AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

CON205

What's new and what's next with Amazon EKS

Nathan Taber
Sr. Manager - Product and Advocacy

Mike Stefaniak
Principal Product Manager

Amazon EKS is now used by a wide range of industries worldwide

RIOT GAMES

nanit

babylon

Southwest

PELOTON

HSBC

verizon

Expedia

EPIC GAMES

Citi

arlo

amazon

Aurora

Fidelity

GoDaddy

MassMutual

Goals

Standardize IT operations in order to accelerate delivery and changes
rapid change == innovation

Reduce fixed expense
eliminate complex contracts and management overhead

Enable the entire organization
support multiple environments and different use cases

Plan for the future and reduce risk
standards enable hiring and long-term development efforts

Our mission

Security first

Open standards

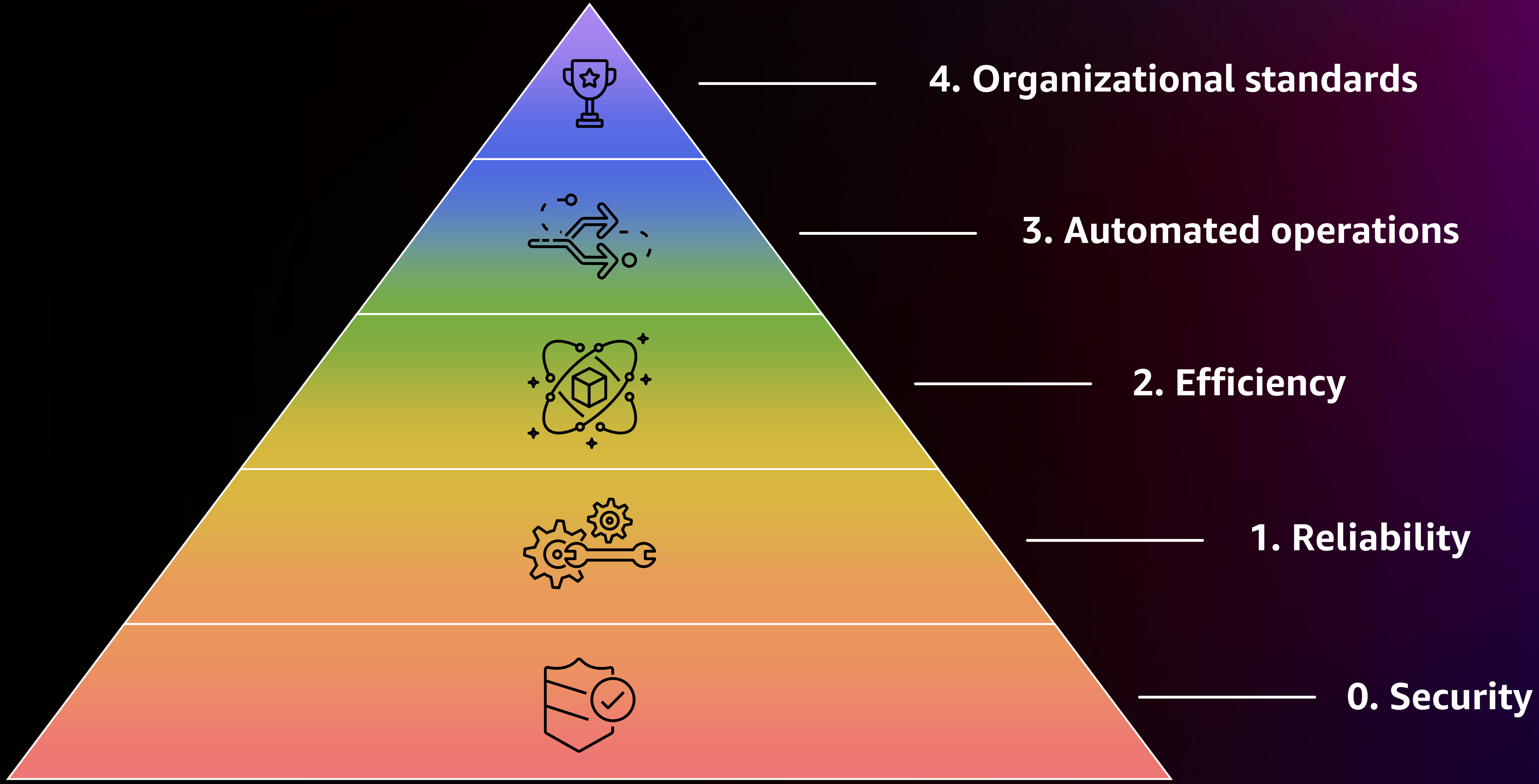
Built-in best practices

Seamless integrations

Always Supported

Application-ready, production Kubernetes in the cloud and the data center

Hierarchy of Kubernetes priorities



4. Organizational standards

3. Automated operations

2. Efficiency

1. Reliability

0. Security

Security requirements

Supply chain

The software and systems you use are safe and the environment is protected from attack.

Compliance

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

Controls

Systems include options that allow you to ensure control over access, information processing, record keeping, and remediation.

Kubernetes version support

Supported

1.24 Launched on November 15th 2022 – this version removed Dockershim, changes included improvements to Kubelet certificate issuance security.

1.23 Launched on August 11th 2022, this version enabled EBS CSI Migration and ephemeral containers.

1.22 Launched on April 4th 2022, end of support scheduled June 2023.

1.21 Launched on July 20th 2021, end of support scheduled February 2023.

End of support

1.20 End of support on November 1st 2022.

1.19 End of support on August 1st 2022.

1.18 End of support on March 31st 2022.

1.17 End of support on November 2nd 2021.

New in 2022

Security improvements

Log4j incident response

Built and released Log4j CVE node agent daemonset to perform JVM hot patch in running containers.

Bottlerocket Hotdog – set of OCI hooks that inject the Log4j hot patch into containers on Bottlerocket hosts.

Amazon GuardDuty audit log support

Analyze, investigate, and identify the root cause of security findings or suspicious control plane activity on EKS clusters.

Roadmap: GuardDuty runtime protection

Expanded support to include running containers in EKS clusters.

Coming Soon

AWS PrivateLink support

Private access to EKS APIs

Manage the lifecycle of EKS clusters from a Virtual Private Cloud (VPC) without exposing traffic to the public internet.

Advanced access configuration

Attach VPC endpoint and IAM policies to interface endpoints to control who can call the EKS APIs.

Simplified Security Model

No internet gateway, NAT device, or public IP address needed to connect to the EKS API from a VPC.

IAM cluster access management

Coming Soon

Simplified access management

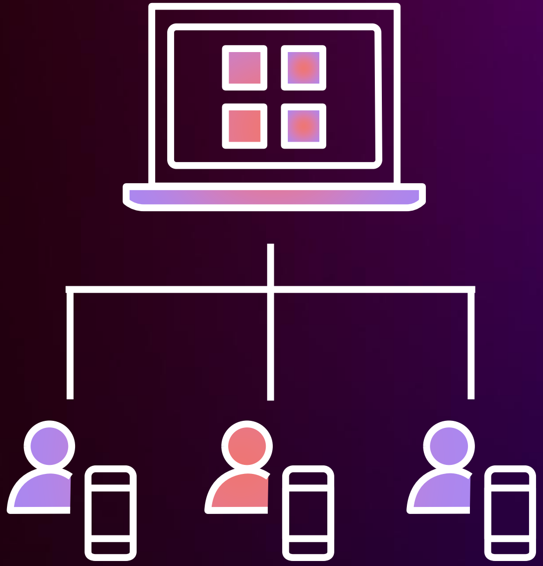
Manage authentication and authorization of IAM identities to Kubernetes via EKS APIs.

Leverage upstream user-facing roles

Easily configure common Kubernetes access permission sets like cluster admin or viewer directly through the EKS.

Leverage specialized AWS services with EKS

Use access management to simplify workflow of granting access to AWS services like EMR and AWS Batch.



Coming Soon

VPC CNI network policy support

Security out of the box

Secure intra-cluster network traffic without need to install 3rd party plugins.

Compatibility

Network policy support that is compatible with existing VPC CNI features such as pod security groups.

Performant

eBPF-based network policy rules ensure performance in even the largest clusters.

Working on it

Simplified IAM Roles for Service Accounts (IRSA)

Leverage roles across any number of clusters

Create roles that can be easily used across any number of EKS clusters. Trust policies are no longer scoped to a specific clusters.

Centralized IAM roles mapping

Apply IRSA role to service account mapping via an EKS API. No need to annotate YAML files.

Session tag support

Minimize number of roles and policies required to implement fine-grained permissions.

Reliability requirements

SLA/SLOs

The system has a guarantee for uptime and stability. Ensure your architecture will enable redundancy to meet or exceed your desired SLA.

Scale

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

Change management

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

New in 2022

Cluster updates and creates

Faster updates

Average time to update a cluster reduced from 40 minutes to < 10 minutes.

Support for all types of updates including version upgrades and OIDC provider associations.

Roadmap: Upgrade with more confidence

Generate a report from EKS on the readiness of your cluster to upgrade to the next version. Get notified and resolve incompatibilities ahead of time.

Roadmap: Faster cluster creates

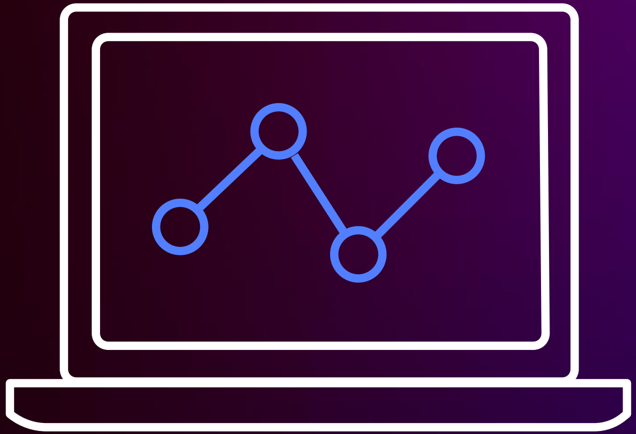
Create and use clusters in < 5 mins.

New in 2022

Kubernetes control plane scaling

New in 2022
Clusters react to load changes faster to maintain high performance at all cluster sizes.

Roadmap: Enhanced vertical cluster autoscaling
Scale clusters beyond the upstream limits of 5,000 nodes.



New in 2022

EKS support for IPv6

Scale and performance

Scale far beyond IPv4 limits with globally unique IPv6 address per pod. Faster pod launch times with pre-allocated IP addresses.

Simplified networking setup

Pod to internet connectivity without network address translation.

Designed for easy transition

Egress IPv4 traffic support gives you best of both worlds. Move to IPv6 on EKS before the rest of your org supports it.

New at re:Invent!

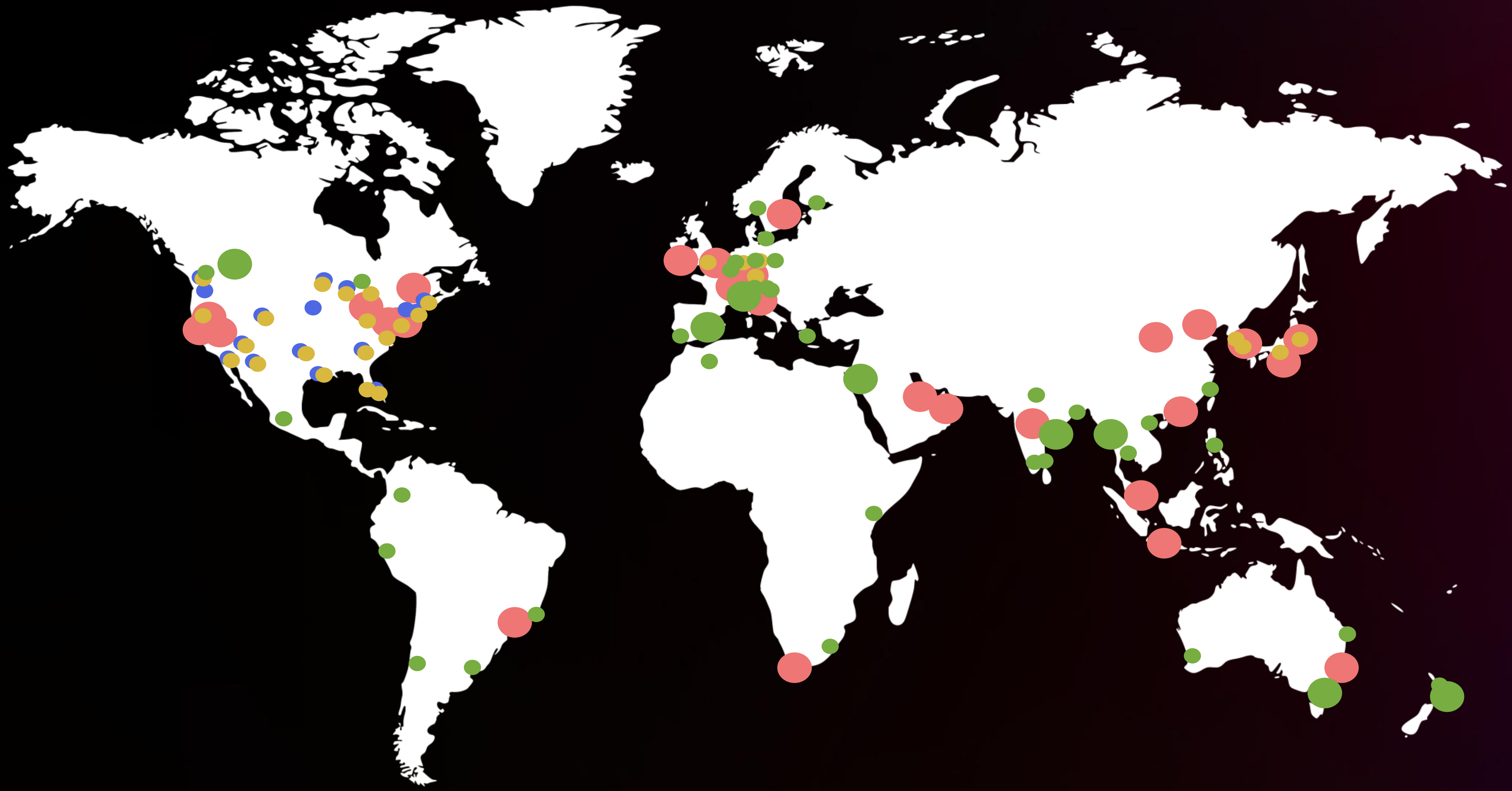
Support for Amazon VPC Lattice

Fully managed application networking with VPC Lattice
Lattice provides layer 7 application networking capabilities directly in the VPC – no need for sidecars.

Kubernetes native
Configure Lattice using the upstream standard Kubernetes Gateway API.

Cross cluster/VPC/account communication
Lattice automatically routes traffic across network isolation boundaries. No requirement to use VPC Peering, Transit Gateway, etc.

Amazon global reach



30 geographic regions

96 Availability Zones

21 Local Zones

29 Wavelength Zones

Coming soon

5 new geographic regions

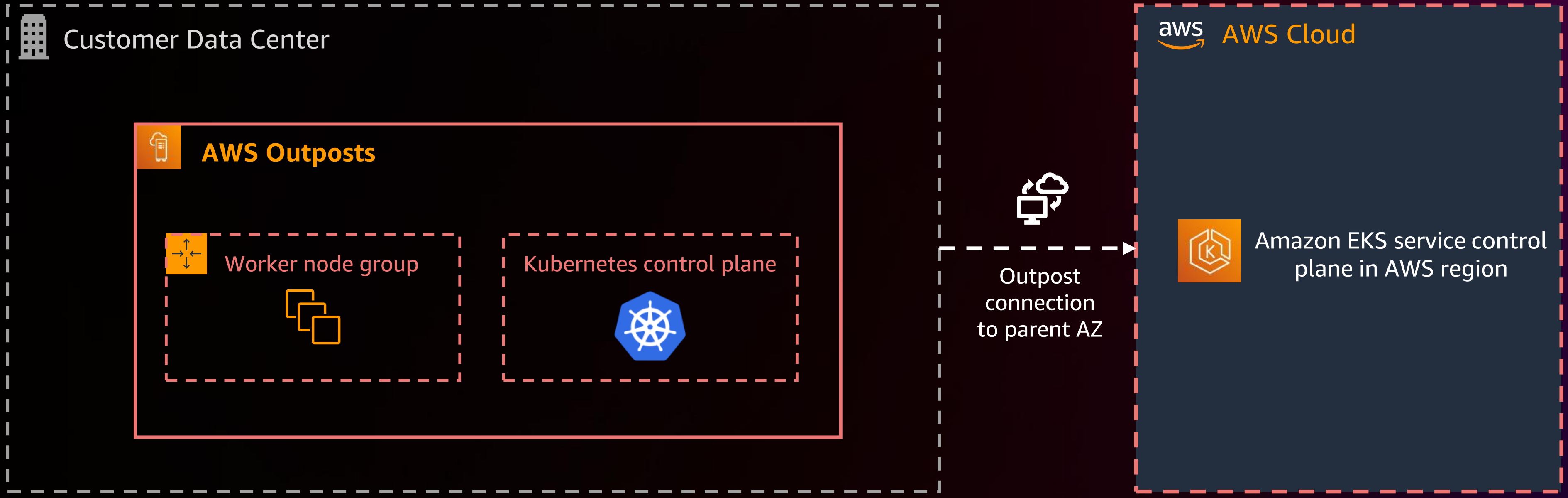
15 new Availability Zones

30 new Local Zones

New in 2022

Local cluster on Outposts

New deployment option for Amazon EKS on AWS Outposts that enables customers to maintain availability of their Kubernetes applications during network disconnects to the cloud



Amazon EKS Anywhere infrastructure options

DEPLOY IN ANY ENVIRONMENT

Amazon EKS Anywhere

Cluster API providers

- VMware — GA
- bare metal — New in 2022
- Apache CloudStack — New in 2022
- AWS Snowball Edge — Coming Soon
- Nutanix — Coming Soon

OS

- Ubuntu
- Bottlerocket
- RHEL

Efficiency Requirements

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.

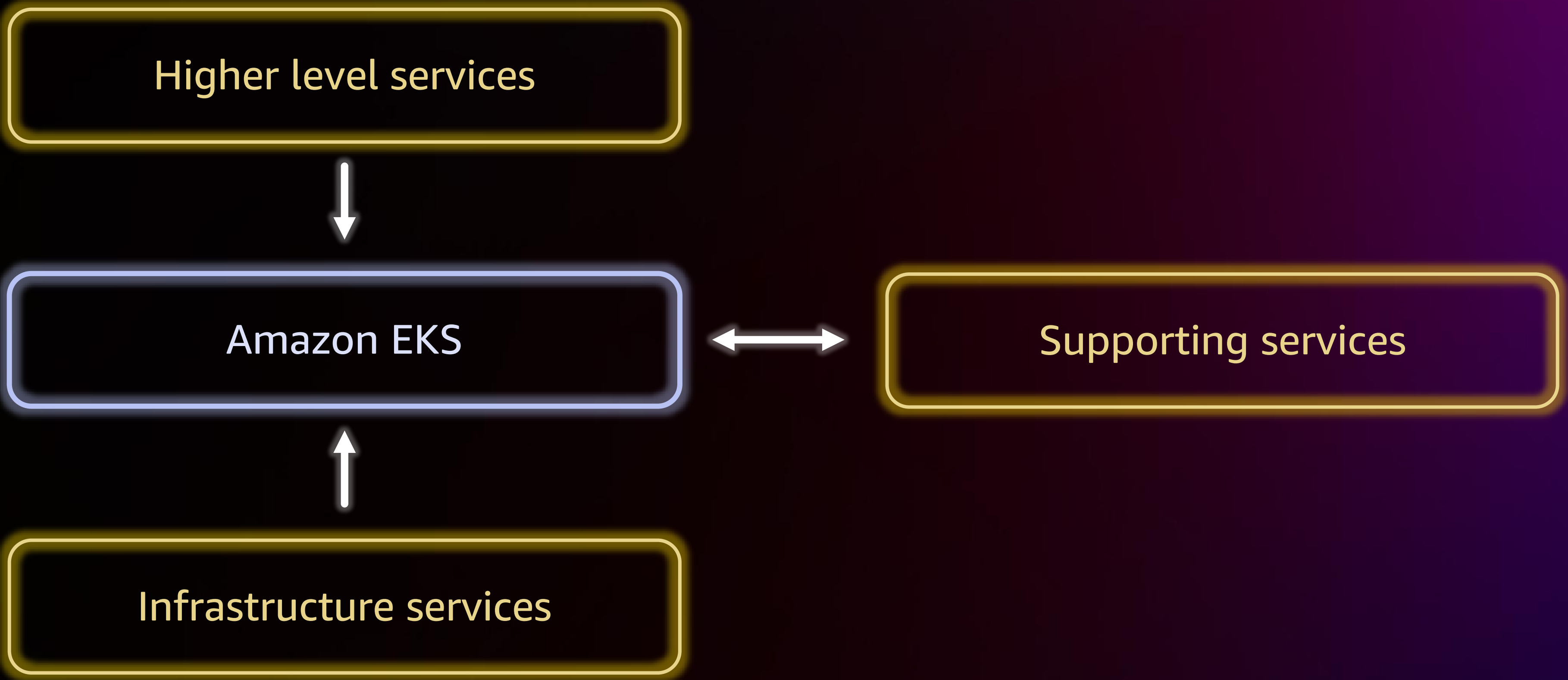
Density

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

Flexibility

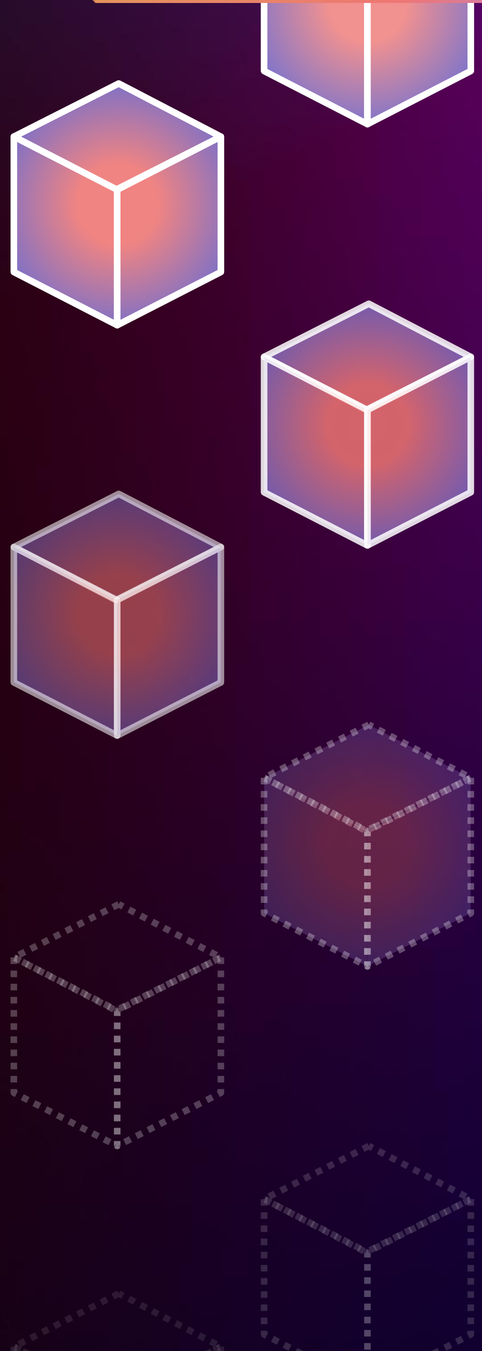
You can trade availability for cost (example: spot) or adjust compute resources to achieve higher utilization (example: moving to larger instance sizes).

Kubernetes access to AWS services



New in 2022

Managed node groups scale to zero



Optimize compute costs

Scale non mission critical managed node groups to zero during downtime to save costs.

Simplified setup

Cluster Autoscaler now calls EKS node group APIs directly to discover metadata needed to scale back up from zero.

Working on it

EKS managed nodes roadmap

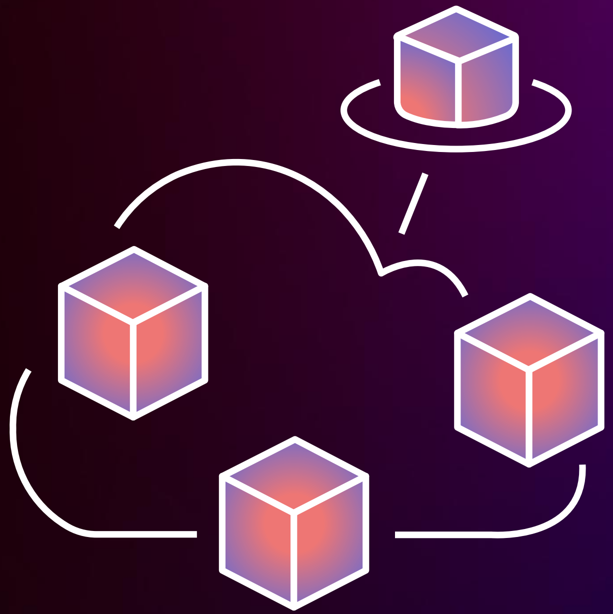
Upgrade enhancements
Automatic AMI upgrades, configurable timeouts, improved notifications/logging, pre-flight checks, and upgrade windows.

Amazon Linux 2022-based EKS optimized AMI
Next-generation Linux OS from AWS with improved security and stability

Node health monitoring and auto-repair
Surface EC2 instance health issues and, when possible, automatically remediate

Warm pool integration
Decrease scale-out latency for workloads with exceptionally long boot times

Managed nodes on Outposts & Local Zones
Unify EKS architecture and operations for managed on-premises clusters



Generally Available in 2022

Karpenter

Right node in the right place

Karpenter selects the most optimal nodes for your cluster based on pod requirements, availability, and your custom preferences.

Improve efficiency

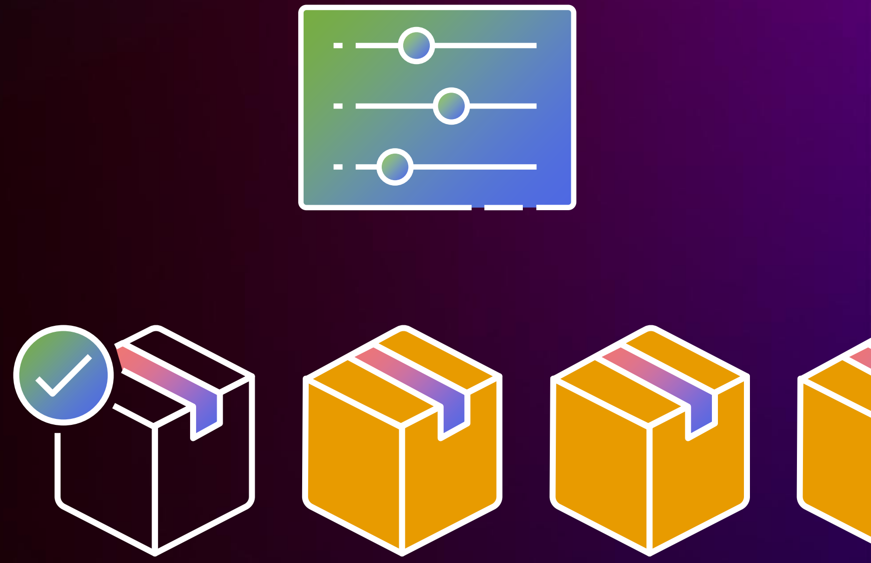
Karpenter adds and removes nodes in as little as 15 seconds, reducing costly overprovisioning and preventing slow, expensive scale-downs.

Built for scale

Scaling decisions are made in seconds when demand changes, even in the largest Kubernetes clusters.

Ready for production

Karpenter is fully supported by AWS and regularly used in production.



Learn more at:
github.com/aws/karpenter

Generally Available in 2022

Karpenter

Recent Launches

- Workload consolidation
- Support for custom user data and AMIs
- EBS volume and kubelet configuration
- AZ-aware scheduling for stateful workloads
- Node termination handling, e.g. Spot
- IPv6 support
- Weighted provisioners

Learn more at:
github.com/aws/karpenter

Working on it

Karpenter what’s next

Instance type settings overrides

Specify per instance type overrides such as reserved CPU/memory thresholds.

Enhanced node upgrade control

More control over when and how many nodes are upgraded. Reconciliation when a node's AMI drifts from provisioning requirements.

Managed Karpenter

Provision right sized compute out of the box on EKS.

New in 2022

Fargate profile wildcard namespaces

Launch on Fargate by default

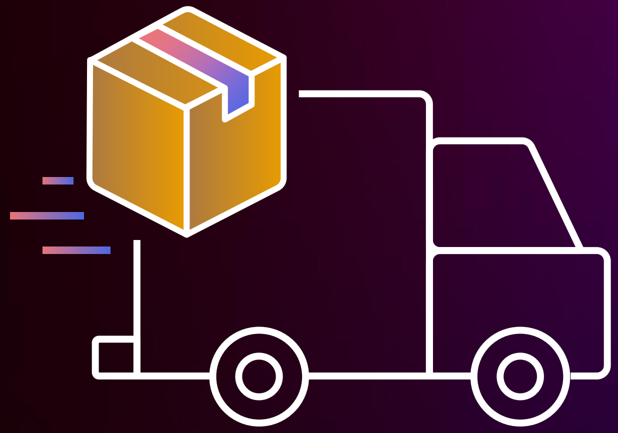
Create fewer profiles to serve the entire cluster.

New namespaces can be automatically used to run pods on Fargate.

Use * and ? wildcard characters

Specify a range of namespaces for pods to run on Fargate.

No need to hardcode profile names for all namespaces.



New in 2022

EC2 Cost & Usage system tag propagation

Use tags to get visibility into Kubernetes usage on AWS

EKS automatically propagates AWS Cost and Usage Reports (CUR) tags to accurately track usage and total EC2 cost associated with EKS clusters.

No more custom tagging

Tagging 100s of Kubernetes resources can be cumbersome and error prone.

Automate compliance checks and improve reporting

Automate security and compliance checks.
Get better understanding of overall cost of running Kubernetes on AWS.

New in 2022

Kubecost support

Gain deep insight into EKS cost

Sort costs by Kubernetes concepts like namespace and pod.

Select enterprise features at no additional charge

Single-cluster cost visibility, 15-day metric retention and an optional AWS Cost and Usage integration.

Easy installation via Helm and now EKS add-ons

Install Kubecost with a single Helm install command. Container images and Helm chart are pulled from Amazon ECR public. Additionally, now install through EKS add-ons.

Requirements for automated operations

Lifecycle operations

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

Core tooling

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

Best practices

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

Actionable insights

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

It takes a lot of work to make a cluster production ready

Monitoring

Networking

Security

Observability

Storage

Cost management

EKS add-ons

Lifecycle management

Start, update, and remove core add-ons for EKS clusters through the EKS APIs. Metadata API includes compatibility for all K8s and add-on versions.

Control at startup

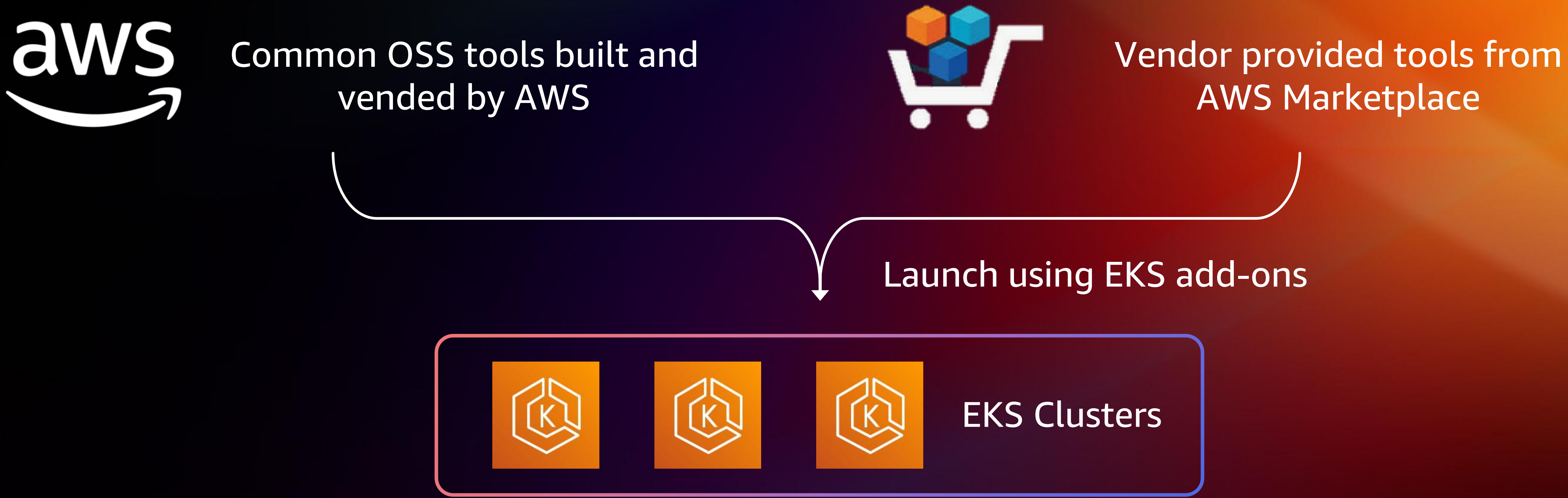
Customize or remove an add-on completely when the cluster starts, no more waiting.

Ready-to-go clusters

Start a cluster that's ready to run your applications without any additional steps.

New at re:Invent!

Now launch Marketplace Software with EKS add-ons



Common OSS tools built and vended by AWS

Vendor provided tools from AWS Marketplace

Launch using EKS add-ons

EKS Clusters

New at re:Invent!

Expanded add-ons catalog powered by AWS Marketplace

Launch partners

- kubecost
- Teleport
- factor house
engineering insights
- Tetrate Istio Subscription
- dynatrace
- upbound

Coming soon

- portworx
- Lightrun
- Shoreline
- AEROSPIKE
- NeuVector
Full Lifecycle Container Security
- Kong
- paloalto NETWORKS
- TRILIO
- nOps
- PARALUS
- sysdig
- LACEWORK
- kasten by Veeam
- DataStax
- new relic.
- RAFAY
- DATADOG
- StormForge
- datree
- nirmata
- HAPROXY

Coming Soon

EKS add-ons configuration

Lifecycle management

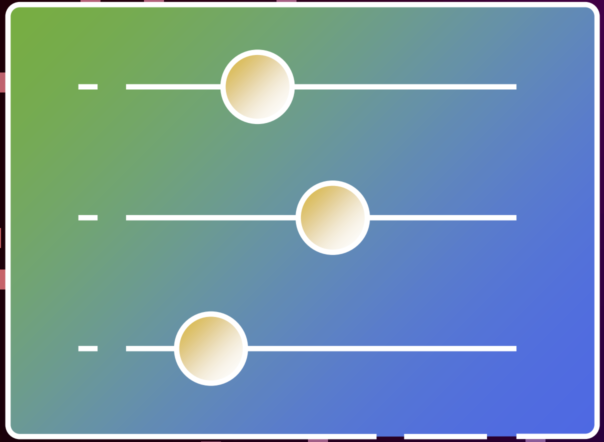
Start, update, configure, and remove add-ons for EKS clusters through the EKS APIs. Metadata API includes compatibility for all K8s and add-on versions.

Control without workarounds

Customize an add-on when its created without secondary configuration.

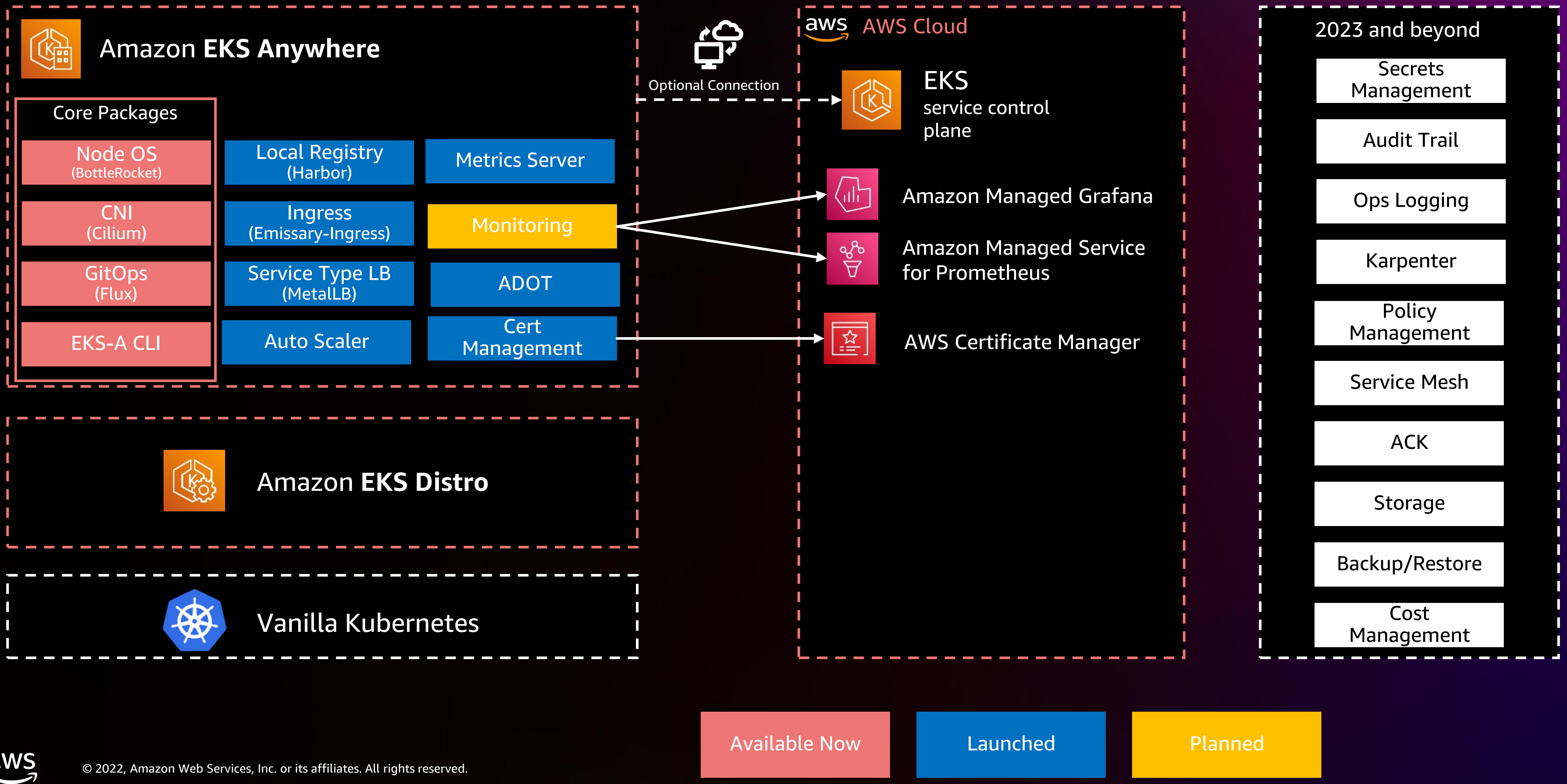
Modify configuration any time

Modify the configuration of an add-on during or post add-on deployment.



New in 2022

EKS Anywhere Curated Packages



Amazon **EKS Anywhere**

Core Packages

- Node OS (BottleRocket)
- CNI (Cilium)
- GitOps (Flux)
- EKS-A CLI

Local Registry (Harbor)

Ingress (Emissary-Ingress)

Service Type LB (MetalLB)

Auto Scaler

Metrics Server

Monitoring

ADOT

Cert Management

Optional Connection

Amazon **EKS Distro**

Vanilla Kubernetes

aws AWS Cloud

EKS service control plane

Amazon Managed Grafana

Amazon Managed Service for Prometheus

AWS Certificate Manager

2023 and beyond

- Secrets Management
- Audit Trail
- Ops Logging
- Karpenter
- Policy Management
- Service Mesh
- ACK
- Storage
- Backup/Restore
- Cost Management

Available Now

Launched

Planned

New in 2022

EKS console updates

See everything

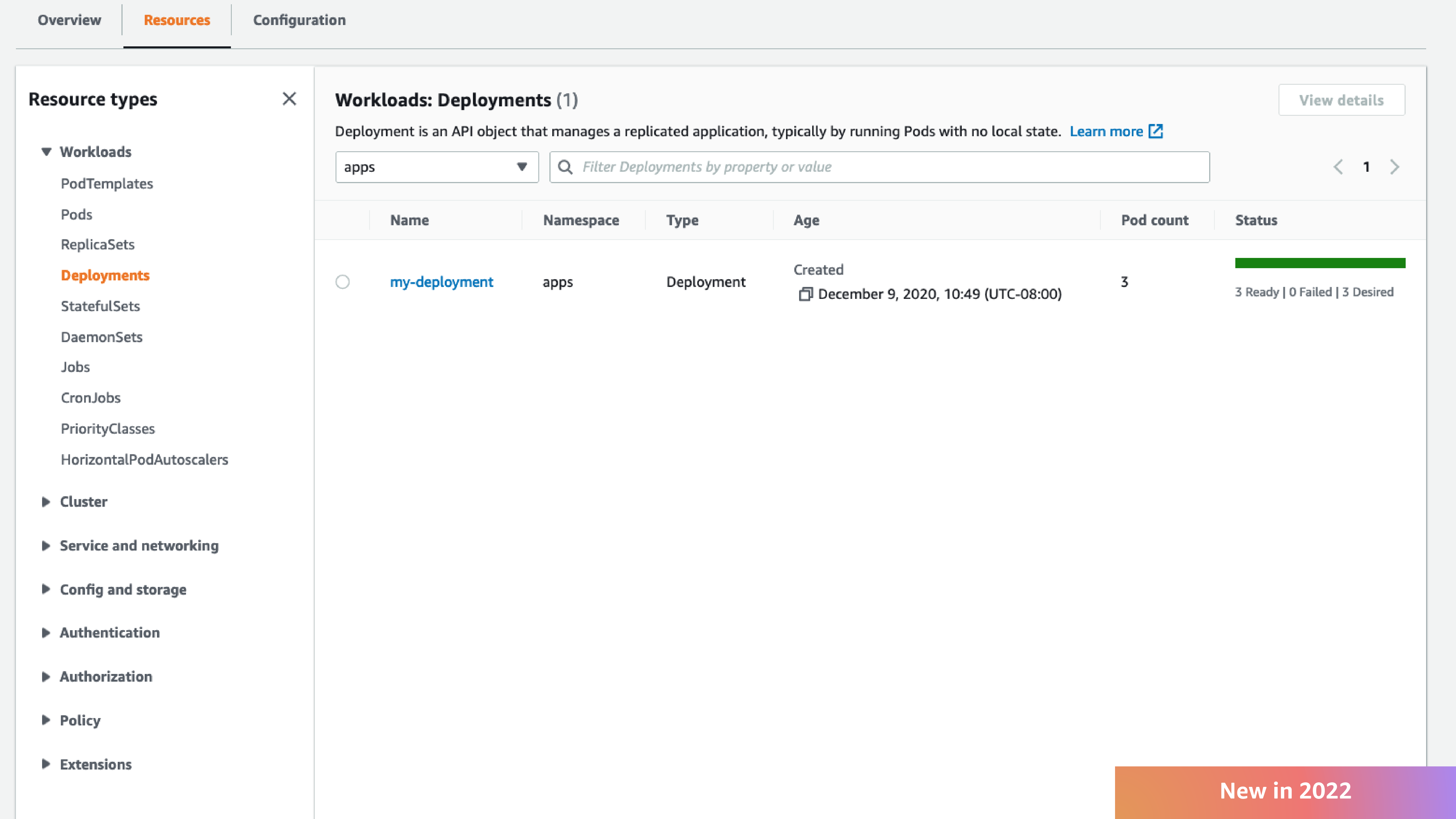
Navigate every object in the cluster including complete configuration data and deep-linked AWS resources

Integrated metrics

Quickly see the status of your applications.

Connect everywhere

EKS connector lets you visualize any cluster from anywhere in the EKS console.



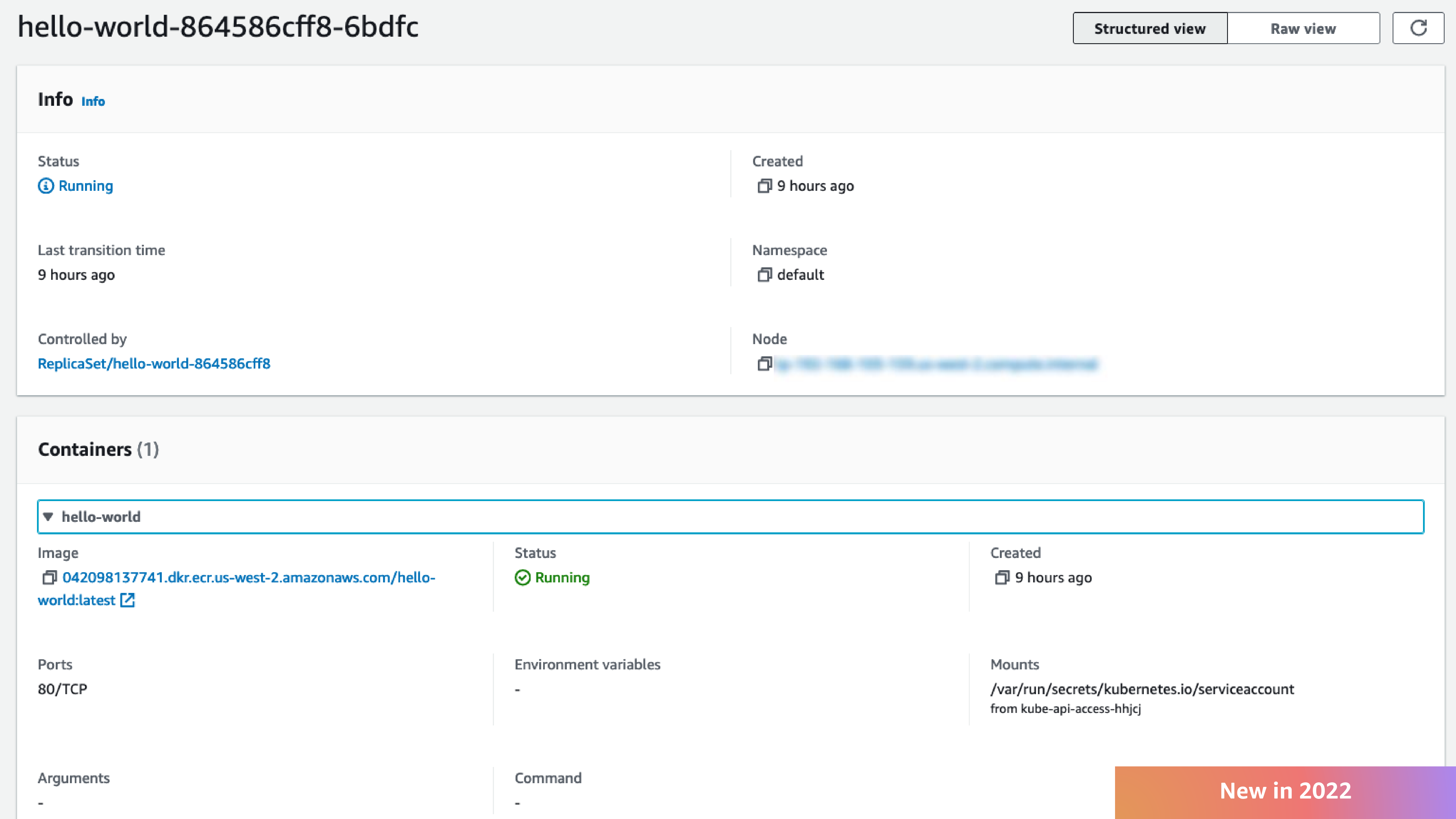
Workloads: Deployments (1)

Deployment is an API object that manages a replicated application, typically by running Pods with no local state. Learn more

Namespace: apps

	Name	Namespace	Type	Age	Pod count	Status
○	my-deployment	apps	Deployment	Created December 9, 2020, 10:49 (UTC-08:00)	3	🟩 3 Ready | 0 Failed | 3 Desired

New in 2022



hello-world-864586cff8-6bdfc

Info Info

Status
Running

Created
9 hours ago

Last transition time
9 hours ago

Namespace
default

Controlled by
ReplicaSet/hello-world-864586cff8

Node
[redacted]

Containers (1)

▼ hello-world

Image
042098137741.dkr.ecr.us-west-2.amazonaws.com/hello-world:latest

Status
Running

Created
9 hours ago

Ports
80/TCP

Environment variables
-

Mounts
/var/run/secrets/kubernetes.io/serviceaccount
from kube-api-access-hhjcj

Arguments
-

Command
-

New in 2022

Requirements for organizational standards

Supported

Same consistent, supported Kubernetes experience across all of your environments.

Enforce best practices

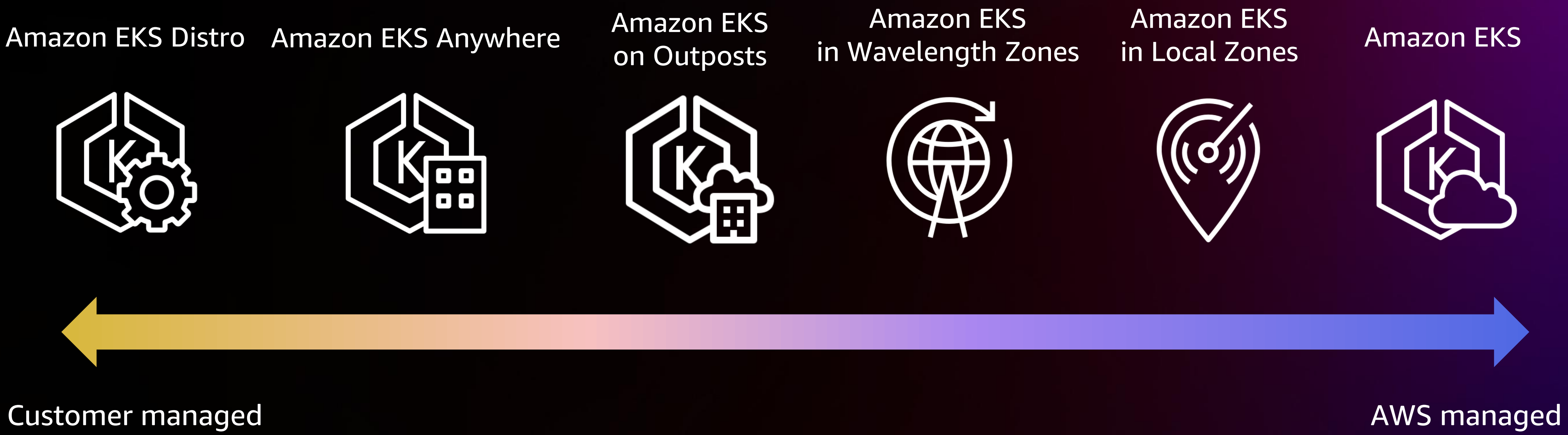
Tooling makes it easy to standardize and enforce best practices that augment, and do not disrupt workflows.

Portability

You can run in the environments you require without significant changes to your applications and configuration. You can take advantage of unique features in an environment without significantly altering application configuration.

Amazon EKS portfolio

DEPLOY IN ANY ENVIRONMENT



Amazon EKS Distro

Amazon EKS Anywhere

Amazon EKS on Outposts

Amazon EKS in Wavelength Zones

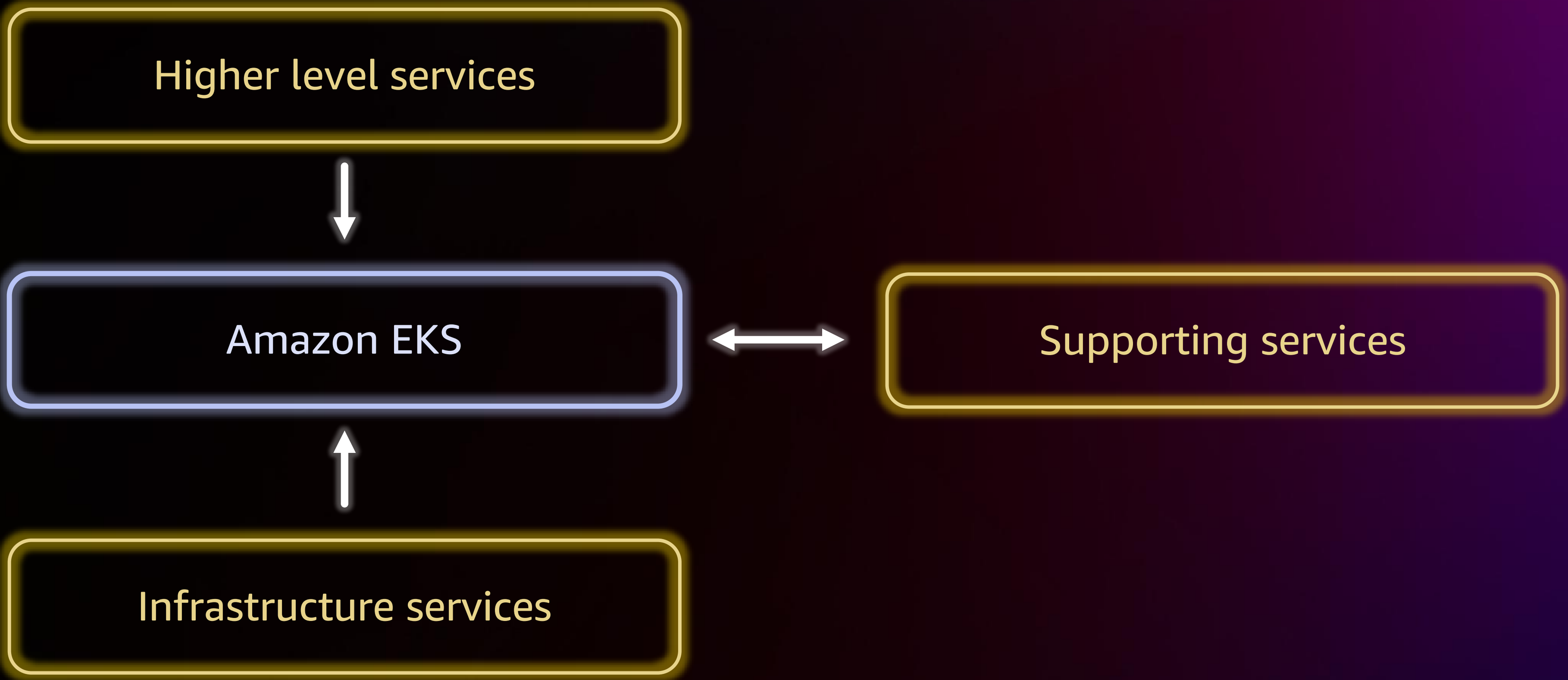
Amazon EKS in Local Zones

Amazon EKS

Customer managed

AWS managed

Kubernetes access to AWS services



Higher level services

Amazon EKS

Supporting services

Infrastructure services

Available Now

AWS Controllers for Kubernetes (ACK)

Harness AWS

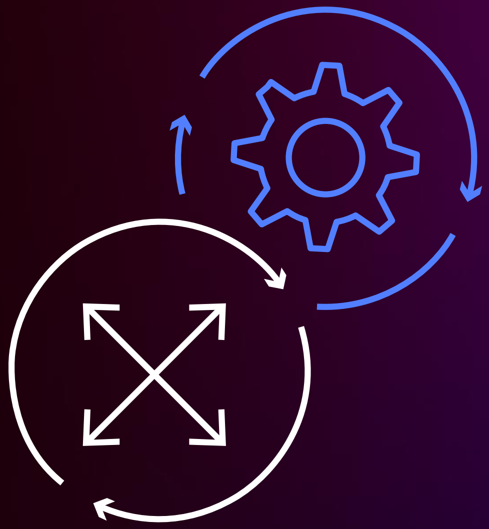
Create and use AWS resources directly within your cluster. Improve reliability and uptime at any scale.

Cloud-native control

Kubernetes custom resources and controllers enable you to 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.



github.com/aws-controllers-k8s

Available Now

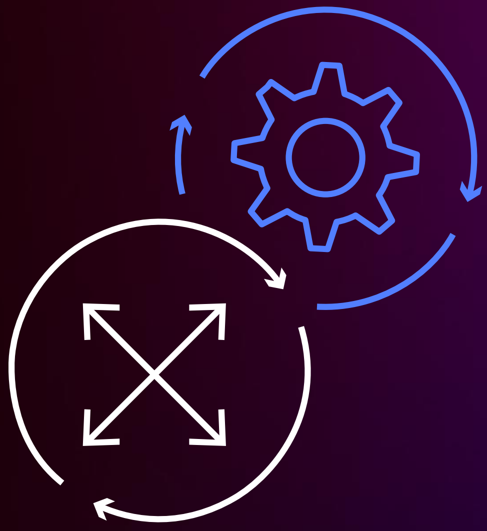
AWS Controllers for Kubernetes (ACK)

Generally Available Now

- Amazon Managed Service for Prometheus Service
- AWS API Gateway v2
- AWS Application Autoscaling
- Amazon DynamoDB
- Amazon EC2
- Amazon ECR
- Amazon EKS
- AWS KMS
- AWS Lambda
- Amazon RDS
- Amazon S3
- Amazon SageMaker
- AWS Step Functions
- EMR Containers

Coming soon

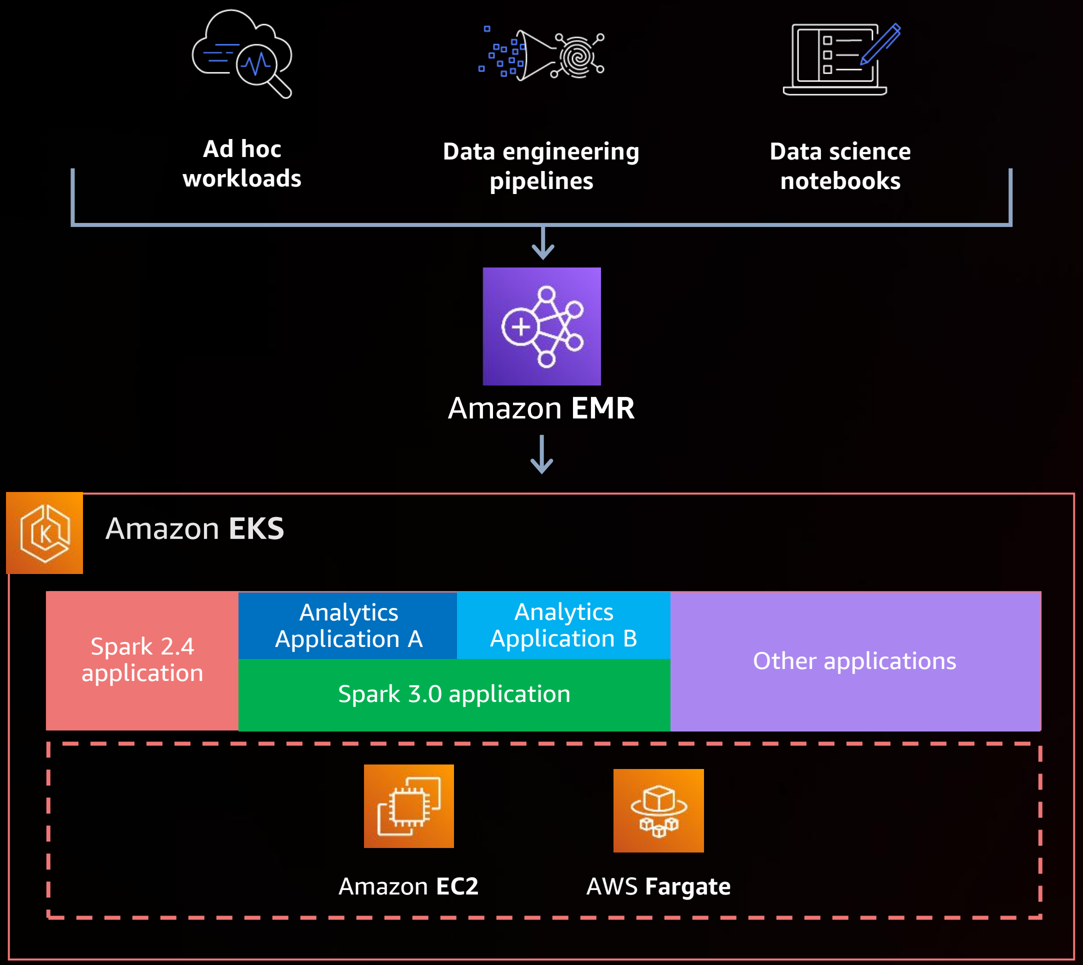
- Amazon API Gateway
- Amazon CloudFront
- AWS CloudTrail
- Amazon ElastiCache
- AWS IAM
- Amazon MSK (Kafka)
- Amazon Kinesis
- Amazon MemoryDB
- Amazon MQ
- Amazon OpenSearch Service
- Amazon SNS



github.com/aws-controllers-k8s

Generally Available

Amazon EMR on Amazon EKS



✓ Consolidate compute across the organization to optimize cost

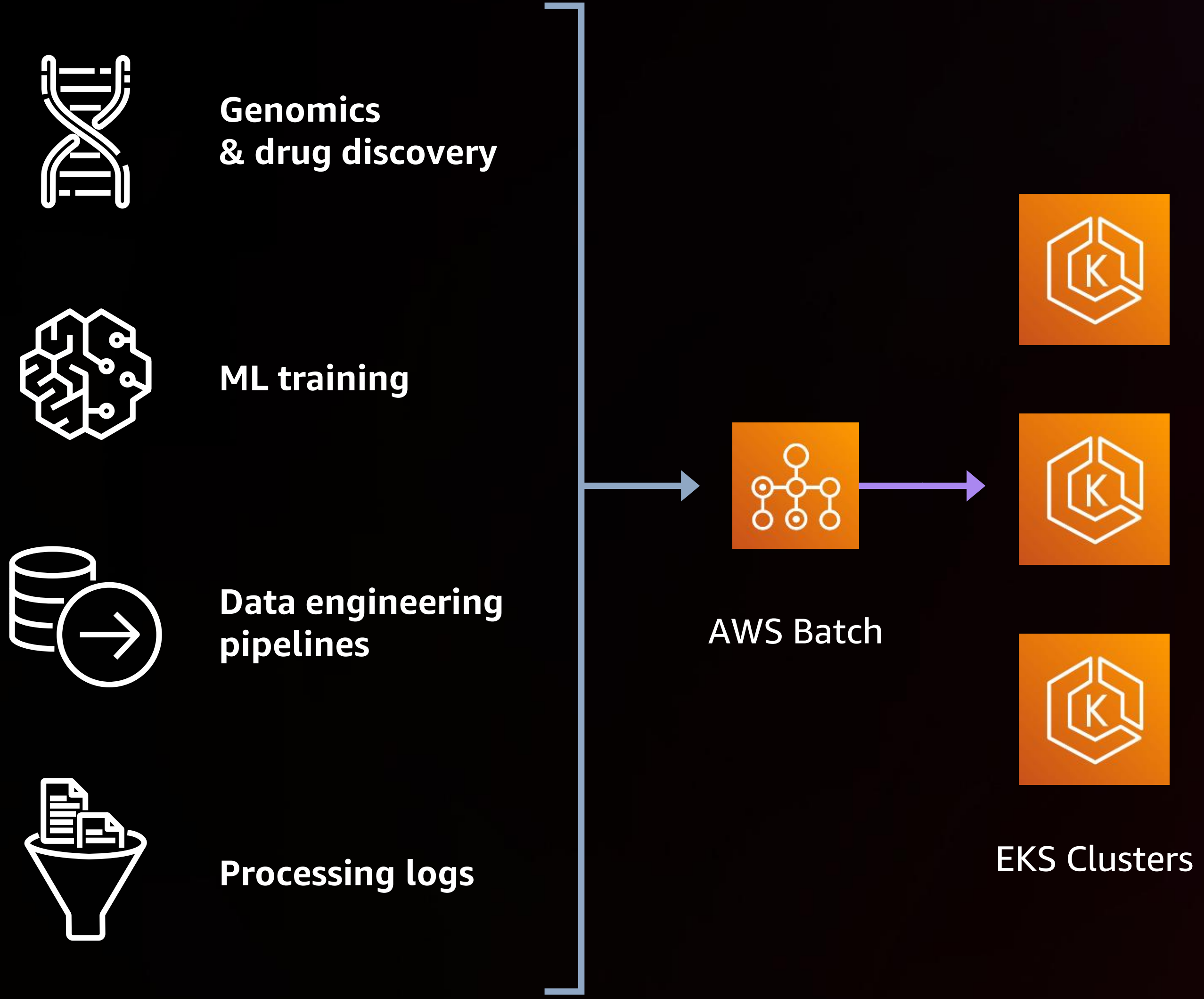
✓ Allocate resources by team, application, or job to meet performance requirements

✓ Start jobs quickly by taking advantage of existing capacity or using AWS Fargate

✓ Run highly available data processing workloads across multiple Availability Zones

New in 2022

AWS Batch for EKS



Features

- Fully managed batch computing, offload operations to AWS
- Multi-cluster aware scheduling
- Workload-aware scaling and scheduling
- Compatible with any EKS cluster

Use preferred monitoring and governance tooling.

Batch manages application isolation from other EKS workloads.

Follow our public roadmap

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

github.com/aws/containers-roadmap

Thank you!

Nathan Taber

linkedin.com/in/natetaber

Mike Stefaniak

linkedin.com/in/mike-stefaniak

Please complete the session survey in the **mobile app**