
AWS
re:Invent
DECEMBER 2 – 6, 2024 | LAS VEGAS, NV

KUB315

Securing Kubernetes workloads in Amazon EKS

Micah Hausler
Principal Software Engineer
AWS

George John
Senior Product Manager
AWS

Agenda

01 Cluster scoped security controls

02 Infrastructure scoped security controls

03 Application scoped security controls

Kubernetes

84%

Using in production or evaluating

CNCF Annual Survey 2023, cncf.io/reports/cncf-annual-survey-2023

AMAZON EKS

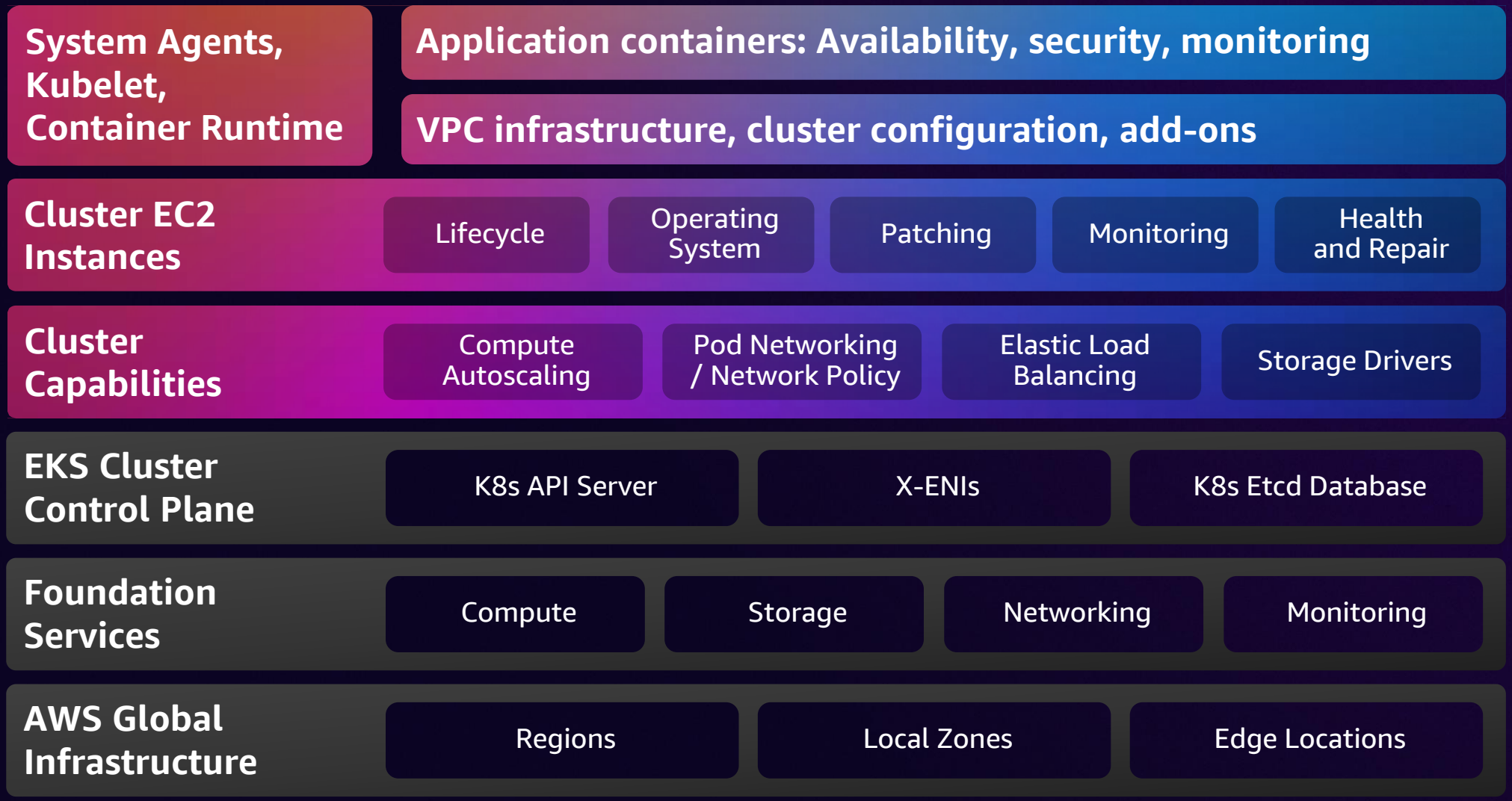
Runs tens of millions

of clusters every year

Amazon EKS

- The most trusted and secure way to run Kubernetes
- Allows you to build reliable, stable, and secure applications in any environment
- Fully upstream and certified conformant Kubernetes

Shared Responsibility Model with EKS – *Existing*



Managed by Customers

Managed by Amazon Web Services

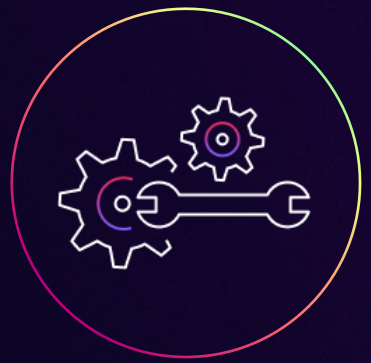
Cluster scoped security controls

Access into the cluster – *Previously*

AWS-AUTH CONFIG MAP

Complex setup

Setting up access required both AWS and Kubernetes APIs



Brittle

Malformed configurations can lock users out

Creator privileges

Cluster creator has implicit permissions

Access into the cluster – *Now*

CLUSTER ACCESS MANAGEMENT

AWS APIs

Automate access through EKS APIs with infrastructure as code (IaC)

Simplified configuration

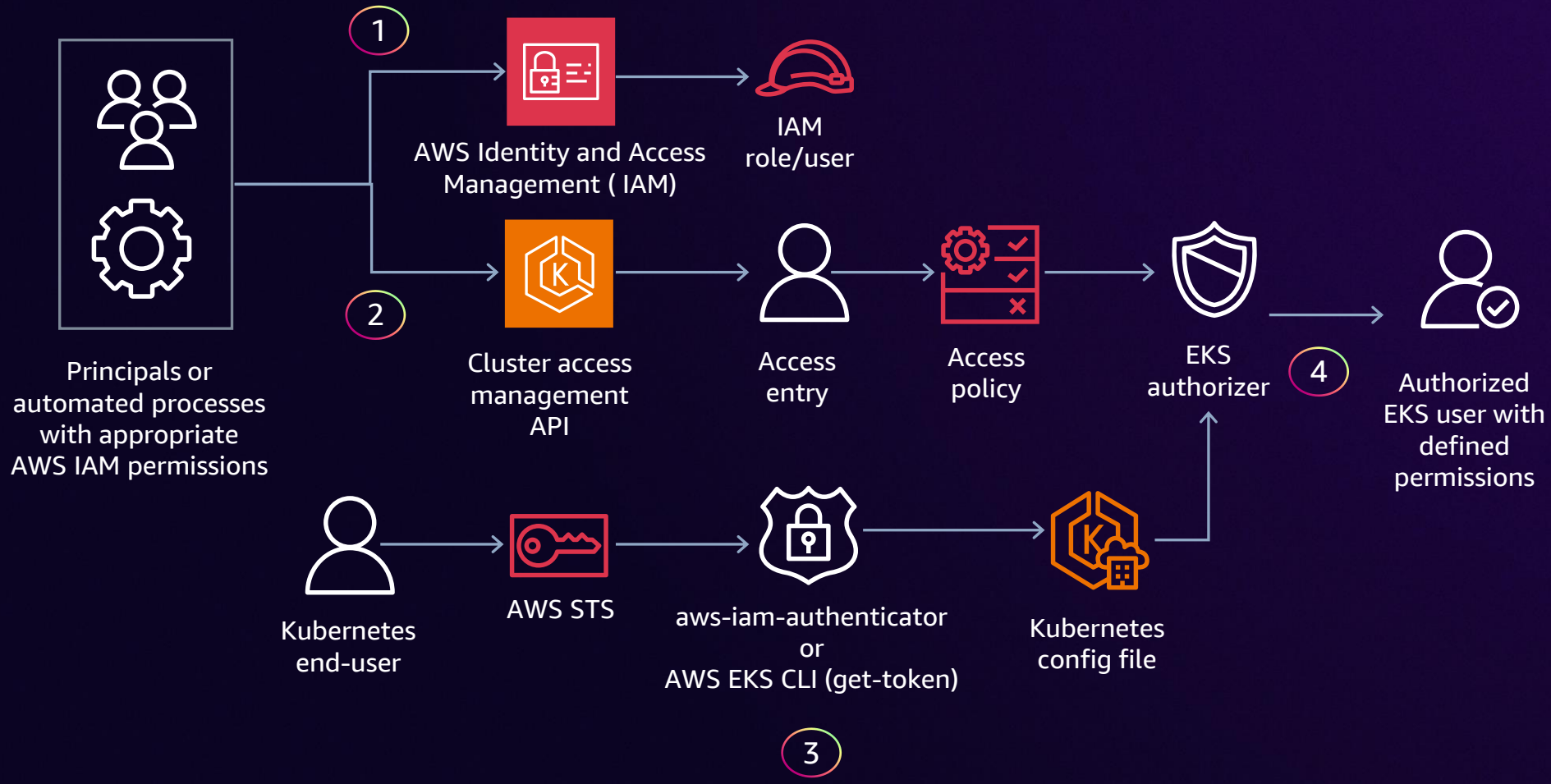
Streamline administration of clusters with multiple users and AWS services

Granular control

Disable or revoke access for any user, including the cluster creator

aws.amazon.com/blogs/containers/a-deep-dive-into-simplified-amazon-eks-access-management-controls/

Cluster access management



Cluster access management

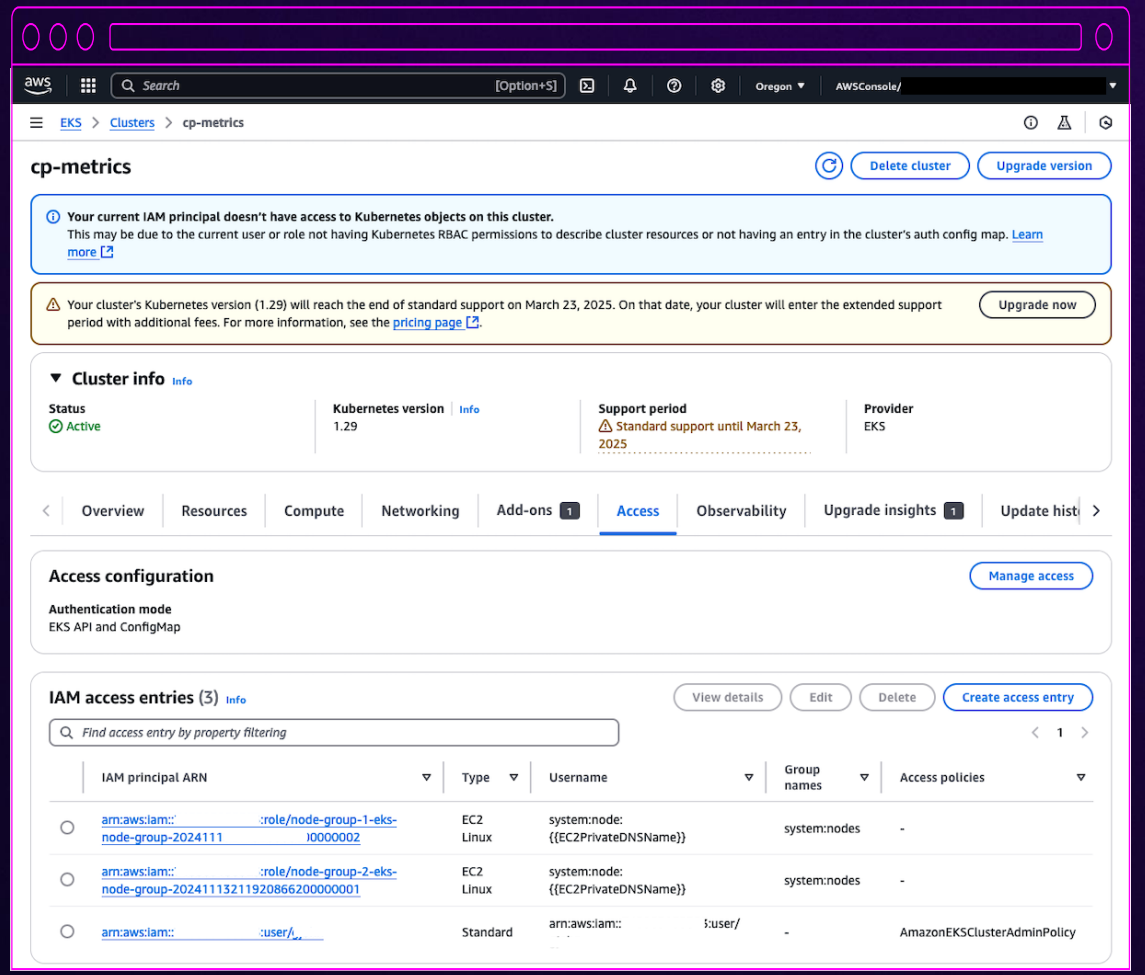
EKS APIS

```
aws eks create-cluster\
  --access-config authenticationMode=API \
  --no-bootstrap-cluster-creator-
    admin-permissions

aws eks create-access-entry \
  --clusterName my-cluster \
  --principal-arn my-iam-principal-arn

aws eks associate-access-policy \
  --clusterName my-cluster \
  --principal-arn my-iam-principal-arn \
  --policy-arn my-policy-arn \
  --access-scope type=cluster
```

EKS CONSOLE



Access from the cluster – *Classic*

IAM ROLES FOR SERVICE ACCOUNTS (IRSA)

Elevated permissions

Requires IAM admin permissions for Identity provider (IdP) and IAM role configuration

Cluster scoped

Requires bookkeeping of IAM role trust policies to cluster lifecycle

Bounded

Trust policy size and IdP provider limits

Access from the cluster – *New*

EKS POD IDENTITY

Simplified trust

Establish trust one time with EKS Service

Scalable ABAC

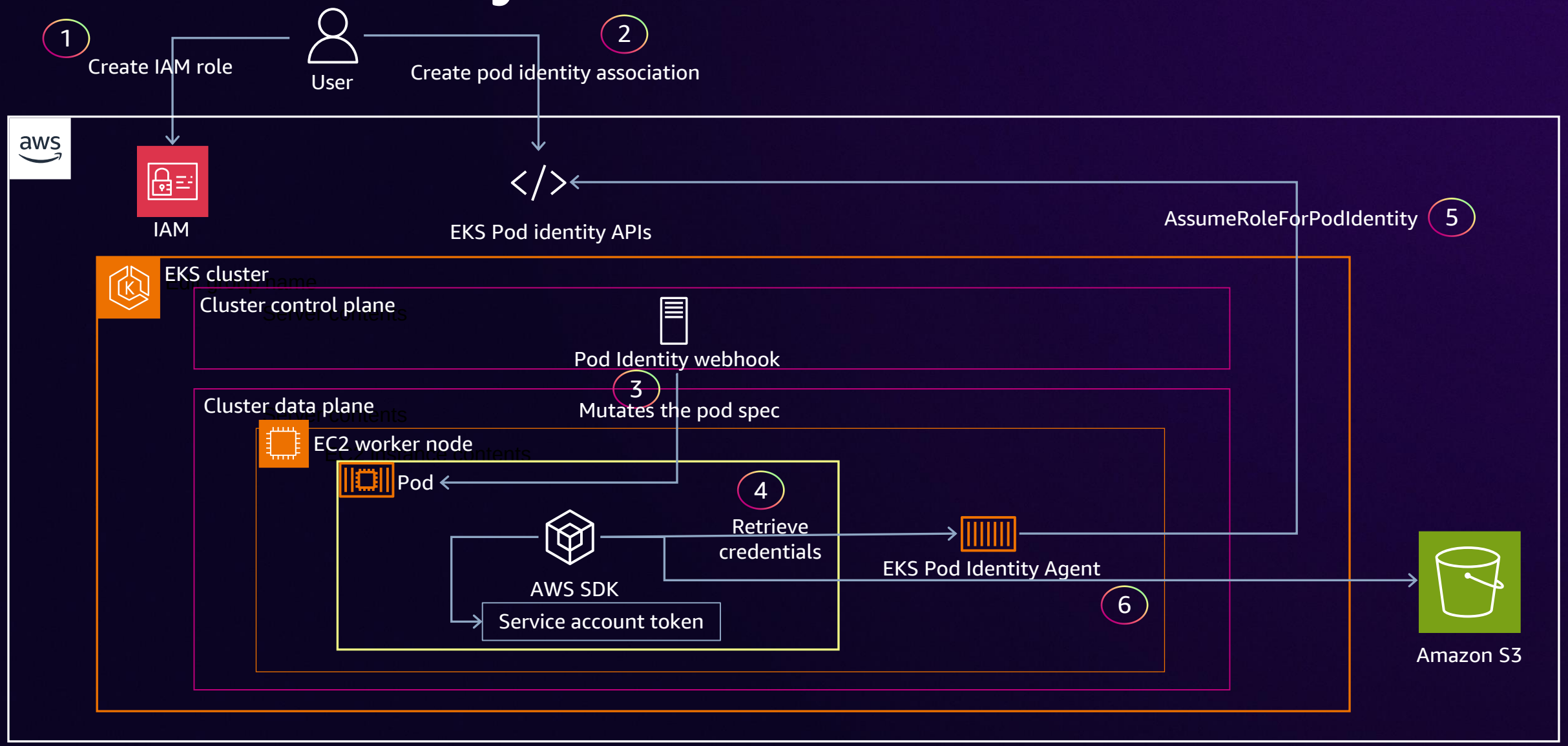
Supports attribute based access control with IAM role session tags

Ready to go

Application-ready clusters

aws.amazon.com/blogs/containers/amazon-eks-pod-identity-a-new-way-for-applications-on-eks-to-obtain-iam-credentials/

EKS Pod Identity



What’s new in EKS Pod Identity?

Expanded region support

Open sourced EKS Pod Identity agent

EKS Add-on support for Pod Identity

Detective controls

Analyze K8S API access with EKS control plane audit logs and CloudWatch Logs Insights

Create alarms for suspicious behaviors (such as increased HTTP 403 Forbidden or HTTP 401 Unauthorized)

Analyze EKS API access with AWS CloudTrail logs and CloudTrail Insights

Amazon Detective can visualizes and diagnose VPC flow logs from EKS cluster

Data encryption

- Amazon EBS, EFS, and FSx for Lustre support encryption at rest
- Encryption using AWS managed keys or customer managed keys
- Encrypt K8s secrets with AWS KMS
- Automatic rotation of keys with AWS KMS

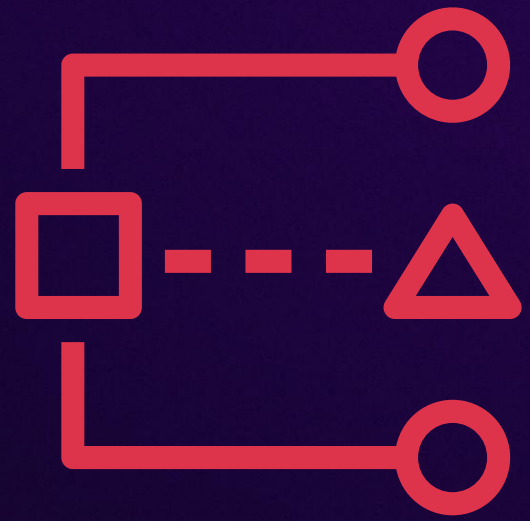
Other cluster scoped security controls

Control access to K8s cluster endpoint

Enable private access to EKS service management endpoint with AWS PrivateLink

Use managed components (EKS Add-ons, EKS Optimized AMIs) when possible

Evaluate your cluster with AWS Security Hub



Infrastructure scoped security controls

INTRODUCING AMAZON EKS

Auto Mode

Automate your entire Kubernetes cluster infrastructure

WHY AMAZON EKS

Auto Mode

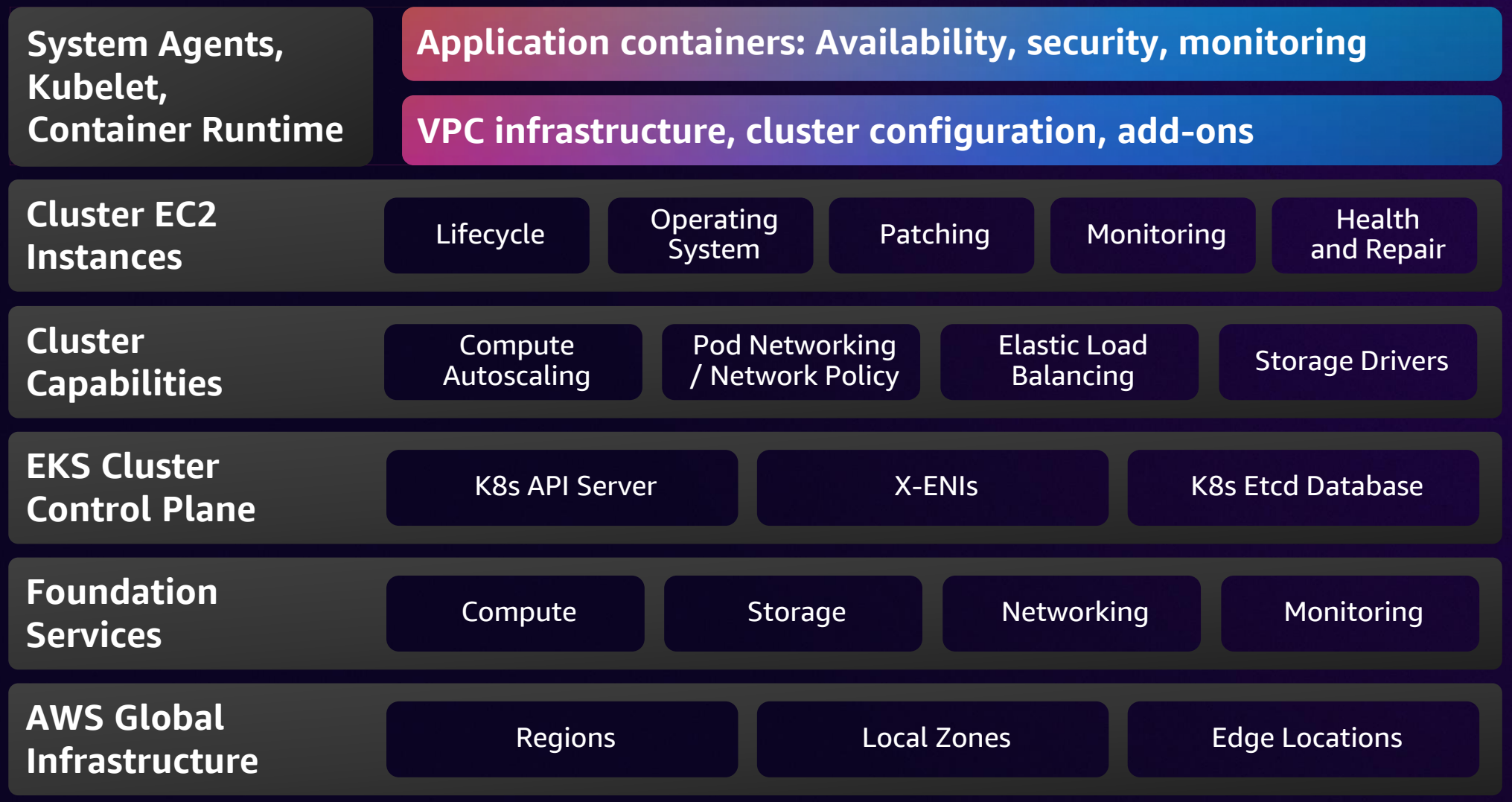
- Improve performance and optimize resources
- Simplify Management
- Reduce operational overhead

WHY AMAZON EKS

Auto Mode

- Increase agility and accelerate innovation by offloading cluster operations to AWS
- Improve performance, availability, and security of your applications with AWS operational excellence
- Optimize compute costs with automatic capacity planning and dynamic scaling

Shared Responsibility Model with EKS Auto Mode



Managed by Customers

Managed by Amazon Web Services

Cluster network security

Kubernetes network policy

Enforce pod-level network rules on hosts

EC2 security group per pod

Analyzes operating system-level, networking, and file events

aws.amazon.com/blogs/containers/amazon-vpc-cni-now-supports-kubernetes-network-policies/

Amazon GuardDuty detective controls

Audit log protection

Detect potentially suspicious activities in EKS cluster audit logs

Runtime protection

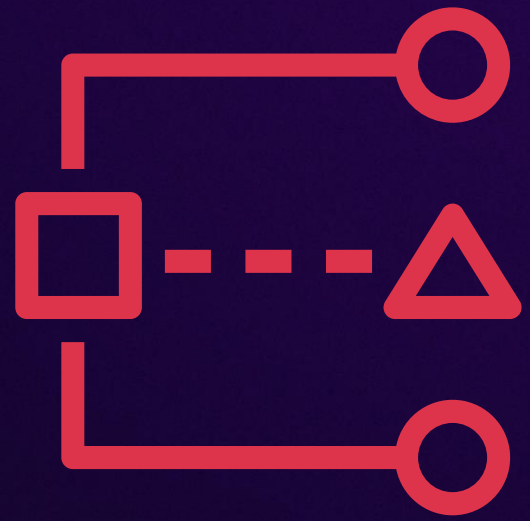
Analyzes operating system-level, networking, and file events

Other infrastructure scoped security controls

Restrict & minimize instance access with AWS System Manager (SSM)

Use container optimized OS - EKS Optimized AMIs, Bottlerocket

Verify configuration with CIS Amazon EKS Benchmark



Application scoped security controls

Pod security

- Pod Security Standards/policy-as-code solutions
- Limit privileged containers
- Disable service account token mounts
- Restrict use of hostPath
- Set up images with read-only file system

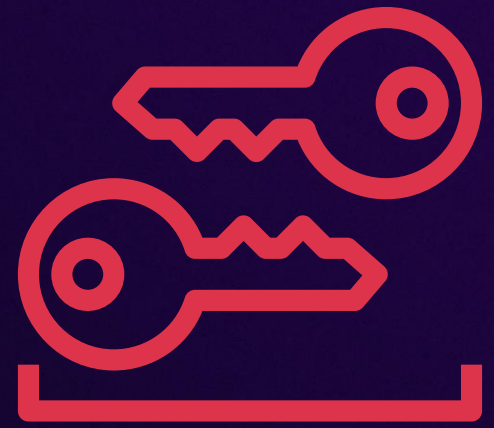


Image security

- Scanning images for vulnerabilities regularly with Amazon ECR & Amazon Inspector
- Restrict Amazon ECR endpoint access
- Configure images to use a non-root user

Kubernetes authorization – *New*

CEDAR

- Consolidated authoring experience for policies
- Enhanced authorization features

github.com/awslabs/cedar-access-control-for-k8s

Cedar policy

```
permit (
    principal is CustomUserType,
    action in [Action::"get", Action::"list"], // match multiple actions
    resource is MyResourceType
)
// optional positive condition clause
when {
    principal in MyGroupType::”a-group-identifier” &&
    resource.some_attribute_name == "cool_value"
}
// optional negating condition clause
unless {
    resource.my_kind_attribute == "secret"
};
```

Cedar demo

Resources

EKS Best Practices Guide

Deep dive into advanced best practices

Regularly updated and curated by AWS experts

docs.aws.amazon.com/eks/latest/best-practices/introduction.html

EKS Workshop

Free and open training for using EKS

Modules from 200–400 level

New! Developer workshop

eksworkshop.com

EKS Blueprints

Frameworks and examples for deploying complete clusters

Available for Terraform and AWS CDK

aws-ia.github.io/terraform-aws-eks-blueprints

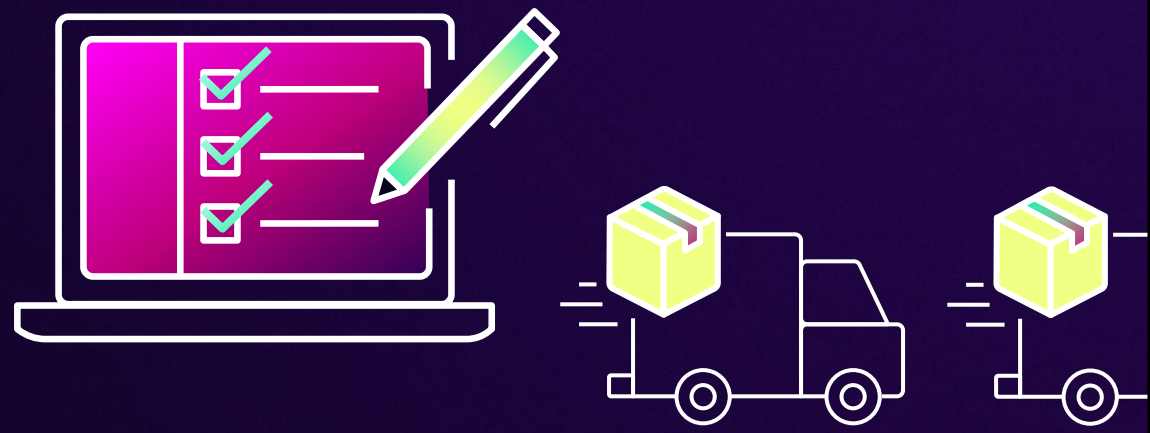
aws-quickstart.github.io/cdk-eks-blueprints/

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!

Please complete the session survey in the mobile app

Micah Hausler

@micahhausler

@micahhausler.com

George John

linkedin.com/in/find-george-john