AWS re:Invent

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

CON304

Deep dive on Amazon EKS

Mike Stefaniak (he/him)
Sr. Product Manager, Amazon Elastic Kubernetes Service
AWS

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

What is Amazon EKS?



Amazon **EKS**

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

Amazon EKS helps you build reliable, stable, and secure applications in virtually any environment

aws

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

Why Kubernetes?



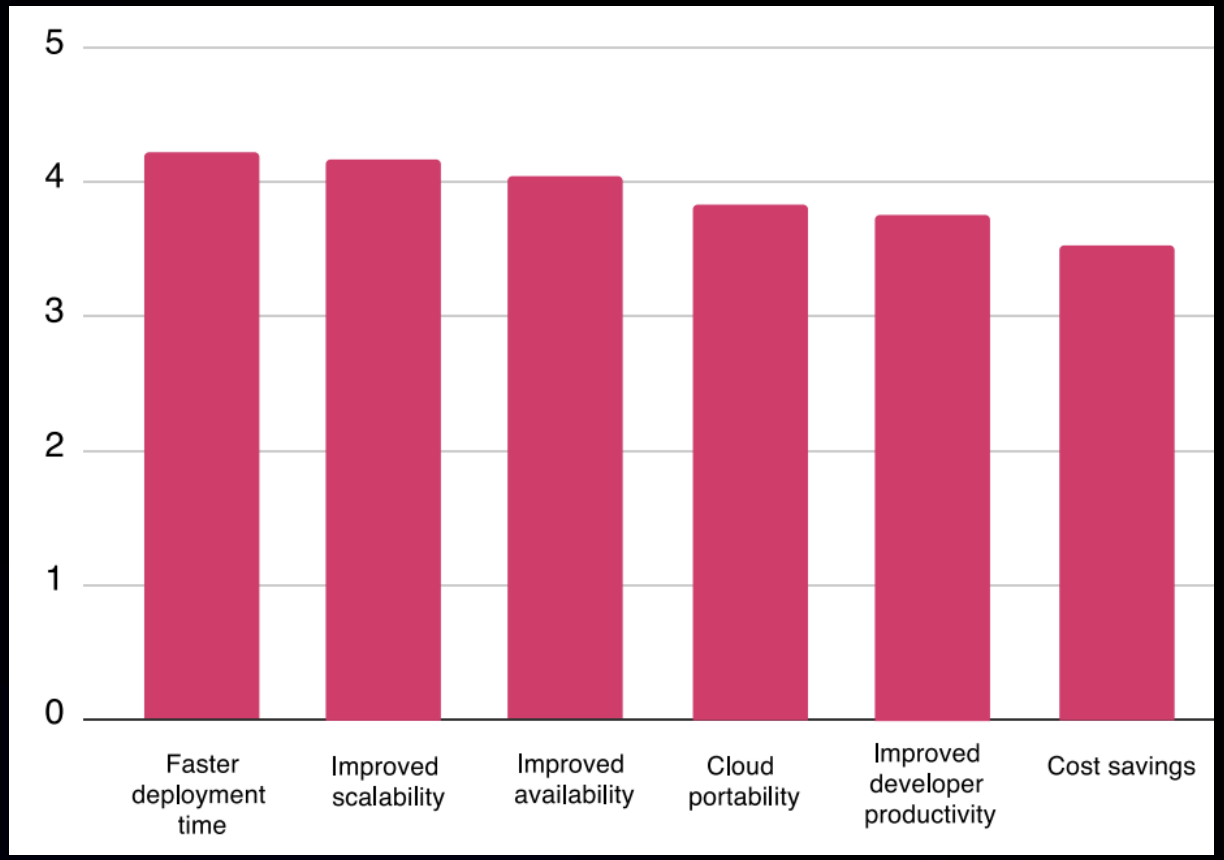
Open-source container management platform governed by the community



Run containers at scale, integrating networking, storage, and compute



Take advantage of open-source tools that are designed to run on Kubernetes



Source: CNCF Survey – Rate Kubernetes benefits 1 to 5

aws

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

Why Amazon EKS?



Running and scaling Kubernetes can be difficult and requires significant investment



Securing Kubernetes increases the operational overhead of running applications

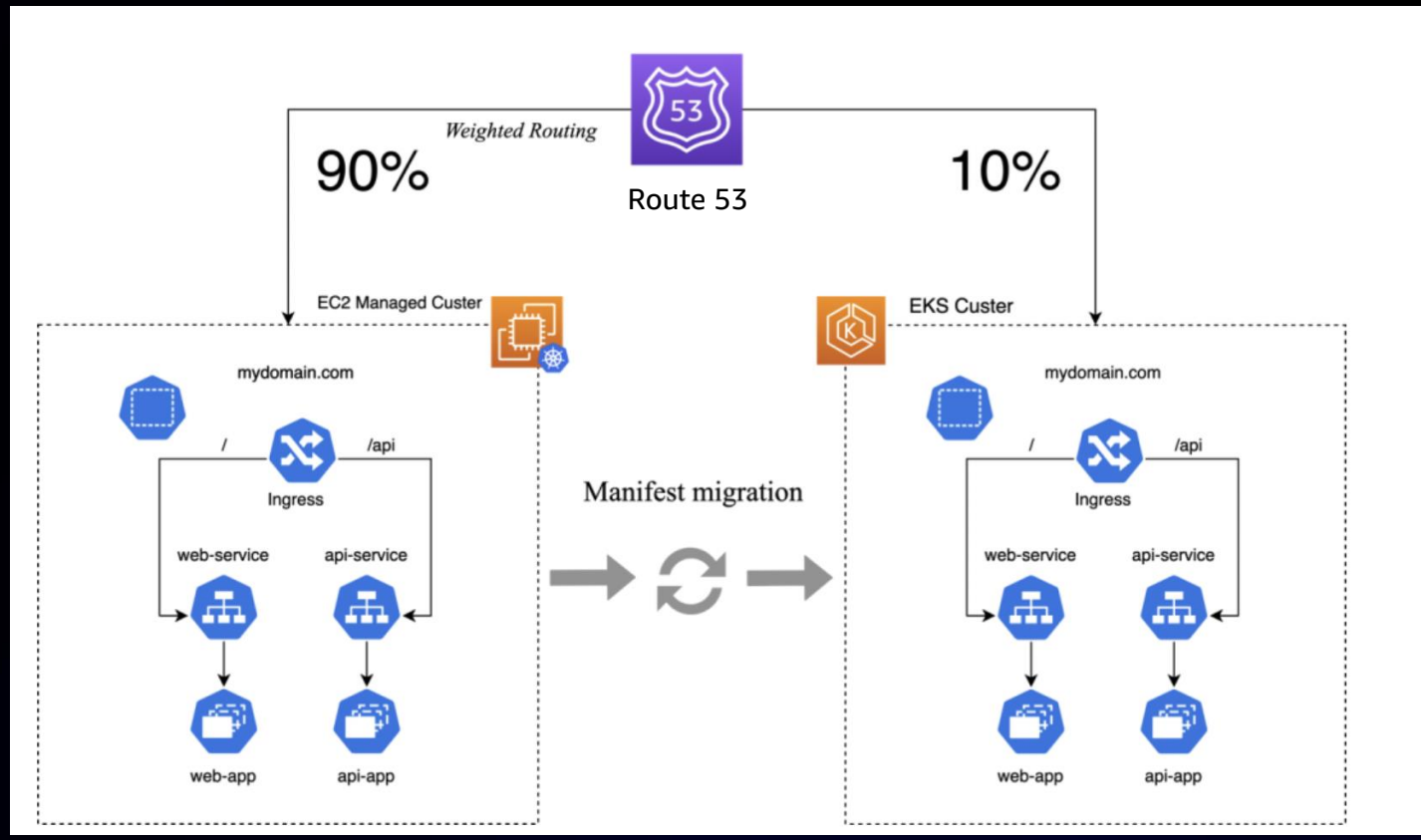


Applications need a native way to integrate with other AWS services securely and reliably

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

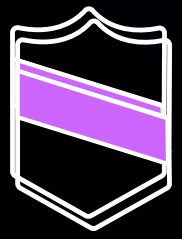
How do I migrate from self-managed Kubernetes to Amazon EKS?

- Qualify your applications on the latest Kubernetes versions
- Check user authentication practices
- Evaluate cluster lifecycle management tooling
- Perform load testing
- Choose between backup/restore or simply redirect CI/CD
- Use Amazon Route 53 weighted DNS to shift traffic over to new cluster

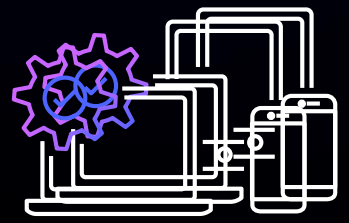


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are the Amazon EKS tenets?



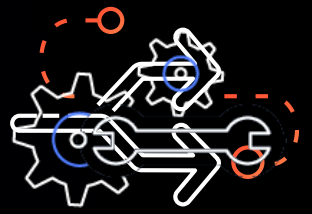
Security
Security first



Reliability
Built for production



Efficiency
Seamless cloud integrations



Cluster
Native and upstream operations



Portability
Committed to open source

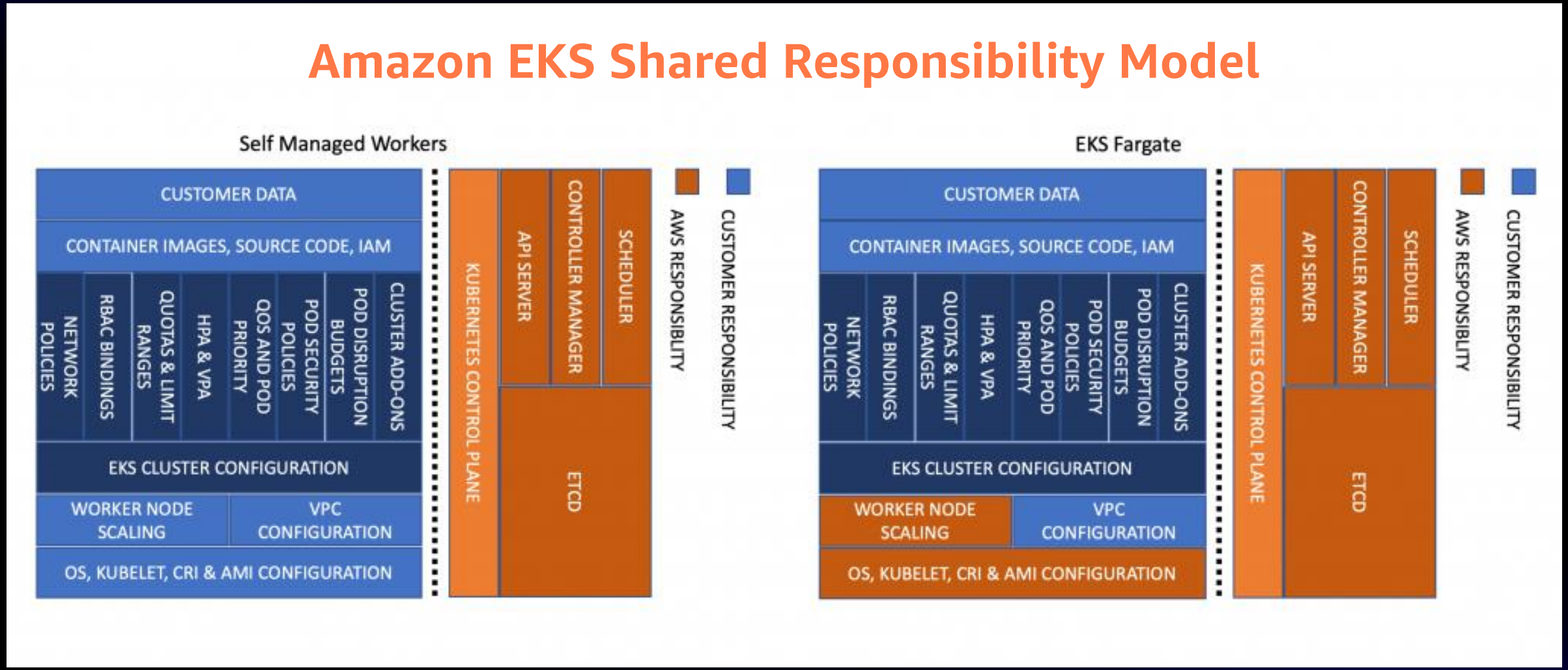
aws

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

Security

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

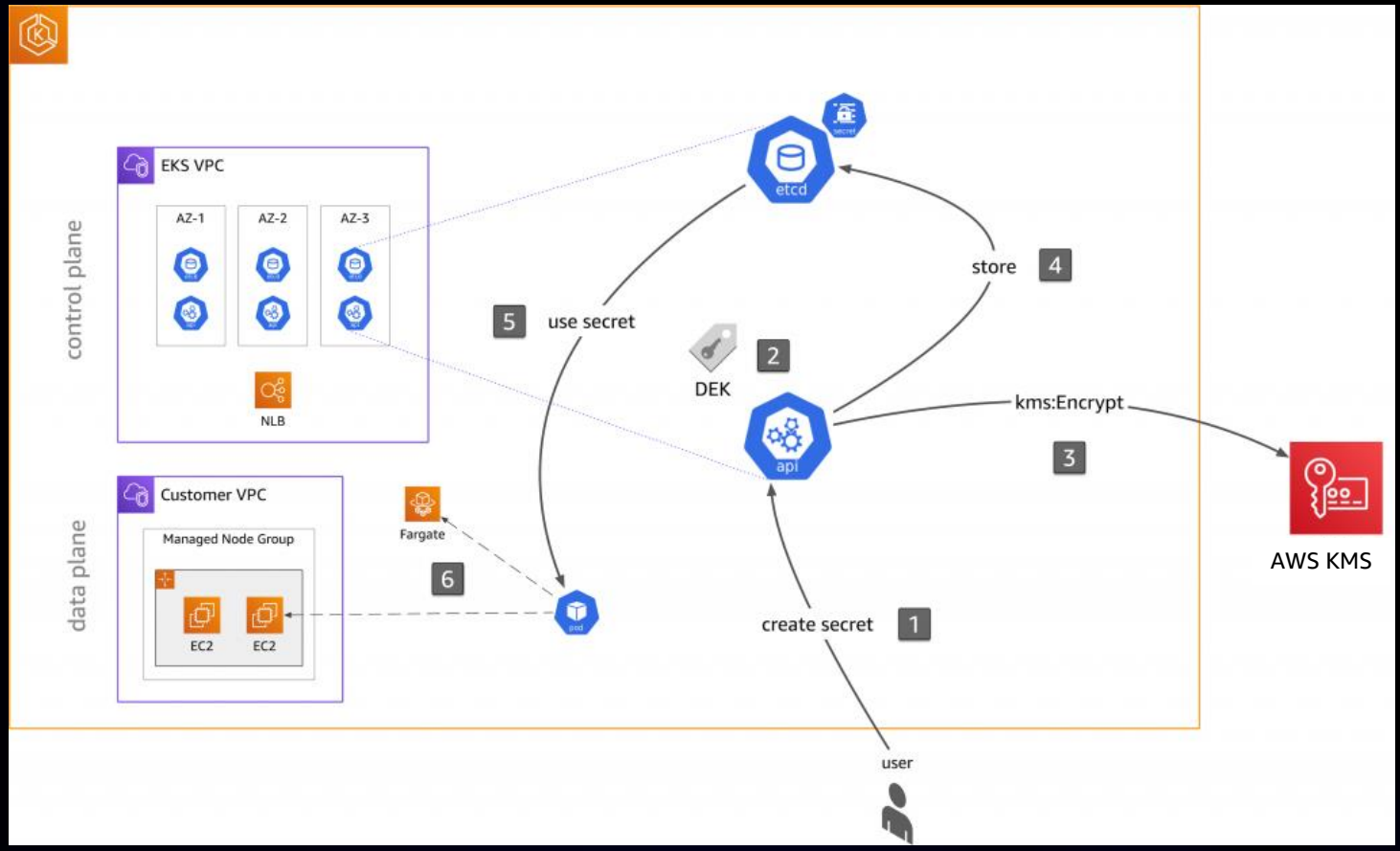
How do I secure my cluster?



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

How do I secure sensitive cluster data?

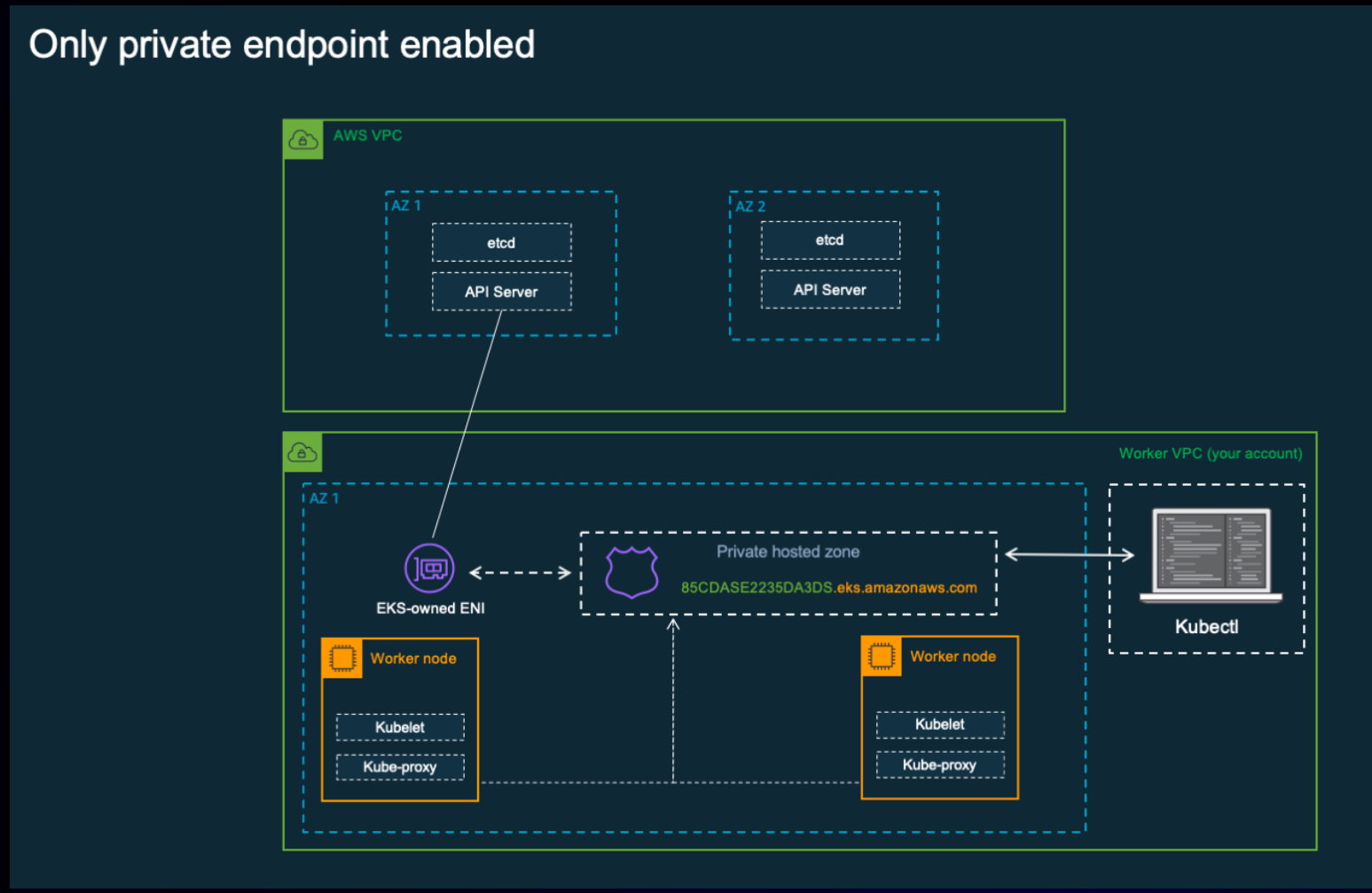
- Encrypt your secrets with AWS Key Management Service (AWS KMS)
- Store secrets outside the cluster and retrieve using AWS Secrets Manager CSI driver
- Use AWS Certificate Manager Private CA Issuer cert-manager plugin to generate TLS certificates



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

How do I limit access to the cluster endpoint?

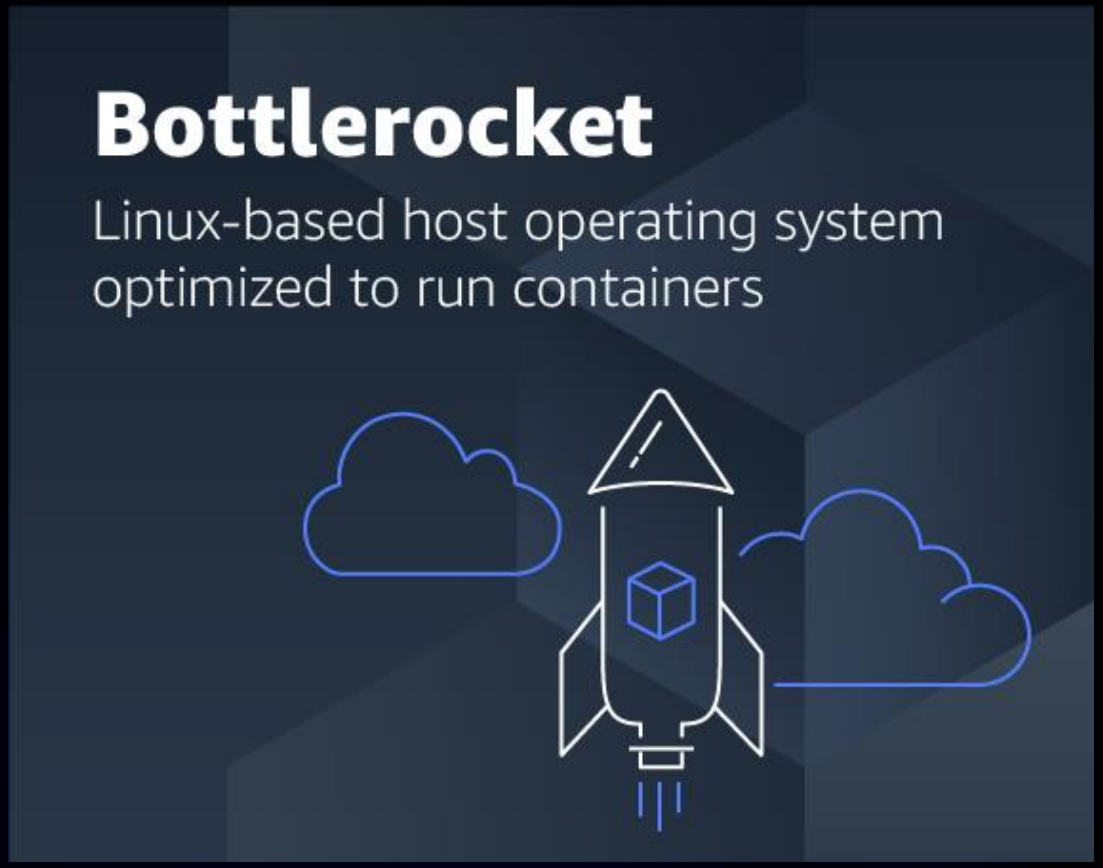
- If possible, disable public endpoint
- If not, restrict access to public endpoint with CIDR blocks
- Private endpoint and private only subnets – if no internet communication required



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

How do I run secure worker nodes?

- Use an OS optimized for containers, such as Bottlerocket
- Treat worker nodes as immutable
- Use AWS Systems Manager instead of SSH
- Validate custom AMIs with CIS Amazon EKS Benchmark
- Or, pass off this responsibility to AWS Fargate

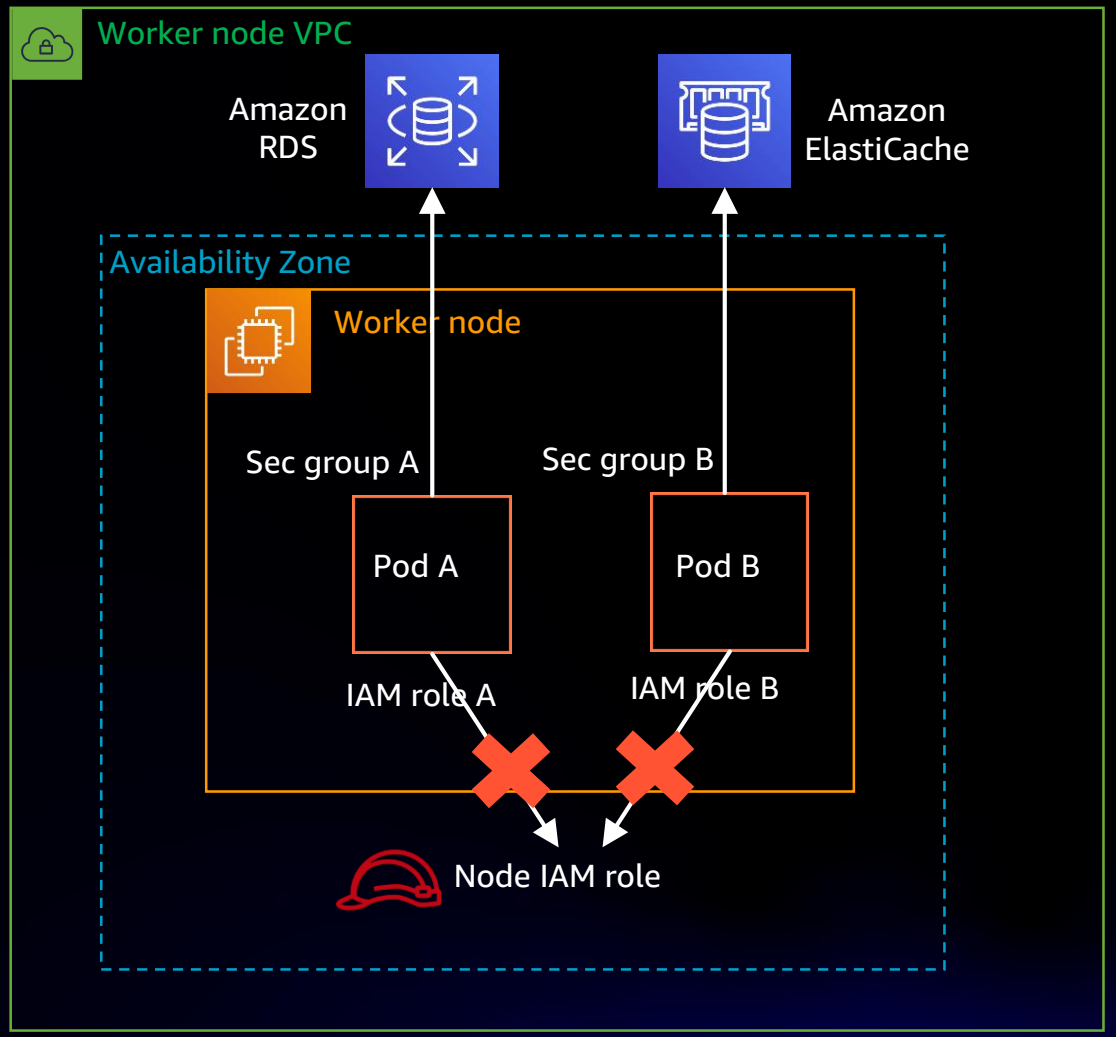


aws

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

How do I implement security at the pod level?

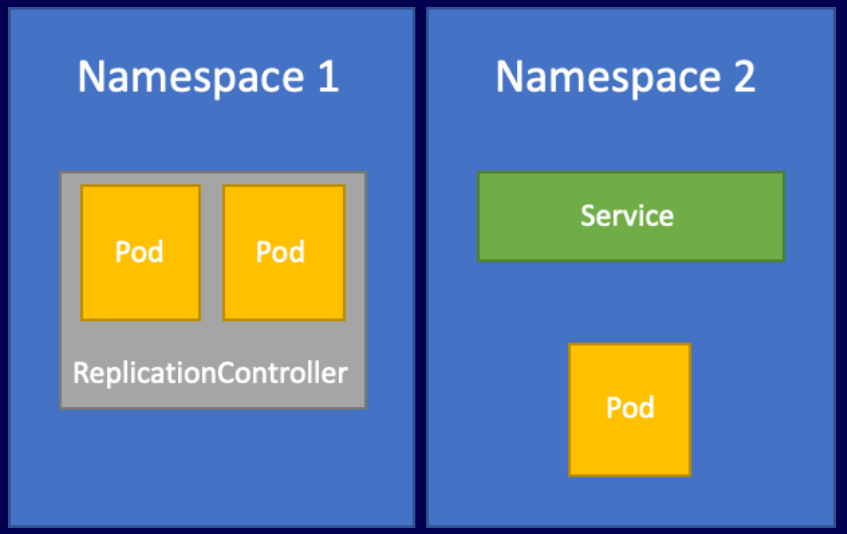
- Scope down IAM permissions to pods instead of nodes with IAM roles for service accounts (IRSAs)
- Restrict pod access to instance metadata service (IMDS)
- Use K8S NetworkPolicy to restrict network traffic within cluster
- Use EKS SecurityGroupPolicy to restrict network traffic to AWS services like Amazon RDS



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

What are additional security best practices?

- Namespaces and role-based access controls (RBAC) to logically isolate trusted tenants
- Quotas and limit ranges to control consumption of compute resources
- API priority and fairness (v1.20+) to limit API server requests
- Pod priority and preemption for quality of service (QoS)
- Enforce policies and limit what dev teams can run with agents like Gatekeeper
- Default network policies that deny all cross namespace ingress and egress traffic
- Defense-in-depth with VM-level isolation using Fargate



Important: Kubernetes is a single-tenant orchestrator

Namespaces are not a hard security boundary

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

Which compliance standards does EKS meet?



Payment Card Industry (PCI) Security Standard



FedRAMP High



DOD Cloud Security Req's Guide (SRG) – On road map



Criminal Justice Information Service Security Policy (CJIS)



U.S. Health Insurance Portability and Accountability Act (HIPAA)



Federal Information Processing Standard Pub (FIPS) 140-2



SP 800-53 (rev 4)
SP 800-171



Health Information Trust Alliance Common Security Framework (HITRUST CSF)

aws

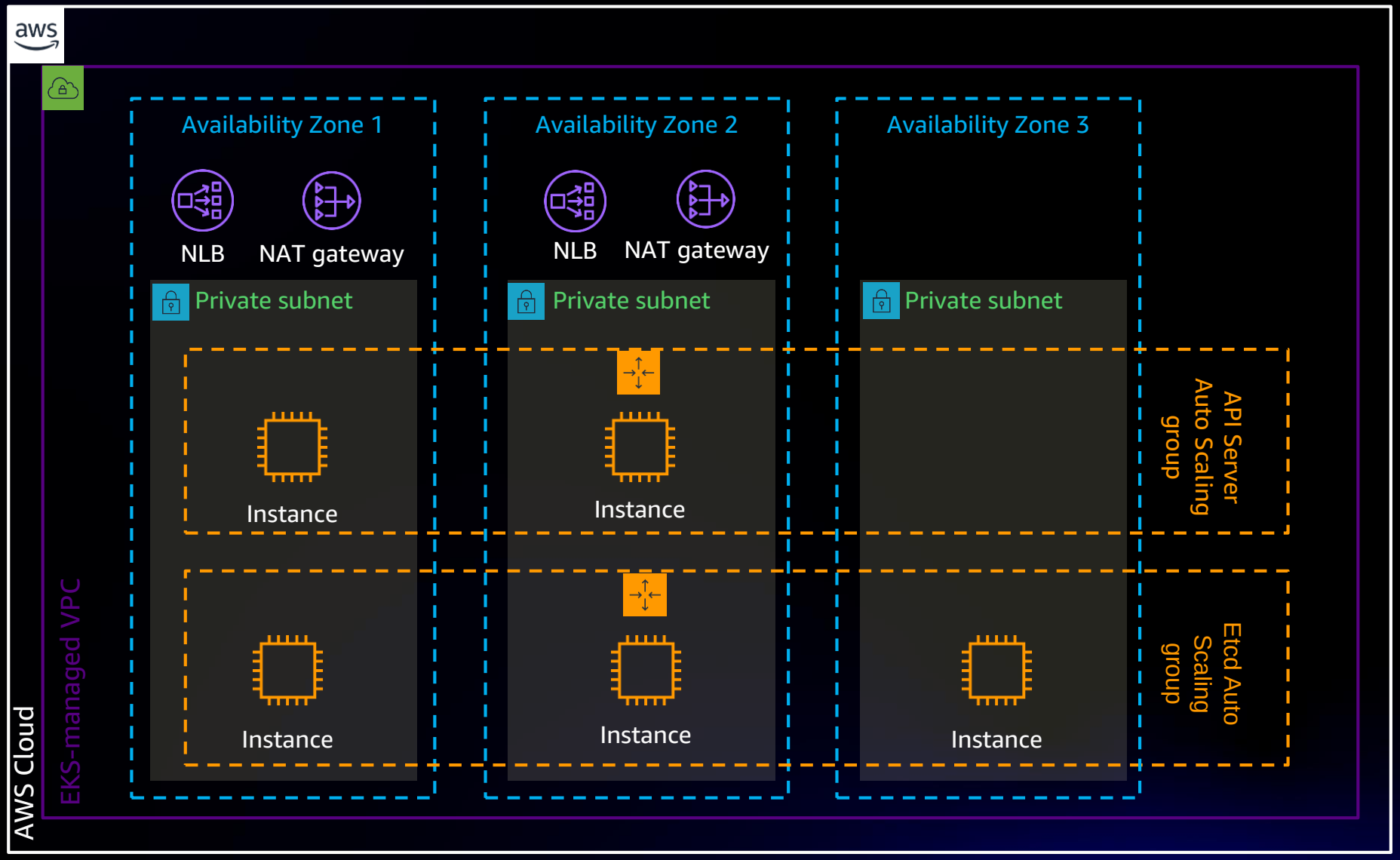
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Reliability

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

How does EKS ensure high availability?

- Survive single-AZ events
- Highly available NLB endpoint
- Rolling control plane upgrades
- Automated etcd snapshots
- 99.95% SLA
- 24x7x365 support



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

Can EKS handle the scale of my applications?

Yes, but it's a shared responsibility

Amazon EKS side

- Auto scaling of control plane instances
- Auto tuning of control plane parameters such as *maxRequestsInFlight*
- Take advantage of the latest AWS infrastructure enhancements
- Test clusters with up to 15K worker nodes

Your side

- Monitor Kubernetes control plane Prometheus metrics
- Visualize metrics in Amazon CloudWatch or Grafana
- Enable control plane logging and query audit logs to identify top callers

aws

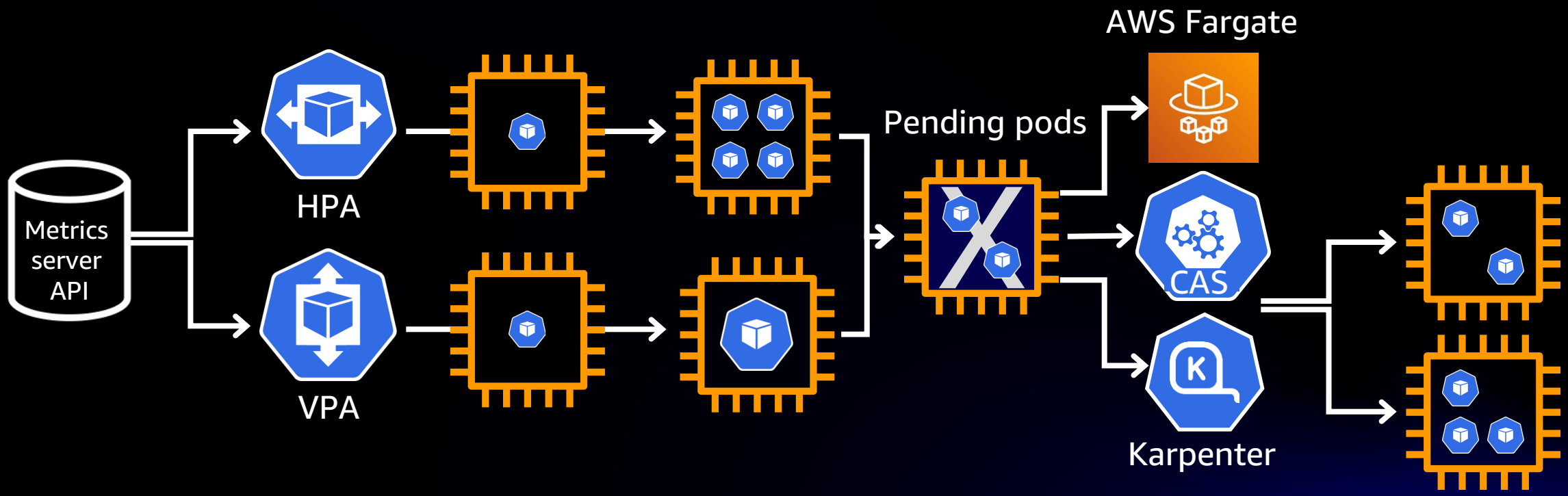
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Efficiency

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

How do I right-size compute capacity?

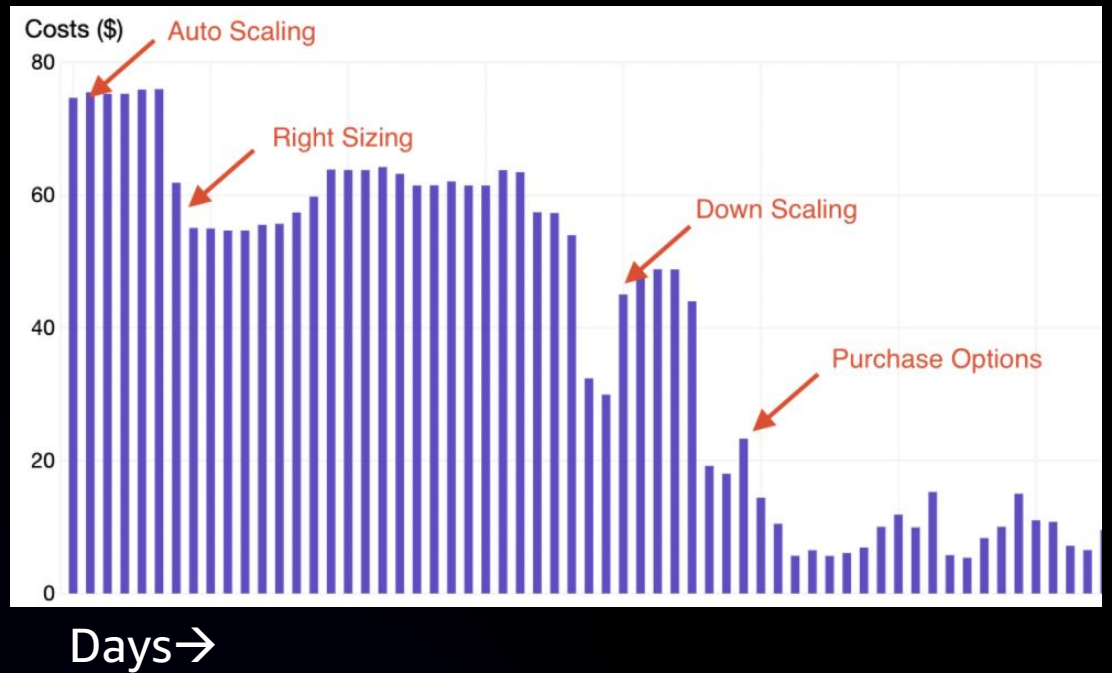
- Scale pods horizontally/vertically based on usage
  Set pod resource requests close to actual utilization
- Scale node resources based on pod requirements
  Limit overprovisioning of compute capacity



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

How can I reduce costs in my cluster?

- Use Spot Instances with managed node groups and save up to 90% off on-demand pricing
- Use Cluster Autoscaler priority expander to prioritize lower-cost node groups
- Utilize Savings Plan for Amazon EC2/Fargate
- Move to latest generation EC2 instances
- Move workloads to EC2 Graviton
- Try out Karpenter in large clusters with fast scaling requirements



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

How do I scale applications in a cluster running in a VPC with limited IPv4 space?

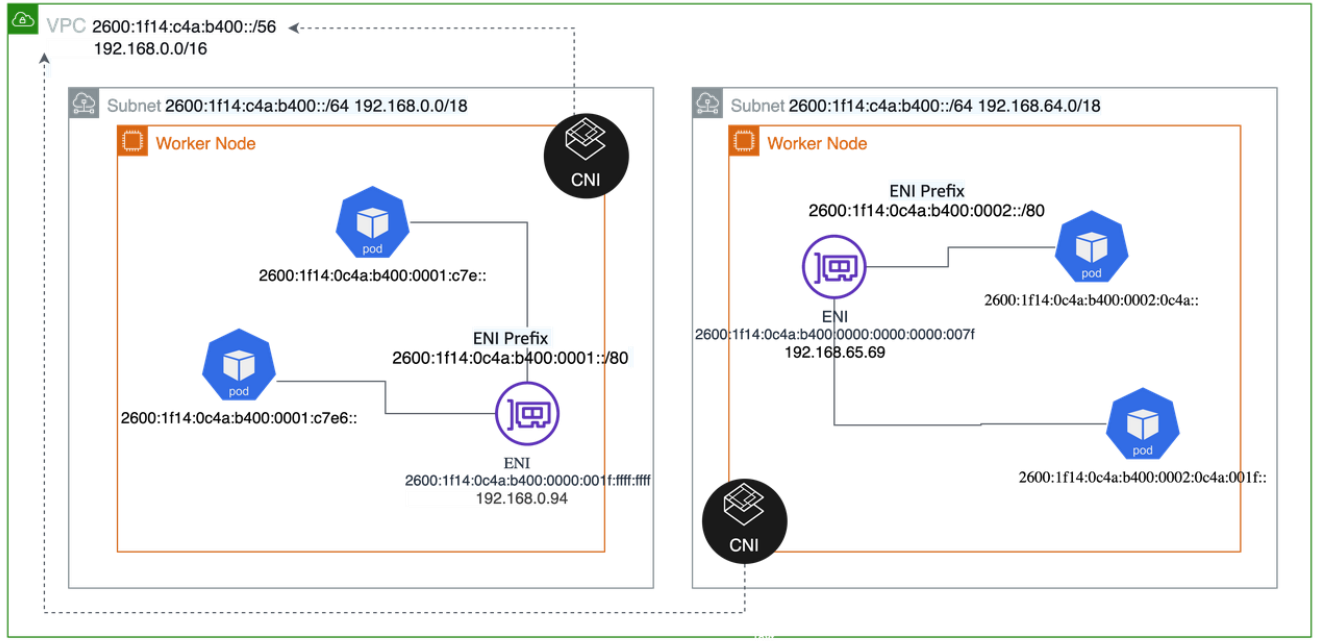
IPv6

- Scale far beyond IPv4 limits with globally unique IPv6 address assigned per pod
- Simplified pod-to-internet routing without network address translation
- Faster pod launch times
- Egress IPv4 traffic support

VPC CNI custom networking

- Add additional IPv4 CIDR blocks to existing VPC
- Run pods in subnets separate from primary ENI of worker nodes

EKS IPv6 networking setup



Important: Worker nodes can run in subnets separate from subnets registered during EKS cluster creation

aws

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

Should I run lots of small clusters or fewer large clusters?

SPLIT WHEN YOU HAVE TO, MERGE WHEN YOU CAN

- At a minimum, separate clusters per environment
- Step 1 – Analyze constraints: untrusted tenants, organizational boundaries, area of impact concerns
- Step 2 – Optimize within constraints; fewer clusters leads to more efficient bin packing and use of resources



Source: https://learnk8s.io/how-many-clusters

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

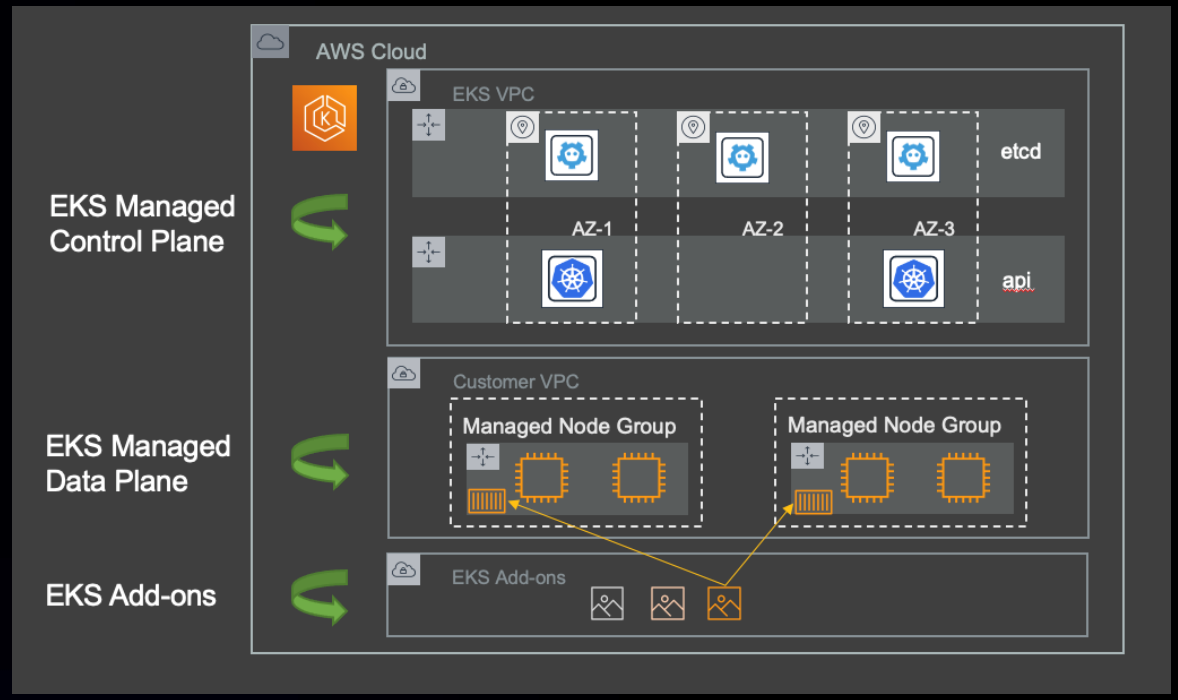
Cluster operations

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

How do I upgrade my cluster?

WHICH VERSION OF KUBERNETES DO I USE?

- Amazon EKS aims to be ~100–150 days behind upstream release
- You must plan for version upgrade at least yearly, ideally 2x-3x/yr
- Use EKS managed capabilities to simplify upgrades
- Run upgrade process in test env. first
- Check EKS and Kubernetes release notes
- Test your application manifests against deprecated/removed APIs









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

How do I manage user access to the cluster?

Authentication

AWS IAM

- No need to maintain separate identity store
- Assume IAM roles for simplified multi-user access control
- Built on open-source AWS IAM Authenticator for Kubernetes
- Integrated with cloud-hosted EKS Kubernetes console

OpenID Connect (OIDC)

- Use your organization's existing identity management system
- Built on open standards
- Use as alternative or in addition to IAM users/roles
- Simplified migration from self-managed Kubernetes and EKS Anywhere

Authorization

Kubernetes role-based access control (RBAC)

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

How do I monitor the state of my cluster?

Control plane side

- Enable control plane logging for audit, API server, and authentication
- Collect and monitor control plane Prometheus metrics for API request latency

Recommendation: Run kube-state-metrics to easily surface cluster state information

Application side

- EKS add-ons support for AWS Distro for OpenTelemetry
  - Output metrics/traces to CloudWatch, Amazon Managed Service for Prometheus, or partner destinations
- AWS Distro for Fluent Bit logging
  - EKS/Fargate built-in Fluent Bit
- CloudWatch Container Insights to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices

aws

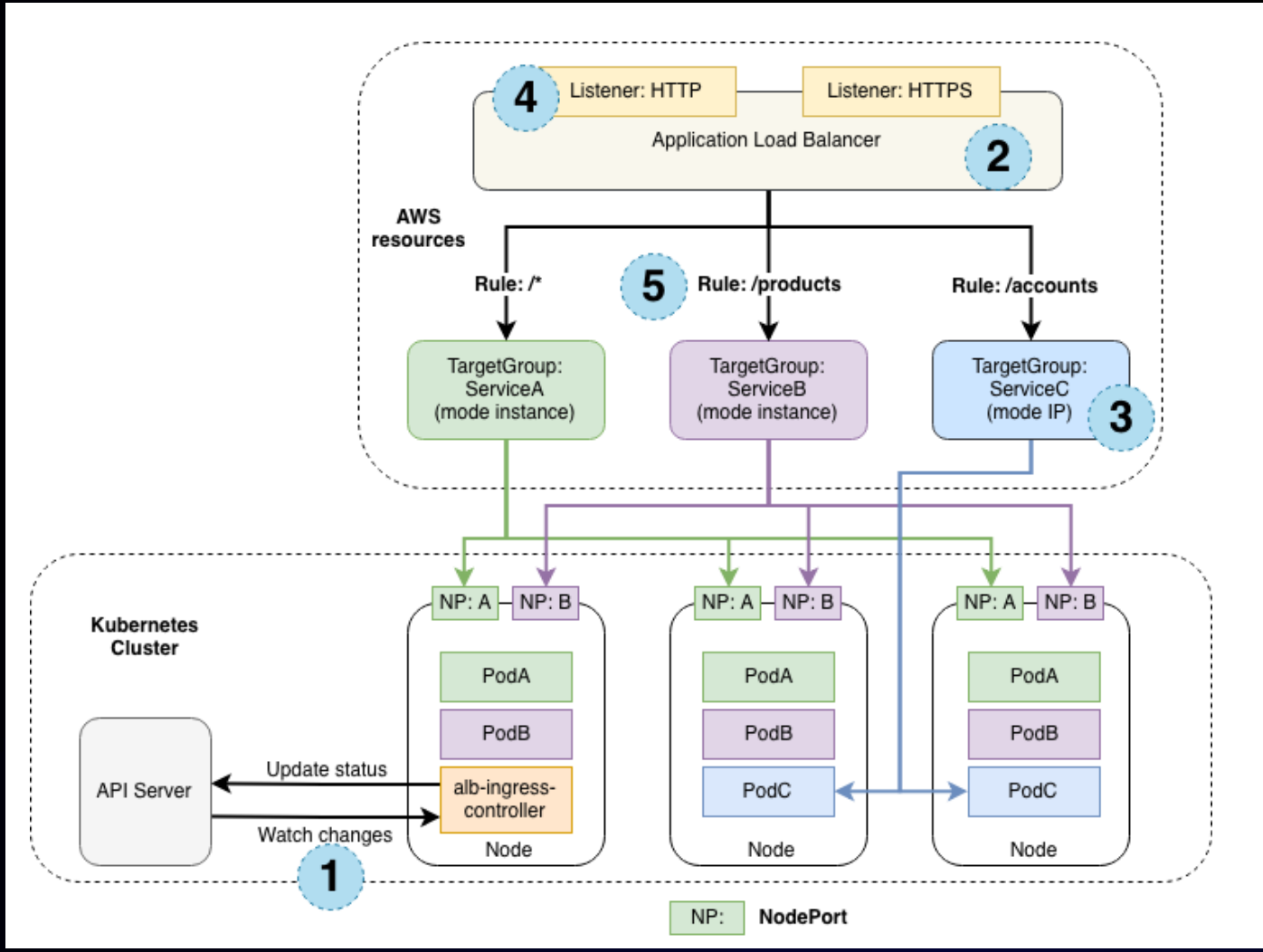
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How do I route external traffic to my cluster?

AWS Load Balancer Controller

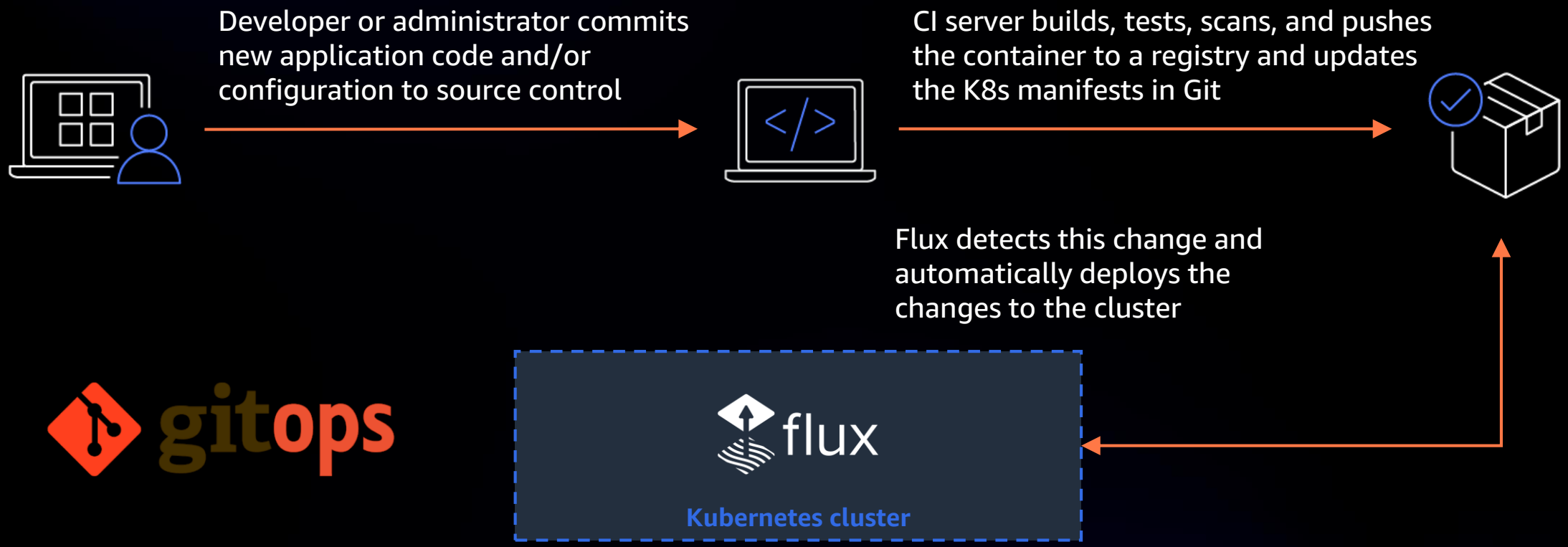
- Provision AWS Network Load Balancers in response to Kubernetes services
- Provision AWS Application Load Balancers (ALBs) in response to Kubernetes ingress
- Skip kube-proxy and route directly to pods with IP targeting and VPC CNI
- Group multiple Ingresses under a single ALB

Note: The in-tree Kubernetes service controller is deprecated



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

How do I ensure a fleet of clusters has a consistent set of configuration?



Note: eksctl now supports Flux v2

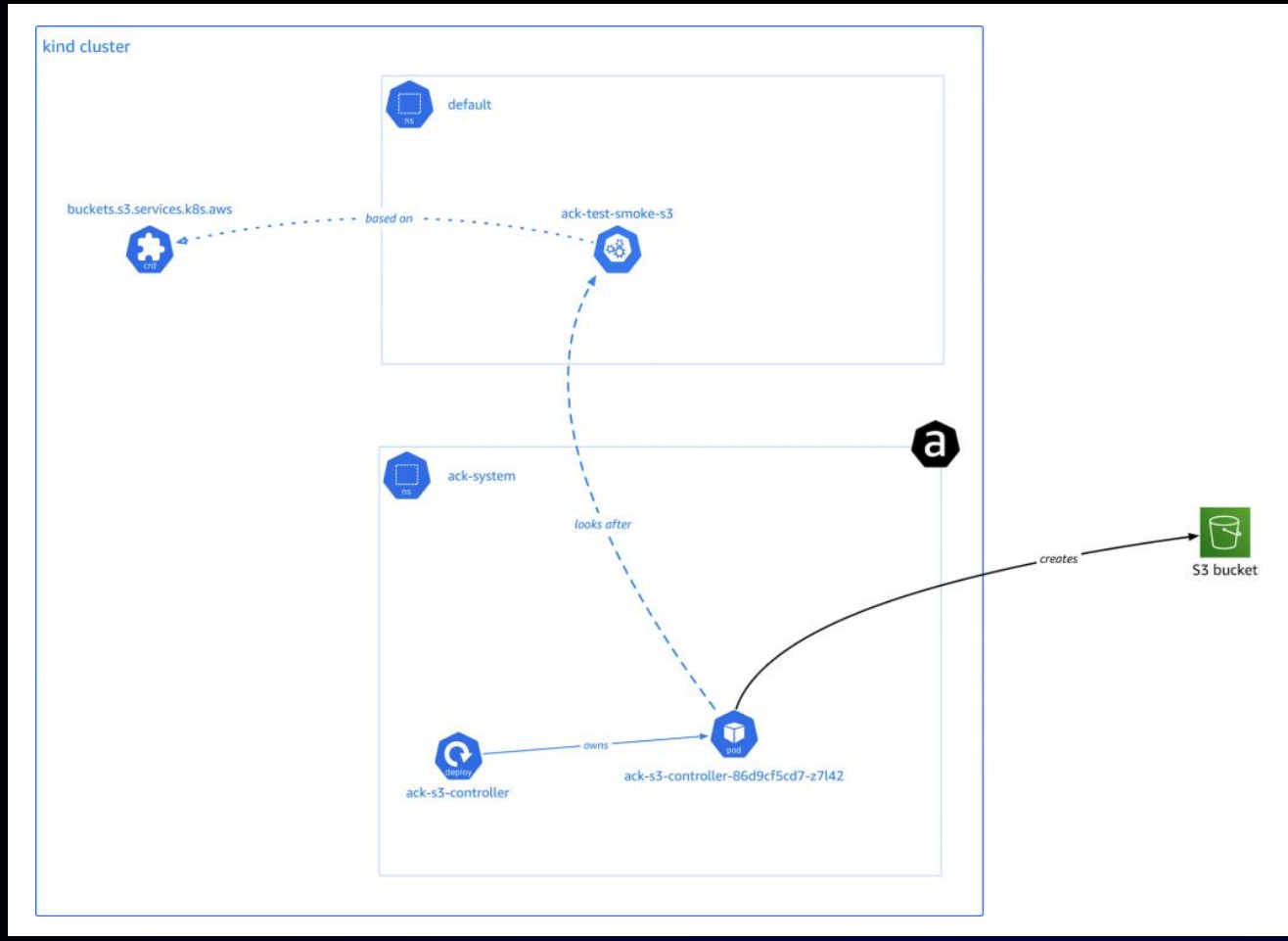
aws

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

How do I provision and access AWS services from Kubernetes workloads?

AWS Controllers for Kubernetes (ACK)

- Application developers create Kubernetes custom resources representing AWS services along their deployment manifests
- ACK service controller is then responsible for reconciling the desired AWS resources
- Controller code is automatically generated from AWS Go SDK, enabling fast support for new AWS service features

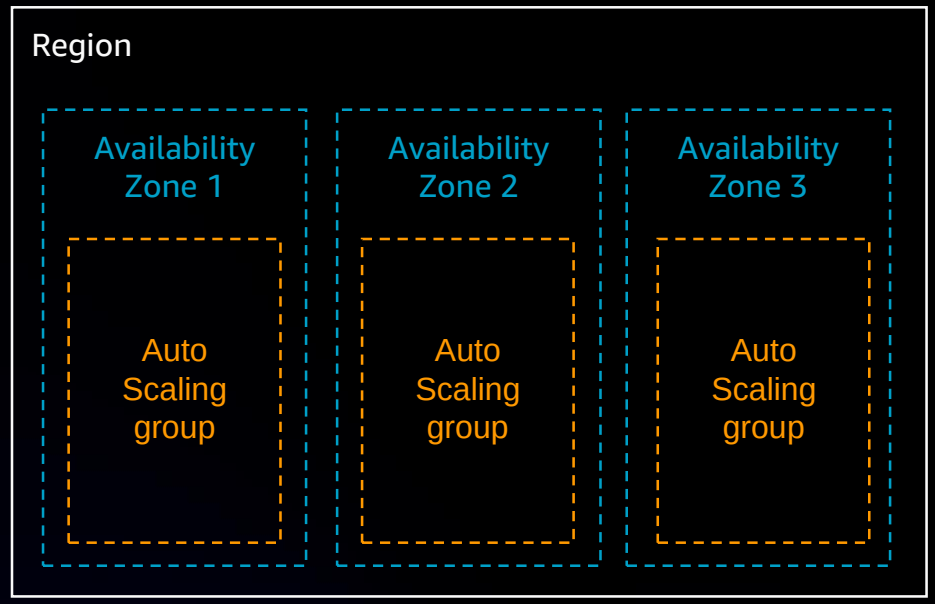


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How do I run stateful workloads in EKS?

- Amazon EBS CSI driver for high-performance use cases (ex. databases)
- Amazon EFS CSI driver for storage that needs to be shared across pods (ex. content management)
- Single-AZ Auto Scaling groups for workloads that require Amazon EBS volumes
- Dedicated node groups for stateful workloads – Disable Amazon EBS CSI tolerateAllTaints
- Lower max. Amazon EBS attachments per node, or use VPC CNI prefix assignment – to solve for ENI slot contention

Recommended Auto Scaling group setup for EBS stateful workloads



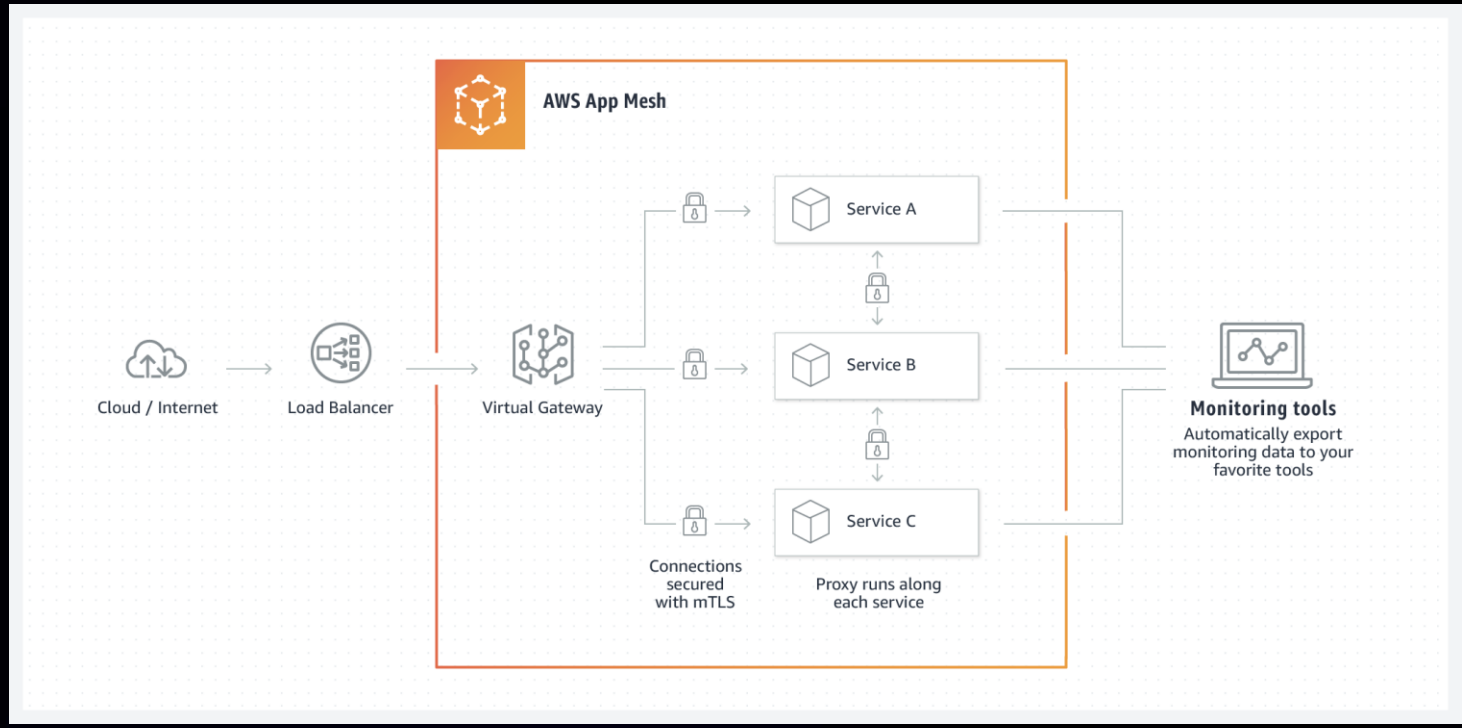
Recommendation: Use AWS managed services (through ACK) when possible

aws

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

How do I discover services running in other clusters?

- AWS Cloud Map Multi-Cluster Services Controller
- AWS App Mesh Kubernetes controller for fully managed service mesh
  - Encryption in transit
  - Traffic shaping
  - Canary deployments
  - Service discovery
  - Service authentication
  - Observability
- Bring your own service mesh



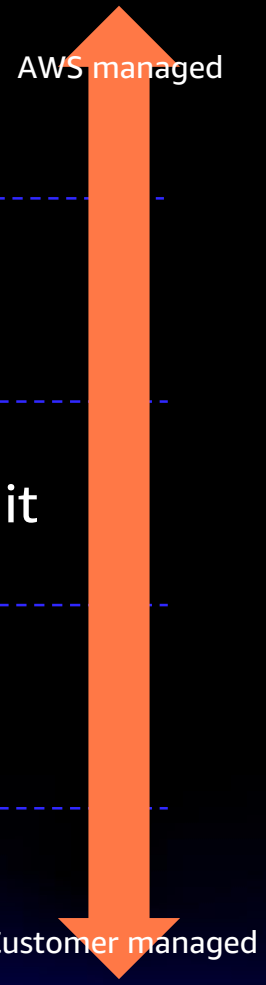
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Portability

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

How do I run consistent Kubernetes across environments?

Amazon **EKS** in AWS	Best, scale, performance & cost
Amazon **EKS** + AWS **Local Zones**	Fully managed, latency optimized
Amazon **EKS** + 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

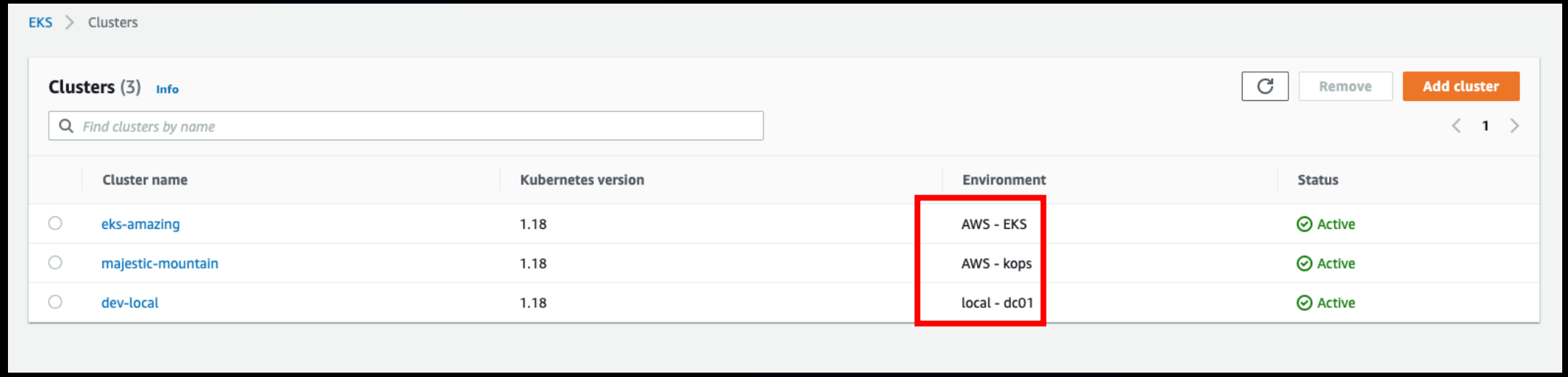


aws

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

How can I see all my clusters in one place?

The Amazon EKS console provides you a unified view and operational visibility across all your Kubernetes environments



EKS Connector allows you to connect any conformant Kubernetes cluster to AWS and visualize it in the Amazon EKS console

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

Wrap up

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

Where can I learn more?

EKS Best Practices Guide

- Open-sourced best practices guide
- Check back often for new chapters

aws.github.io/aws-eks-best-practices

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

Where can I give feedback and submit feature requests?

Containers roadmap

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

tinyurl.com/3bp4tnzn



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

Thank you!

Mike Stefaniak

@mikestef9

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