Tern and the State of Cloud Native Compliance

Rose Judge

Open Source Engineer
VMware Open Source Technology Center

FOSDEM SCA Devroom – February 4, 2021

Agenda

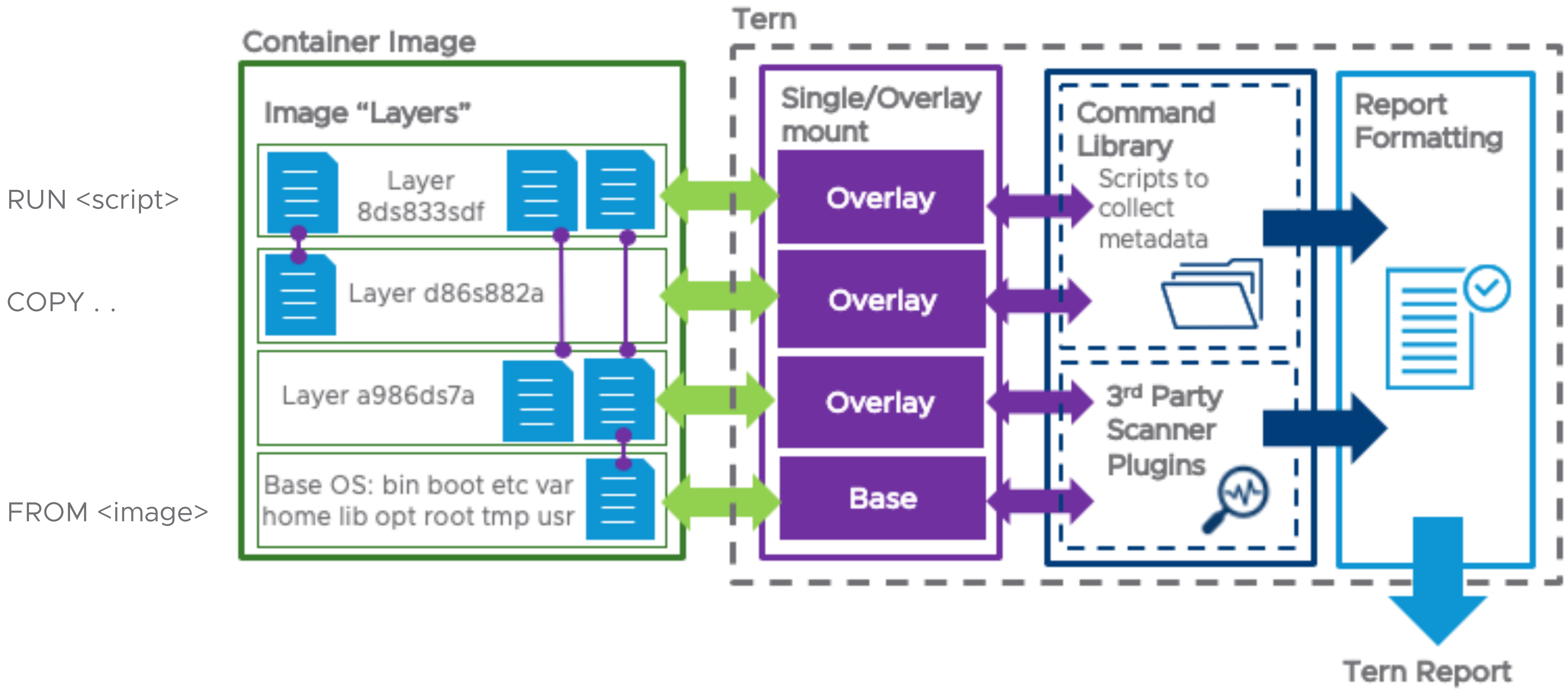
Tern

The State of Cloud Native Compliance

Looking ahead: A Better Compliance Strategy

Tern

https://github.com/tern-tools/tern



Capabilities

Inspects container images to produce SBoM

Dockerfile build and inspection to produce SBoM

Integration with other analysis tools (Scancode)

Limitations

Tern is not a “be-all-end-all” solution

- Requires presence of base OS shell + package manager
  - Scancode still available without shell
- Dependent on correctness of package manager
- Docker dependent (for now)
  - Root privileges required

Use Cases

Basic Developer inventory

Include in your CI/CD pipeline

The State of Cloud Native Compliance

Gaps in Cloud Native Compliance

Current industry standard is to scan containers post-build

No way to distribute a container image with its SBoM

Cloud Native applications/containers are increasing in complexity

Multiple SBoM specifications used (if at all)

Looking Ahead

A Better Compliance Strategy

Compliance in a distributed environment

Some requirements for SBoMs and sources

Small, Independent components

Identifiable by artifact

Composable SBoM and retrievable sources

Distributable with artifact

Work to fill the gaps in Tern

Current

- JSON and tag-value SPDX documents for container images

Future work

- Inventory and generate SBoM during container build
- Generate SBoM per layer
- Embed SBoM in container image

Related efforts

- SPDX 3.0 Linkage profile

Thank You

Contact: rjudge@vmware.com

https://github.com/tern-tools/tern