AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

CON206

Kubernetes at AWS: Strategy, road map, and vision

Allan Naim
Sr. Manager Product Management,
Amazon EKS
AWS

Anubhav Dhoot
VP of Engineering
Salesforce

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Amazon EKS strategy

Recap of 2021

Journey into Hyperforce – Salesforce

Amazon EKS road map and vision

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is Amazon EKS?



Amazon EKS

- Amazon EKS runs vanilla Kubernetes; EKS is an upstream and certified conformant version of Kubernetes (with backported security fixes)
- Amazon EKS supports 4 versions of Kubernetes, giving customers time to test and roll out upgrades
- Amazon EKS provides a managed Kubernetes experience for performant, reliable, and secure Kubernetes
- Amazon EKS makes Kubernetes operations, administration, and management simple

With Amazon EKS, you can build reliable, stable, and secure applications in any environment

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EKS is used in every industry, around the world



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Core tenets



Security first



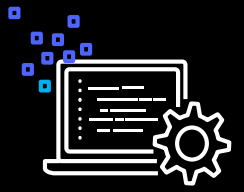
Built for production



Native and upstream



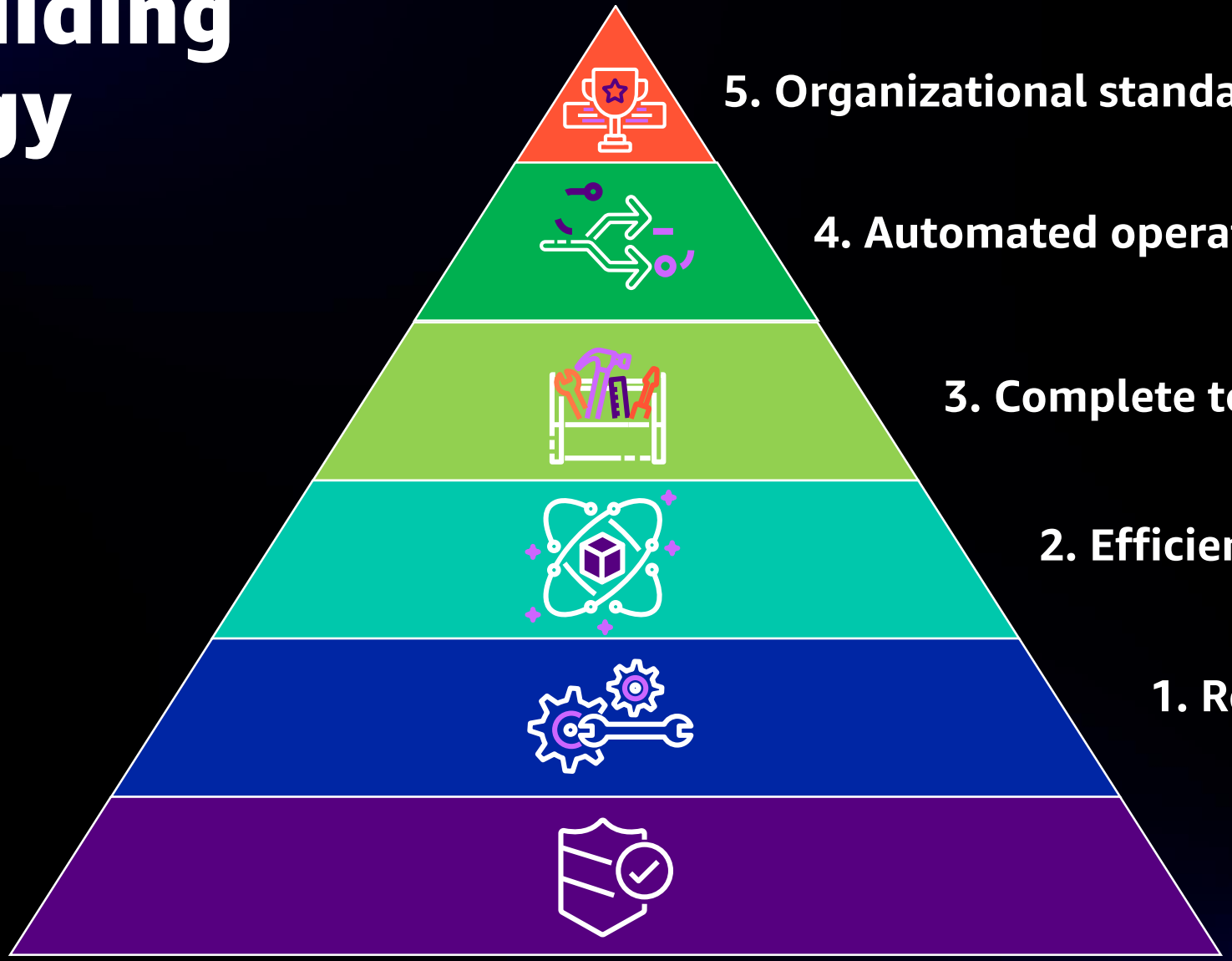
Seamless cloud integrations



Committed to open source

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Our guiding strategy



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recap of 2021

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Deployment options to suit your requirements

Amazon **EKS** on AWS	Best, scale, performance, and cost
Amazon **EKS on** AWS **Local Zones**	Fully managed, latency optimized
Amazon **EKS on** AWS **Outposts**	Fully managed experience where you need it
Amazon **EKS Anywhere**	Your hardware, EKS-consistent tooling
Amazon **EKS Distro**	Your hardware, your management tools



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EKS Anywhere

Now GA!

Create and **operate** Kubernetes in your **data center** and on your **existing hardware** using the same **consistent EKS experience**



Helps customers run with secure, stable, and tested components used to run Amazon EKS



Built on open-source Cluster API



Bundled with components to accelerate readiness of production clusters



Bring your existing bare metal/self-managed compute

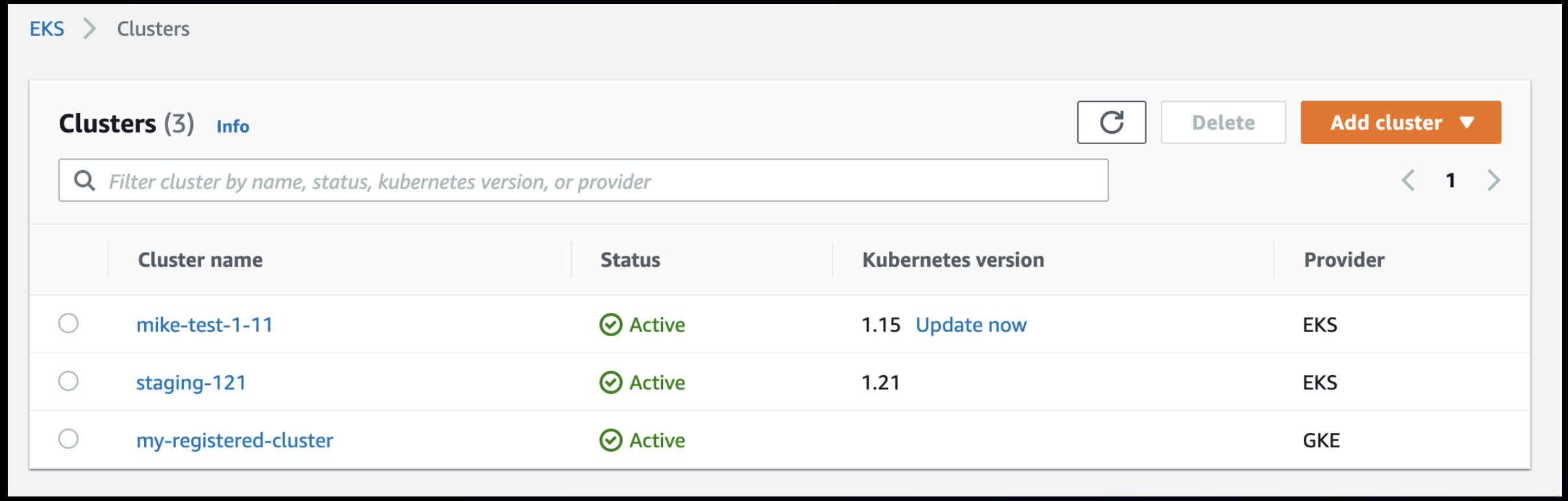
Deploy and manage the lifecycle of EKS Distro clusters on-premises

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Monitor all your clusters with EKS

THE AMAZON EKS CONSOLE–COMBINED AMAZON EKS CONNECTOR PROVIDES A UNIFIED VIEW AND OPERATIONAL VISIBILITY ACROSS ALL YOUR KUBERNETES ENVIRONMENTS



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Karpenter – Ready for production

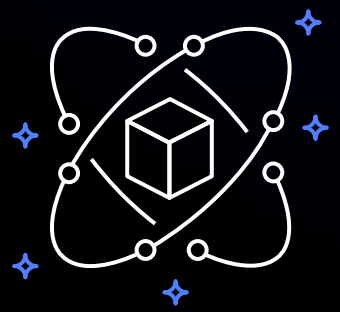
Karpenter is an open-source, flexible, and high-performance Kubernetes cluster autoscaler

- Dynamically chooses best-suited compute resources
- Automatically adds or removes compute resources required
- Scale tested for high performance
- AWS Support in EKS clusters



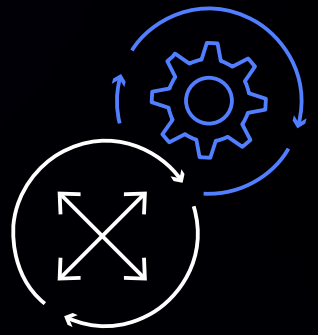
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Managing AWS resources via AWS Controllers for Kubernetes (ACK)



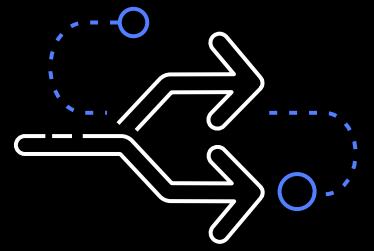
Harness AWS

Create and use AWS resources directly within your cluster; improve reliability and uptime at any scale



Cloud-native control

With Kubernetes custom resources and controllers, you can define the AWS resources your applications need directly within the cluster



Always up to date

ACK generates automatically using the AWS SDKs; this ensures controllers are up to date with the latest features and functionality

Interested in contributing?

https://github.com/aws/aws-controllers-k8s

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CDK for Kubernetes (CDK8s) now GA

Supported programming languages





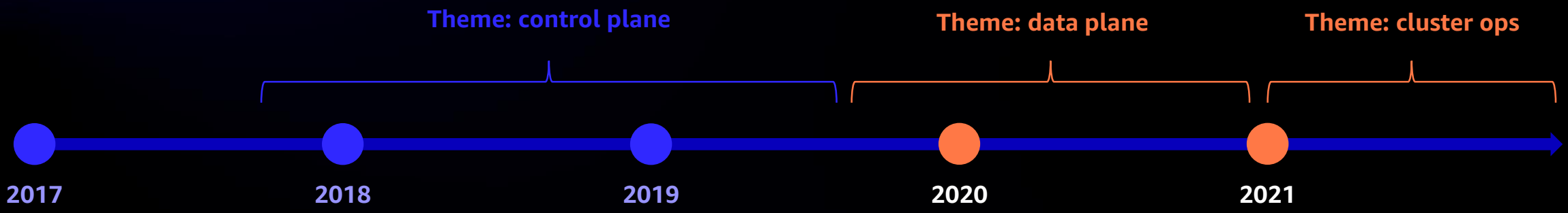
cdk8s

Cloud Development Kit for Kubernetes

Editor's note: CDK8s allows you to generate Kubernetes manifests with your preferred programming language. Recently it was announced as Generally Available (1.0) with support for Kubernetes 1.21 and Golang!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recent launches



Highlighted Amazon EKS launches in the last year

Security and reliability
- FedRAMP Moderate, High
- Secrets encryption with AWS KMS
- External OIDC authentication
- AWS Certificate Manager (ACM) Private Certificate Authority
- AWS Secrets Manager CSI driver

Storage and networking
- Amazon EBS CSI driver GA
- Amazon EFS CSI driver GA w/dynamic provisioning
- Amazon VPC CNI increased pod density
- Pod-level security groups
- AWS Load Balancer Controller GA
- Multus CNI support

Tooling
- AWS CDK for Kubernetes (cdk8s)
- AWS Controllers for Kubernetes (ACK)
- Amazon EKS add-ons
- Hosted Kubernetes console
- Remote Cluster Connector
- eksctl instance selector

Nodes
- Managed node groups custom launch templates
- Karpenter node provisioning
- P4d/Elastic Fabric Adapter support
- Parallel node group upgrades
- Containerd support
- Amazon EKS/AWS Fargate built-in logging

Region/version expansion
- Osaka Region
- Fargate Region expansion – Frankfurt, Oregon, Singapore, Sydney, Cape Town, Osaka, and Milan
- Support for Kubernetes versions 1.19, 1.20, 1.21

Environment expansion
- Amazon EKS Distro
- Amazon EKS Anywhere GA

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Journey into Hyperforce

How Salesforce used Amazon EKS to build an internal microservices platform

Anubhav Dhoot
VP of Engineering, Salesforce



Who is Salesforce?

The Cloud Computing Pioneer

Enterprise Cloud Computing

No Hardware/Software

Instant Scalability

Automatic Updates 3x/year

Fast Deployments

Customer Success Platform

Out-of-the-Box Business Applications

Enterprise Application Development

AppExchange (Public or Private)

Built-In Mobile, Social, Analytics

Legacy of Innovation

#1 CRM Company Worldwide (Gartner)

Most Innovative Company (Forbes x9 Years)

Government Cloud Plus (FedRAMP High)

1:1:1 Philanthropy Model



Introducing Hyperforce

Accelerate **infrastructure agility** by making Salesforce **available anywhere** with trust, elasticity, and ease for our customers



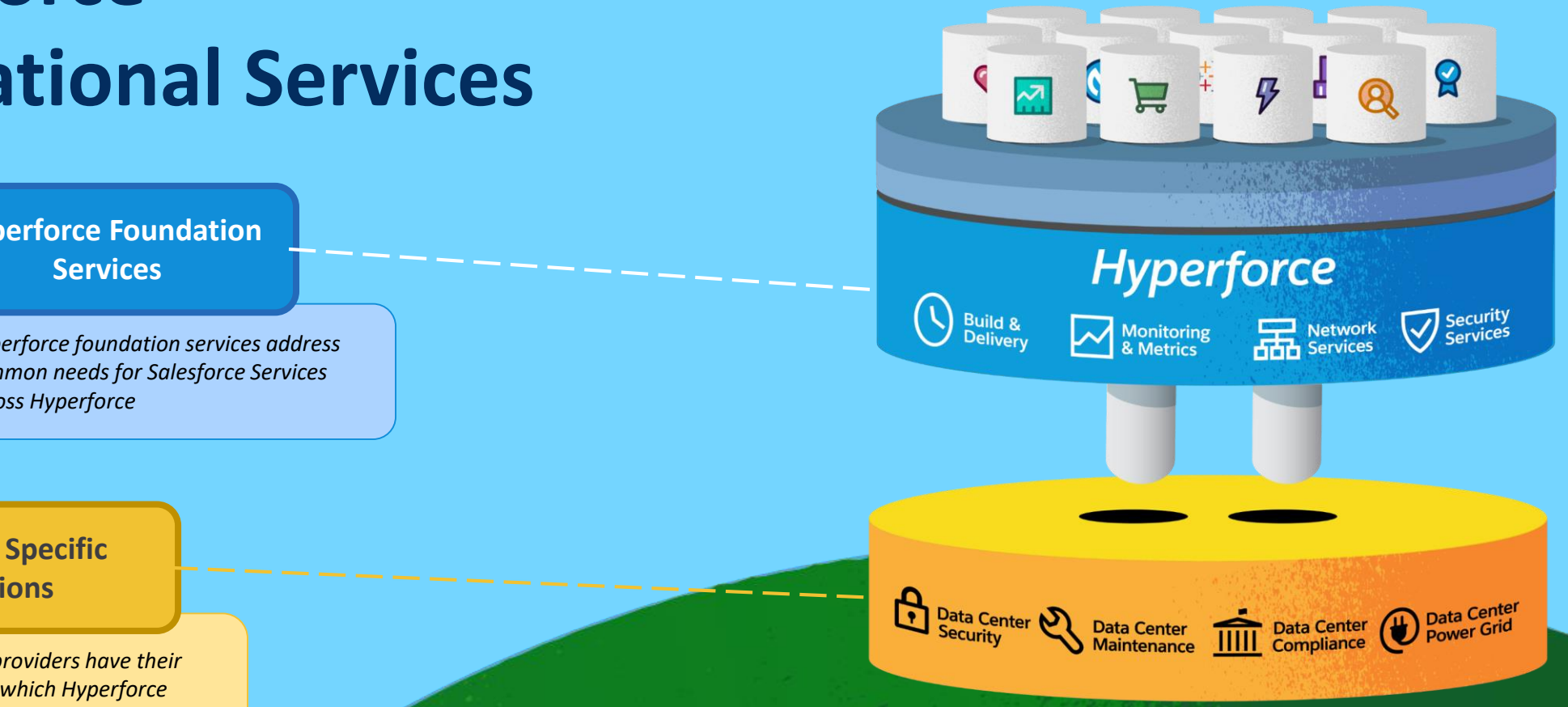
Hyperforce Foundational Services

Hyperforce Foundation Services

Hyperforce foundation services address common needs for Salesforce Services across Hyperforce

Substrate Specific Functions

Infrastructure providers have their own functions, which Hyperforce builds on top of



Hyperforce Needed A Compute Platform

Who better to ask than our own developers...

How are we building Hyperforce?

The majority of Salesforce Hyperforce services are built on top of Kubernetes

kubernetes

What are our future goals?

We wanted to provide a multi-substrate platform for Hyperforce to expand to in the future

aws

How are we managing Integrations?

Management of Salesforce integrations

Security

Monitoring

Connectivity

What were our Day 2 Requirements?

There were many…

Scale

Patching

Upgrades

Availability

Visibility

Cost-to-serve

etc.

Hyperforce Needed A Compute Platform

So what did we do?



Hyperforce Kubernetes Platform

We built an internal platform

and

Amazon EKS

We decided to use EKS for Kubernetes on AWS

Hyperforce Kubernetes Platform (HKP)

Our Mission

Service overview

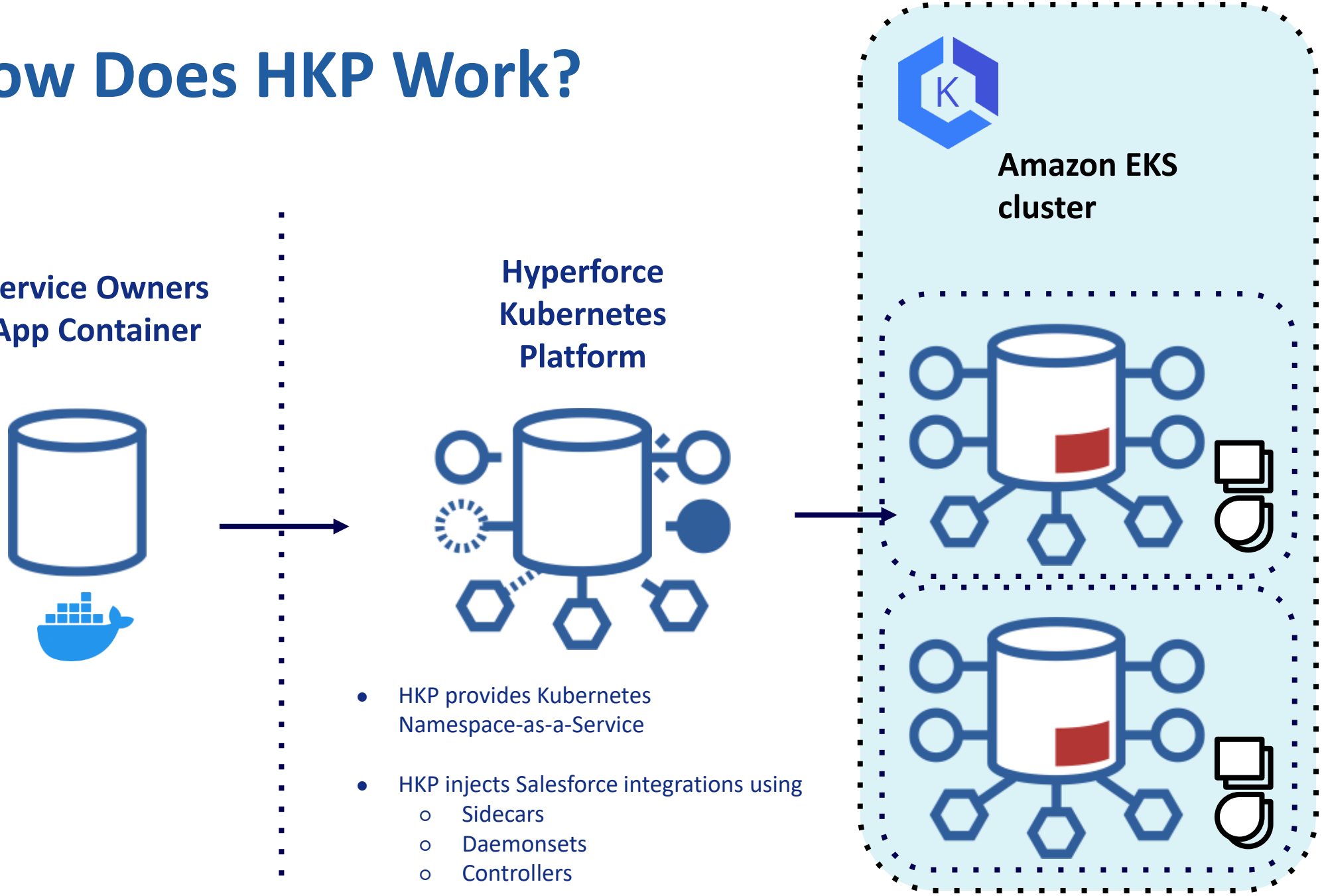
HKP provides multi-substrate managed Kubernetes with Salesforce integrations as a service on of top of cloud K8s engines for internal service teams

Mission

We empower service owners to focus on the unique value of their service, **without having to focus on infrastructure**, increasing developer agility while decreasing operational costs and complexity



How Does HKP Work?



- HKP provides Kubernetes Namespace-as-a-Service
- HKP injects Salesforce integrations using
  - Sidecars
  - Daemonsets
  - Controllers

Hyperforce Kubernetes Platform Value Proposition

Let teams focus on their service while we handle the infrastructure

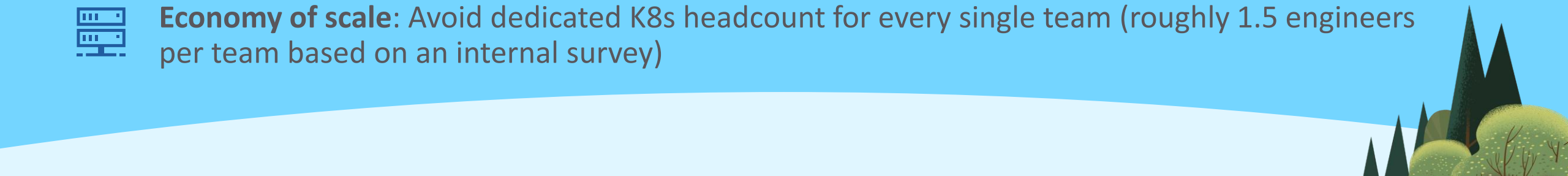
Higher agility: Faster time to market for Salesforce services to move to Hyperforce and reduce operational overhead

Salesforce integration lifecycle management: Release certification, rollout, and continuous synthetic monitoring of Salesforce integrations with Kubernetes

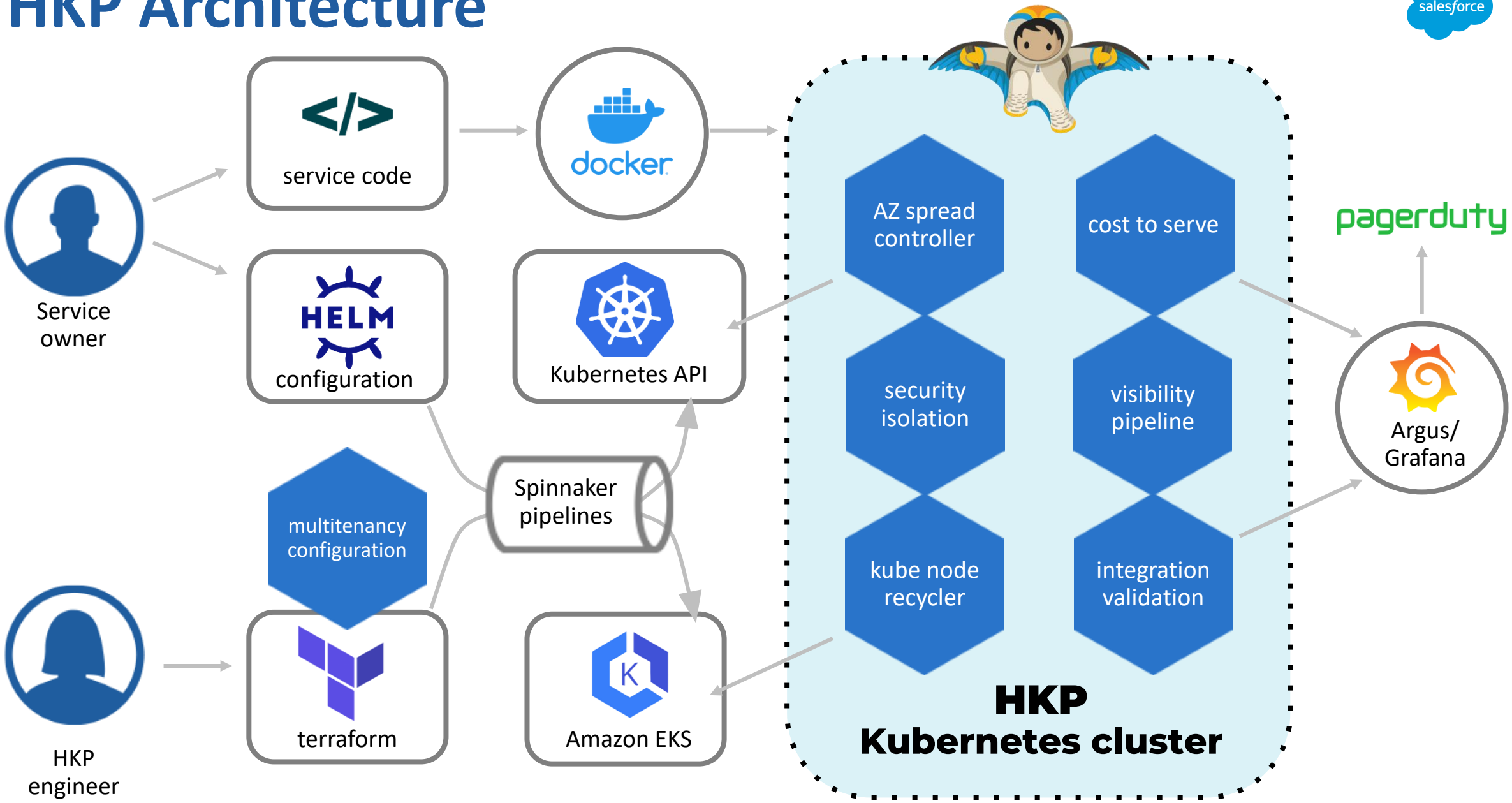
Trust: Maintain Security and Trust by running the most up-to-date, secure and patched version of Kubernetes and Salesforce integrations in Hyperforce

Cost optimization: Employ strategies to lower costs for the same availability across teams, e.g. faster auto scaling by sharing buffer capacity

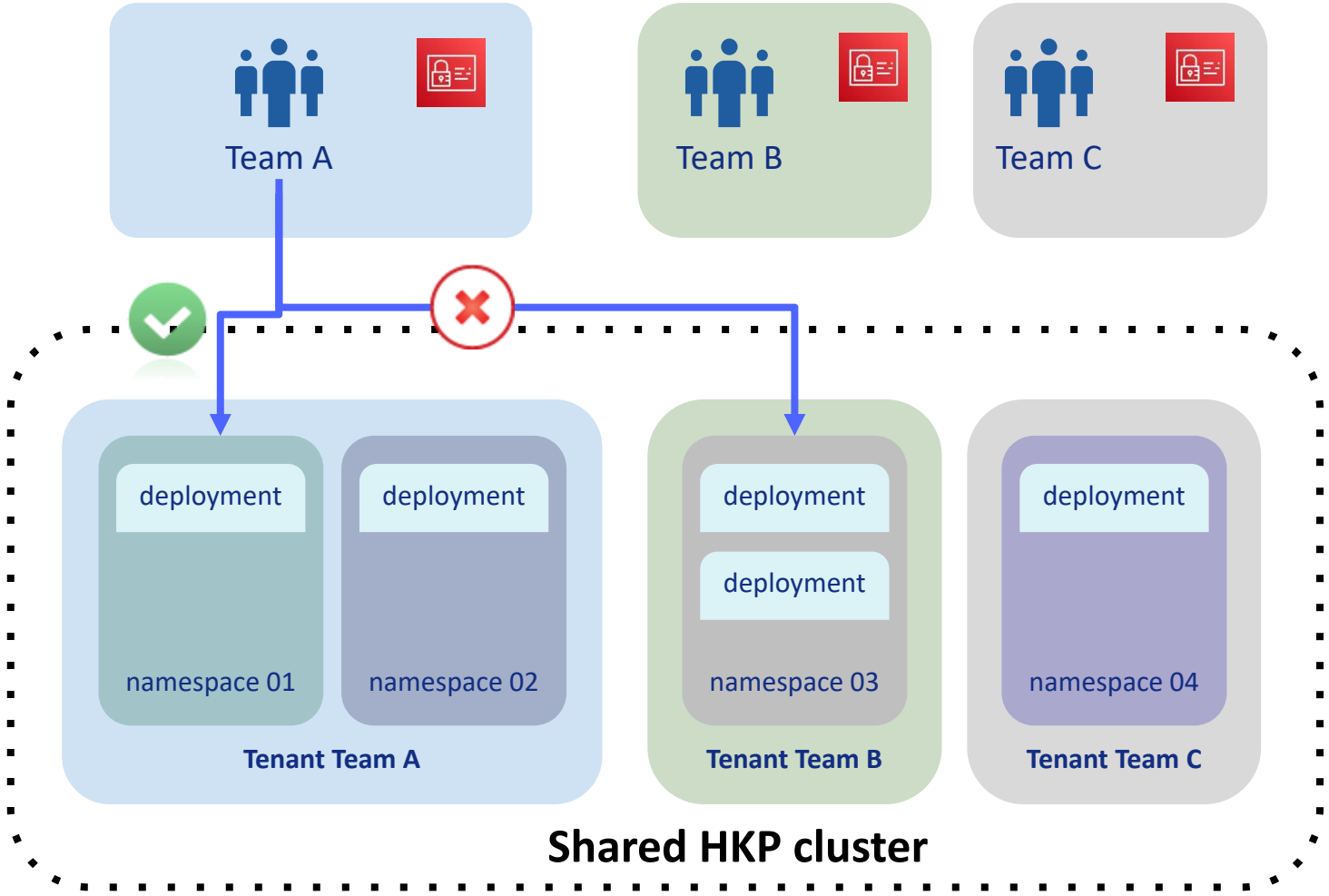
Economy of scale: Avoid dedicated K8s headcount for every single team (roughly 1.5 engineers per team based on an internal survey)



HKP Architecture

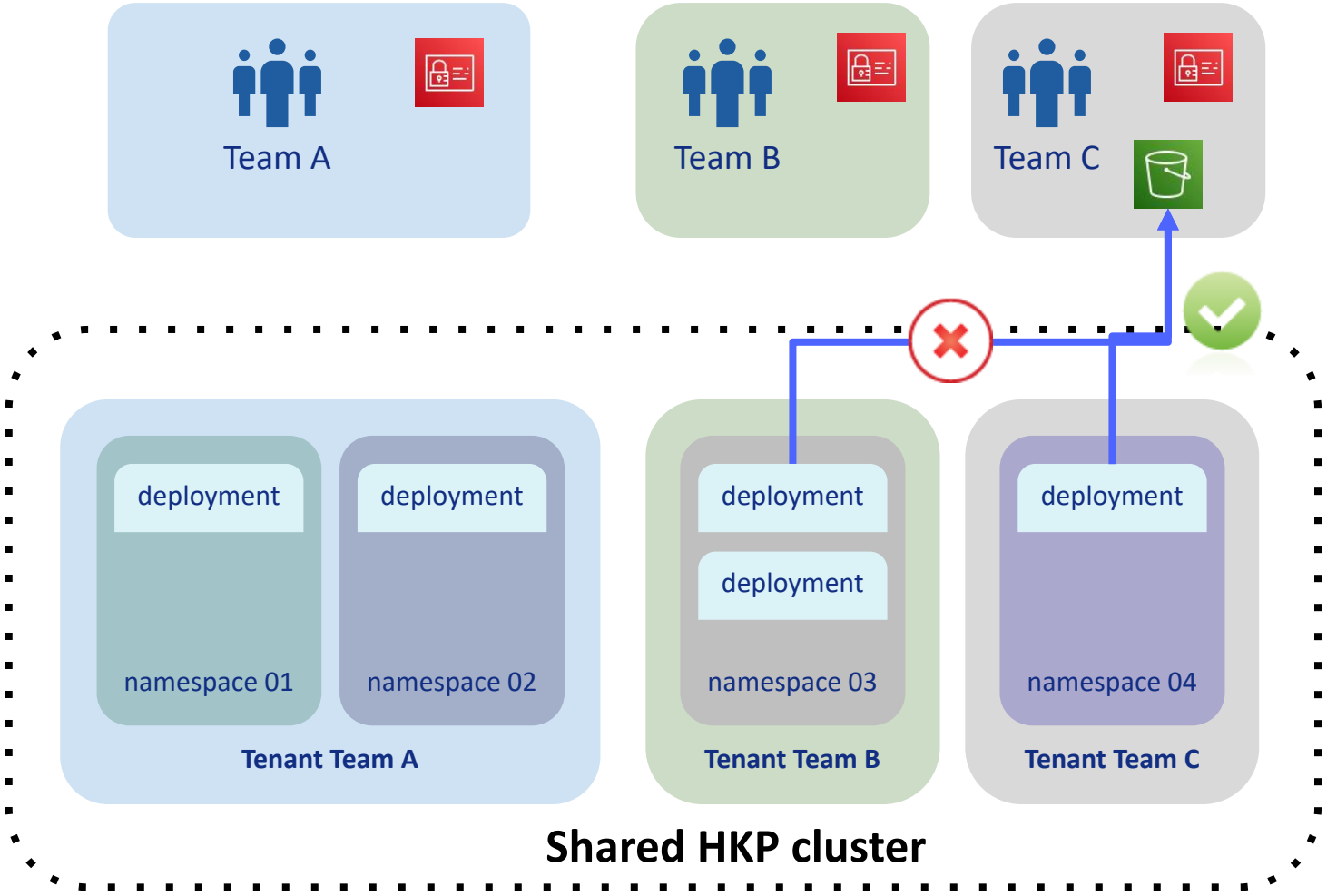


Multitenancy via K8s Namespaces



- Each tenant gets an AWS account
- *(User identity)* HKP uses K8s RBAC to limit access to the namespaces to tenant's AWS account
- Use Amazon EKS aws-auth ConfigMap for authorization

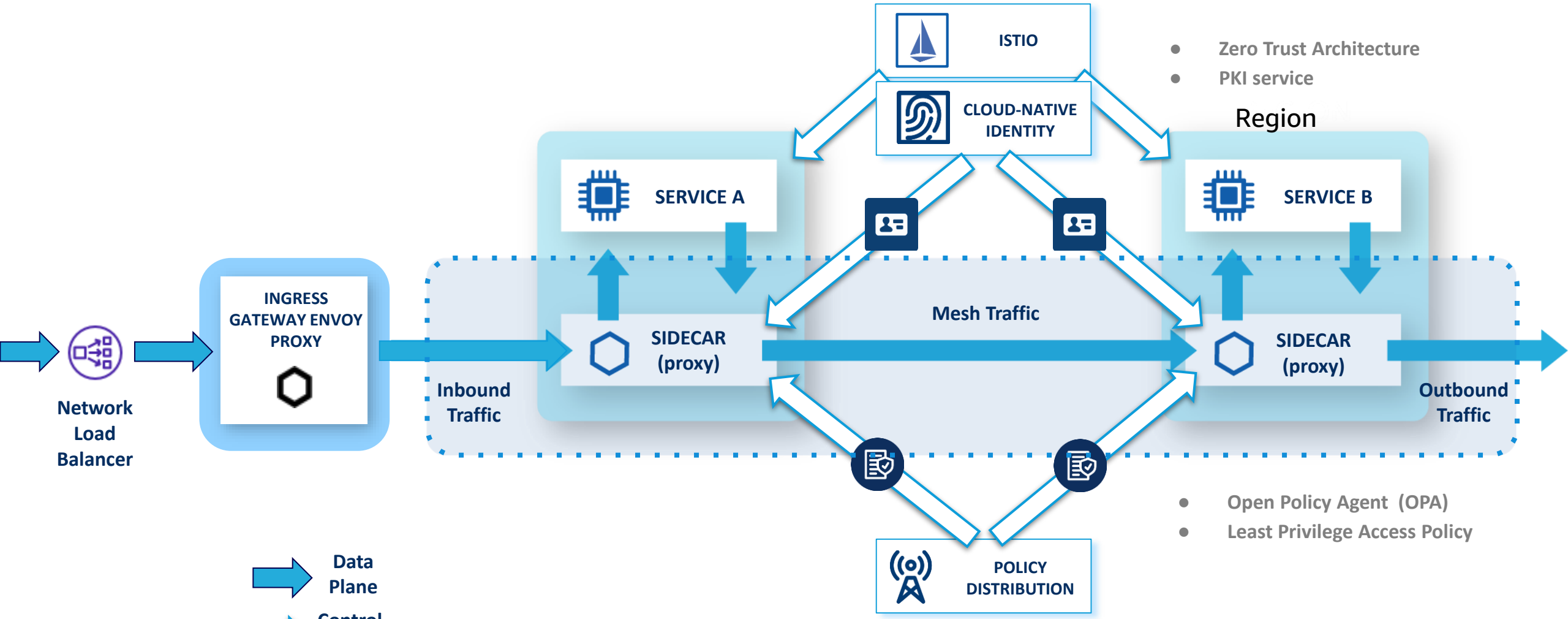
Using AWS EKS Features for Easy Access Control



- Each deployment gets associated with a role from the team's AWS account
- We rely on the Amazon EKS IAM role for the Kubernetes service account feature to make this happen
- Teams can now set up IAM permissions for resources in their account such as Amazon S3 or Amazon RDS

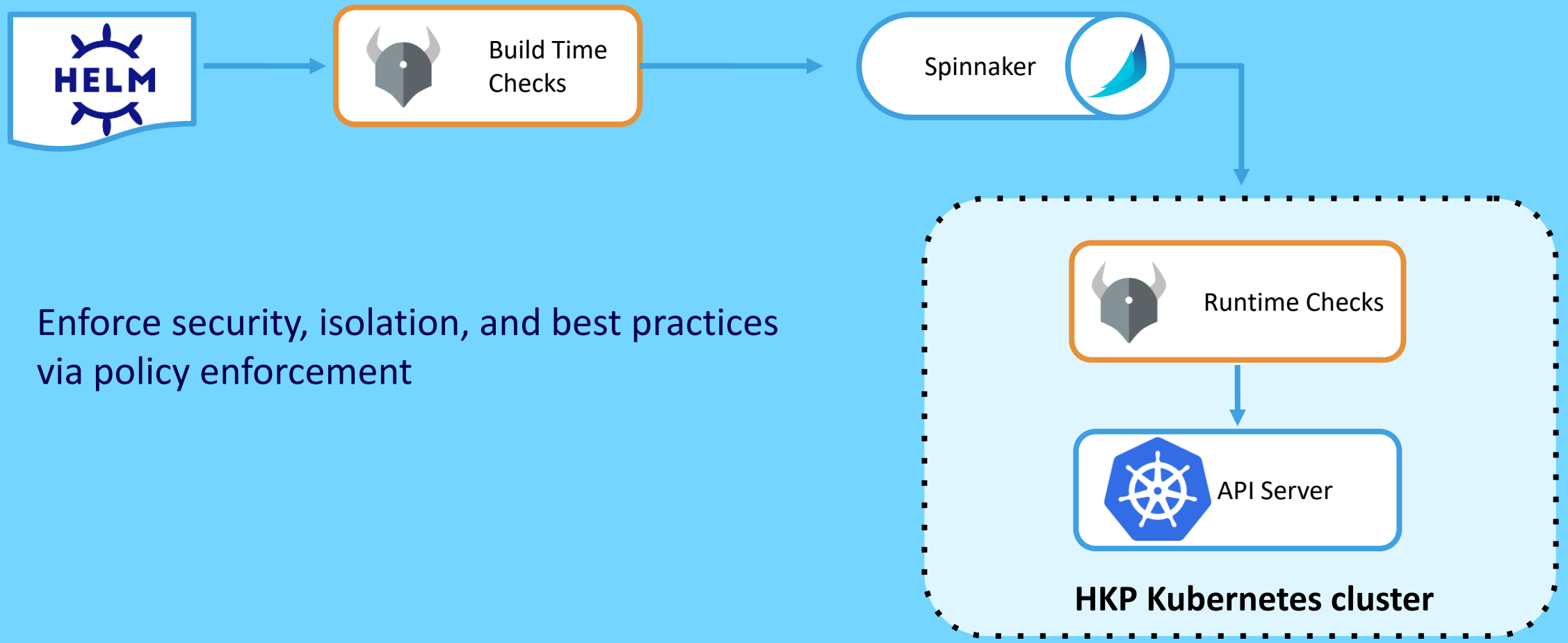
Service Mesh Using Istio and Envoy

Services authentication, authorization, and encryption at every step



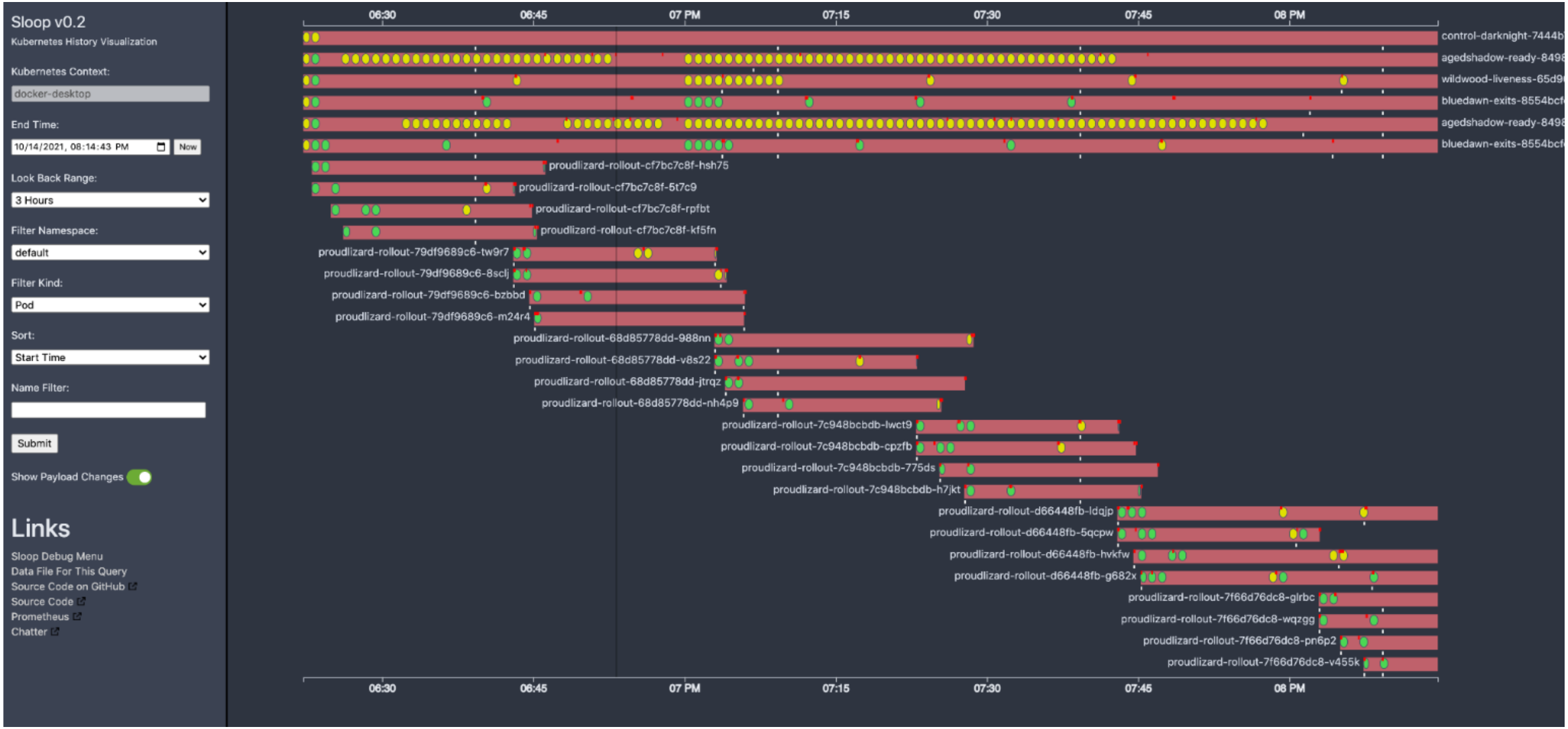
Policy Enforcement

Policy Enforcement at build and runtime using Open Policy Agent (OPA)



Enforce security, isolation, and best practices via policy enforcement

Sloop and Visibility Pipeline



Open Source Contributions, Talks and Blogs



Sloop (github.com/salesforce/sloop) - Sloop monitors Kubernetes, recording histories of events and resource state changes and providing visualizations to aid in debugging past events

Sidecar injection (github.com/salesforce/generic-sidecar-injector) - Generic framework for injecting sidecars and related configuration in Kubernetes using Mutating Webhook Admission Controllers

KubeCon ‘20 (https://sfdc.co/hkp20), KubeCon ‘19 (https://sfdc.co/hkp19), KubeCon ‘17 (https://sfdc.co/hkp17) - Various talks over the years at KubeCon

Grace Hopper 2020 - Sloop: The journey from hackathon idea to Open Source project

Blog link (https://sfdc.co/hkpblog) - External blog about our Hyperforce Kubernetes journey

Key Takeaways

Trust & Value

Building a central Kubernetes platform has helped Salesforce achieve agility, maintain trust and security, and make it easy for our teams to focus on their business value

Kubernetes native

The Hyperforce Kubernetes platform adds Salesforce integrations in a Kubernetes-native way on multi-tenant clusters that are fully managed by a central team

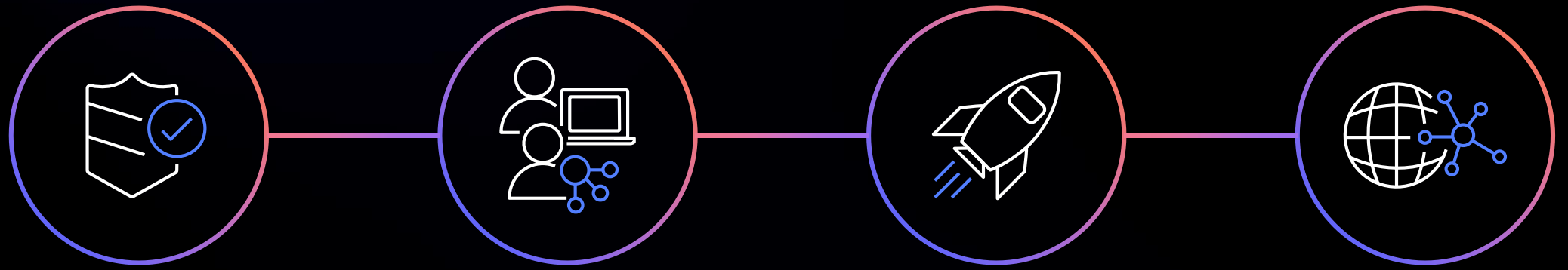
Leverage the Best

Amazon EKS on AWS is a great way to leverage the best of AWS and Kubernetes Open Source


THANK YOU

Amazon EKS road map and vision

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Security and reliability

Management and observability

Performance and scale

Consistency

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security



1

Supply chain

The software and services you consume are safe and the environment is protected from attack.

2

Compliance

Services meet the standards for your organization, industry sector, and government.

3

Supply chain

Services offer capabilities and options that allow you to ensure control over access, information processing, record keeping, and remediation.

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Reliability



1

SLA

Services have a guarantee for uptime and stability; ensure your architecture will enable redundancy to meet or exceed your desired SLA.

2

Scale

Ensure the compute, storage, and networking capacity is available when you need it; systems perform within tolerances at scale and under load.

3

Change management

All changes are tested and made predictably; the state of the system is declared externally and can be easily reverted.

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Security and reliability

- Managed node group taints
- Parallel managed node group upgrades
- Bottlerocket in Managed Node Groups
- Amazon Guard Duty for K8s Audit Logs

- IAM Cluster Access Management API
- EKS API PrivateLink
- ECR Signed Image Validation
- Additional compliance - DoD CC SRG
- IAM Roles for Service Accounts v2
- VPC CNI Network Policy
- Faster cluster creation and upgrades

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Management and observability



1

Automated lifecycle operations

All lifecycle operations for system components can be automated. Once triggered, operations proceed without user intervention.

2

Core tooling

The common tools and services your applications need ship with the system. Installation and management of standard core tooling is minimal.

3

Enforce best practices

Tooling makes it easy to standardize and enforce best practices that augment, and do not disrupt workflows.

4

Actionable insights

Easily ingest and gain deep understanding from multiple data sources to improve performance, reduce cost, and minimize time to resolve issues.

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Management and observability

- EKS Connector
- EKS add-ons - CoreDNS and kube-proxy

- Global cluster console view
- Cluster Performance Insights
- VPC CNI Flow Logs integration
- Cluster Cost Allocation
- Integrated GitOps with Flux
- Optional single click cluster upgrades
- EKS Add-Ons Expansion
  - Open Telemetry
  - CSI Drivers
  - Load Balancer Controller
  - Metrics Server

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Performance and scale



1

Scale

The system can be scaled up or down dynamically to minimize waste. This includes scale to zero or pause when resources are not needed. Kubernetes control plane will respond to any workload demands.

2

Density

You can maximize the utilization of compute resources within a scalable unit. Example: pods within a node and nodes within a cluster.

3

Flexibility

You can trade availability for cost (example: Spot) or adjust compute resources to achieve higher utilization (example: moving to larger instance sizes).

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



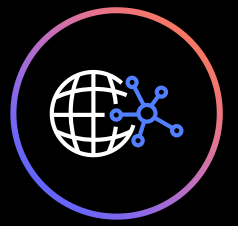
Performance and scale

- VPC CNI increased pod density
- MNG scale to zero phase 1
- Karpenter
- Control Plane Scaling enhancements

- IPv6
- 15k node clusters
- MNG scale to zero phase 2

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Consistency



1

Supported

You get the same consistent, supported Kubernetes experience across all of your environments.

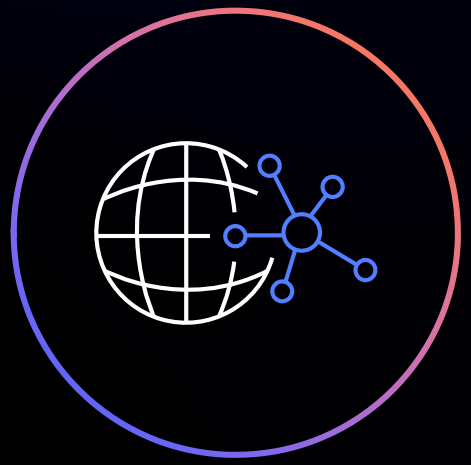
2

Portability

You can run in the environments you require without significant changes to your applications and configuration.

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Consistency

- EKS Anywhere
- ACK controllers preview
- ACK for SageMaker GA
- CDK for Kubernetes (CDK8s) 1.0

- EKS Anywhere bare metal, GPU
- AWS Controllers for Kubernetes
- Multi-cluster service discovery
- EMR on EKS additional frameworks

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

EKS public roadmap

- Stay up to date with what we're working on
- Give us feedback and propose ideas
- Get notified when new features ship

https://tinyurl.com/3bp4tnzn



aws

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.