



Containers on *AWS*



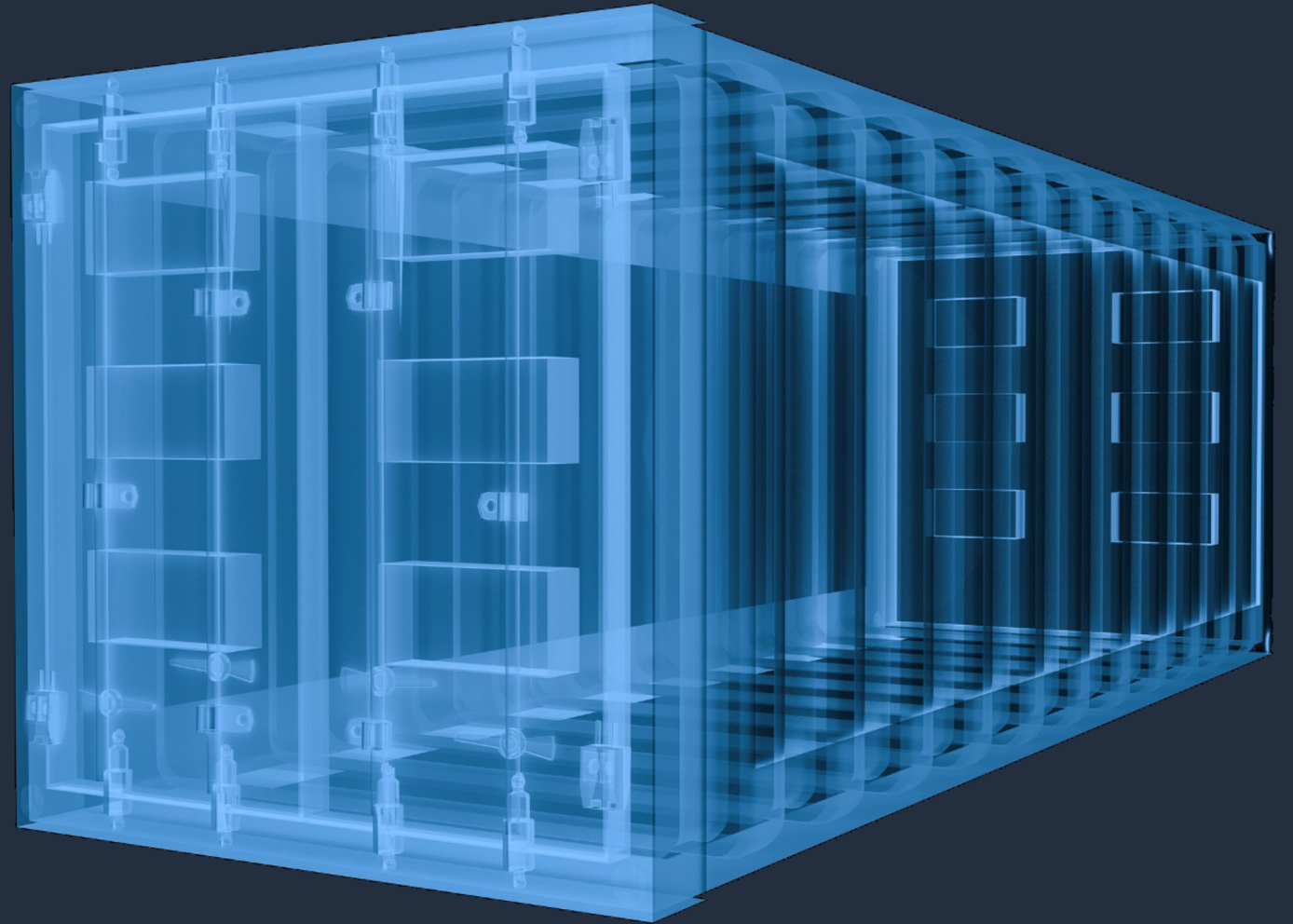
Agenda

- Containerization with Docker
- ECR (Elastic Container Registry)
- ECS (Elastic Container Service)
- AWS Fargate
- EKS (Elastic Kubernetes Service)

Containerization with Docker

First things first...

What are containers and why are customers using them?



Why are companies adopting containers?

- Accelerate software development
- Build modern applications
- Automate operations at web scale

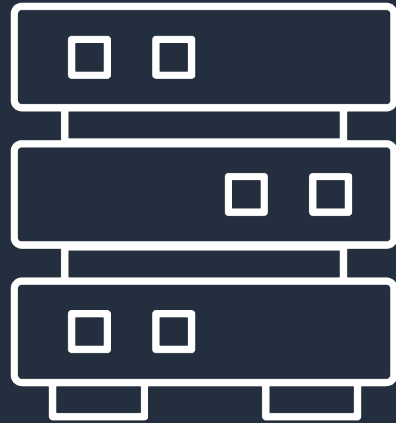
Application environment components



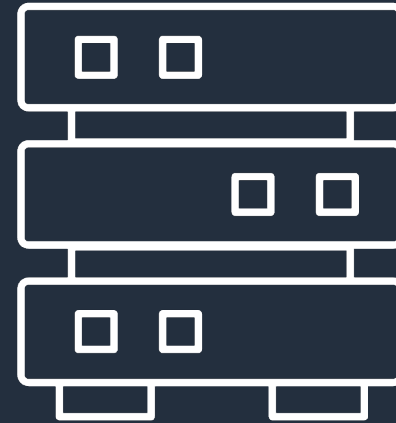
Different environments



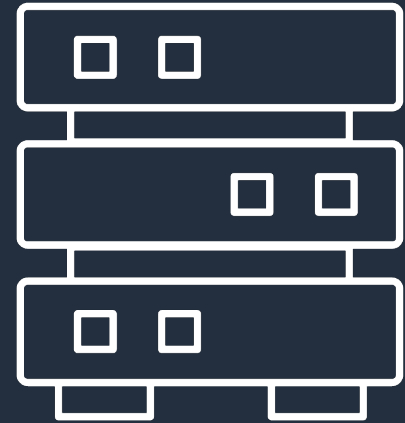
Local Laptop



Staging / QA

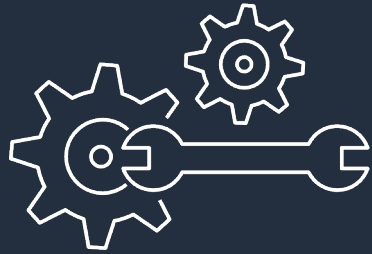


Production



On-Prem

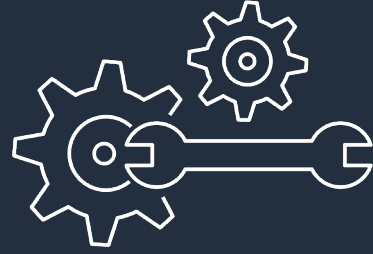
It worked on my machine, why not in prod?



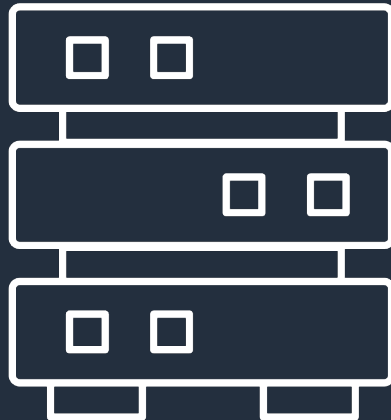
v6.0.0



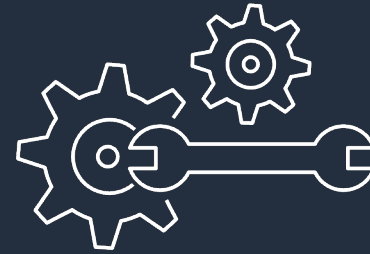
Local Laptop



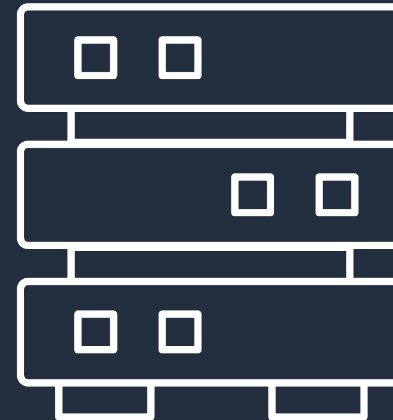
v7.0.0



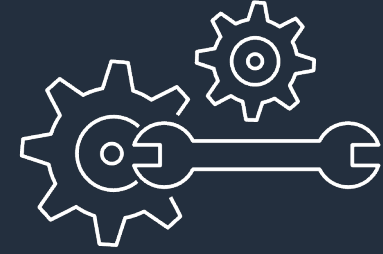
Staging / QA



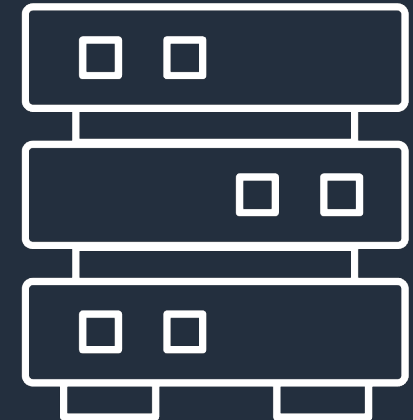
v4.0.0



Production



v7.0.0



On-Prem

Containers to the rescue

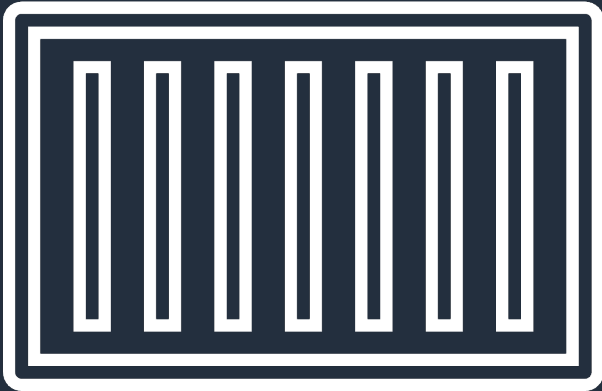
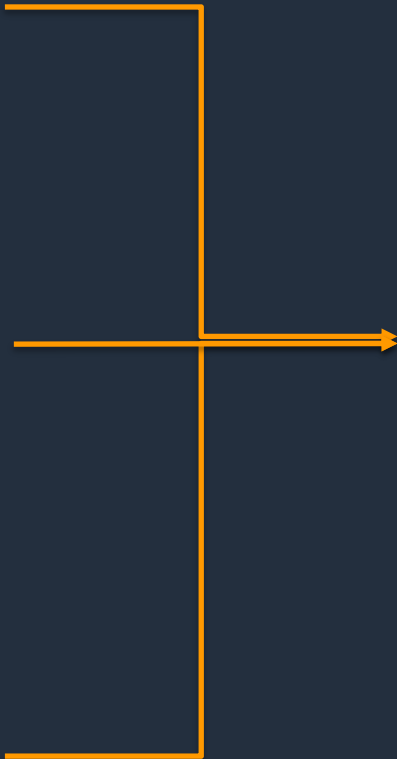
Runtime Engine



Dependencies



Code



What is Docker?

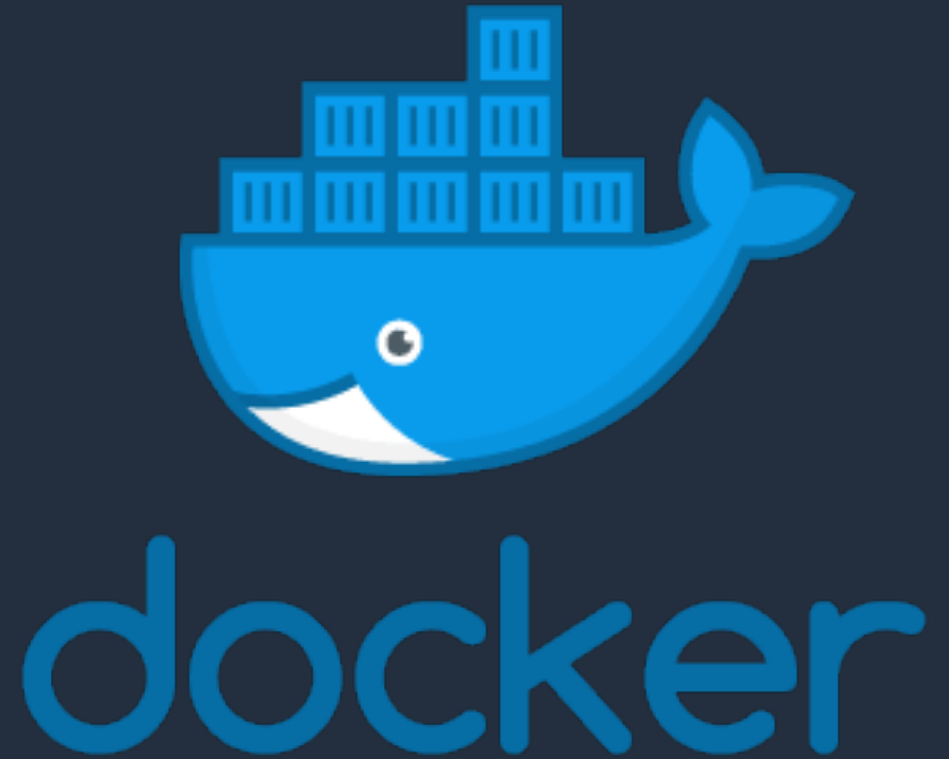
Lightweight container virtualization platform.

Ecosystem of tools to manage and deploy your applications

Licensed under the Apache 2.0 license.

Built by Docker, Inc.

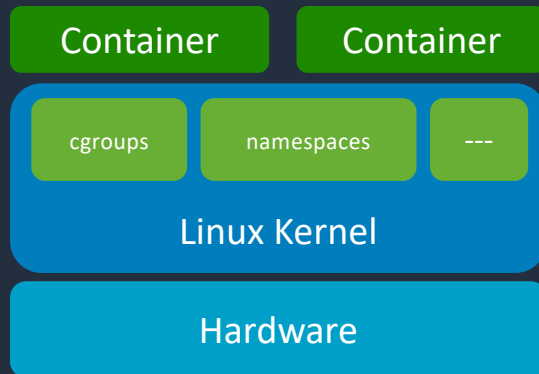
Moby: Open source project



Containers vs VMs

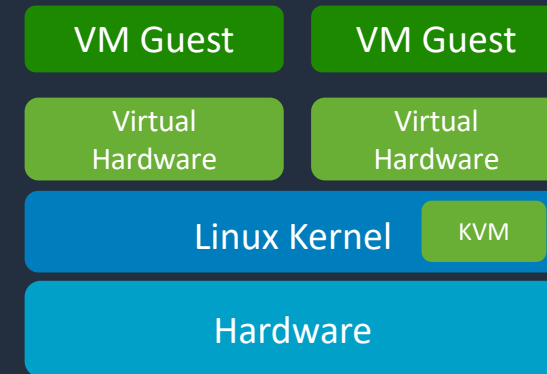
Containers

- Using Linux primitives for isolation
- Share Linux Kernel
- Fast starts, minimal overhead
- Flexible isolation



Virtual Machines

- Virtualisation or emulate hardware components
- Completely separate kernels (maybe not Linux)
- Slower starts, must boot kernel and set-up hardware.

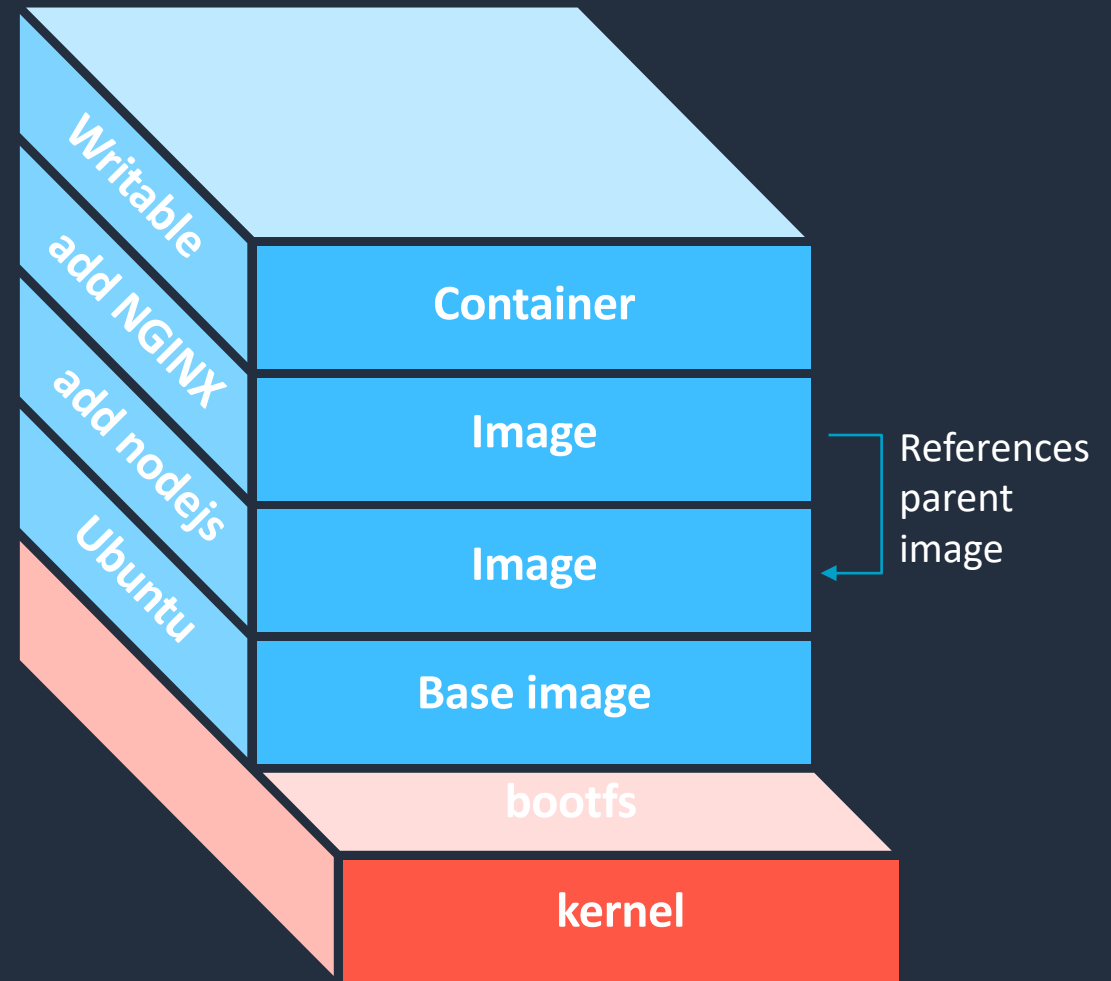


Container images

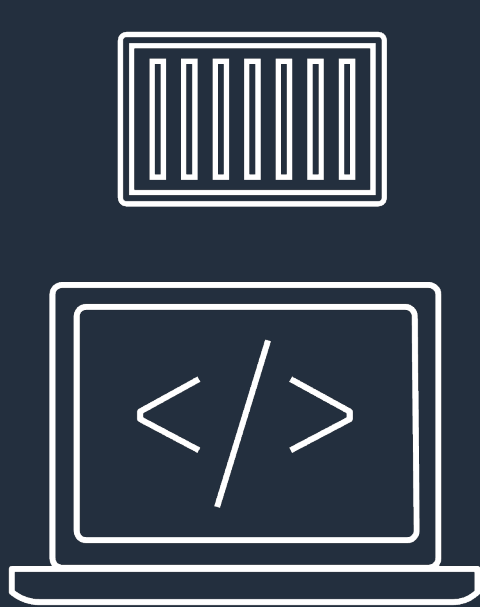
Read only image that is used as a template to launch a container.

Start from base images that have your dependencies, add your custom code.

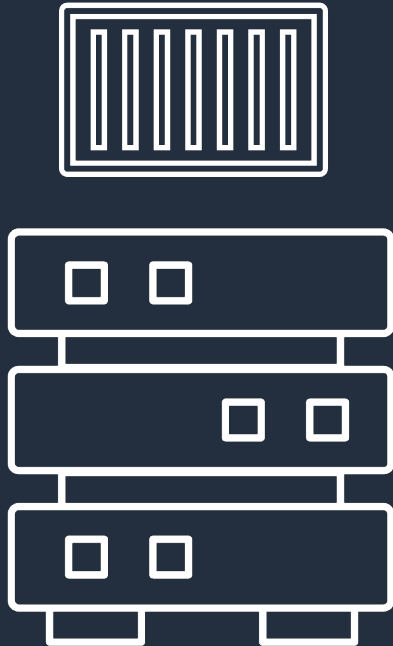
Dockerfile for easy, reproducible builds.



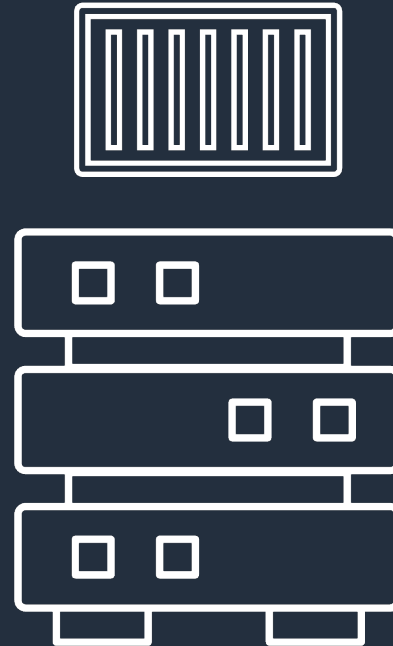
Four environments, same container



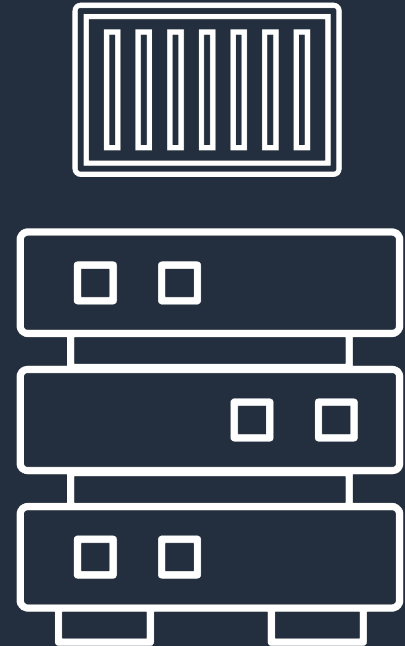
Local Laptop



Staging / QA



Production



On-Prem

Container benefits



Runs reliably everywhere



Run different apps simultaneously



Better resource utilization



Amazon Elastic Container Registry

What is Amazon ECR

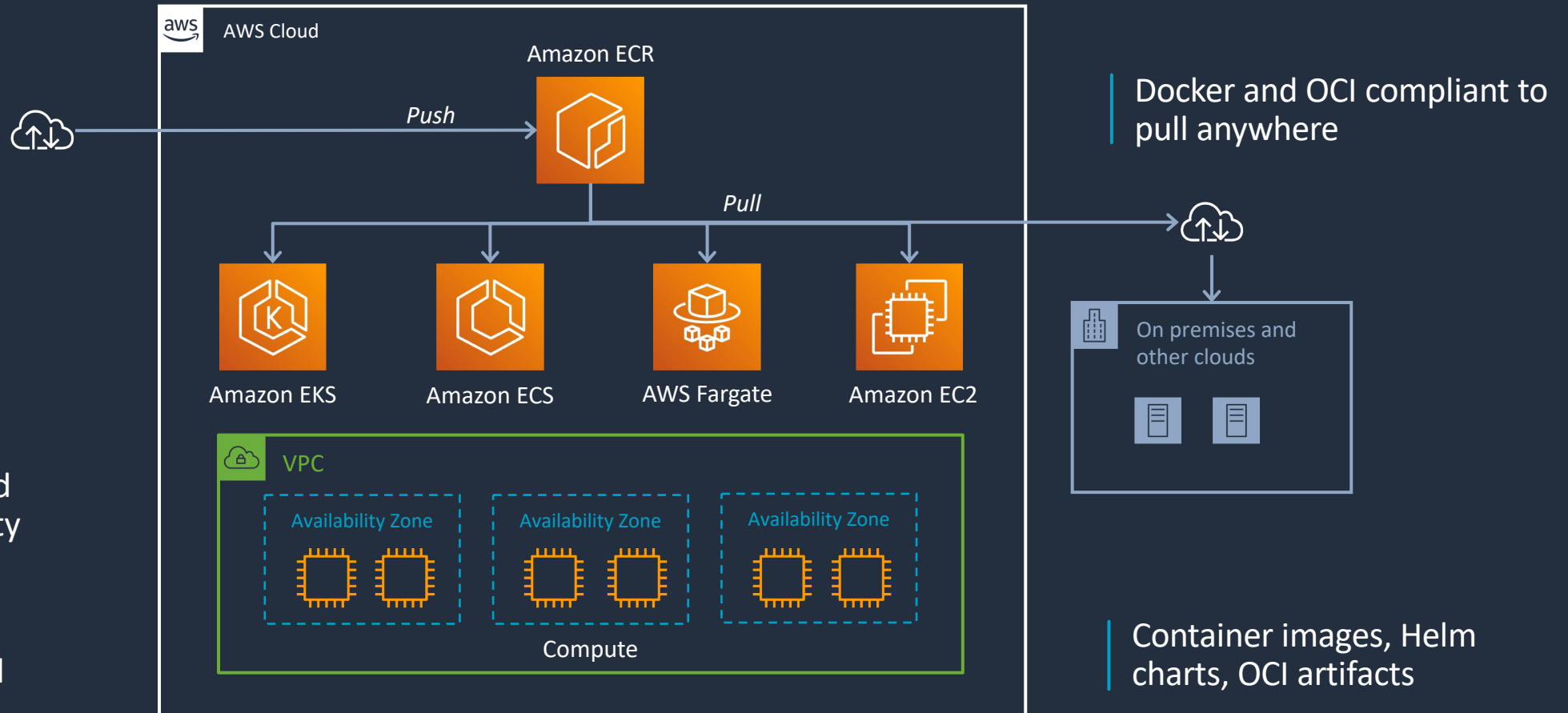
FULLY-MANAGED CONTAINER ARTIFACT REGISTRY

Managed and scalable infrastructure

Highly available, high performance

Security with encrypted images and vulnerability scans

Authenticated access, centralized IAM control



Native integration to AWS orchestrators and compute

Amazon ECR pricing



You only pay for the amount of data you store, and data transferred to the internet. Storage is **\$0.10** per GB-month beyond free tier.



50 GB-month of always-free storage for your public repositories, and **free tier** includes 500 MB-month of storage for one year for your private repositories.



You can transfer 500 GB-month of data to the internet for free from a public repository anonymously, and 5 TB-month with an AWS account.

Container Images: Image scanning

https://205094881157.dkr.ecr.us-west-2.amazonaws.com



Amazon ECR

team-a/web-app



Amazon
EventBridge

My app
image

Overview

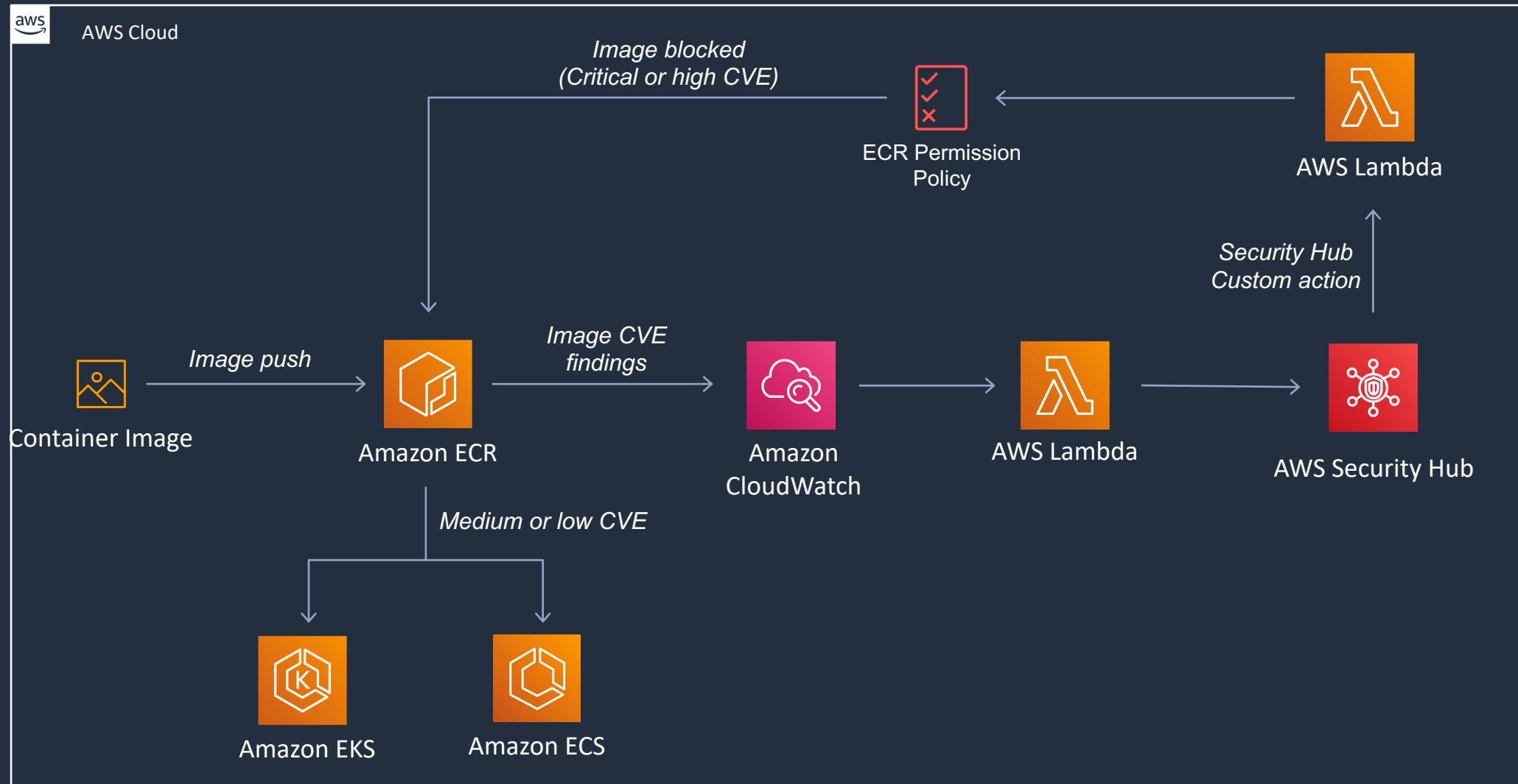
Critical	High	Medium	Low	Informational	Undefined
0	0	4	19	7	0

Vulnerabilities (30)

Find vulnerabilities

Name	Package	Severity	Description
CVE-2016-9085	libwebp:0.6.1-2	MEDIUM	Multiple integer overflows in libwebp allows attackers to have unspecified impact via unknown vectors.
CVE-2020-11724	nginx:1.18.0-Oubuntu1	MEDIUM	An issue was discovered in OpenResty before 1.15.8.4. ngx_http_lua_subrequest.c allows HTTP request smuggling, as demonstrated by the ngx.location.capture API.
			An out-of-bounds read was addressed with improved

Container Images: Automate compliance with image scanning



Amazon ECR Public



registry-alias/web-app

https://gallery.ecr.aws

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "ECR Public Repository Policy",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/username"
      },
      "Action": [
        "ecr-public:DescribeImages",
        "ecr-public:DescribeRepositories"
      ]
    }
  ]
}
```

aws Amazon ECR Public Gallery

Amazon ECR Public Gallery

Share and deploy container images, publicly and privately

Filters [Clear all](#)

Verification [Info](#)

☐ Verified account

Operating Systems

☐ Linux

☐ Windows

Architectures

☐ ARM


☐ ARM 64

☐ x86

☐ x86-64

Repositories

Showing 1 - 20 results (of 45482)



cloudwatch-agent


by [Amazon Cloudwatch Agent](#) Verified account

Registry alias: cloudwatch-agent

976M+ Downloads

Amazon Cloudwatch Agent

Linux x86-64 ARM 64



aws-xray-daemon

by [AWS X-Ray](#) Verified account

Registry alias: xray

Managing many containers is hard





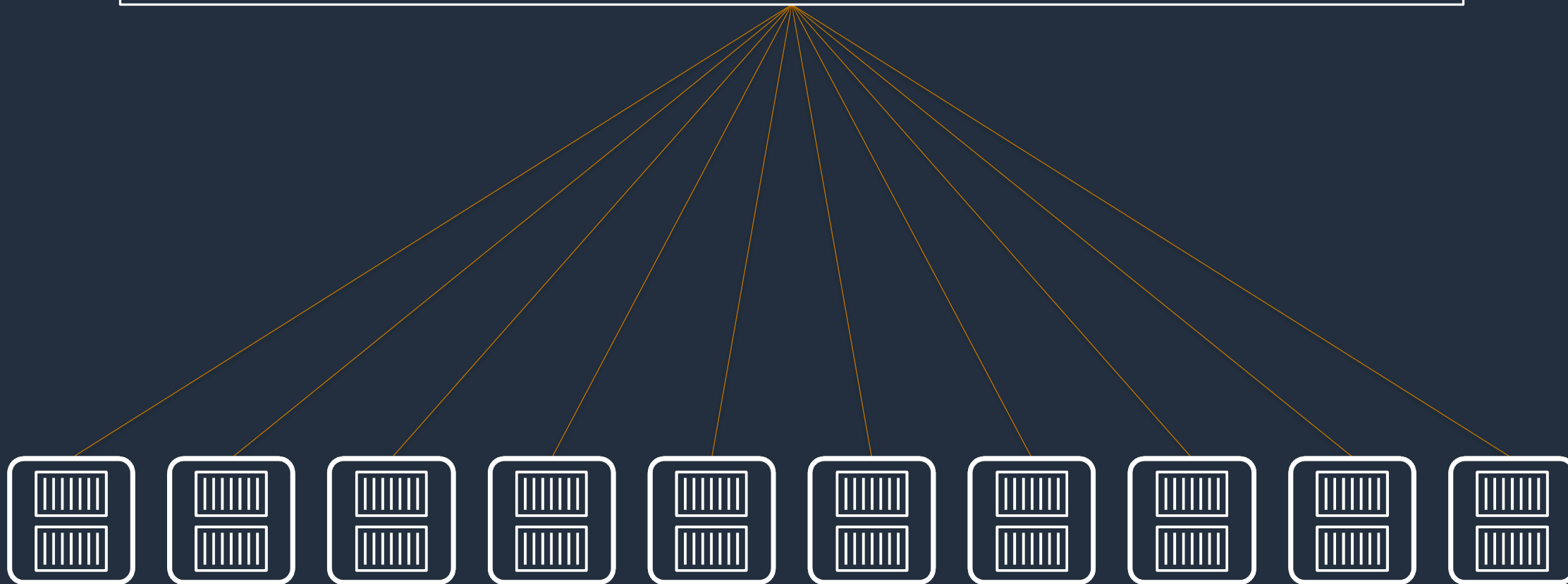
Amazon Elastic Container Service



Scheduling and Orchestration

Cluster Manager

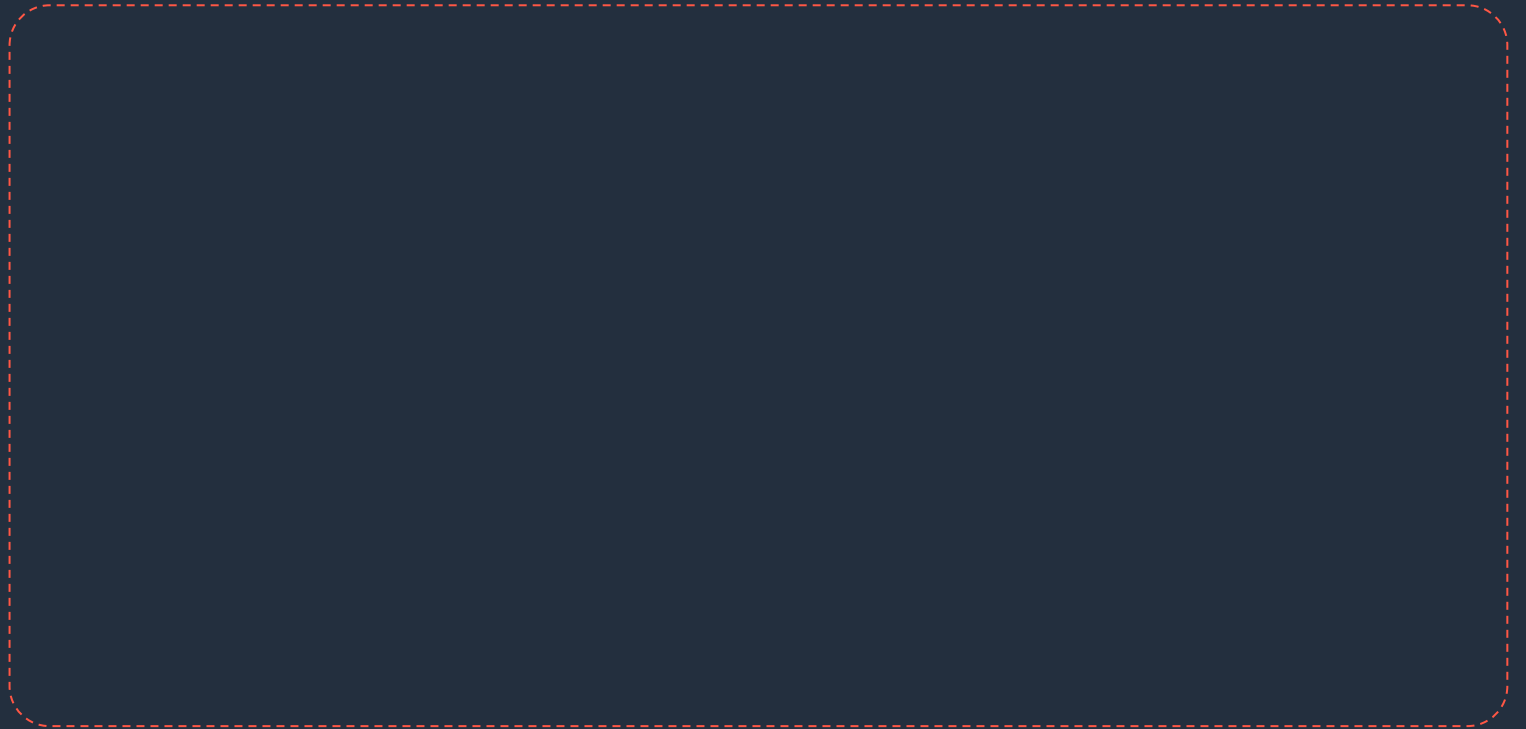
Placement Engine



Amazon ECS constructs

Cluster

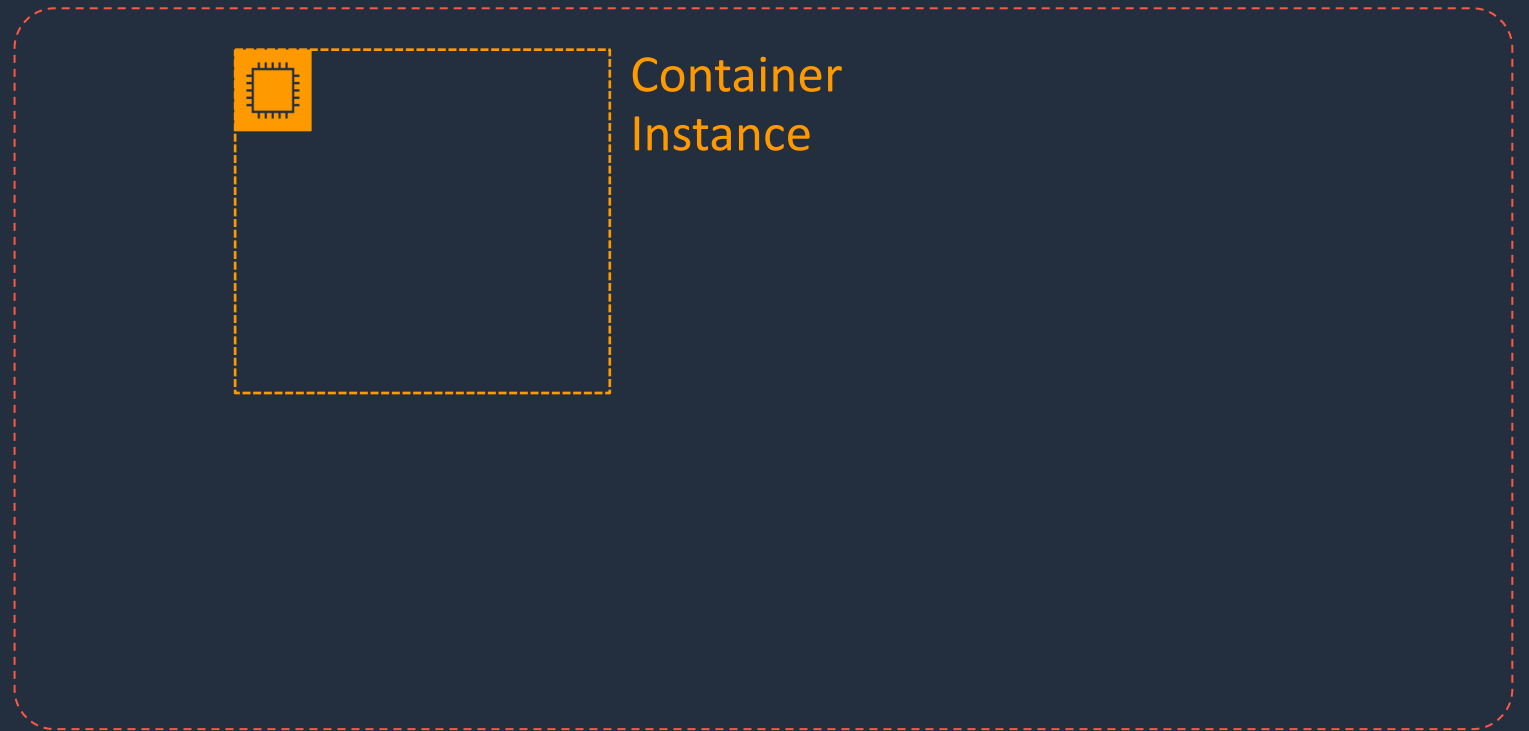
- Resource grouping and isolation
- IAM permissions boundary



Amazon ECS constructs

Cluster

- Resource grouping and isolation
- IAM permissions boundary



Amazon ECS constructs

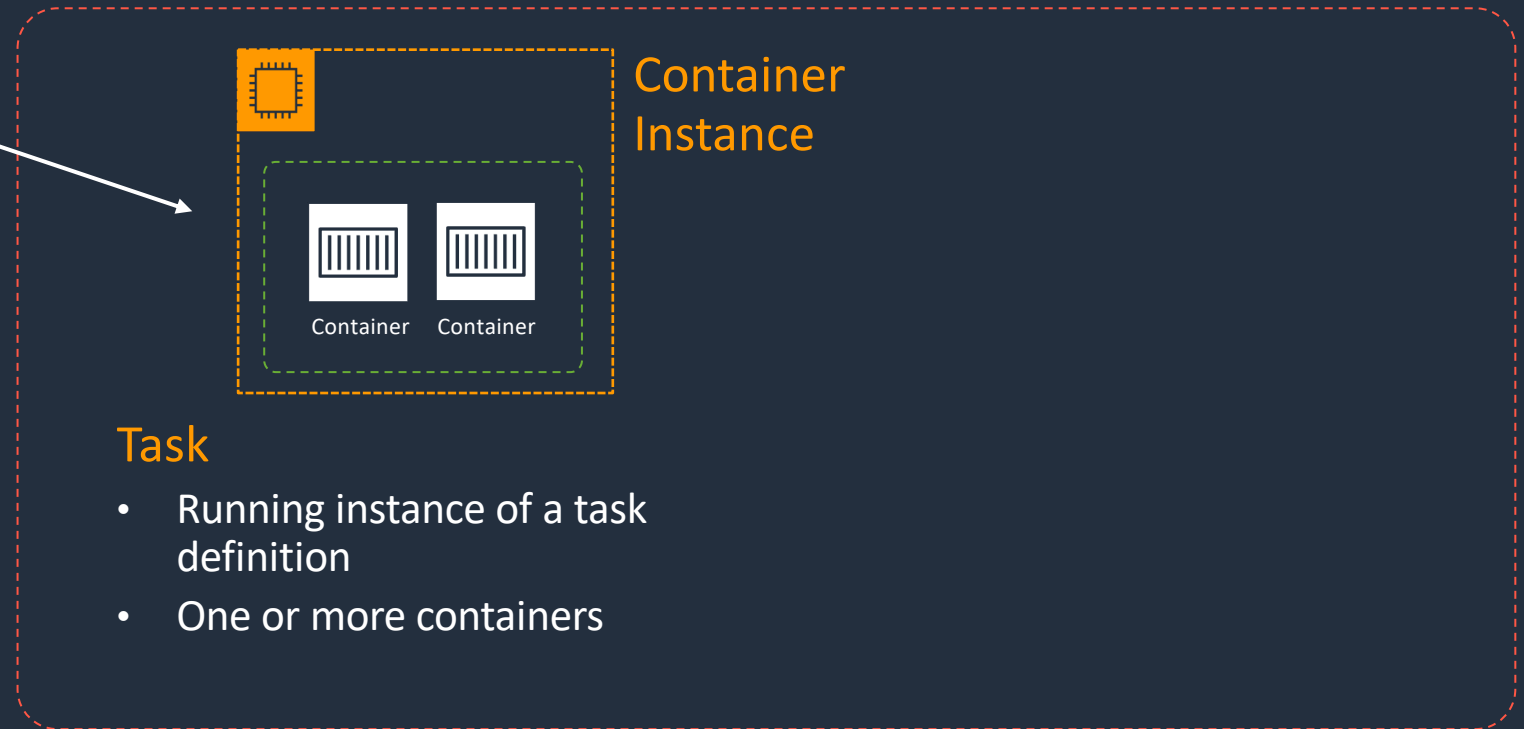


Task definition

- Template used by Amazon ECS to launch tasks
- Parallels to docker run parameters
- Defines requirements:
 - CPU/Memory
 - Container image(s)
 - Logging
 - IAM role
 - Etc.

Cluster

- Resource grouping and isolation
- IAM permissions boundary



Task

- Running instance of a task definition
- One or more containers

Amazon ECS constructs

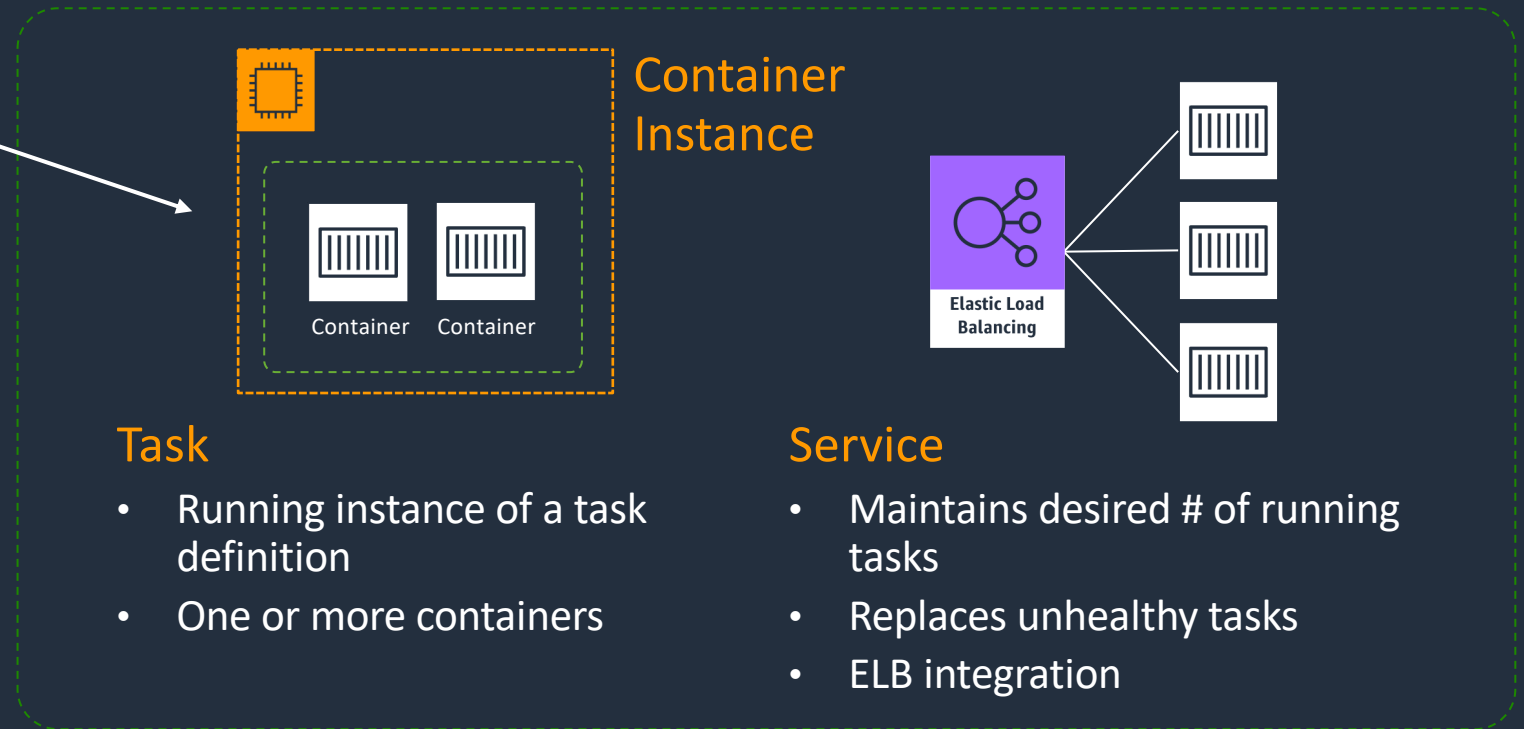


Task definition

- Template used by Amazon ECS to launch tasks
- Parallels to docker run parameters
- Defines requirements:
 - CPU/Memory
 - Container image(s)
 - Logging
 - IAM role
 - Etc.

Cluster

- Resource grouping and isolation
- IAM permissions boundary



Task

- Running instance of a task definition
- One or more containers

Container Instance

Service

- Maintains desired # of running tasks
- Replaces unhealthy tasks
- ELB integration

Deploying on ECS: Tasks vs Services

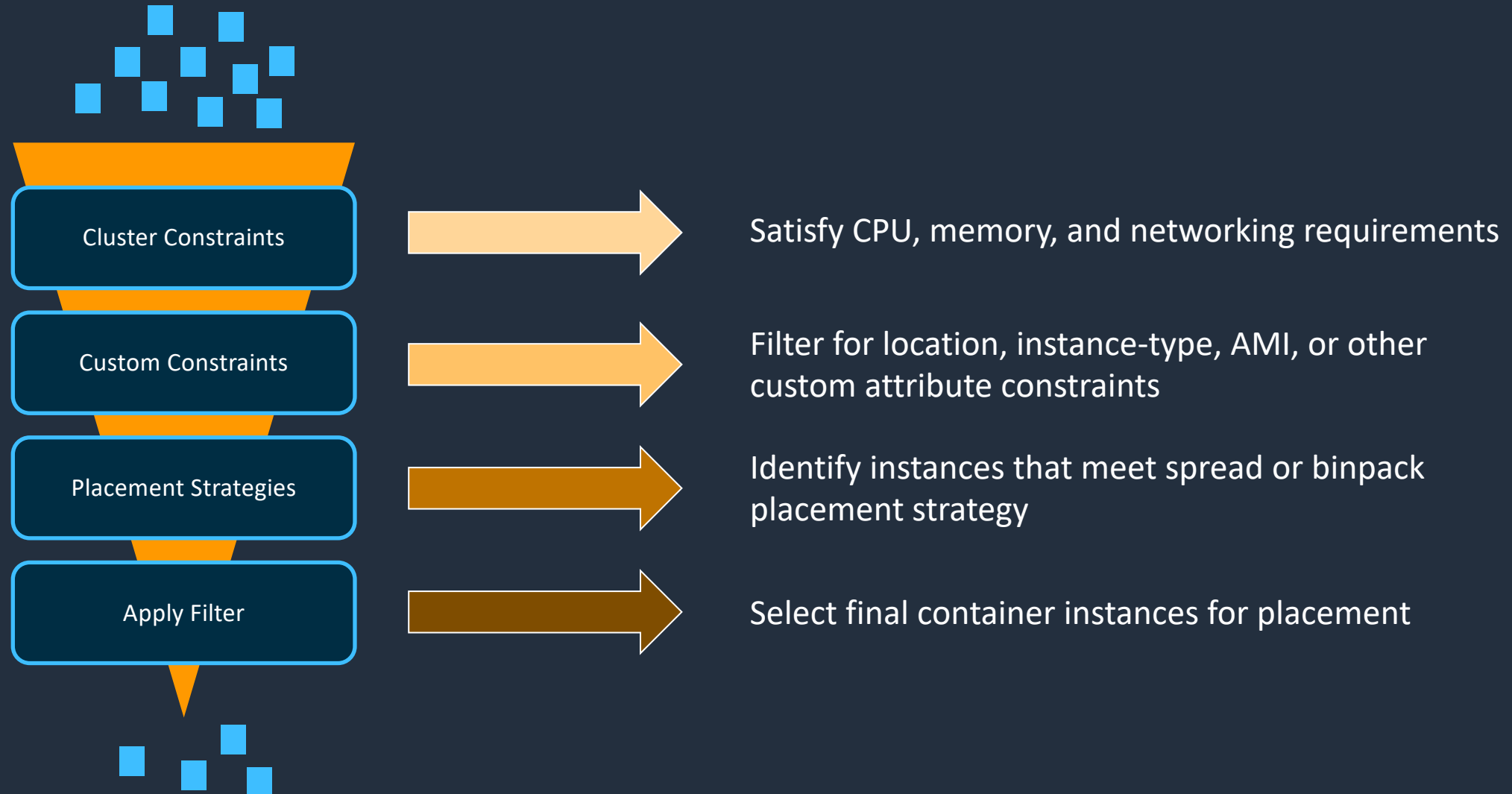
On-Demand Workloads

ECS task scheduler
Run once or at intervals
Batch jobs
RunTask API
StartTask (custom)

Long-Running Apps

ECS service scheduler
Health management
Scale-up and scale-down
AZ aware
Grouped containers

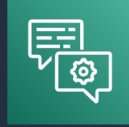
Task placement



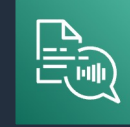
Amazon ECS powers Amazon



Amazon
SageMaker



Amazon
Lex



Amazon
Polly



AWS
Batch

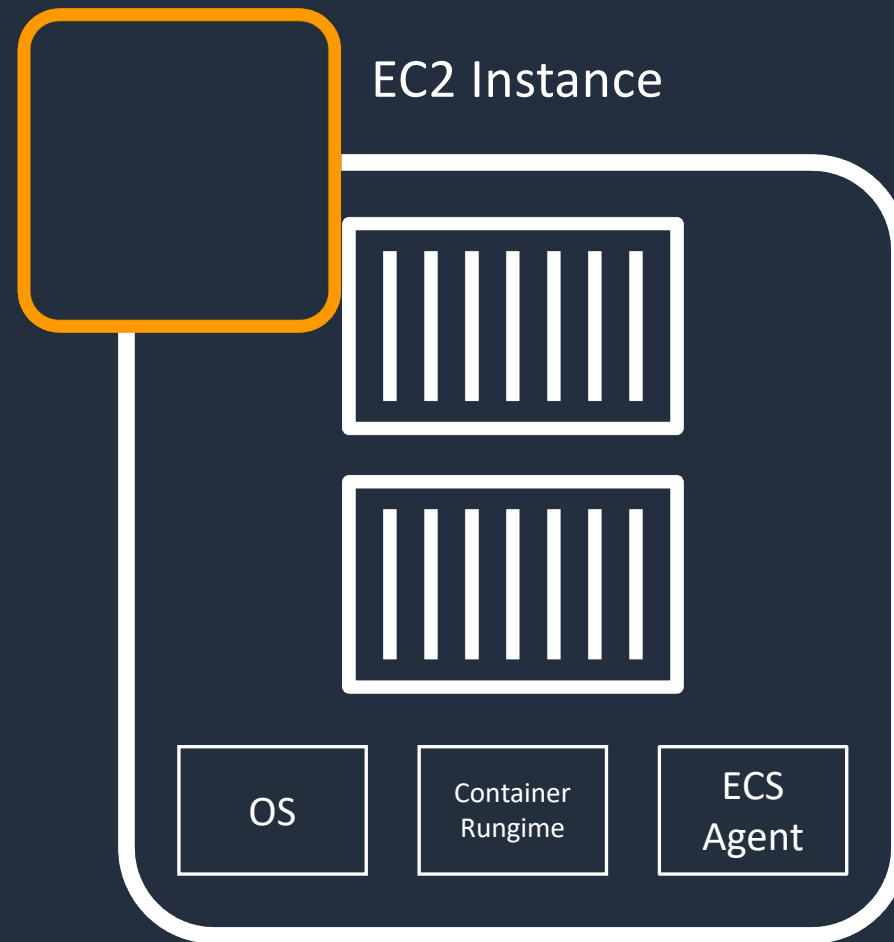
Amazon ECS forms the building blocks
for various services at Amazon

Built for security, reliability, availability, and scale

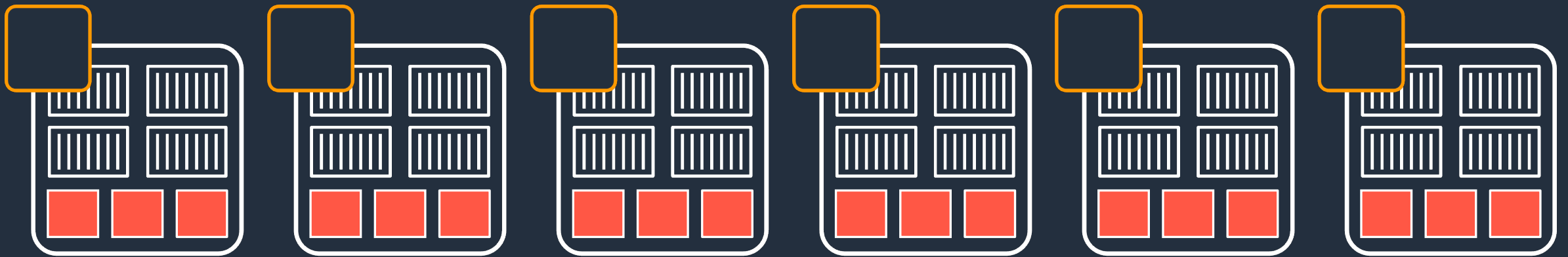


AWS Fargate

Without Fargate, you end up managing more than just containers

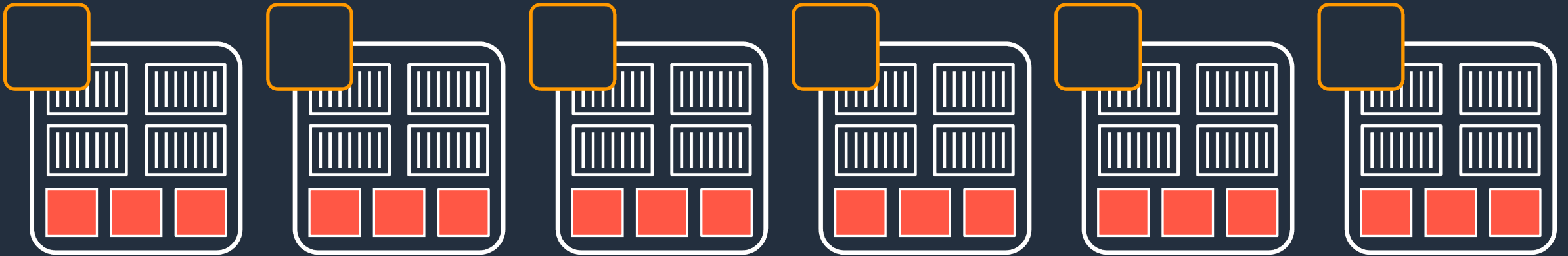


- Patching and Upgrading OS, agents, etc.
- Scaling the instance fleet for optimal utilization



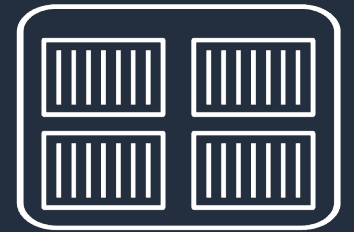
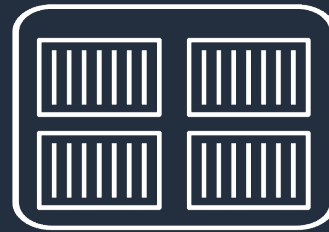
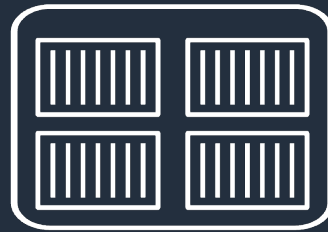
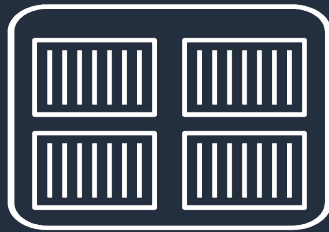
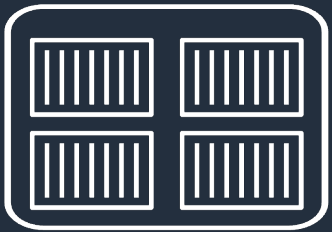


Amazon Elastic Container Service





Amazon Elastic Container Service



AWS Fargate
run serverless containers

Amazon ECS on AWS Fargate

Operating systems supported

- Amazon Linux 2 (**ARM64** and **X86_64**)
- Microsoft Windows Server:
 - 2019 Full (**X86_64**)
 - 2019 Core (**X86_64**)
 - 2022 Full (**X86_64**)
 - 2022 Core (**X86_64**)





**Your containerized
applications**

Managed by AWS

No EC2 Instances to provision, scale or manage

Elastic

Scale up & down seamlessly. Pay only for what you use

Integrated

With the AWS ecosystem: VPC Networking, Elastic Load Balancing, IAM Permissions, CloudWatch and more

Enterprise Grade



Payment Card Industry (PCI)
Security Standard



DOD Cloud Security Req's Guide
(SRG)



FedRAMP Moderate and
High (GovCloud)



Criminal Justice Information
Service Security Policy (CJIS)



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



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



Federal Information Processing Standard
Pub (FIPS) 140-2



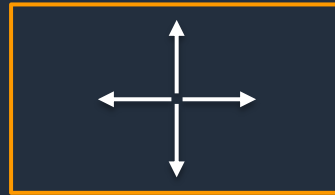
Health Information Trust Alliance
Common
Security Framework

Kubernetes

What is Kubernetes?



**Open source container
management platform**



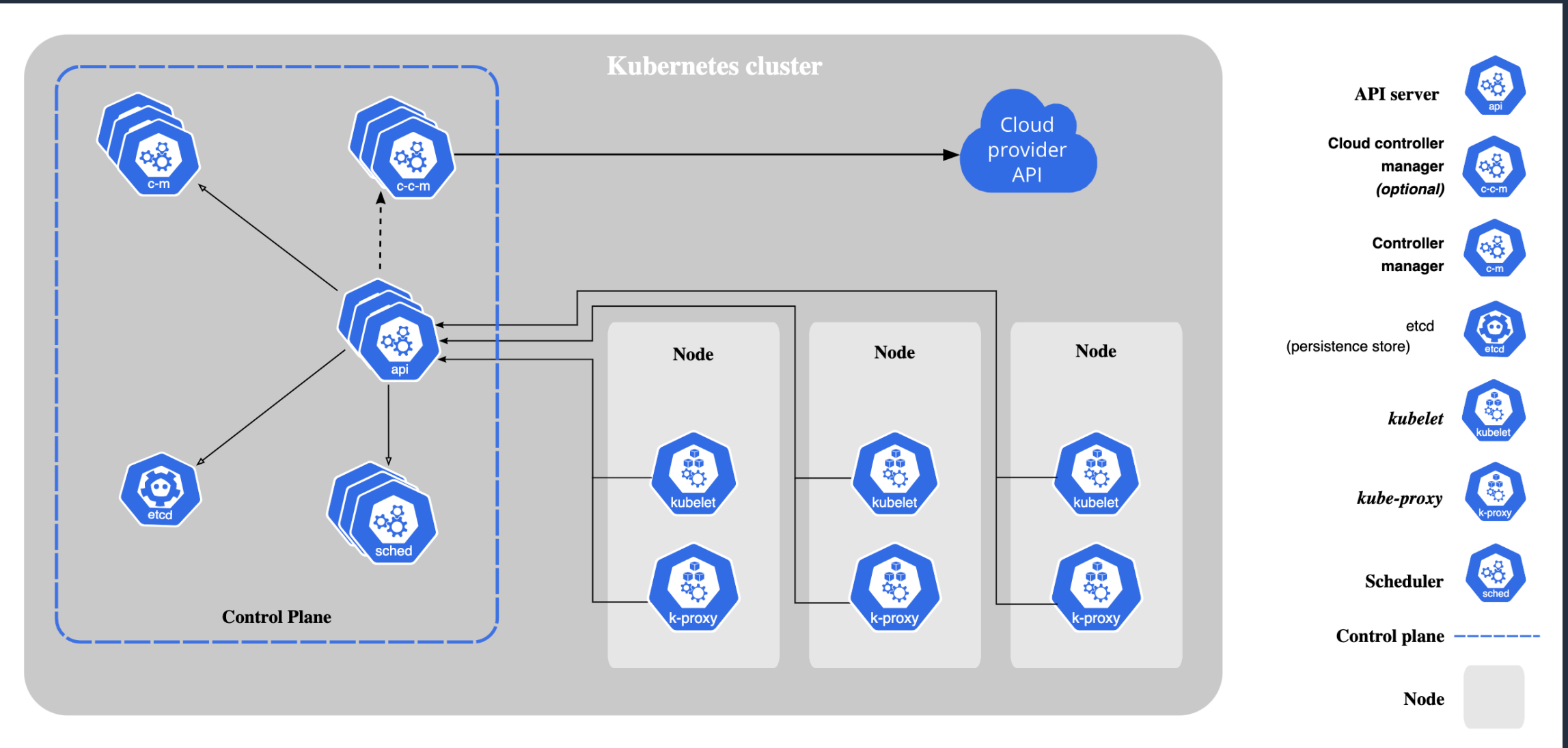
**Helps you run
containers at scale**



**Gives you primitives
for building
modern applications**

<https://kubernetes.io/docs/tutorials/kubernetes-basics/>

Kubernetes basic architecture



Amazon EKS

What is Amazon EKS?



Amazon EKS



Amazon EKS runs vanilla Kubernetes; EKS is upstream and a certified conformant version of Kubernetes (with backported security fixes)



Amazon EKS supports 4 versions of Kubernetes, giving you 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

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

Amazon EKS Control Plane Architecture

Survive single-AZ events

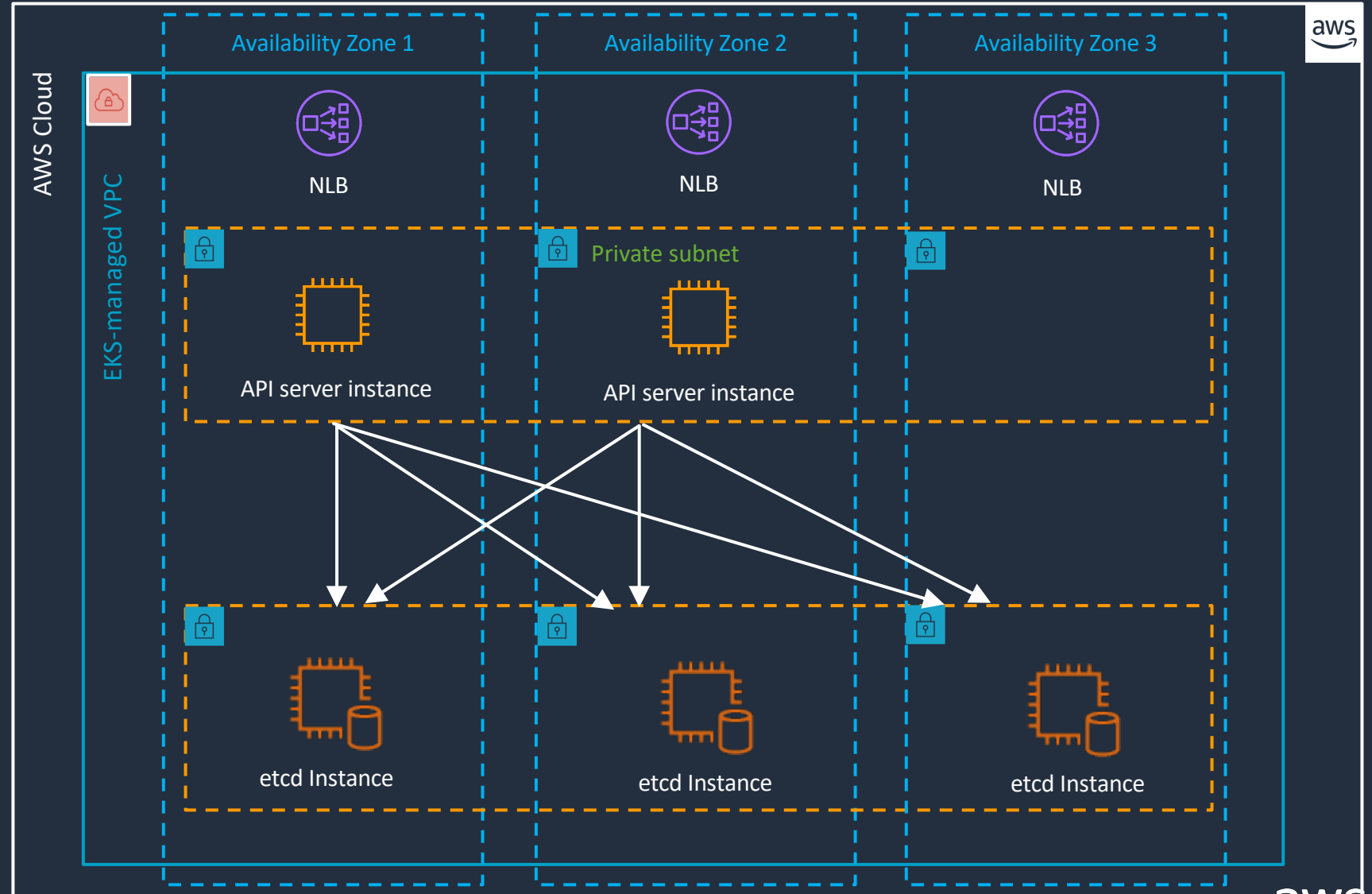
Highly available cluster endpoint

99.95% SLA

24x7x365 support

Automatic Resizing

Increased the volume throughput 6x

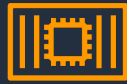


Amazon EKS Runtime Overview

Administrator deploys
Pod



Kubernetes schedules
the pod



Amazon EKS supports running containers on EC2 instances or on AWS Fargate. Clusters can run containers on a single runtime or multiple runtimes at the same time.



Amazon EC2

Run containers on EC2 instances within your account that you manage and configure.



AWS Fargate

A fully managed container environment with no infrastructure management.