KubeCon | CloudNativeCon

North America 2021

RESILIENCE

REALIZED

RESILIENCE
REALIZED

NOTARY:
STATE OF THE CONTAINER SUPPLY CHAIN

Steve Lasker

Principal PM Architect
Azure Container Registries
Steve.Lasker@Microsoft.com
@SteveLasker
.blog SteveLasker.blog
github.com/SteveLasker
github.com/SteveLasker/presentations

Justin Cormack

CTO
Docker
justin@docker.com
@justincormack
.blog cloudatomiclab.com
github.com/justincormack

State of the Container Supply Chain

- There are multiple efforts
- Focusing on different stages of the supply chain
- Some overlap
- Innovation happening at the speed of …

Stages of the Supply Chain

- **Creation of Content**
  - The building of content (binaries, packages, images)
- **Distribution of Content**
  - Distributing the content to consumers
  - Distribution includes promotion across different environments
- **Consumption of Content**
  - To build other content
  - To import from other sources
  - To deploy

Notary v2

How Do You Deploy Today?

- Unique tags? (`my-service:ag-123`)
- Digests? (`my-service@sha256:abs8a23823aaa8a8d8d8a...`)
- Convert a tag to a digest?
- What do digests promise?
- Do you track all the digests created,
  and who created them?

Signing – what does it promise?

- “All deployed content must be signed”
  - By who?
  - Who **do you** trust?
  - Who **don’t you** trust?
  - Who do you/don’t you trust for a **given environment**?

- If you had signed content, from entities you trust, would you need to track individual digests?

Attesting To Entity Promotion

- Checking Into the Airport

Artifact Promotion

Wabbit Networks

Artifact Build Environment

PIPELINE

Image

SBoM

Scan Results

src

Spacely Sprockets

Artifact Build Environment

PIPELINE

Image

SBoM

Scan Results

Cogswell Cogs

Artifact Build Environment

PIPELINE

Image

SBoM

Scan Results

Docker Hub (Distributor)

Wabbit Networks

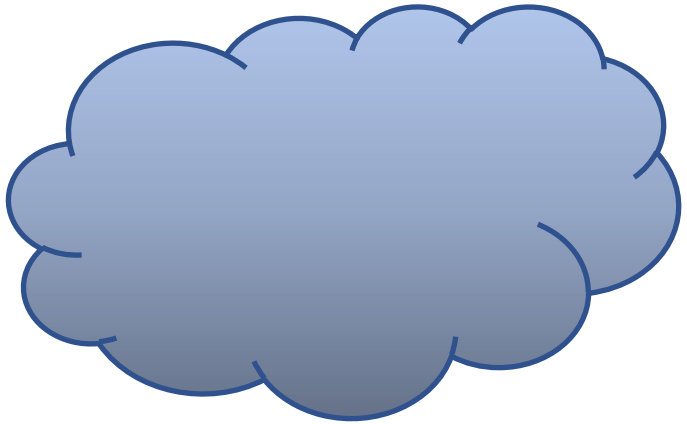
Image

SBoM

Scan Results

src

Spacely Sprockets



ACME Rockets

Trust Policy

Docker Hub
Spacely Sprockets
Cogswell Cogs

Internal Registry

Air-gapped network

Private Registry

Policy Management

Container Host

Air-gapped network

Private Registry

Policy Management

Container Host

Air-gapped network

Private Registry

Policy Management

Container Host

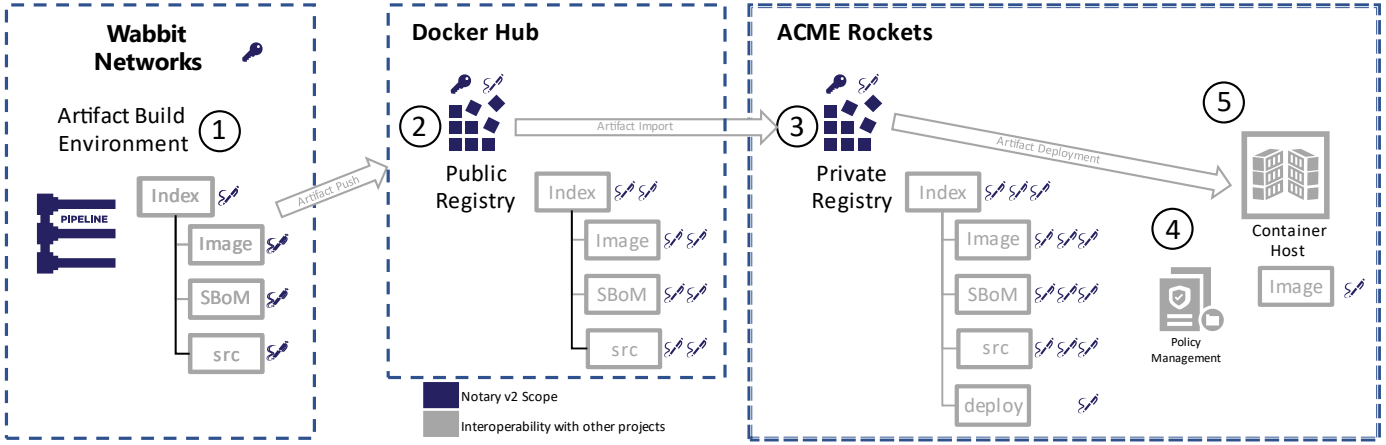
Location Independence

- Which Public Registry, for which content?

docker hub	ecr public	mcr	github	your registry

Supply Chain Artifact Challenges

- Artifacts are promoted across environments
  - Pubic → Shared Internal → Dev → Staging → Prod
- Many of these destinations are within restricted networks (Vnets)
- The supply chain objects should travel with the artifacts
- Enabling evaluation and validation of the supply chain objects, where the content is consumed from



How Notary v2 Enables Secure Workflows

- Signatures are associated with a **subject** artifact
- Signatures are promoted ***with*** the artifact
- ***Multiple*** signatures may be associated with a given artifact
- Signatures are separable,
  enabling protection from trojan horse attacks

Demo

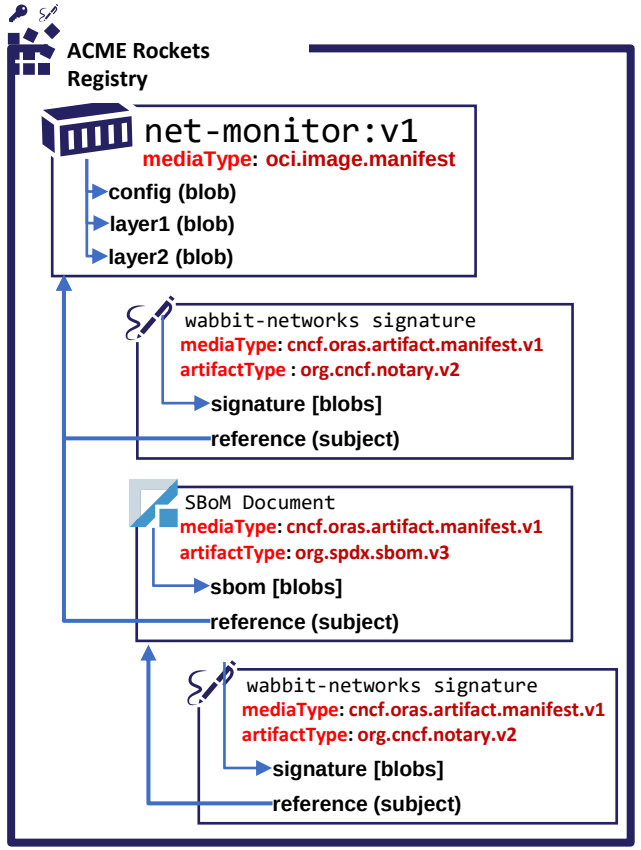
Signing and Validation

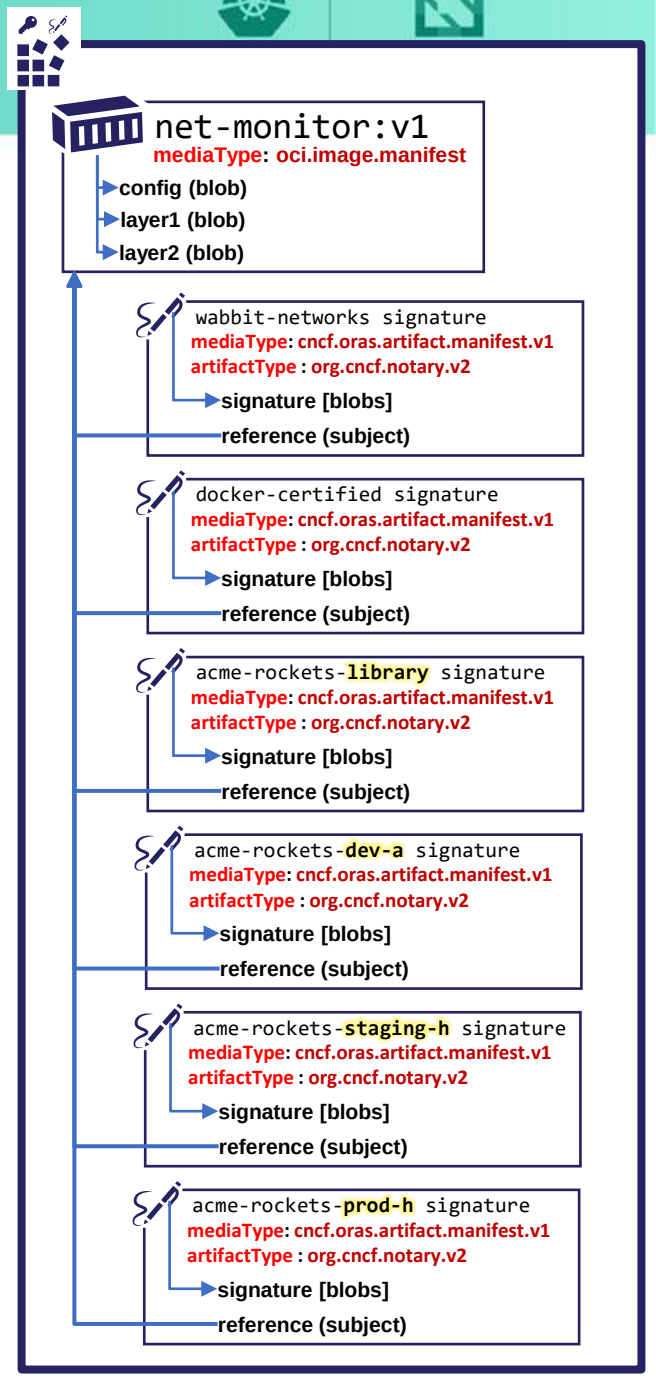
Promoting Artifacts

- How to promote a graph of artifacts?
- Several tools were used to create various artifacts
  - Container Build Tools (Docker)
  - SBoM Creation (CycloneDX, SPDX)
  - Image Scan Results (Aqua, Palo Alto, Snyk)
  - Signatures (Notary, Cosign)
- Should each tool be used to promote the graph?

ORAS Artifacts

- Enhances OCI Registries to understand graphs of content
- Artifacts are pushed with a **`subject`**, linking to another artifact
  - Signatures → container images
  - SBoMs → container images
  - Signatures → SBoMs
  - Scan Results → Container images
  - Signatures → Scan Results





http://github.com/oras-project/artifacts-spec/

```
oras copy wabbit-networks.io/net-monitor:v1 \
      acme-rockets.io/net-monitor:v1 -r

registry.wabbit-networks.io/net-monitor:v1
├── application/vnd.cncf.notary.v2
│   └── sha256:8c0e82624475a4ad64ddca2d68c0f82e316ec758591cb916049fe59eaf27b5b4
├── application/vnd.org.snyk.results.v0
│   └── sha256:95b97532a5b2d0c36cfcefd403b02779fb5afca07479a66bd509a635d5681e7f
│       └── application/vnd.cncf.notary.v2
│           └── sha256:02f35a789d1ec2267727ac32c4f8ad643e88288528e648e4b71af42c2912699b
└── sbom/example
    └── sha256:82d89db16266d13ab7680badfea3dbd91fd8e311c3b4291d9c0d4f9cff86fa50
        └── application/vnd.cncf.notary.v2
            └── sha256:413e8b4de5f09c1b458d9d0ab8f1cc510d4276ffaa710073daff721e89b07aa2
```

Demo

`oras copy [source] [destination] --recursive`

Notary v2 Policy Management

- Notary v2 enables policy-based management, per environment
- You configure which keys you trust, per environment
- Integrate *with* OPA/Gatekeeper and other policy managers
- Notary v2 supports key provider extensibility

Wait, There's More

- Key and Signature Revocation
  - Important for public content
  - Private content is under private control
- TUF Integration
  - Working through cross registry promotion scenarios
- OCI Distribution 1.0 Registry Fallback
  - Notary and ORAS will have degraded fallback support

Wrapping Up

- Signatures enable attestation of an artifact by a given entity
- You choose which entities you trust, for each environment
- As you promote, stamp with a signature for that environment
- Notary v2 references, generalized for all supply chain reference types
- ORAS enables promoting a graph of artifacts into the environment you trust
  - …and have access to

Thank You

- Notary v2: github.com/notaryproject/notaryproject
- OCI Artifacts: github.com/opencontainers/artifacts
- ORAS Artifact Reference Types: github.com/oras-project/artifacts-spec
- ORAS CLI: github.com/oras-project/oras
- ORAS Library: github.com/oras-project/oras-go
- CNCF Distribution Reference Types: github.com/oras-project/distribution

Steve Lasker

Principal PM Architect
Azure Container Registries
Steve.Lasker@Microsoft.com
@SteveLasker
.blog SteveLasker.blog
github.com/SteveLasker
github.com/SteveLasker/presentations

Justin Cormack

CTO
Docker
justin@docker.com
@justincormack
.blog cloudatomiclab.com
github.com/justincormack