KubeCon CloudNativeCon Europe 2022

Distributing Supply Chain Artifacts with OCI & ORAS Artifacts

Steve Lasker

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

Agenda

- Supply Chain Artifacts:
  - What will you use to store all the new artifact types?
  - Why the “what” matters
- Build or Extend?
- Registries
  - Elegance and Evolution
  - OCI and ORAS Artifacts

Supply Chain Artifacts

Yeah, and ohhh my

Supply Chain Artifacts – What/Where

Software

- Containers
- Packages
- Binaries
- IoT Deployments
  - Vehicles to Medical
- Virtual Machine Images

SBOM

Scan Results

Claims

Licenses

gitBOM

Policies

Attestations

Docs

Deployment Templates

Supply Chain Artifacts – What/Where

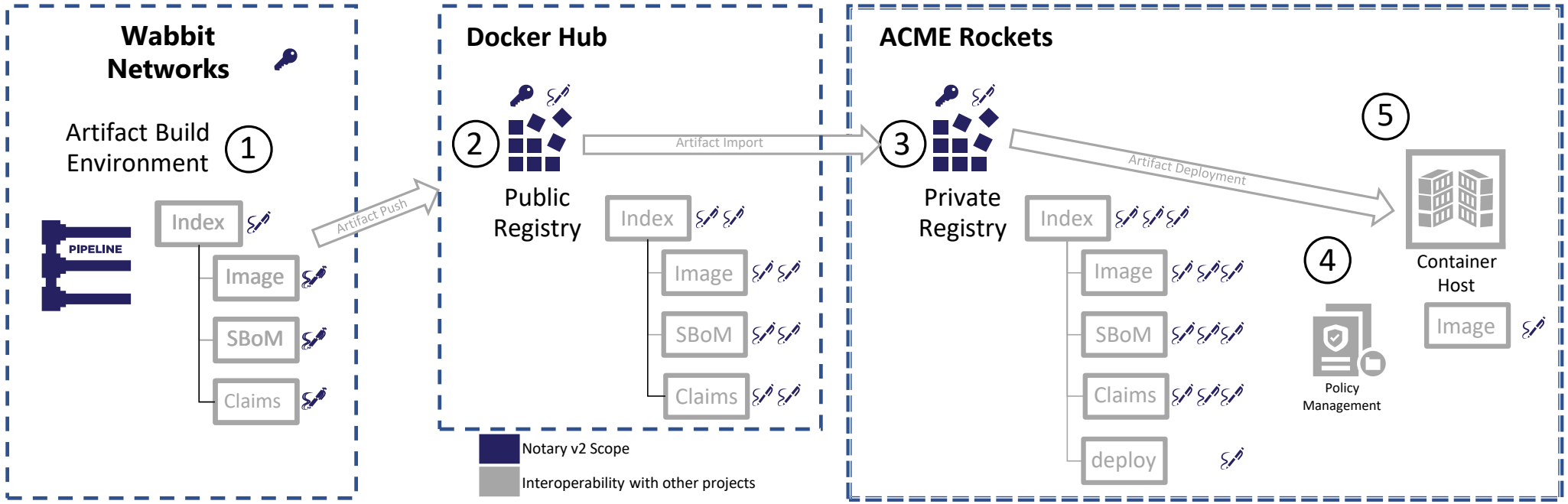
Where will you store them?

Will you distribute them?

How will you manage their lifecycle?

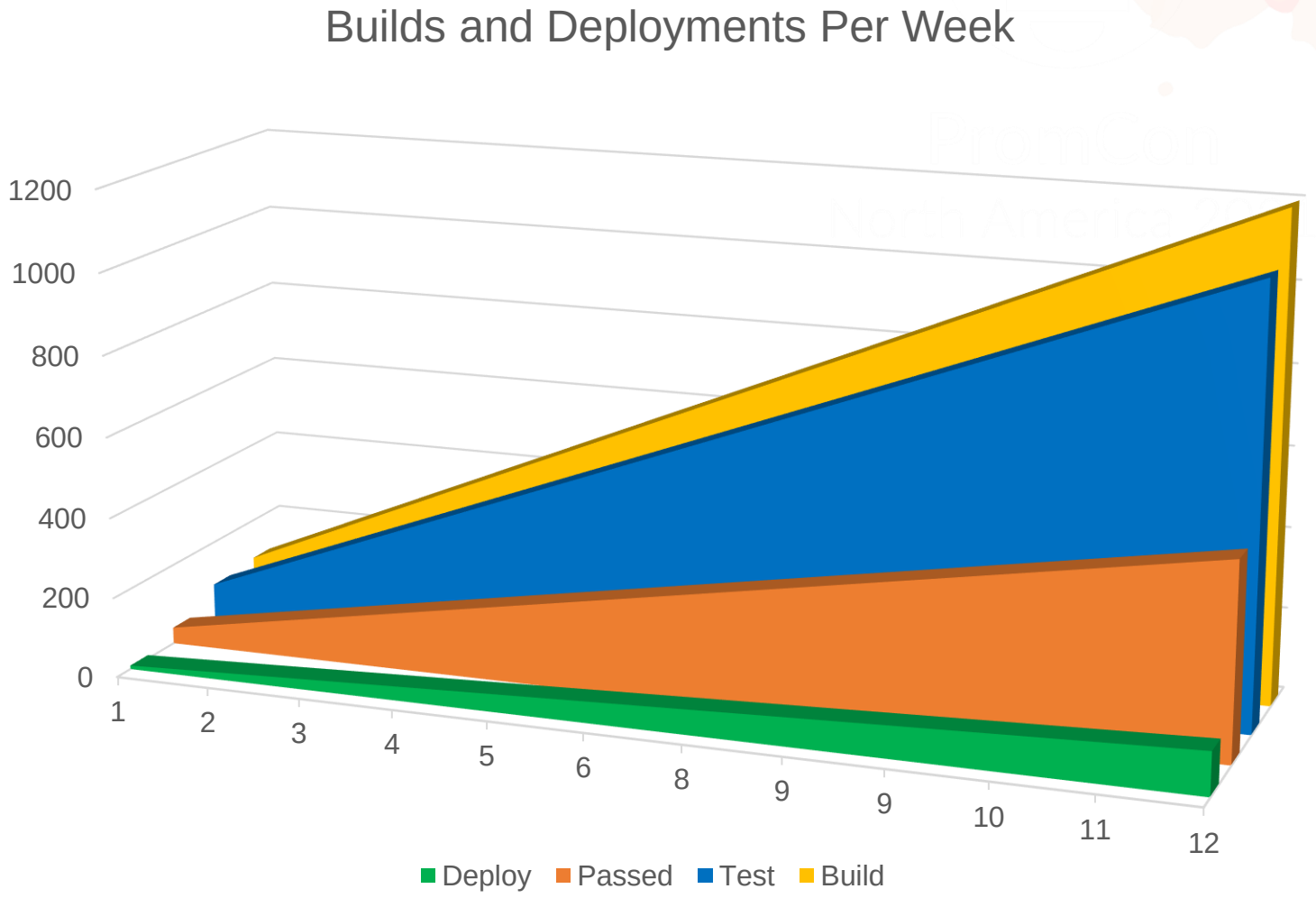
Supply Chain Artifact Distribution

- Best practice:
  Own a copy of your dependencies, in an environment you own
- Ship the SBOM, gitBOM, Scan Result, Claims alongside…



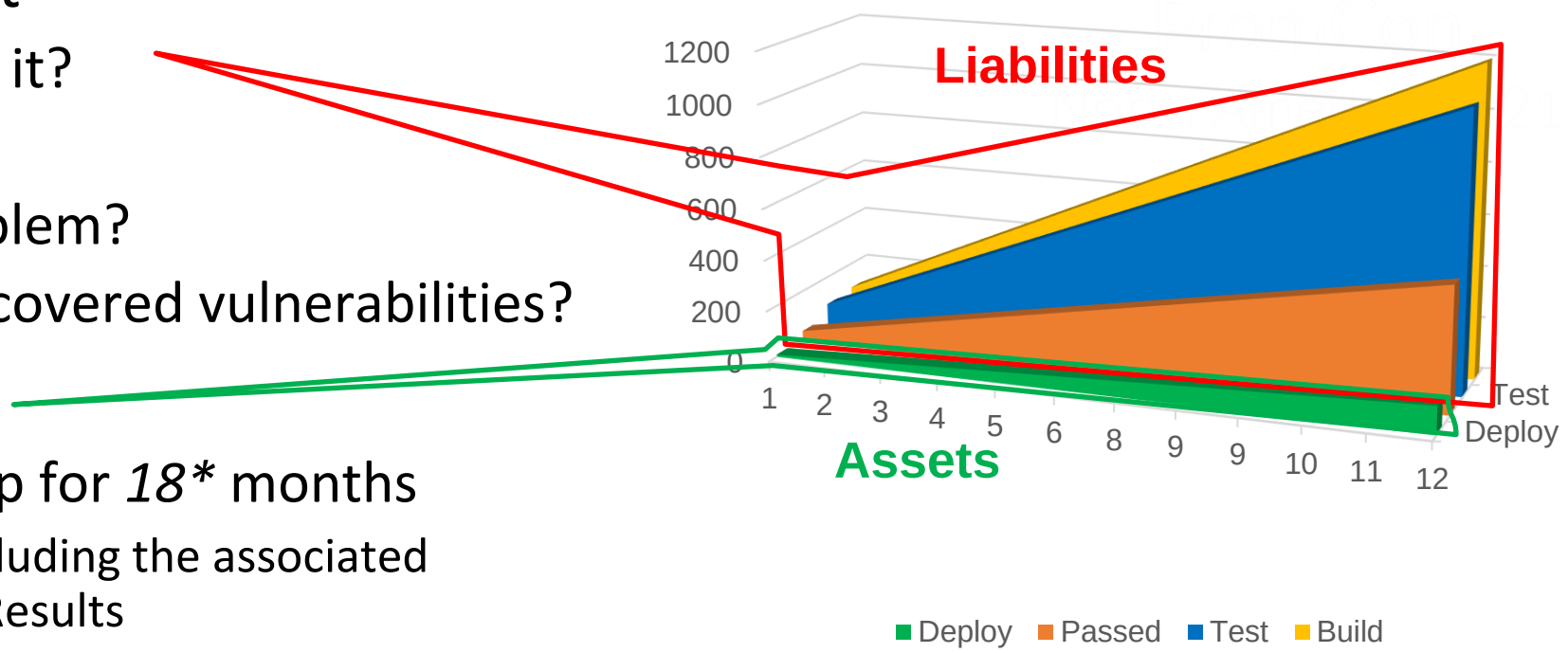
Supply Chain Artifact Lifecycle Management

- How many builds do you:
  - produce in a week?
  - test in a week?
  - deploy in a week?
- For each build:
  - SBOM
  - gitBOM
  - Scan Result
  - Claims & Attestations
  - Signatures
  - Deployment Template



Assets & Liabilities

- Non-Deployed Content
  - How long do you keep it?
  - Should you keep it?
  - Is it *just* a storage problem?
  - What about newly discovered vulnerabilities?
- Deployed Content
  - Compliance: must keep for *18** months
    - Deployed binaries, including the associated SBOMs, Claims, Scan Results
- Archived Binaries
  - What about new vulnerabilities, in deployed content, from 2 months ago?
  - Do you patch the archived binaries, saved for compliance?



How to secure access to your artifacts?

What scoping of access will you use?

Equal access to all things?

Create, Update, Delete rights?

Listing?

Metadata?

\Thing1
\Thing2
\Thing3
\TeamA\Thing4
\TeamA\Thing5
\TeamB\Thing6
\TeamC\Thing7

Production Capabilities

Reliability & Performance: Geo-Replication / Availability Zone Support

Promotion Across Storage Services

Promotion across cloud providers and on-prem

Diagnostics: Logging access, success, failure, denials, performance metrics

Network Security: Virtual Private Networks and Air-Gap Environments

Support: Who, how, what is the SLA?

Running A Storage Service

- Authentication
  - What will you use?
  - Will it integrate with the rest of “the platform”
- Security
  - How do you prevent hacks, DOS attacks, abuse?
- Costs
  - Will you justify the costs to run the YASS?
  - Will you charge, offer for free- your YASS?
- Multiple clouds?
  - Will other cloud vendors host this YASS for you?

VNET & Firewall Rules?

Documentation?

Compliance

Regional Replication?

Signing?

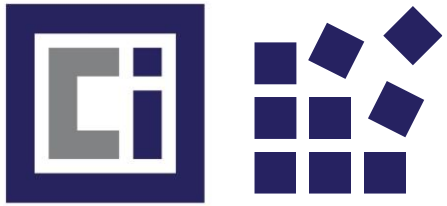
Distributing Supply Chain Artifacts

- ❑ Supply chain artifacts should be distributed
- ❑ Distributed across clouds and on-prem
- ❑ Secure access (RBAC) is kinda important
- ❑ Lifecycle management can’t be an afterthought
- ❑ Production capabilities from V-Net, replication, diagnostics, support to reliability are core requirements

Build or Invest?

Existing Storage Services to Invest In

- Git
- Existing Package Managers
- Raw storage accounts
- Various ISV Products
- **OCI Distribution Spec**



The Elegance of Registries

OCI Distribution Specification

Artifact Addressability

- User Perspective:

```
registry.wabbit-networks.io/monitoring/net-monitor:v1
```

Registry Endpoint (REST) Login URL

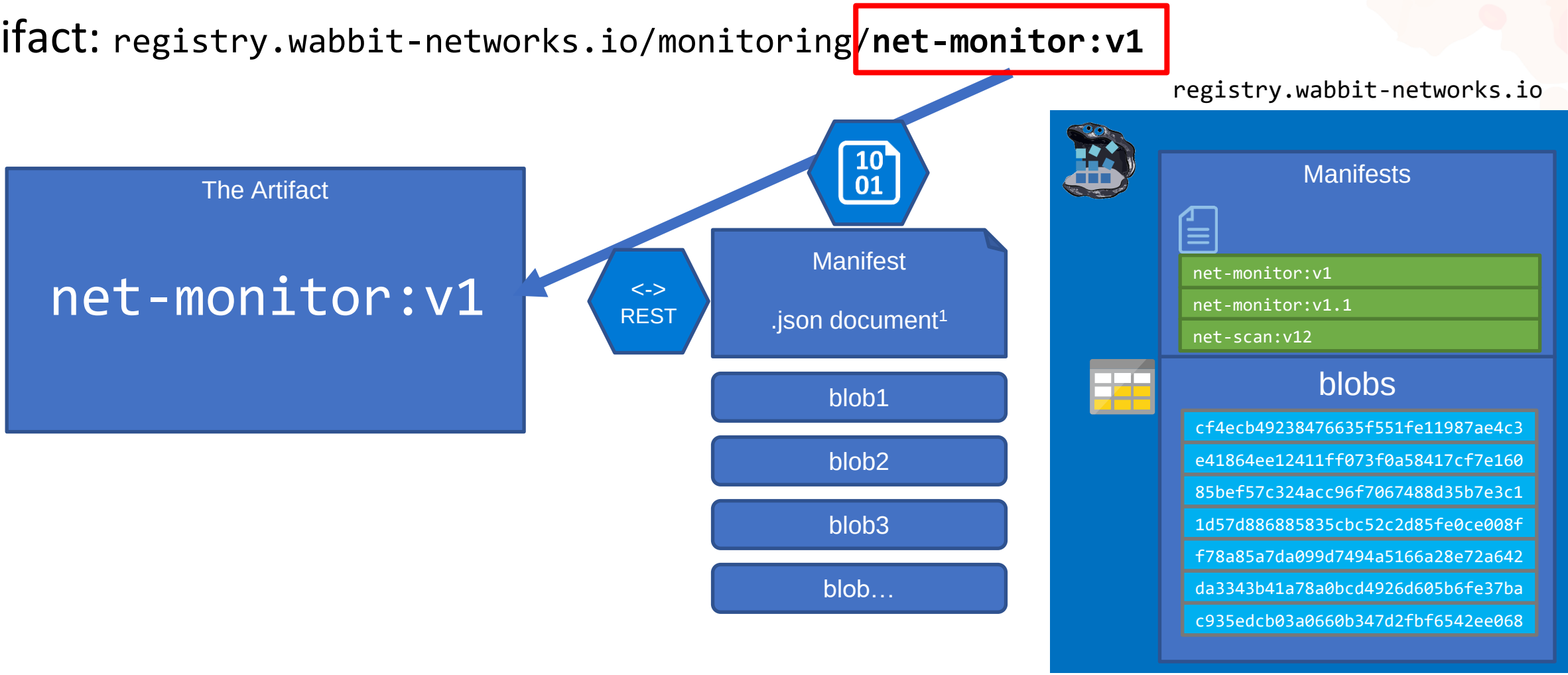
Namespace

~~Image~~ Artifact

Version

Under the covers

Artifact: `registry.wabbit-networks.io/monitoring/net-monitor:v1`



1. *Existing manifests happen to be .json, but can be any "document" type*

Docker Pull


```
docker pull registry.wabbit-networks/net-monitor:v1
```

Container Host Service

Manifest:
What layers do I already have? *(decompressed)*

Image Cache

IMAGE ID	REPOSITORY	TAG	SIZE
694950fbcb3f	wabbitnetworks/net-monitor	v1	1.2B

Layer Cache

LAYER ID

- sha256:cf4ecb49238476635f551fe11987ae4c3
- sha256:e41864ee12411ff073f0a58417cf7e160

1. Pull
2. Manifest Returned
3. Delta of Blob Requests
4. Blob URLs Returned
5. Blob Request
6. Blobs Returned

Pull:
I want this “thing”, represented by a collection of blobs

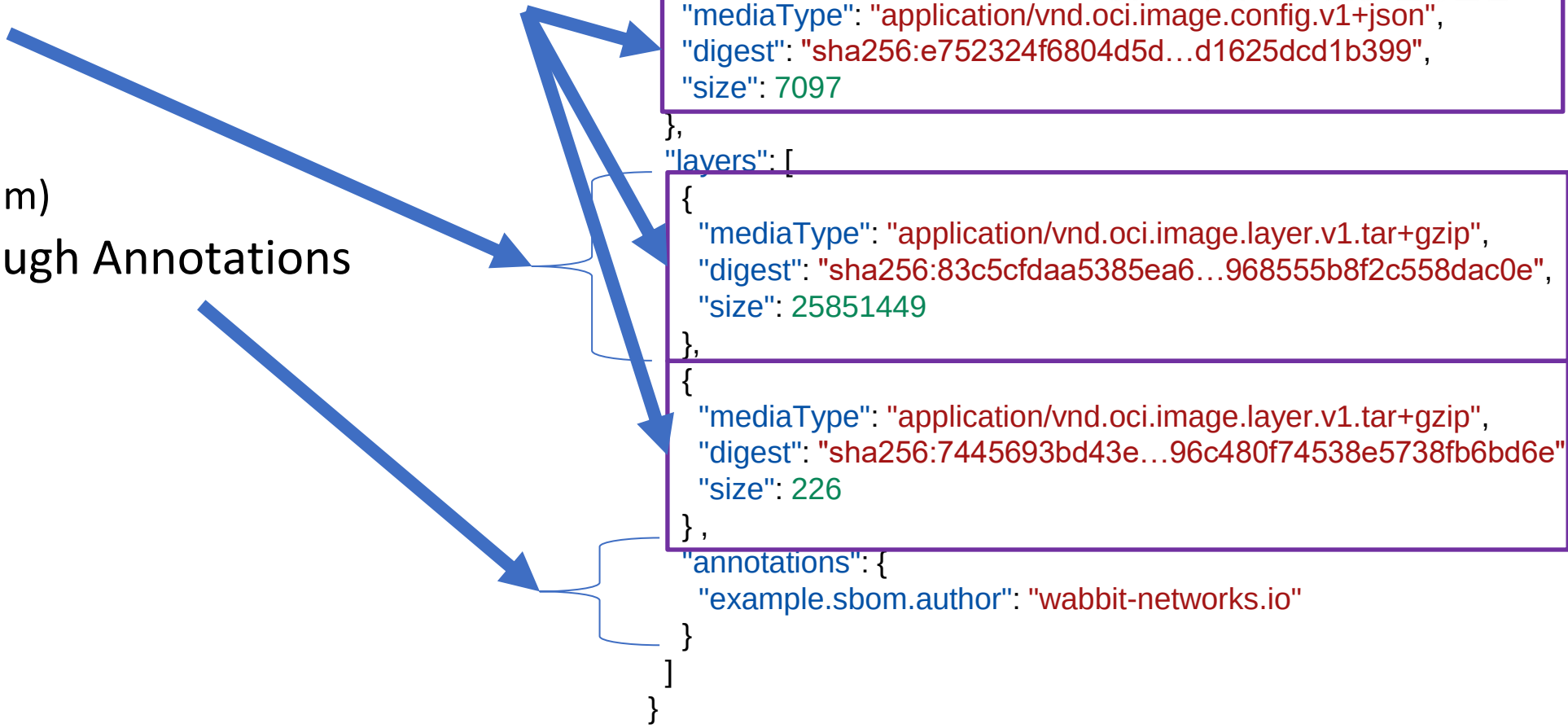
Manifest:
List of blob ID’s representing the entire thing

Blobs Please:
List of *compressed* blob URLs

- 85bef57c324acc96f7067488d35b7e3c1
- 1d57d886885835cbc52c2d85fe0ce008f
- f78a85a7da099d7494a5166a28e72a642
- da3343b41a78a0bcd4926d605b6fe37ba
- c935edcb03a0660b347d2fbf6542ee068

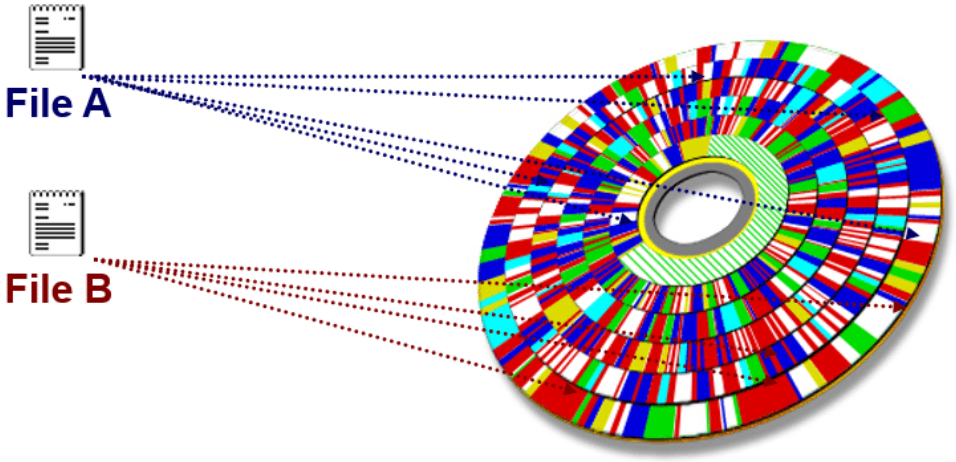
Elegance - Manifest

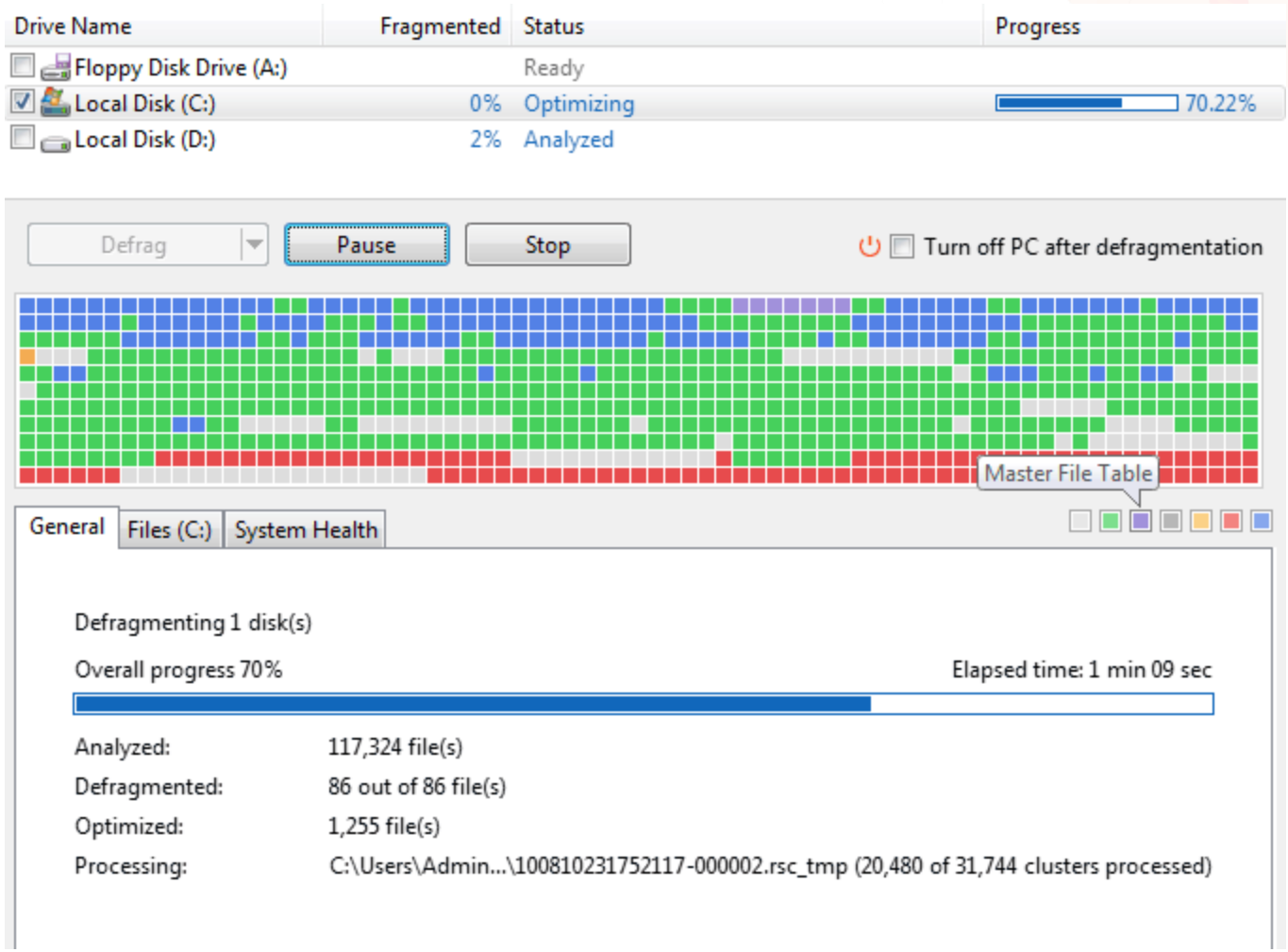
- Manifests provide:
  - Collections of Blobs (1* or more)
  - Descriptor
    - Type
    - Hash
    - Size (checksum)
  - Metadata through Annotations



Files

- foo.txt





Elegance - Manifest

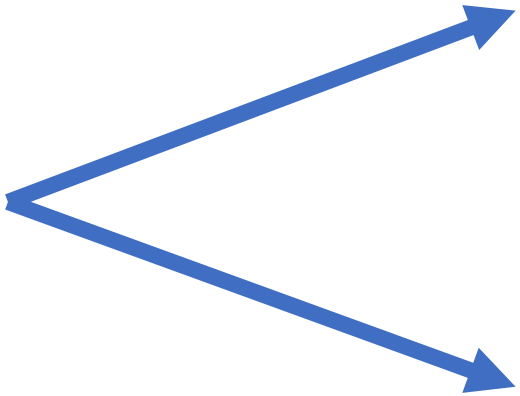
- **Manifest** = An Artifact (a container image is a type of artifact)
- **Blobs** = The content of the thing, segmented into 1 or more blobs

- Several Manifest Types
  - Docker Manifest — application/vnd.docker.distribution.manifest.v2+json
  - OCI Image Manifest — application/vnd.oci.image.manifest.v1+json

  - Docker Manifest List — application/vnd.docker.distribution.manifest.list.v2+json
  - OCI Index — application/vnd.oci.image.index.v1+json
  - … — but wait, there's more

Tags

net-monitor:v1



put manifest

```
{
  "mediaType": " application/vnd.oci.image.manifest.v1+json",
  "digest": " sha256:83c5cfdaa5385ea6…968555b8f2c558dac0e",
  "size": 12454
}
```

put manifest

```
{
  "mediaType": " application/vnd.oci.image.manifest.v1+json",
  "digest": " sha256: e752324f6804d5d…d1625dcd1b399",
  "size": 12454
}
```

Elegance of Distribution

- Manifest = Artifact
- Blobs = content of the artifact
  - Blobs can/should be de-duped[1]
- Secured in namespaces
- All content has unique identifiers (digests aka descriptors)
- Tags = pointers to a unique manifest descriptor
- Artifacts can be payloads from KB to GB and beyond

1. De-duping has security implications. Typically, de-duping within a controlled security boundary.

Kinda Useful

- Is there anything really unique to container images?

Adding Helm Repos to Azure Container Registry

Blog / Announcements

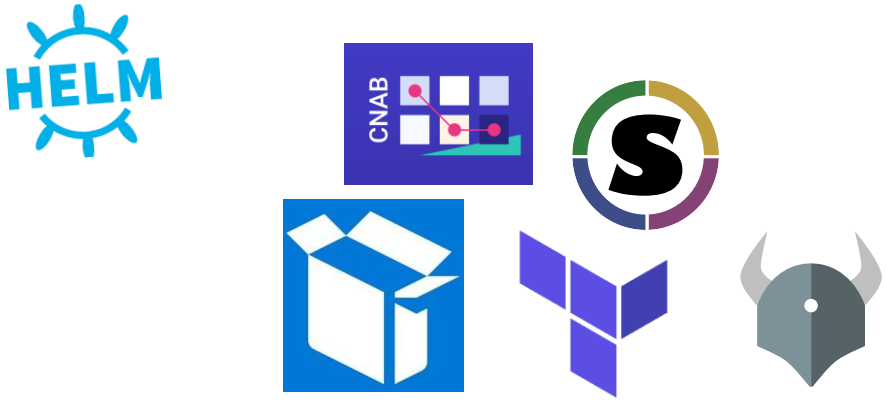
Azure Container Registry: Public preview of Helm Chart Repositories and more

Posted on September 24, 2018

Steve Lasker, Program Manager, Azure Container Registry

With Azure Container Registry (ACR), you can easily store and manage container images for Azure deployments in a central registry. Today we are excited to add native Helm repository support and validation workflows, with ACR tasks and Docker's content trust, to provide a more integrated container lifecycle management experience.

- **ACR Helm Chart Repositories**, available for public preview, provides Kubernetes Helm chart storage as an integrated service for container images and their deployment charts. http://aka.ms/acr/helm-repos



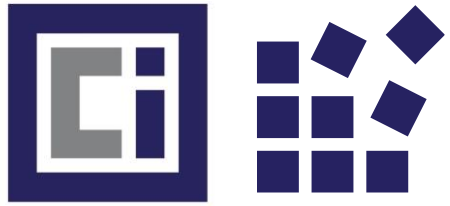
HELM 2

```
$ az login
$ az acr helm repo add -r $registry
$ helm package ./wordpress
$ az acr helm push wordpress-5.7.tgz
$ helm fetch $registry/wordpress --version ..
```

HELM 3 with OCI Artifacts

```
$ helm registry login $registry -u $user -p $pwd
$ helm chart save wordpress/ $registry/wordpress:5.7
$ helm chart push $registry/wordpress:5.7
$ helm chart pull $registry/wordpress:5.7
```

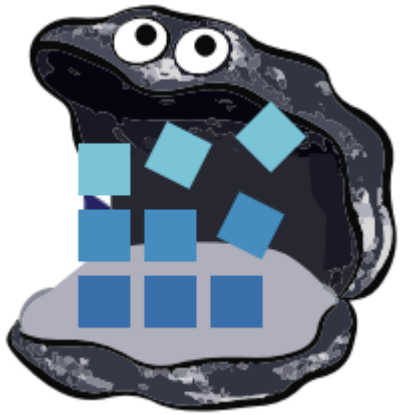
Evolution



Container Registries → Artifact Registries

!

Yet
Another
Storage
Solution



Correlation of Artifacts

- How do you discover different artifact types?
- Is there a relationship between the different types?
- What is it your looking for?
- What do you know?
  - Name of the artifact
    `registry.wabbit-networks.io/monitoring/net-monitor:v1`
  - What do you want to know?
    - Is it signed?
    - Does it have an SBOM, gitBOM, Scan Results, Claims
    - What is it's current support, or revocation status?

How…

- OCI Artifacts generalized registries for all types – individual
- ORAS Artifacts generalizes further, enabling referrers

- Concepts
  - I want to use the original named reference (tag or digest)
  - I want to discover what's related to the named artifact
  - I want to filter on specific artifact types
  - I want to sort the results, as there may be many (scan results)
  - I want to add metadata, to existing artifacts
  - I want to manage the lifecycle of the things as a whole

```
delete registry.acme-rockets.io/net-monitor:v1
```

Evolution

Investing in services that are already ubiquitous

Where to look for …

- You already have a registry, that can store all sorts of stuff
- What if…
  - You could ask the registry for what else it knows for the named thing?

```
oras discover registry.wabbit-networks.io/net-monitor:v1

registry.wabbit-networks.io/net-monitor:v1
├── notary.v2.signature
│   └── sha256:8c0e82624475a4ad64ddca2d68c0f82e316ec758591cb916049fe59eaf27b5b4
├── snyk.scan-results.v1
│   ├── sha256:95b97532a5b2d0c36cfcefd403b02779fb5afca07479a66bd509a635d5681e7f
│   ├── sha256:204e7c423c891d0e4b057c4ecb068a53ffc991ef5a3bb47467f1b8088775dc48
│   └── sha256:1b26826f602946860c279fce658f31050cff2c596583af237d971f4629b57792
├── spdx.sbom.v3
│   └── sha256:82d89db16266d13ab7680badfea3dbd91fd8e311c3b4291d9c0d4f9cff86fa50
├── cyclonedx.sbom.v1
│   └── sha256:c5fbdddecc83f1af8743983ce114452b856b77e92a5c7f4075c0110ea1e35e38
└── gitbom.v1
    └── sha256:fa3114698194096 4ced259bd2edd36c10277207e3be4d161bdb96e5e418fc2e0
```

Where to look for …

- You already have a registry, that can store all sorts of stuff
- What if…
  - You could filter for an artifactType, for your named thing

```
oras discover registry.wabbit-networks.io/net-monitor:v1 \
  artifactType=snyk.scan-results.v1 orderBy=date order=desc

registry.wabbit-networks.io/net-monitor:v1
└── snyk.scan-results.v1
    ├── sha256:95b97532a5b2d0c36cfcefd403b02779fb5afca07479a66bd509a635d5681e7f
    ├── sha256:204e7c423c891d0e4b057c4ecb068a53ffc991ef5a3bb47467f1b8088775dc48
    └── sha256:1b26826f602946860c279fce658f31050cff2c596583af237d971f4629b57792
```

Where to look for …

- You already have a registry, that can store all sorts of stuff
- What if…
  - You could filter for an artifactType, for your named thing

```
oras discover registry.wabbit-networks.io/net-monitor:v1 \
  artifactType=snyk.scan-results.v1 orderBy=date order=desc top=1

registry.wabbit-networks.io/net-monitor:v1
└── snyk.scan-results.v1
    └── sha256:95b97532a5b2d0c36cfcefd403b02779fb5afca07479a66bd509a635d5681e7f
```

Demo

Adding references to existing ~~images~~ artifacts

Evolution: Extending Manifest Support

- Registries already support multiple manifest types
- What if we added a new, generic manifest, that could support related content?

• Docker Manifest	application/vnd.docker.distribution.manifest.v2+json
• OCI Image Manifest	application/vnd.oci.image.manifest.v1+json
• Docker Manifest List	application/vnd.docker.distribution.manifest.list.v2+json
• OCI Index	application/vnd.oci.image.index.v1+json
• **Artifact Manifest**	**application/vnd.cncf.oras.artifact.manifest.v1+json**

Evolution: New Artifact Manifest

registry.wabbit-networks.io/net-monitor:v1
artifactType = container runtime image

```
{
 "mediaType": "application/vnd.oci.image.manifest.v1+json",
 "config": {
  "mediaType": "application/vnd.oci.image.config.v1+json",
  "digest": "sha256:e752324f6804d5d…d1625dcd1b399",
  "size": 7097
 },
 "layers": [
  {
   "mediaType": "application/vnd.oci.image.layer.v1.tar+gzip",
   "digest": "sha256:83c5cfdaa5385ea6…968555b8f2c558dac0e",
   "size": 25851449
  },
  {
   "mediaType": "application/vnd.oci.image.layer.v1.tar+gzip",
   "digest": "sha256:7445693bd43e…96c480f74538e5738fb6bd6e",
   "size": 226
  },
  "annotations": {
   "example.sbom.author": "wabbit-networks.io"
  }
 ]
}
```

registry.wabbit-networks.io/net-monitor@sha256:abc123...
artifactType = sbom/example

```
{
 "mediaType": "application/vnd.cncf.oras.artifact.manifest.v1+json",
 "artifactType": "sbom/example",
 "blobs": [
  {
   "mediaType": "application/tar",
   "digest": "sha256:9834876dcfb05cb167a5c…8f2f9d09af107ee8f0",
   "size": 32654
  },
  {
   "mediaType": "sbom/example.config.v1+json",
   "digest": "sha256:e752324f6804d5d…d1625dcd1b399",
   "size": 7097
  }
 ],
 "subject": {
  "mediaType": "application/vnd.oci.image.manifest.v1+json",
  "digest": "sha256:73c803930ea3b…51fe7b00369da519a3c333",
  "size": 16724
 },
 "annotations": {
  "org.cncf.oras.artifact.created": "2022:05:02T08:24:33:53",
  "example.sbom.author": "wabbit-networks.io"
 }
}
```

Evolution: Manifest

- Additional annotations
  - Information added after initial creation
  - No blobs, just annotations
  - Annotations may be indexed for querying across various artifacts

```
{
  "mediaType": "application/vnd.cncf.oras.artifact.manifest.v1+json",
  "artifactType": “application/vnd.cncf.oras.v1.annotations/",
  "subject": {
    "mediaType": "application/vnd.oci.image.manifest.v1+json",
    "digest": "sha256:73c803930ea3b…51fe7b00369da519a3c333",
    "size": 16724
  },
  "annotations": {
    “org.cncf.oras.artifact.new-version": “net-monitor:v2@sha256:abc123"
  }
}
```

Return all artifacts (descriptors) with **artifact.deletion-date < today**

Evolution: Referrers API

Template

```
GET /v2/{repository}/_oras/artifacts/referrers?digest={digest}
```

Example

```
GET /v2/net-monitor/_oras/artifacts/referrers?digest=sha256:3c3a4604a545cd…
```


```
{
  "referrers": [
    {
      "digest": "sha256:3c3a4604a545cdc127456d94e421cd355bca5b528f4a9c1905b15da2eb4a4c6b",
      "mediaType": "application/vnd.cncf.oras.artifact.manifest.v1+json",
      "artifactType": "signature/example",
      "size": 312
    },
    {
      "digest": "sha256:3c3a4604a545cdc127456d94e421cd355bca5b528f4a9c1905b15da2eb4a4c6b",
      "mediaType": "application/vnd.cncf.oras.artifact.manifest.v1+json",
      "artifactType": "sbom/example",
      "size": 237
    }
  ]
}
```


github.com/oras-project/artifacts-spec/blob/main/manifest-referrers-api.md

Artifact: Reference Type Principals

- Multiple artifacts exist, and none should have to create YASS
- Persisted alongside the subject artifact
  - Solves the discovery problem & network isolated/air-gapped environments
  - Reference Types artifacts can be copied with the target artifact
- Associated with, but separable from the target artifact
  - Solves the trojan horse validation challenge
- Target artifact must not change when adding new artifacts
  - docker pull registry.acme-rockets.io/net-monitor:v1
  - docker pull registry.acme-rockets.io/net-monitor@sha256:ca9c27f79cfc66befcd93f...
  - Helm chart references
  - Kubedeploy.yaml references

1- YASS- **Y**et **A**nother **S**torage **S**ervic

Thank You

KubeCon CloudNativeCon Europe 2022

- 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
- OCI Reference Types Working Group: github.com/opencontainers/wg-reference-types

Steve Lasker

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