
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

OPN206-R

Why you should use a container-optimized operating system

Kyle Davis (He/Him)

Senior Developer Advocate
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

General purpose and container optimizations

Composition and architecture

Day-to-day with a container-optimized OS

Q&A

Wrap up

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Where do you fall?

Containers

- Used containers
- Used containers in production
- Managed orchestrated cluster(s)
- Managed on-premises orchestrated cluster(s)
- You're a maintainer of Kubernetes

Operating systems and Linux

- Used Linux
- Used a variety Linux distros
- You've contributed to a distro
- You're Linus Torvalds

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

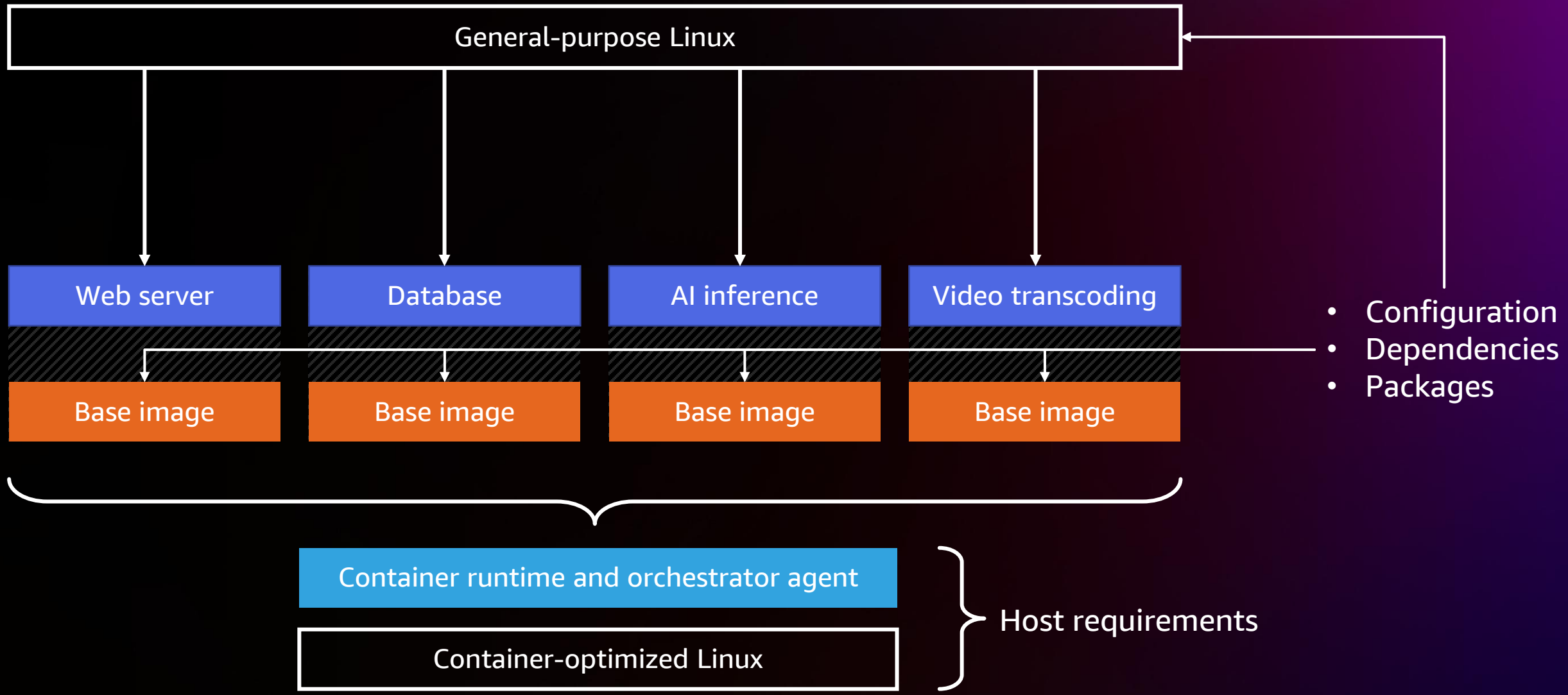
General purpose and container optimizations

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Specialized Linux distros

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Containers: Heterogeneous or homogeneous?



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security profile



Required
- containerd
- kubelet

....
- SSH
- Package manager
- Writable file system
- Management tools

Potential security issues on Non–mission critical components



Required
- containerd
- kubelet

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bottlerocket and friends

- It’s a category, not a single project
- Bottlerocket as a representative
  - Compare/contrast
  - POV: Bottlerocket
- Every effort to represent others accurately
  - Not an expert on each project

Other similar projects:

CoreOS (RIP)

Flatcar

Talos

Container-optimized OS (Google)

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Composition and architecture

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Base image vs. host operating system

Base image

- Specified in the dockerfile `FROM`
- Different images can coexist on a single node
- Relevant to your containerized workload
- Is **above** kubelet and containerd

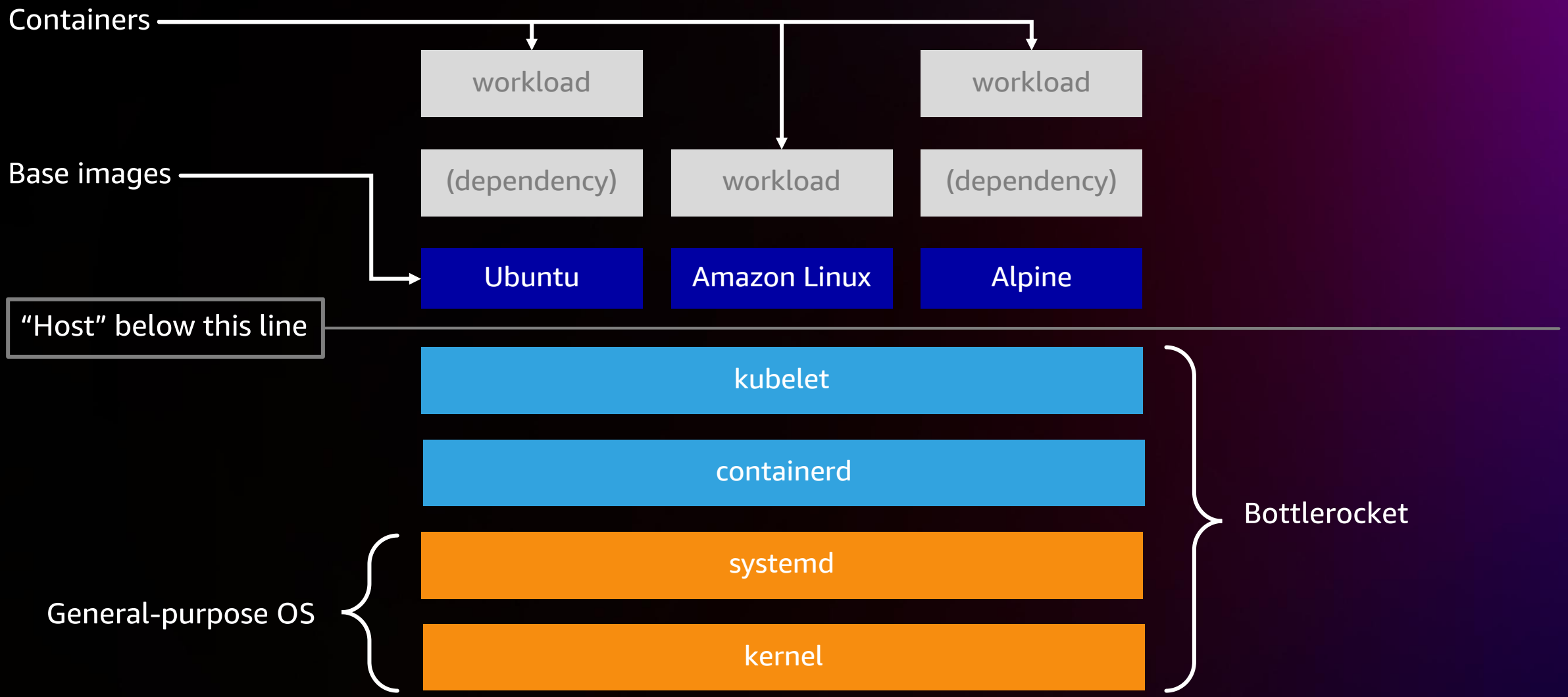
Host operating system

- Installed on the hardware or instance
- One per node
- (Mostly) transparent to your containerized workload
- Is **under** (or includes) kublet and containerd

aws

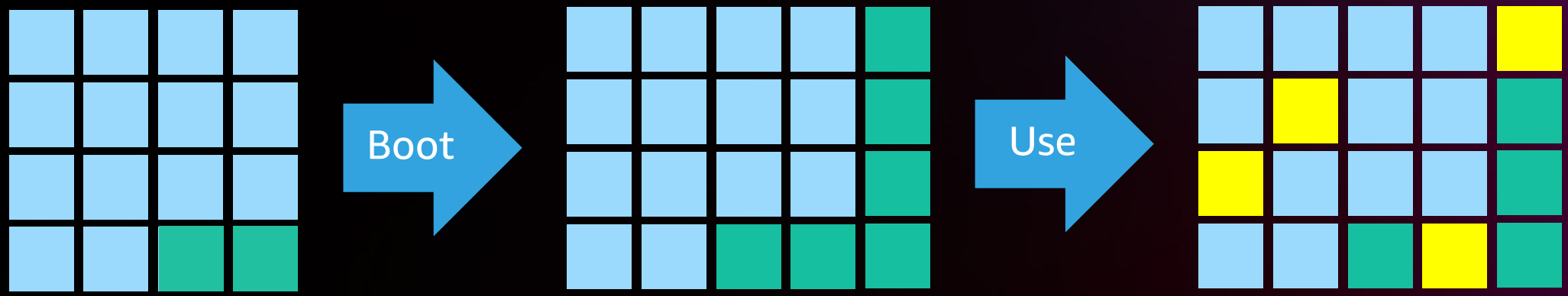
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Base image vs. host operating system illustrated



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

General-purpose distro

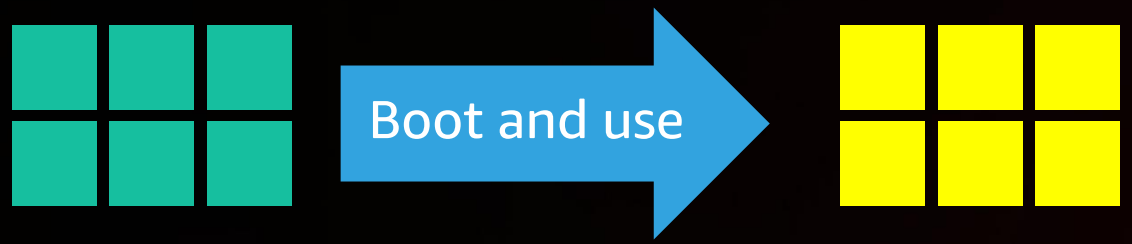


Stock distro

Set-up (mutate) with package manager

Update (mutate) with package manager

Bottlerocket

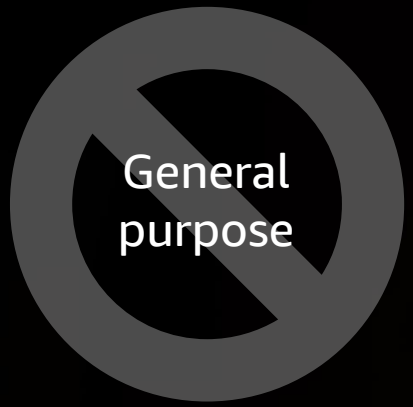


Image

Updated image

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

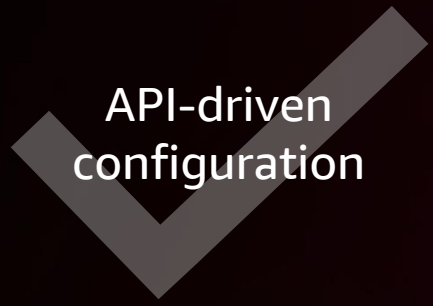
A few big ideas







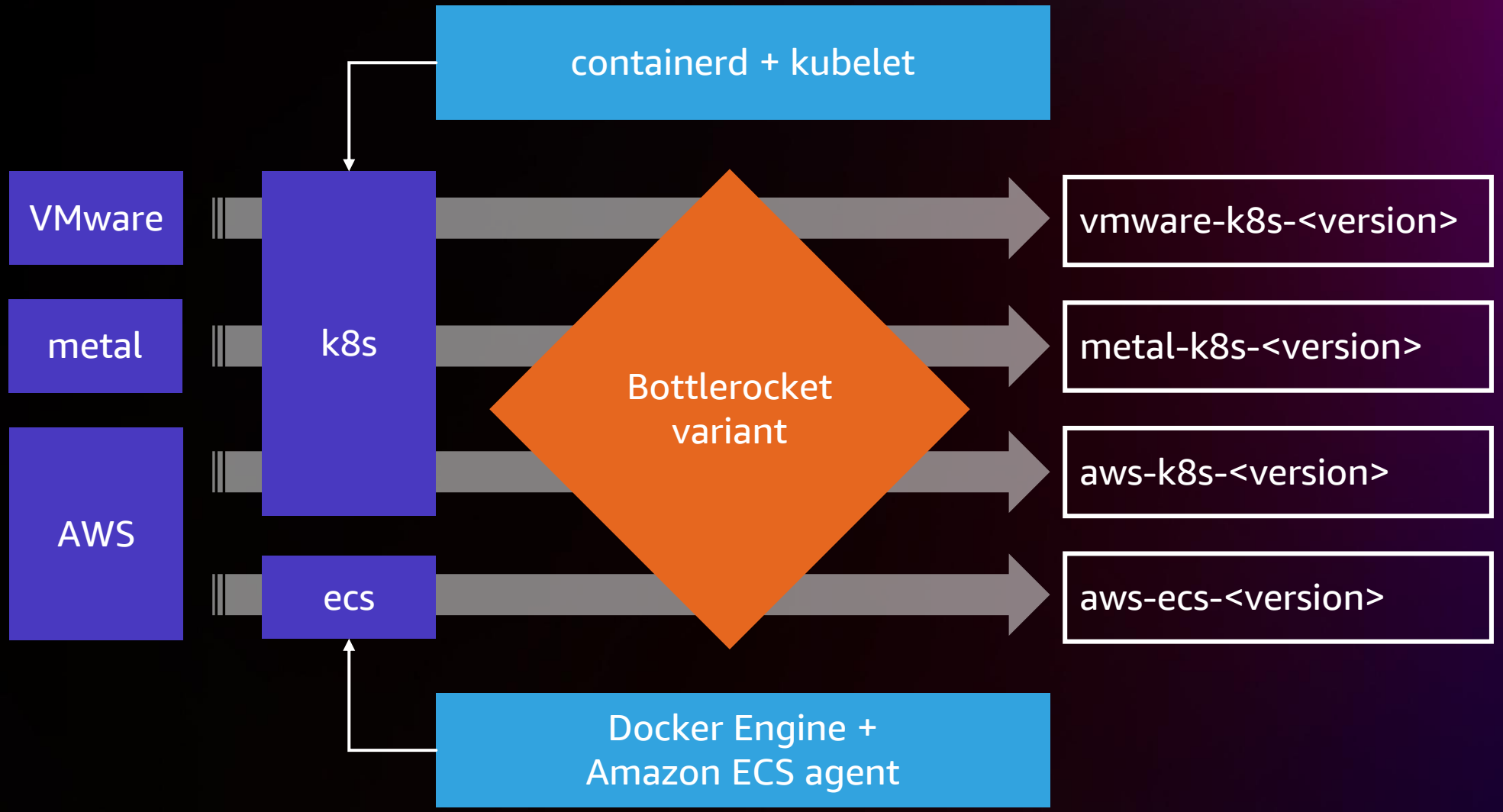






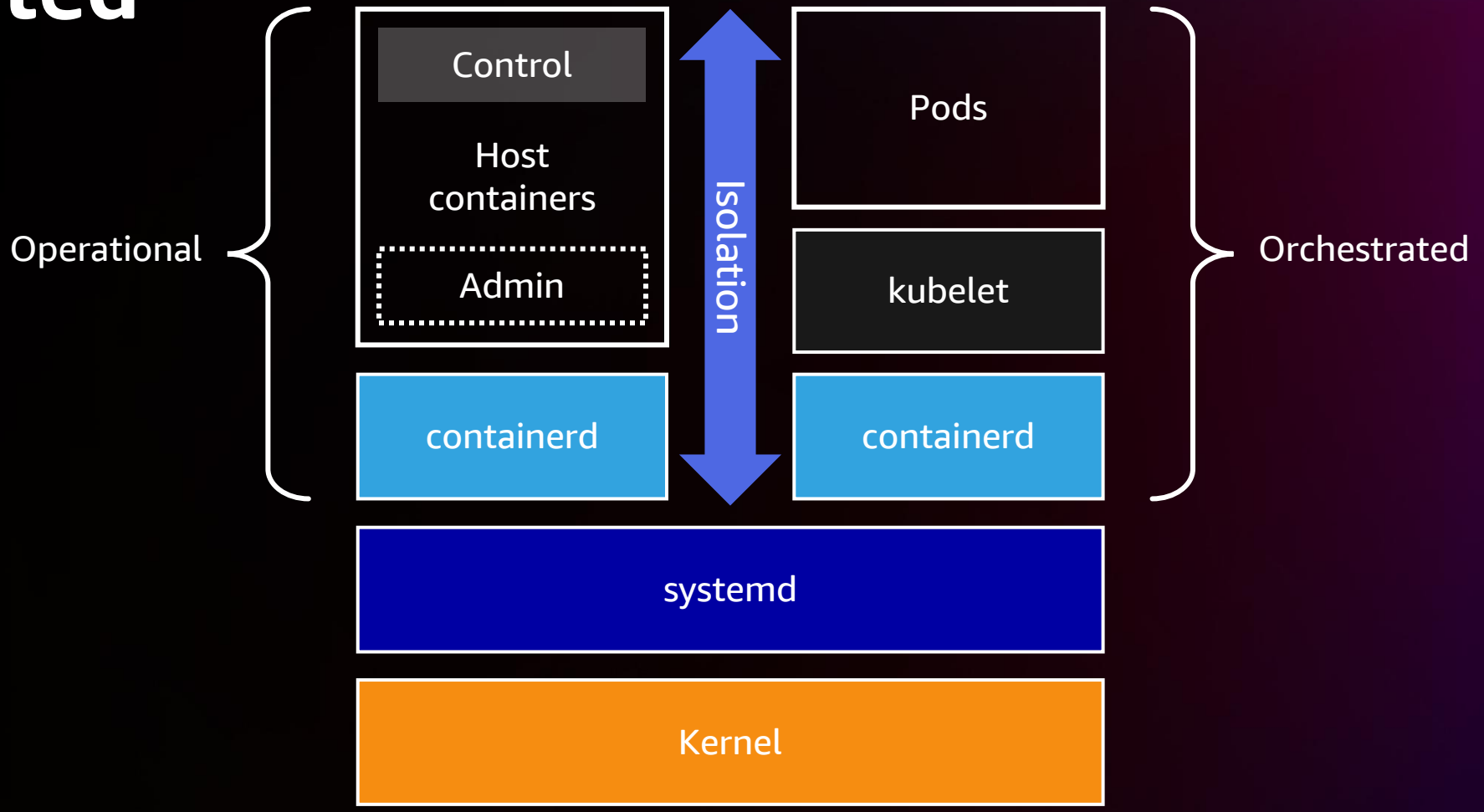
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Only what you need



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bottlerocket: Container-oriented, concerns separated



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

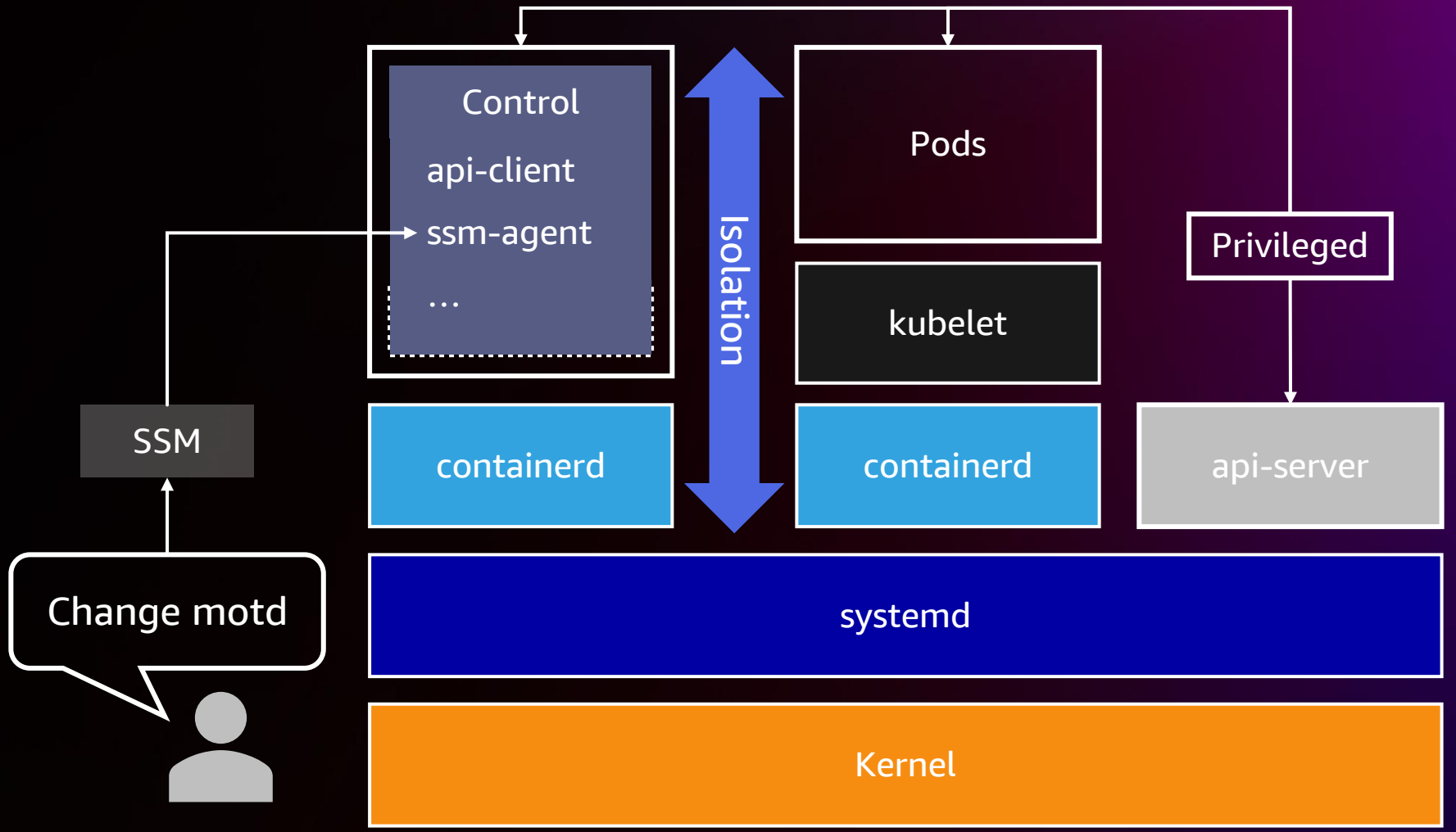
An API-first operating system

Settings are changed via the API

Unix socket between API server and privileged containers

The control container contains the api-client for adhoc changes

SSM can be used to connect to the control container



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Open contribution and development

- Dual license
  - Apache 2.0 or MIT, you pick
  - Well-understood permissions
- No contributor license agreement (CLA)
- Developed in the open, all on GitHub
- Contributions are welcome!

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Day-to-day with a container-optimized OS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Day-to-day: Host and workload interaction

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Day-to-day: Logging with Bottlerocket

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Q&A

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Links and resources

Bottlerocket Repo

github.com/bottlerocket-os/bottlerocket

Bottlerocket on AWS

aws.amazon.com/bottlerocket

Meetup group

meetup.com/bottlerocket-community

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Let’s connect

Kyle Davis

Twitter:
@stockholmux

Mastodon:
@linux_mclinuxface@fosstodon.org

GitHub:
github.com/stockholmux

LinkedIn:
linkedin.com/in/kyle-davis-linux

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Kyle Davis



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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.