
AWS
re:Invent

CON208

GitOps compliant: How CommBank multiplied Amazon EKS clusters

Dário Nascimento
Lead Engineer
Commonwealth Bank of Australia

Michael Hausenblas
Sr. Open Source Product Developer Advocate
AWS Elastic Containers

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

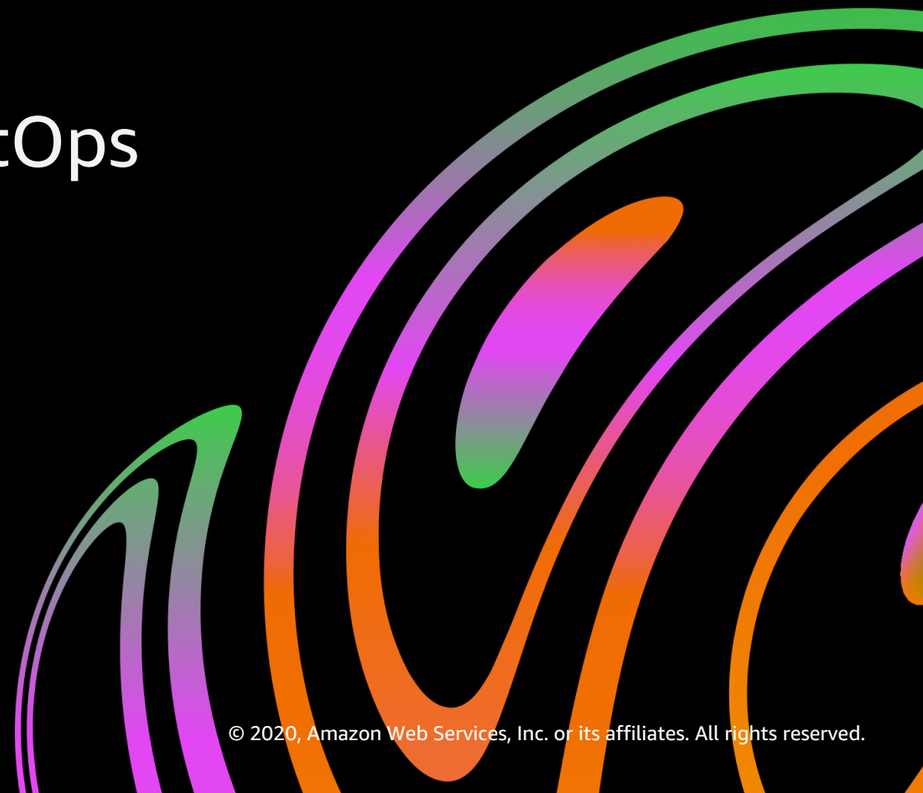
Agenda

How we deployed Amazon EKS using AWS Cloud Development Kit (AWS CDK)

How we run Kubernetes across multiple AWS accounts with multiple tenants

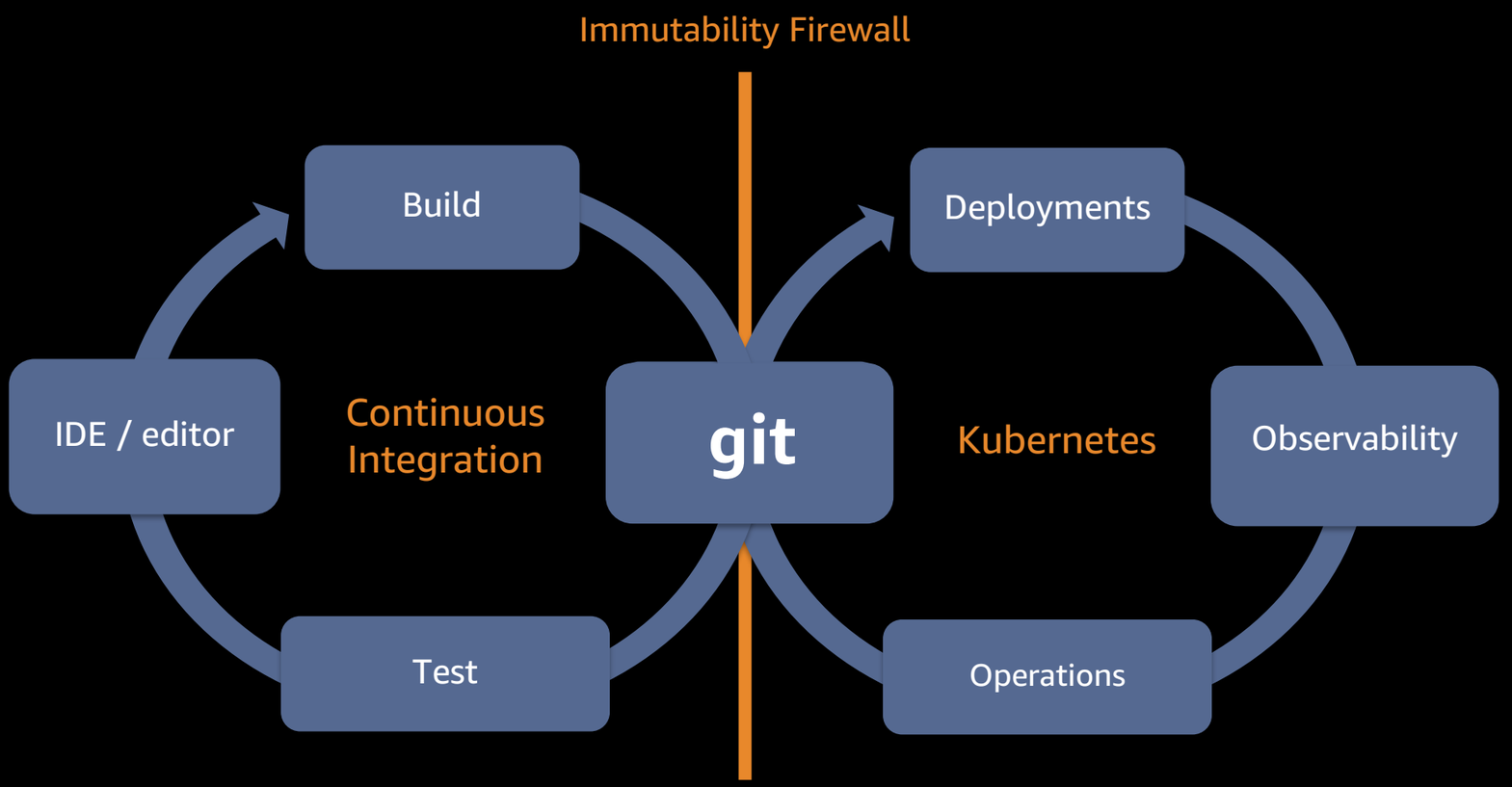
How we enforce regulatory compliance using GitOps

How we consume Kubernetes using CRDs and OPA Gatekeeper



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is GitOps?



A **standardized workflow** for how to **deploy**, **configure**, **monitor, and update** Kubernetes infra and app **as code**

Git as the **single source of truth** of a system's desired state:

→ All intended operations are committed by pull request

→ Automatic convergence between intended and observed state diffs

→ All changes observable, verifiable, and auditable

Standardize and optimize

PROMOTING AND ENFORCING ENGINEERING BEST PRACTICES



Declarative & Immutable

Declare the desired system state, restrict privileged access



Resiliency & Recoverability

Self-healing, fault tolerant, loosely coupled



Observability

Metrics, tracing, logs, vulnerabilities, cybersecurity events and alerting



Security

Automate credential management (secrets, certificates, IAM)

Standardize and optimize

PROMOTING AND ENFORCING ENGINEERING BEST PRACTICES



IT Governance

Automate processes: risk, change, incident management



CI/CD & UX Patterns

Provide outstanding DevUX to promote reliable innovation



Standardization & Compliance

Standard tools and runtime environments compliant with regulatory requirements

Compliance within Kubernetes

- Risk management – identify risks, implement controls to mitigate them
- Organization-wide accredited platform
- Define a shared responsibility model for the platform
- Continuous compliance (e.g., Kubernetes benchmark, security scanning, etc.)
- GitOps operator (ArgoCD) to ensure the running configuration
- OPA Gatekeeper to enforce resource policies

Multi-account
Multi-cluster
Multi-tenant



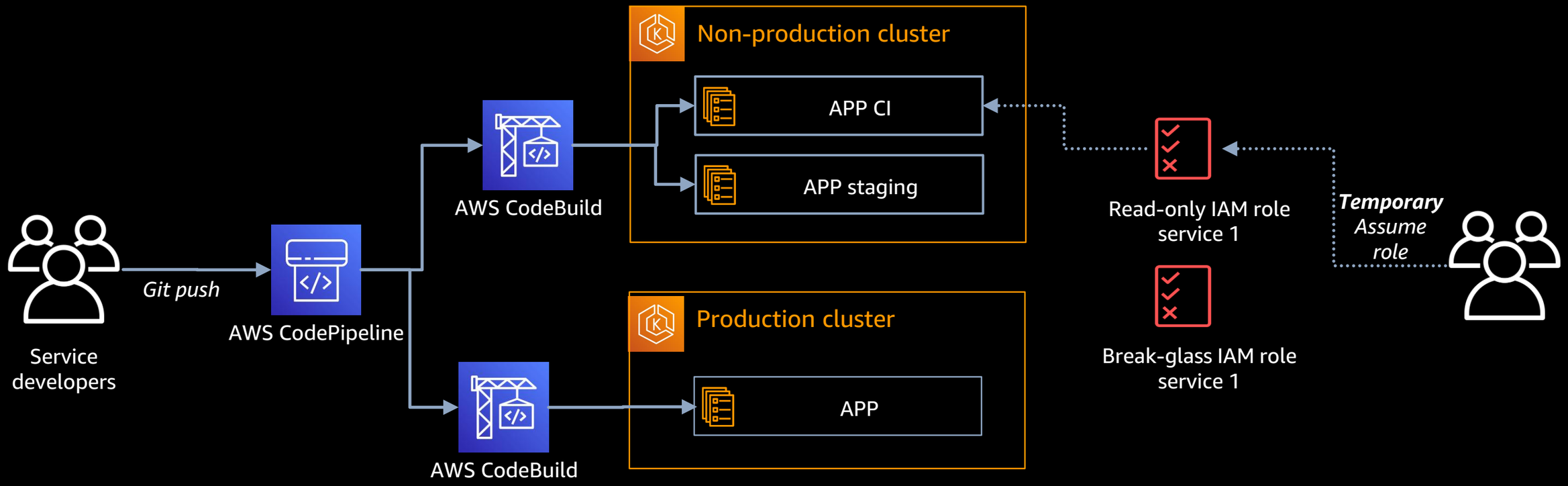
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Blast radius

MULTIPLE CLUSTERS AND ACCOUNTS

Applications in a namespace share secrets, access controls, and IAM roles

Platform team templates namespaces, roles, and quotas



Amazon EKS cell

Container platform cell





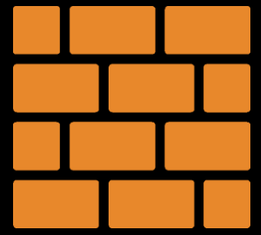



Amazon EKS	Amazon EKS nodes	AWS IAM security groups	Amazon VPC endpoints	AWS CodeBuild	GitOps
	Self-registering AMI via custom launch template	Secure configuration	Keep all API calls within the private network	Self-mutating CI/CD to deploy the cluster	Deploy add-ons and ensure compliance

AWS Cloud Development Kit (AWS CDK)



Type-safe



Composable



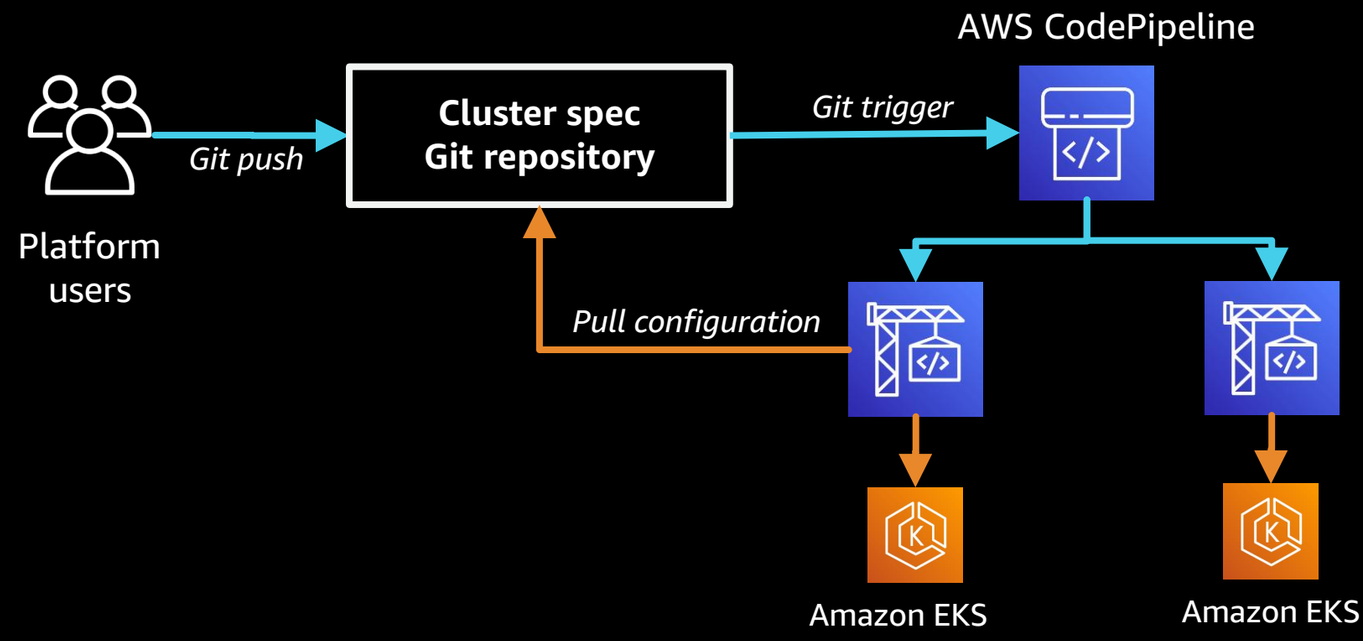
Testable



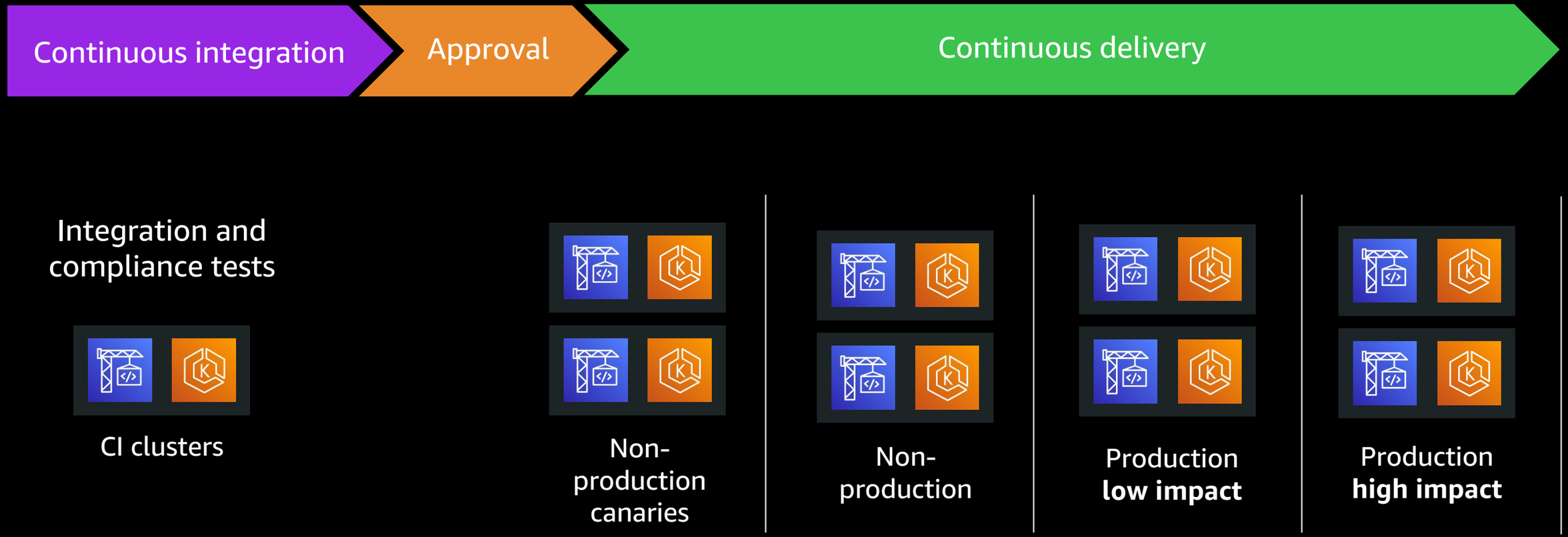
Reusable

Managing multiple Amazon EKS clusters

- Use a mono-repo approach to define clusters, teams, and components
- Include CI/CD in the pattern
- Single deployment pipeline



Managing multiple Amazon EKS clusters

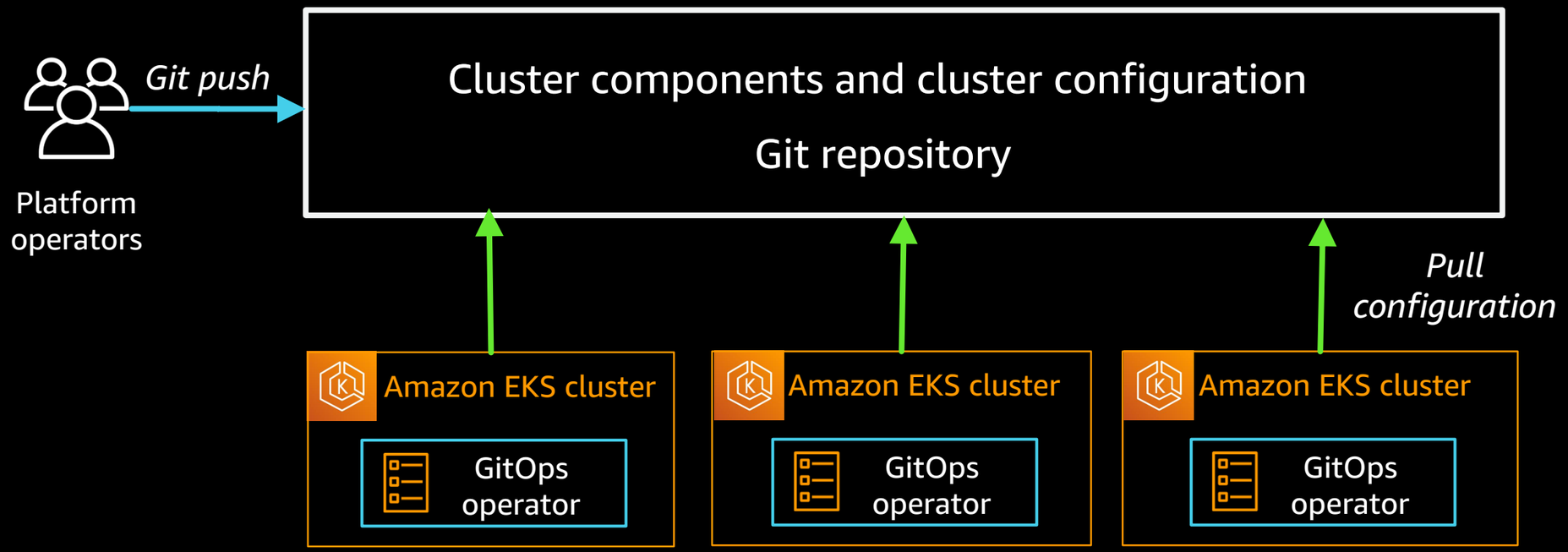


GitOps operators

- Enforce the cluster configuration defined by the platform team in Git
- Prevent, detect, remediate misconfiguration
- Deploy and manage cluster applications



GitOps across multiple clusters



Platform components

- AWS Secrets Manager controller
- Kubernetes certificate manager controller
- AWS controllers for Kubernetes
- External DNS Amazon Route 53 controller
- Application Load Balancer controller
- Fluent Bit logging
- Container IDS
- Velero – cluster backup
- PowerfulSeal – Chaos Monkey
- Prometheus Operator
- OPA Gatekeeper
- Container scanning admission controller

Cluster configuration

- Namespace, IAM roles, resource quotas templating
- Predefined storage classes and Amazon EFS
- Calico network policies
- Pod security policies
- Gatekeeper policies

A cluster must ensure its own data integrity, remaining compliant and consistent without external tools



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Open Policy Gatekeeper



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Open Policy Gatekeeper

- Define policies to ensure Kubernetes data consistency
- Declare policies with Open Policy
- Block resource creation and inform how to make it compliant
- Preview the policy results in Git pull requests

Open Policy Gatekeeper

Use case examples

- Pod disruption budget (PDB) misconfiguration
- Certificate domains
- Tagging
- Container scanning
- Ephemeral storage per container
- Readiness / liveness probes
- Image policies

Create patterns and use GitOps to ensure they are correctly defined and deployed at scale



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Dário Nascimento

Lead Engineer,
Commonwealth Bank
of Australia

Michael Hausenblas

Sr. Open Source Product
Developer Advocate,
AWS Elastic Containers

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.