AWS re:Invent

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

CON315

Enabling new workloads on AWS Fargate

Saloni Sonpal
Senior Product Manager, Fargate
AWS

Re Alvarez Parmar
Principal Containers Specialist
AWS

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

Today’s discussion

- AWS Fargate benefits
- Recent Fargate customer highlights
- What we shipped in the last year
- Roadmap ahead
- Q&A



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

AWS Fargate refresher

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

Introducing Fargate



Fargate is a serverless compute engine for containers



Managed by AWS, no AMIs to maintain, no EC2 instances to provision, scale, or manage – pay for what you need

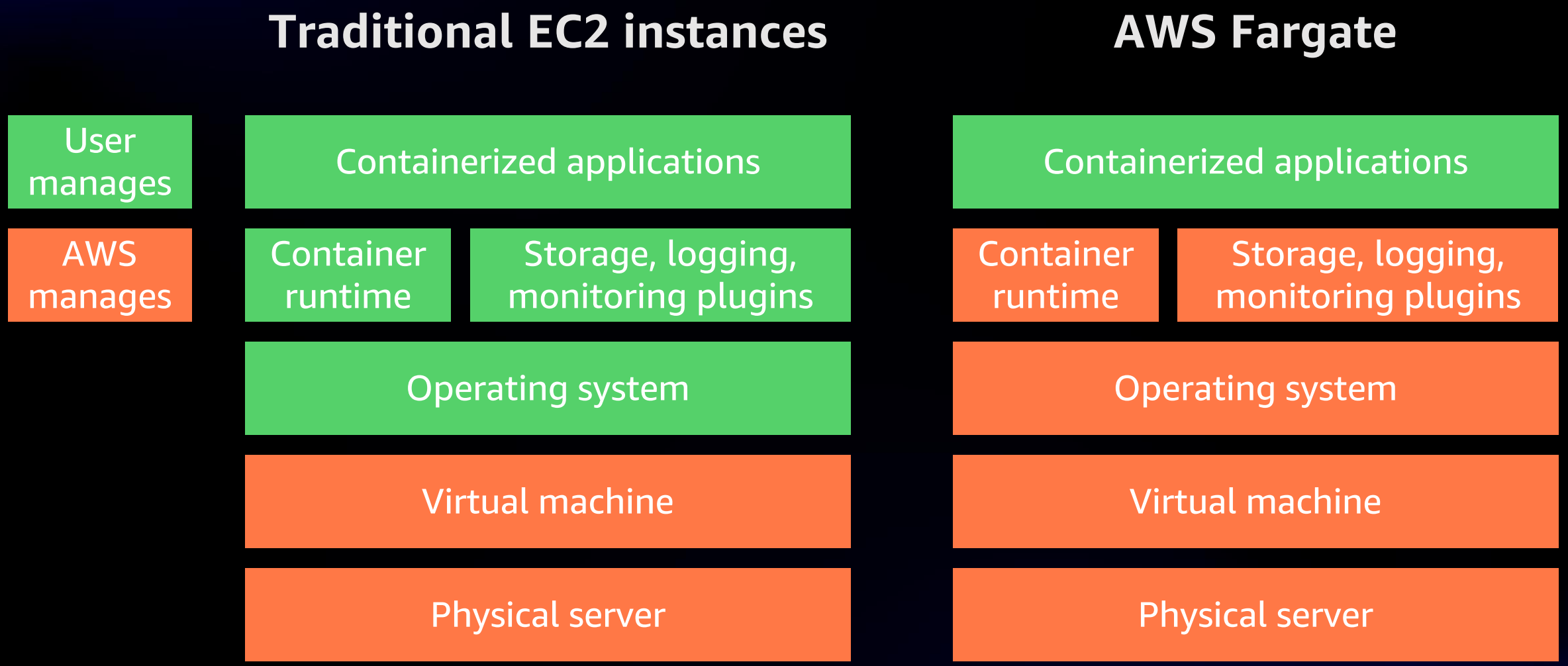


Fargate is where your containers will run – customers don't interact with it directly

aws

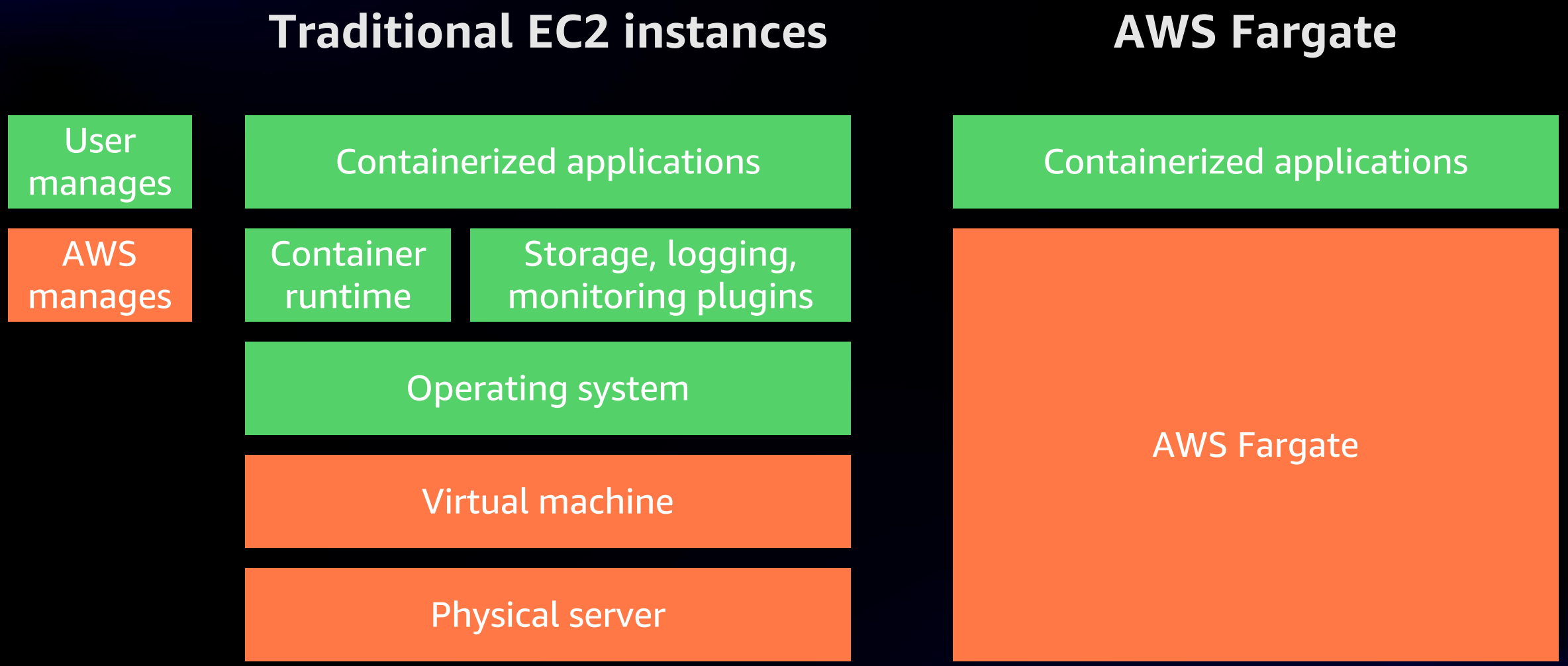
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sharing responsibilities in a managed service model



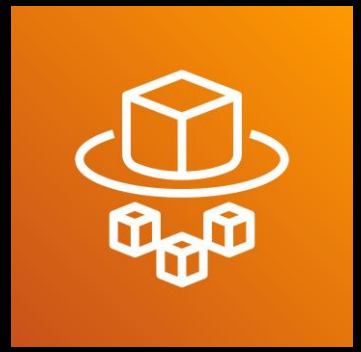
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sharing responsibilities in a managed service model



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

Benefits of Fargate



Serverless

Managed by AWS; no EC2 instances to provision, scale, or manage – simple operations model

Secure by default

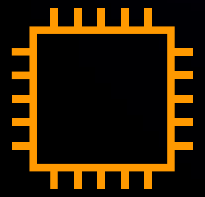
Isolated, patched, and compliant for running the most sensitive workloads

Savings

Elastic on-demand pricing model with granular resource allocations giving you the ability to procure only the vCPU and memory needed when you need it without any excess

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

Security model



Hardware virtualization

Tasks get isolated compute



Network isolation

Tasks get dedicated ENIs



Storage isolation

Tasks get dedicated storage



Credentials isolation

Tasks get credentials scoped to applications



Hands-off patching

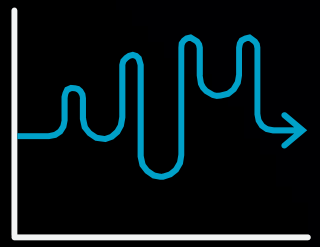
Infrastructure is always patched

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

Purchase options

Fargate on demand

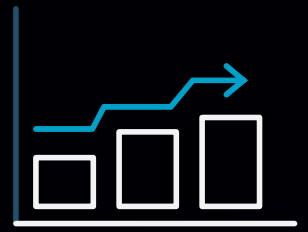
Pay for containers **per second** with no long-term commitment



Capacity needs can change rapidly

Compute Savings Plans

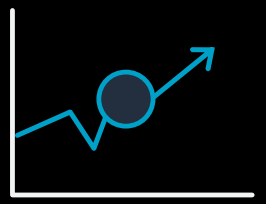
Make a 1- or 3-year commitment and receive an **up to 52% discount**



Baseline compute needs to be known in advance

Fargate Spot

Spare capacity with **savings up to 70%** off Fargate standard pricing (Amazon ECS)



Fault-tolerant, flexible workloads

https://aws.amazon.com/fargate/pricing/

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

AWS Partners extending Fargate's capabilities

Foundation

docker

HashiCorp

Spot by NetApp

Monitoring and logging

DATADOG

dynatrace

moogsoft

New Relic.

splunk>

solarwinds

sumo logic

DevOps and CI/CD

GitLab

GitHub

Pulumi

weaveworks

Security and networking

ALERT LOGIC

aqua

paloalto NETWORKS

sysdig

TREND MICRO

aws

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

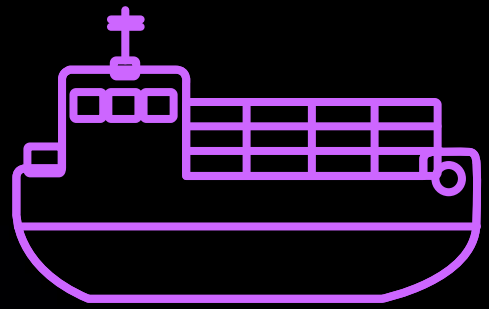
Fargate at a glance



50%
new AWS Containers customers start with Fargate



2.2x
growth for Fargate in one year



Hundreds of millions
of tasks/pods started each week

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

Recent AWS Fargate customer highlights

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

Power Smart TV services across the globe

SAMSUNG

Challenge & solution: Samsung struggled to scale on-premises data centers to handle spikes in traffic brought on by its 140M+ SmartTV devices. Migrating the backend to ECS/Fargate has provided added agility and cost savings to meet the demands of its global customer base.

- Decomposed 1 monolithic app to 13 microservices
- Auto scaling to meet demand regardless of time of day
- Using AWS CDK for infrastructure as code to consistently deploy across 4 regions
- Blending Fargate and Fargate Spot to meet performance needs
- Highly optimized with Savings Plans resulting in a 63% cost savings compared to on-premises data center

(230) AWS re:Invent 2020: Samsung Smart TV: Globally scaling with AWS Fargate Spot
https://bit.ly/300RIR1

aws

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

Image processing with Fargate



Challenge & solution: South African agriculture tech company Aerobotics' container journey took it from Amazon EC2 to GKE/Kubernetes to finally Amazon ECS/AWS Fargate + AWS Step Functions as the best fit for processing its drone imagery to compute tree health

- Reproducible and standardized infrastructure with Terraform
- Low infrastructure costs: pricing model is perfect for an on-demand use case
- Unit tracking for accounting purposes: ability to dynamically tag resources that link directly to the AWS bill

https://aws.amazon.com/blogs/containers/delivering-tree-insights-at-scale-at-aerobotics/

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

Scaling 3x in a month due to Covid



Challenge & solution: Online language learning site Babbel, with more than 10 million subscribers, wanted to modernize its application to accelerate development time, reduce maintenance work, and easily scale with the least amount of effort. Babbel selected Amazon ECS and AWS Fargate as its containerized services.

- Reduced deployment times from 30 minutes to seconds
- Seamlessly scaled to meet a rapid traffic increase in March 2020 because of the pandemic
- Reduced costs by 4x because of more time for application optimizations
- Increased security with Fargate and Amazon ECR image scanning

https://aws.amazon.com/blogs/containers/choosing-serverless-babbels-migration-story/

aws

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

Increasing investor value using Fargate

Vanguard®

Challenge & solution: Security is of the utmost importance in the highly regulated financial services industry. Migrating microservices from on-premises to Amazon ECS/ Fargate has provided security by design, increased speed to market, reduced costs by 50%, and improved disaster recovery and scalability story.

- Risk-conscious company migrating from on-premises infrastructure to AWS
- Fully managed compute from a security and maintenance perspective
- Increased speed to market of microservices from 3 months to 24 hours
- Consumption-based model gave transparency down to lowest asset levels
- Fargate Spot reduced unit costs by 50%
- Strengthened disaster recovery, scalability, and resiliency

https://aws.amazon.com/solutions/case-studies/vanguard-ecs-fargate-case-study/

aws

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

What was shipped in the last year

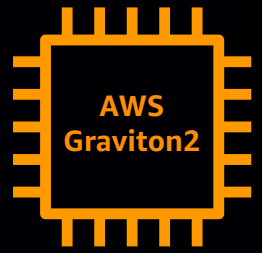
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key launches in the last year



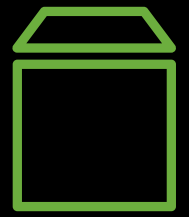
Windows Server
Operating System

Modernize Windows
workloads



ARM
CPU architecture

Get up to 40% better
price-performance



Configurable
ephemeral storage

Run data-intensive
applications with
increased local storage

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

Key launches in the last year

- Amazon ECS Exec for debugging containers
- Increased default concurrent task/pod service quotas to 1000
- Improved task launch rate to 20TPS sustained and 100TPS burst
- Clock accuracy in task metadata
- Running Airflow on Fargate
- AWS Batch integration with Amazon ECS/AWS Fargate
- AWS App Runner launch with Fargate as the compute layer

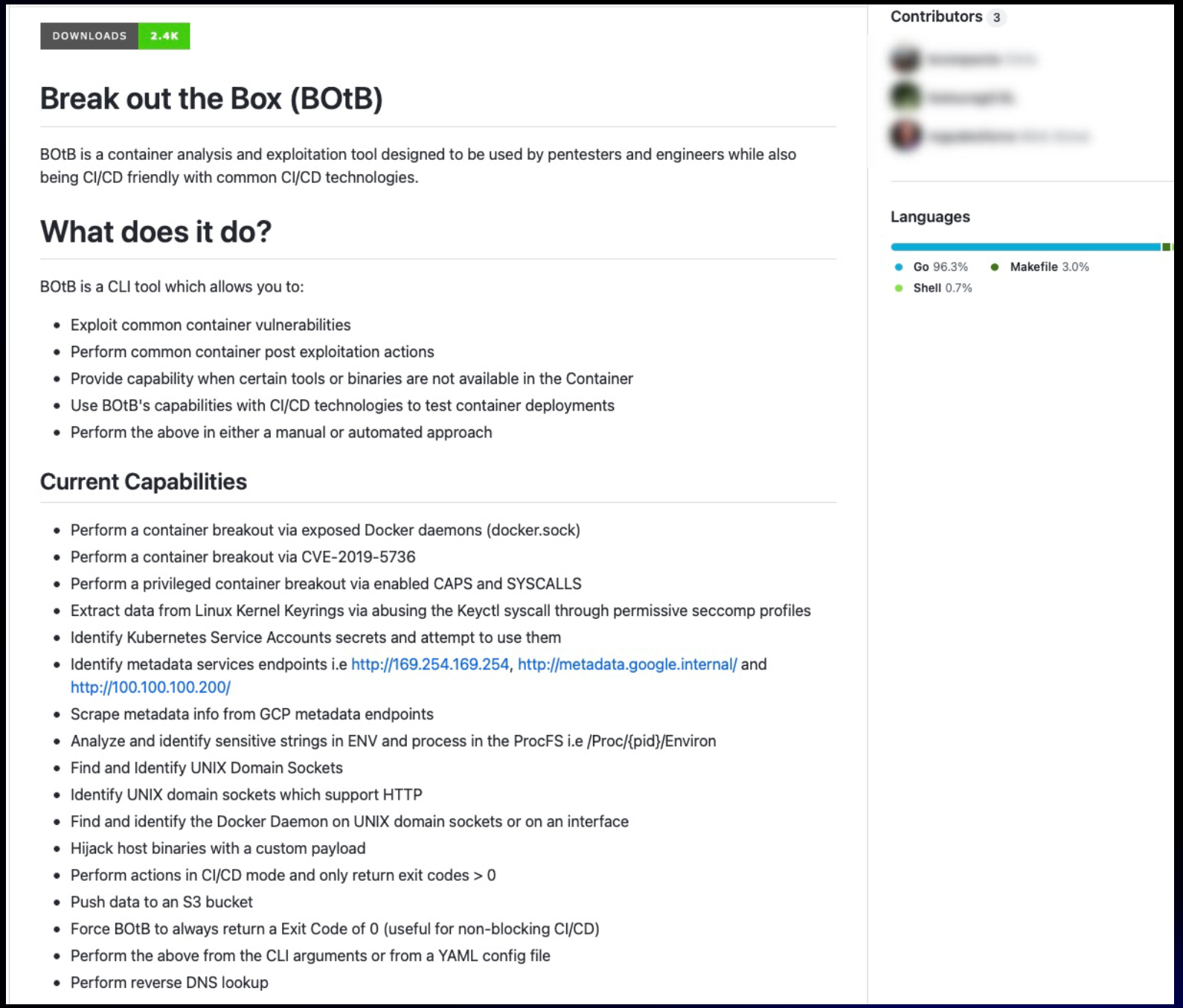
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Improving Amazon EKS on Fargate

- Built-in logging support using Fluent Bit
- Fluent Bit Kubernetes Filters to enrich log files with metadata
- Container insights support for metrics
- Built-in tracing support via AWS Distro for OpenTelemetry
- Custom security groups for pods
- Amazon EMR on Amazon EKS/AWS Fargate

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

Image



DOWNLOADS 2.4K

Break out the Box (BOtB)

BOtB is a container analysis and exploitation tool designed to be used by pentesters and engineers while also being CI/CD friendly with common CI/CD technologies.

What does it do?

BOtB is a CLI tool which allows you to:

- Exploit common container vulnerabilities
- Perform common container post exploitation actions
- Provide capability when certain tools or binaries are not available in the Container
- Use BOtB's capabilities with CI/CD technologies to test container deployments
- Perform the above in either a manual or automated approach

Current Capabilities

- Perform a container breakout via exposed Docker daemons (docker.sock)
- Perform a container breakout via CVE-2019-5736
- Perform a privileged container breakout via enabled CAPS and SYSCALLS
- Extract data from Linux Kernel Keyrings via abusing the Keyctl syscall through permissive seccomp profiles
- Identify Kubernetes Service Accounts secrets and attempt to use them
- Identify metadata services endpoints i.e http://169.254.169.254, http://metadata.google.internal/ and http://100.100.100.200/
- Scrape metadata info from GCP metadata endpoints
- Analyze and identify sensitive strings in ENV and process in the ProcFS i.e /Proc/{pid}/Environ
- Find and Identify UNIX Domain Sockets
- Identify UNIX domain sockets which support HTTP
- Find and identify the Docker Daemon on UNIX domain sockets or on an interface
- Hijack host binaries with a custom payload
- Perform actions in CI/CD mode and only return exit codes > 0
- Push data to an S3 bucket
- Force BOtB to always return a Exit Code of 0 (useful for non-blocking CI/CD)
- Perform the above from the CLI arguments or from a YAML config file
- Perform reverse DNS lookup

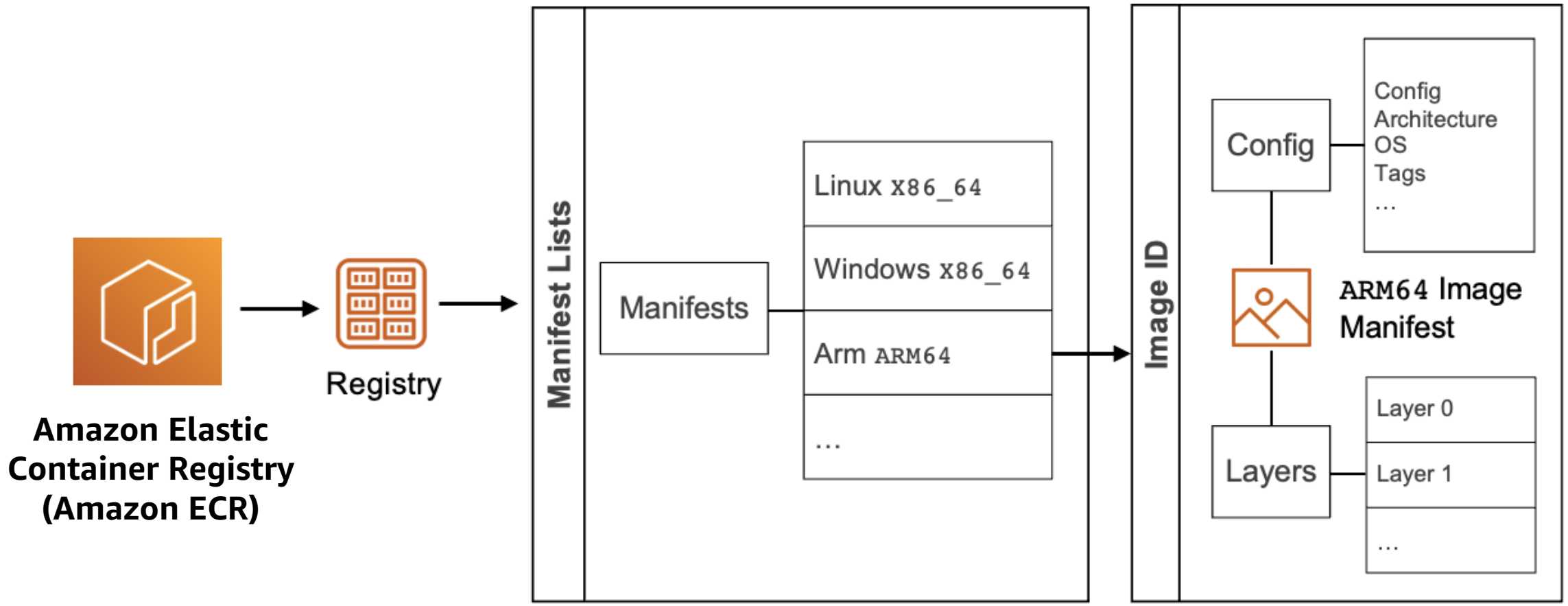
Contributors 3

Languages

Go 96.3% Makefile 3.0%
Shell 0.7%

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

Multi arch images



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

Task definition

```
{
 "family": "myarmapp",
 "networkMode": "awsvpc",
 "containerDefinitions": [
    {
        "name": "break-out-of-the-box",
        "image": "096198301477.dkr.ecr.ap-south-1.amazonaws.com/fargate-testing-arm:multiarch",
        "essential": true,
        "command": [ "echo hello" ],
        "entryPoint": [ "sh", "-c" ]
    }
 ],
 "requiresCompatibilities": [ "FARGATE" ],
 "cpu": "1 vCpu",
 "memory": "3 GB",
 "runtimePlatform": { "cpuArchitecture": "ARM64" },
 "executionRoleArn": "arn:aws:iam::1234567890:role/ecsTaskExecutionRole"
}
```

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

AWS Copilot

```
copilot task run--image <multi-arch image> --platform-os linux --platform-arch arm64
```

Automatically creates:

1. Network resources: VPC, subnets, NACLs
2. Amazon ECS: Cluster, task definition, services, and tasks
3. IAM Roles, CloudWatch logs

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

IAM Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssmmessages:CreateControlChannel",
                "ssmmessages:CreateDataChannel",
                "ssmmessages:OpenControlChannel",
                "ssmmessages:OpenDataChannel"
            ],
            "Resource": "*"
        }
    ]
}
```

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ecs-exec.html

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

What’s coming

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

Roadmap ahead

- Expand compute options (larger sizes, GPUs)
- Extend storage capabilities
- Improve performance consistency and scaling
- Enhance runtime security
- Open-source engagements (Firecracker, containerd, Fluent Bit)
- Partner integrations (security and observability)
- Delight customers across multiple orchestrators (Amazon ECS, Amazon EKS, AWS Batch)

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

Thank you!

Saloni Sonpal

Senior Product Manager, Fargate
AWS
@SaloniSonpal

Re Alvarez Parmar

Principal Containers Specialist
AWS
@realz

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