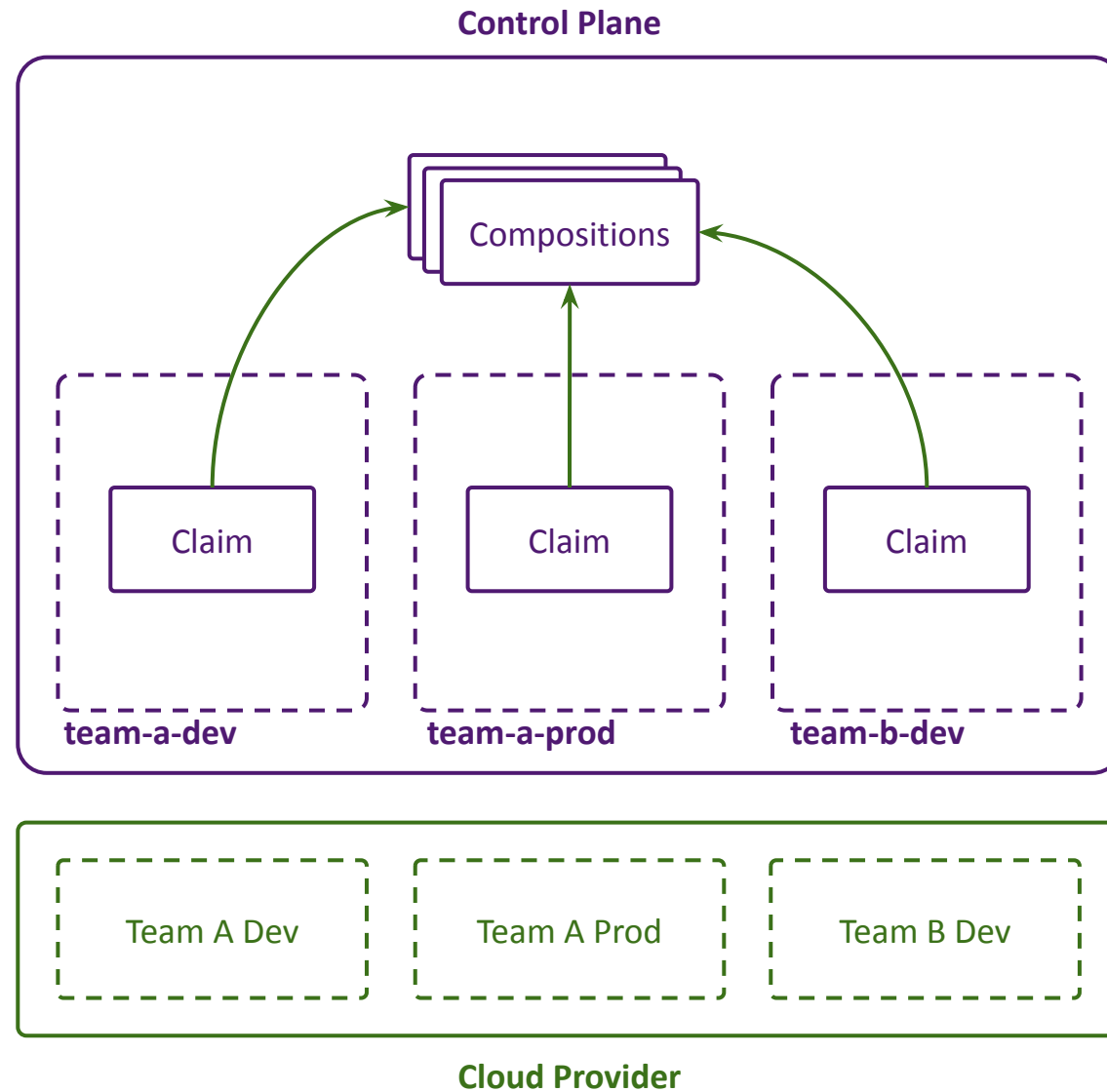


KubeCon



CloudNativeCon

North America 2023



# Building ProviderConfig Reference

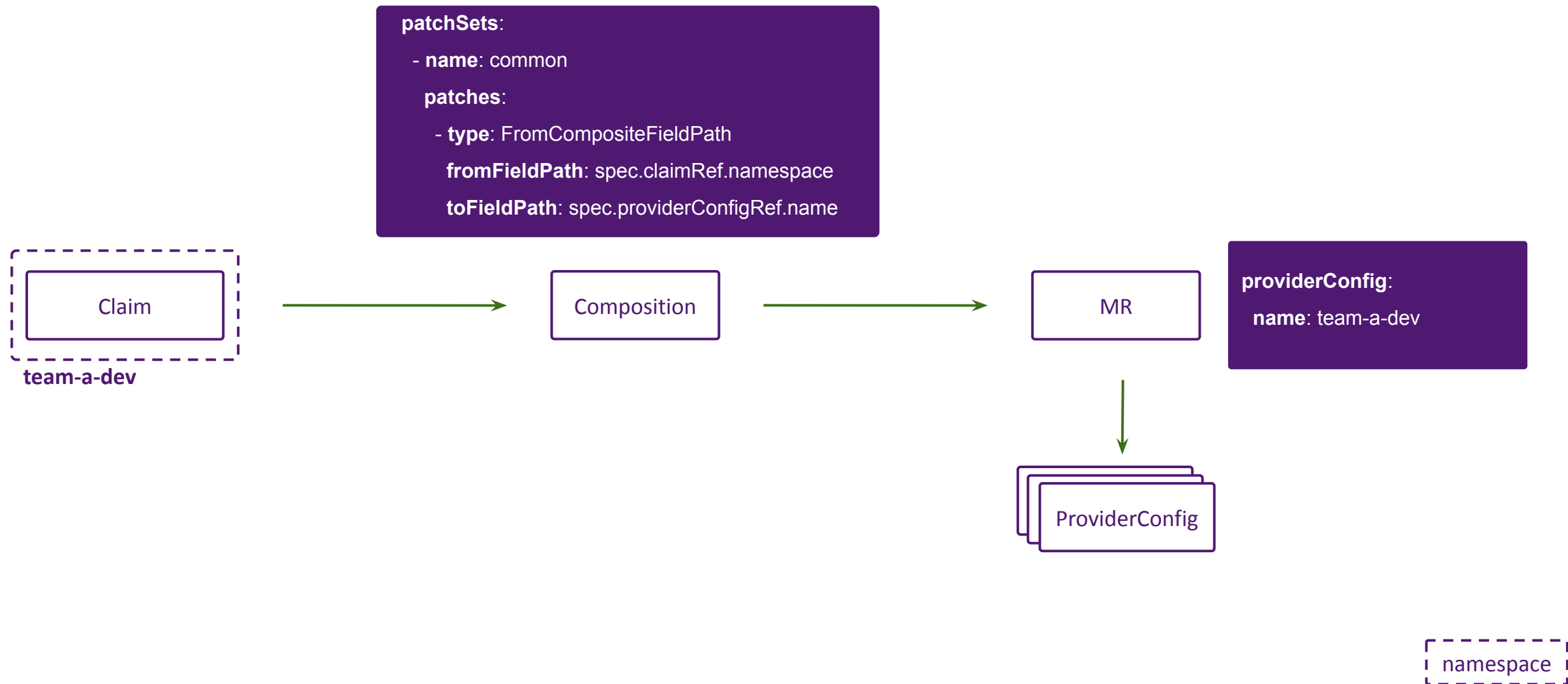


KubeCon



CloudNativeCon

North America 2023



# Naming Convention



KubeCon



CloudNativeCon

North America 2023

**patches:**

- **type:** CombineFromComposite

**toFieldPath:** metadata.name

**combine:**

**variables:**

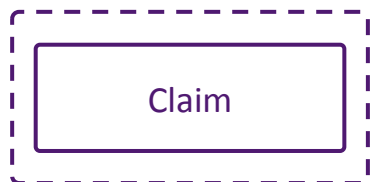
- **fromFieldPath:** spec.claimRef.namespace

- **fromFieldPath:** spec.claimRef.name

**string:**

**fmt:** "%s-%s"

*XRD name could be prefixed if the MR type is use as part of  
another composition to avoid conflicts*



team-a-dev

Composition

MR

**metadata:**

**name:** team-a-dev-<claim>

namespace

# Tenant Management



KubeCon



CloudNativeCon

North America 2023

```
apiVersion: consensys.io/v1
kind: XTenant
metadata:
  name: team-a
```

Management Namespace

Observability Tenant

Argo CD Instance

Subdomain & Certificate

XRD

MR

# Environment Management



KubeCon



CloudNativeCon

North America 2023

```
apiVersion: consensys.io/v1
kind: Environment
metadata:
  namespace: team-a
  name: dev
```

User Namespace

ProviderConfig

IAM (Roles, Policies and OIDCs)

Argo CD Project

XRD

MR

# Tenant and Environment Overview

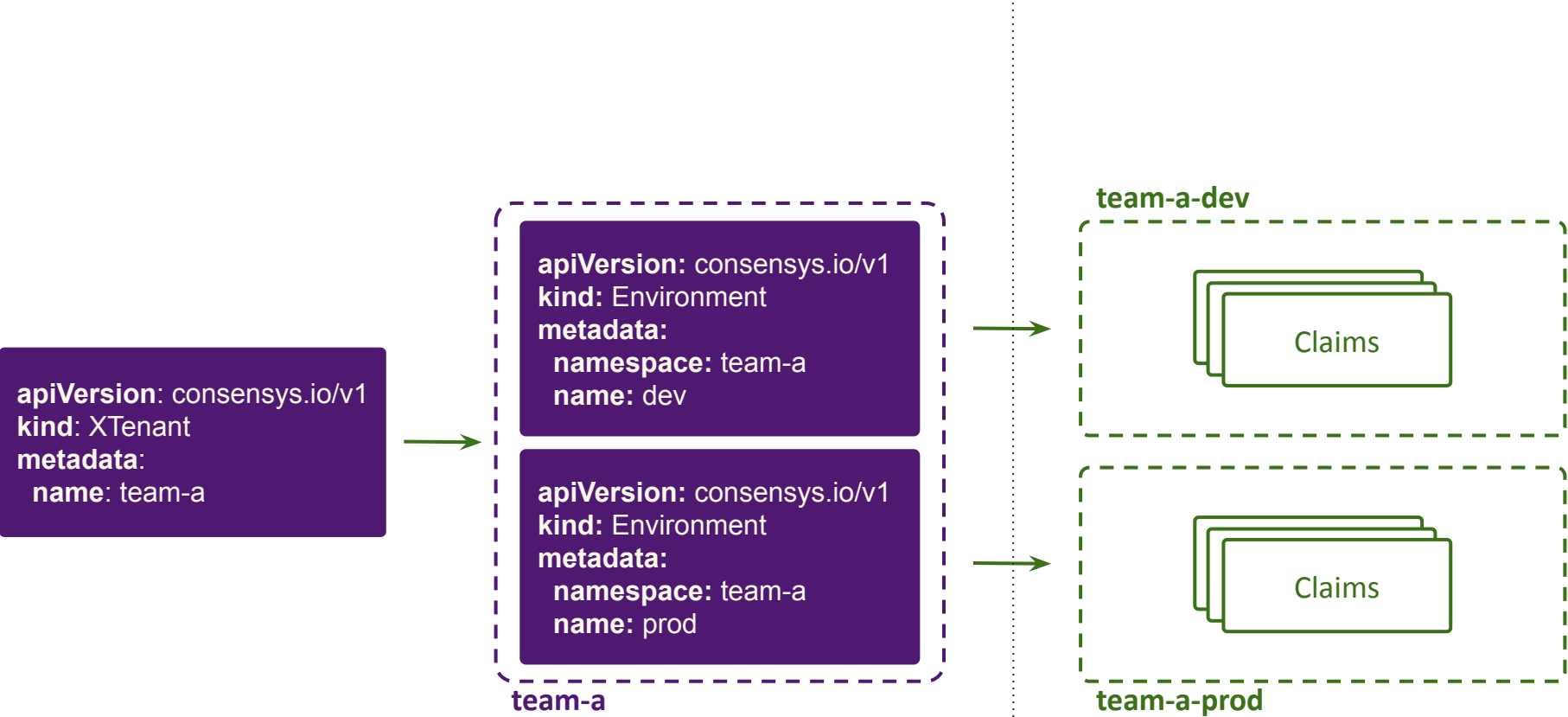


KubeCon



CloudNativeCon

North America 2023



Management Consumption

namespace

# ArgoCD Isolation

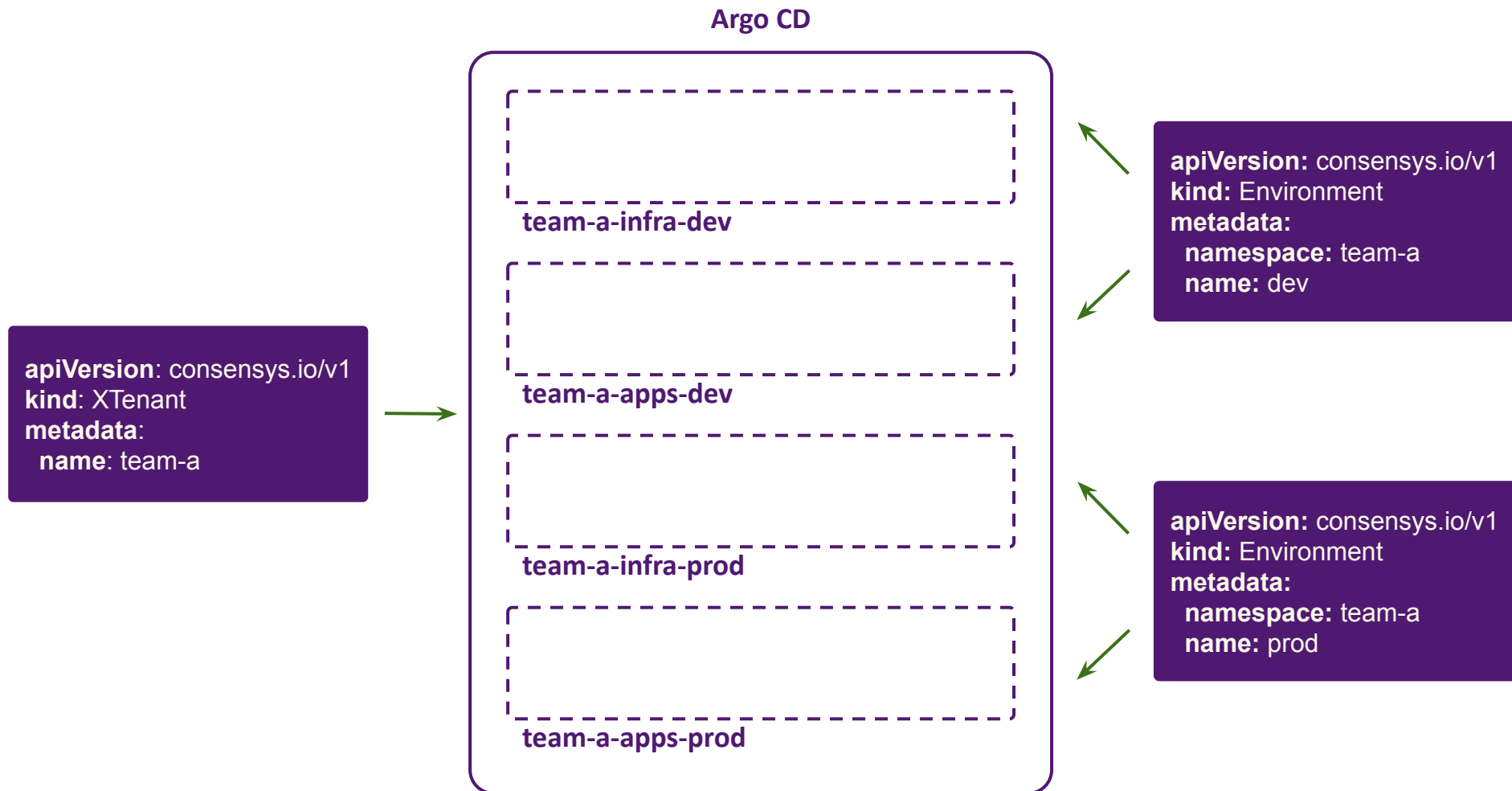


KubeCon



CloudNativeCon

North America 2023



# ArgoCD Permission



KubeCon



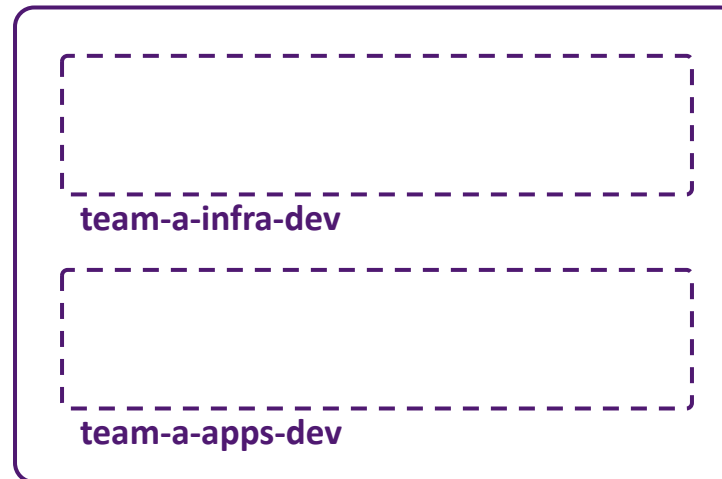
CloudNativeCon

North America 2023

```
destinations:
- name: "in-cluster"
  namespace: "<tenant>-<environment>"
clusterResourceWhitelist:
- group: ""
  kind: ""
namespaceResourceWhitelist:
- group: "kubernetes.consensys.io"
  kind: "Cluster"
- group: "s3.consensys.io"
  kind: "Bucket"
- ...
```



Argo CD



```
destinations:
- namespace: "*"
  server: "!https://kubernetes.default.svc"
- namespace: "!kube-system"
  server: "*"
- namespace: "!kube-node-lease"
  server: "*"
- ...
clusterResourceWhitelist:
- group: ""
  kind: ""
namespaceResourceWhitelist:
- group: "*"
  kind: "*"
- ...
```

Project MR

Project





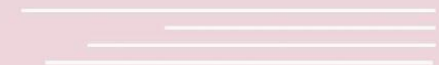
**KubeCon**



**CloudNativeCon**

———— North America 2023 ————

# Claim References



# Example Reference




KubeCon



CloudNativeCon

North America 2023

```
apiVersion: database.consensys.io/v1
kind: SQLInstance
metadata:
  name: demo
  namespace: team-a-dev
spec:
  cluster: demo
  storageGB: 10
  engine: postgres
  version: 12
```



```
apiVersion: kubernetes.consensys.io/v1
kind: Cluster
metadata:
  name: demo
  namespace: team-a-dev
spec:
  version: "1.28"
  region: us-east-1
```

- Select appropriate region
- Connect DB to Cluster VPC (using label matching)
- Generate credentials or SA binding in workload cluster

# Going further

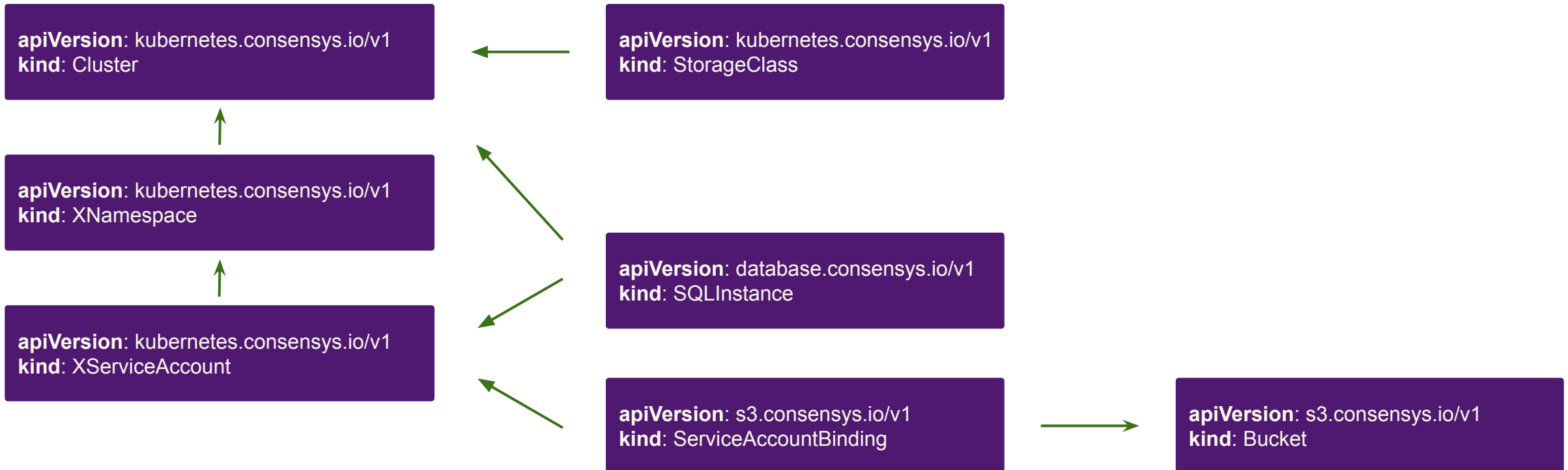


KubeCon



CloudNativeCon

North America 2023



- Provides context to a **Composition** about the runtime environment
  - Reuse same **Composition** in different environments
  - Allows arbitrary unstructured data, e.g., Crossplane's **ConfigMap**
  - Multiple **EnvironmentConfig** can be selected/merged into a **Composition**
- Two main scenarios to write data to an **EnvironmentConfig**
  - From external data sources and systems
  - In **Compositions** to share data across compositions/resources/patches
- Shipped as **alpha** since v1.11, lots of production adoption
  - Maturing to **beta** in v1.15 (Late Jan '24)
  - feedback encouraged! join [#sig-composition-environments](#)

# Creating an EnvironmentConfig



KubeCon



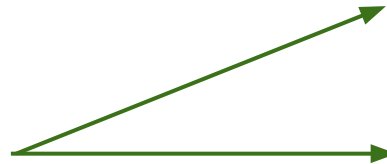
CloudNativeCon

North America 2023

```
apiVersion: kubernetes.consensys.io/v1
kind: Cluster
metadata:
  namespace: team-a-dev
  name: demo
spec:
  region: us-east-1
  ...
```



XCluster



EnvironmentConfig

## patches:

- **fromFieldPath:** spec.claimRef.namespace  
**toFieldPath:** metadata.labels[consensys.io/environment]
- **fromFieldPath:** spec.claimRef.name  
**toFieldPath:** metadata.labels[cluster.kubernetes.consensys.io/name]
- **fromFieldPath:** status.accountId  
**toFieldPath:** data.accountId
- **fromFieldPath:** spec.region  
**toFieldPath:** data.region
- **fromFieldPath:** status.oidc  
**toFieldPath:** data.oidc

```
apiVersion: apiextensions.crossplane.io/v1alpha1
kind: EnvironmentConfig
metadata
  labels:
    consensys.io/environment: team-a-dev
    cluster.kubernetes.consensys.io/name: demo
data:
  accountId: "00000"
  region: us-east-1
  oidc: https://endpoint.example
```

# Retrieving the EnvironmentConfig



KubeCon



CloudNativeCon

North America 2023

```
apiVersion: database.consensys.io/v1
kind: SQLInstance
metadata:
  namespace: team-a-dev
  name: hello-world
spec:
  cluster: us-east-1
...
```



XSQLInstance

```
environmentConfigs:
- type: Selector
  selector:
    matchLabels:
      - key: cluster.kubernetes.consensys.io/name
        type: FromCompositeFieldPath
        valueFromFieldPath: spec.cluster
      - key: consensys.io/environment
        type: FromCompositeFieldPath
        valueFromFieldPath: spec.claimRef.namespace
```



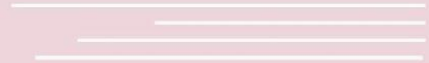
**KubeCon**



**CloudNativeCon**

North America 2023

# Cluster Components



# Argo CD Topology

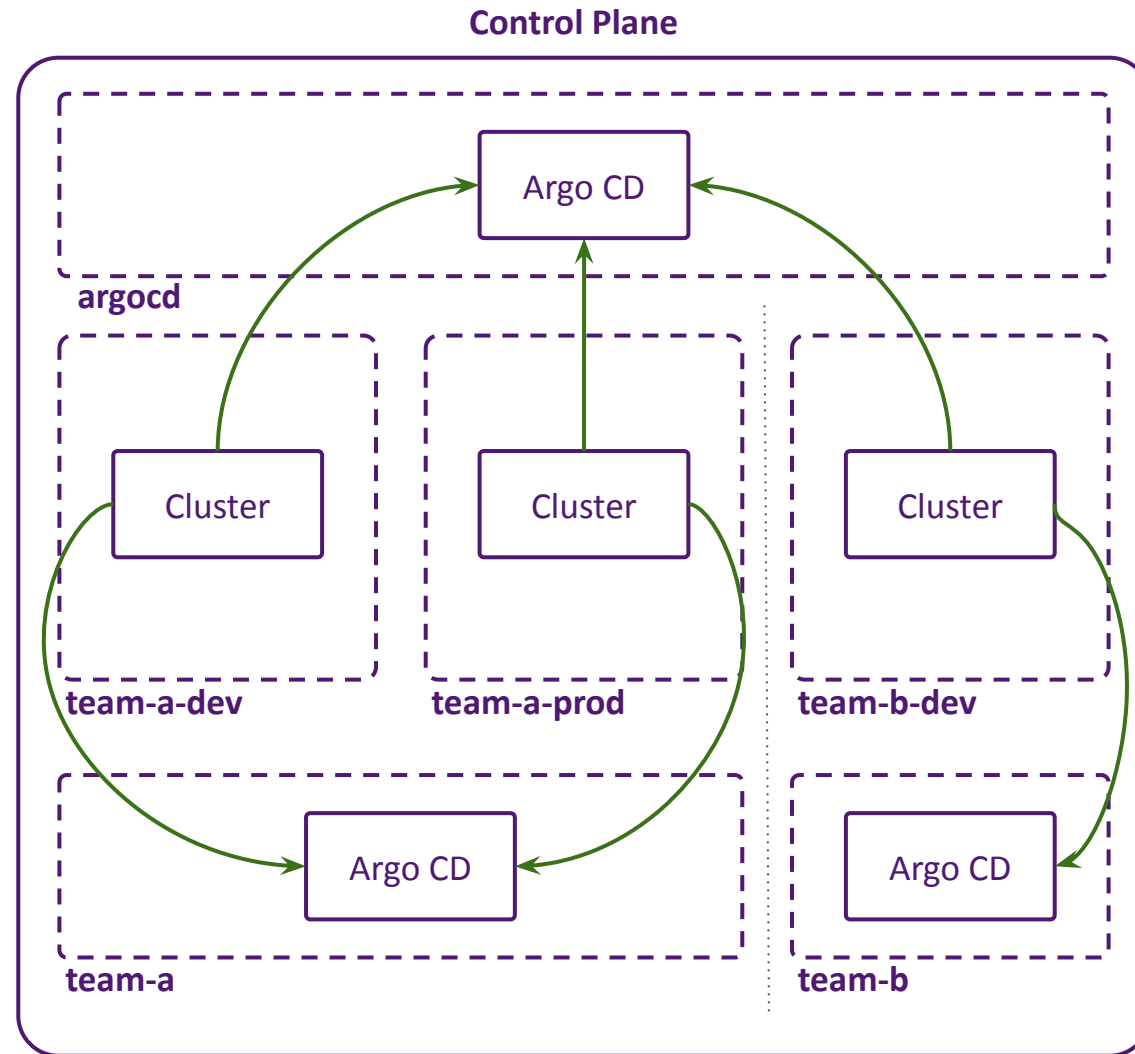


KubeCon



CloudNativeCon

North America 2023



namespace



# Cluster Components

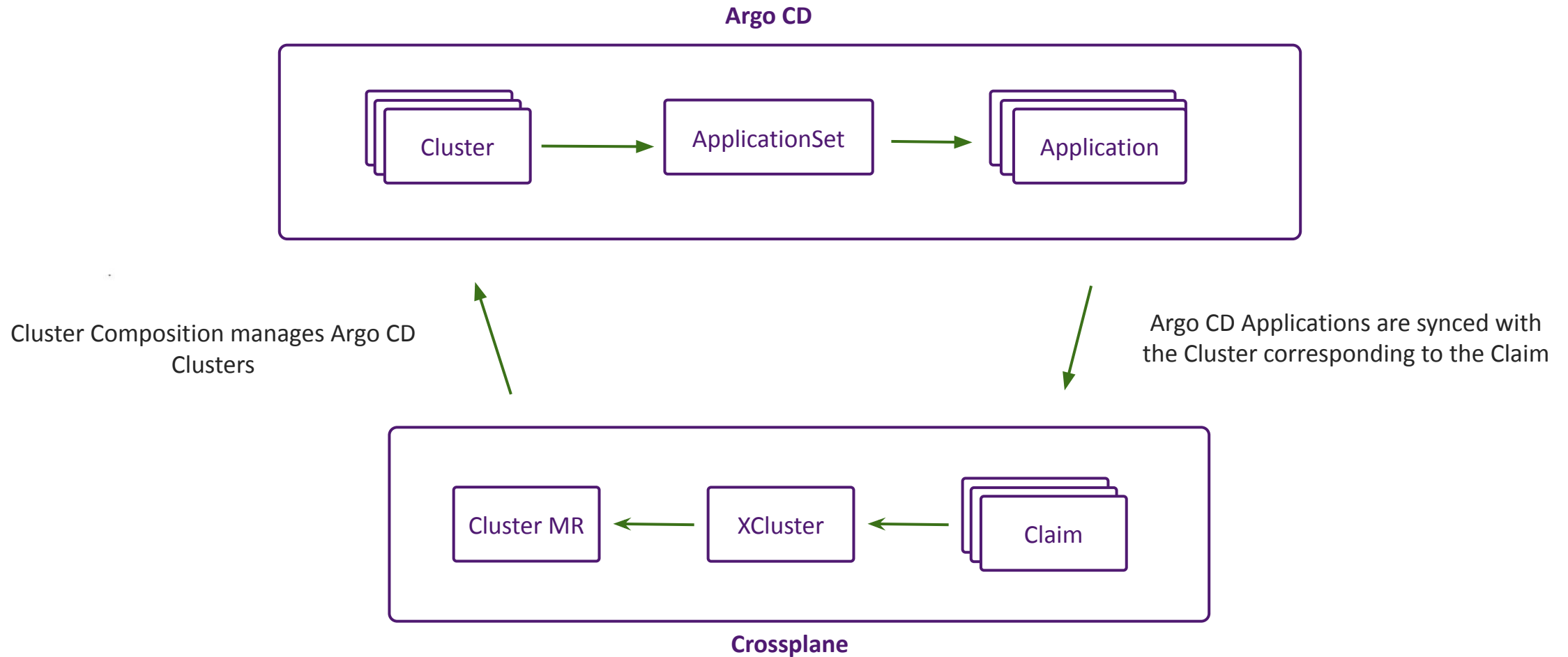


KubeCon



CloudNativeCon

North America 2023



# Add On Mechanism



KubeCon



CloudNativeCon

North America 2023

```
apiVersion: kubernetes.consensys.io/v1
kind: Cluster
spec:
  version: "1.27"
  region: us-east-1
  autoscaler: karpenter
  addOn:
    downscaler: "true"
```



XCluster



```
patches:
- fromFieldPath: spec.autoscaler
  toFieldPath: spec.forProvider.labels.autoscaler
- fromFieldPath: spec.addOn.downscaler
  toFieldPath: spec.forProvider.labels.downscaler
- fromFieldPath: spec.addOn.realoder
  toFieldPath: spec.forProvider.labels.realoder
```

```
apiVersion: cluster.argocd.crossplane.io/v1
kind: Cluster
spec:
  forProvider
    labels:
      autoscaler: karpenter
      downscaler: "true"
      realoder: "false"
```

Argo CD



```
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
spec:
  generators:
    clusters:
      selector:
        matchLabels:
          downscaler: "true"
```



Application



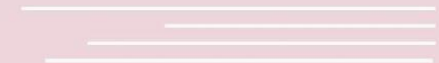
**KubeCon**



**CloudNativeCon**

———— North America 2023 ————

# Conclusion



# Conclusion



KubeCon



CloudNativeCon

North America 2023

- A consistent platform story across your dev teams is critical
- A unified control plane can manage all your teams and environments with the right multi-tenancy approach
- Platforms don't scale unless golden paths are codified and presented for dev team self-service
- Automate all the things!
- Cloud native ecosystem plays well together all speaking K8S API



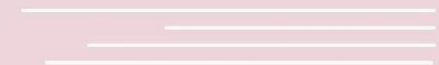
**KubeCon**



**CloudNativeCon**

North America 2023

# Q&A





PromCon  
North America 2021



**Please scan the QR Code above  
to leave feedback on this session**