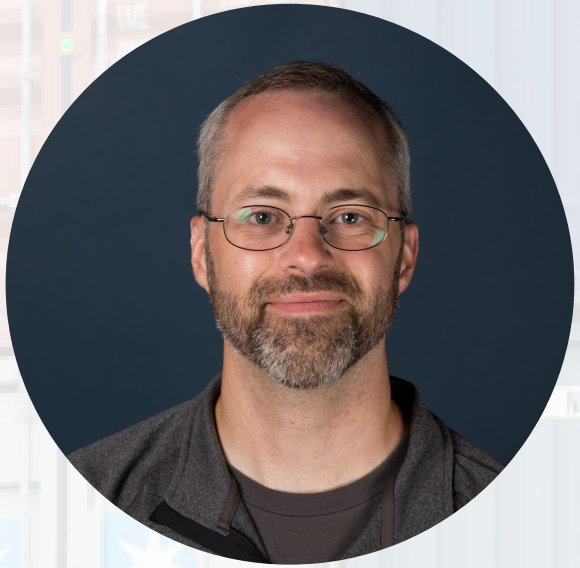
OCI IMAGE AND DISTRIBUTION SPEC 1.1

KCD DC 2024

Brandon Mitchell

2024-09-24



WHOAMI

```
$ whoami
- Brandon Mitchell
- OSS Developer
- OCI Maintainer, regclient, Docker Captain
- StackOverflow, CNCF, OpenSSF
```

OCI

- Open Container Initiative
- Under the Linux Foundation
- Defines the specifications for containers

OCI SPECS

1. runtime-spec
2. image-spec
3. distribution-spec

ARTIFACTS

- Formally defined in image-spec
- Uses the image manifest
- Added `artifactType` to manifests
- Defined an "empty" blob

ASSOCIATING ARTIFACTS

- Artifacts can be associated with another manifest
- Image signing, attestations, and other metadata
- Added a `subject` field to the manifest

QUERY ASSOCIATIONS

- Registries added a `referrers` API
- Clients fallback to managing a tag
- Returns an Index listing all manifests matching the `subject`
- Each pointer includes the `artifactType` and annotations

DATA FIELD

- base64 encoding of content inlined in a manifest
- Used when overhead of another registry round trip is greater than base64 encoding overhead

MANIFEST MAXIMUM SIZE

- Registries and tooling should support 4MiB manifests
- Don't pack everything in the data field or abuse annotations

DEPRECATED NON-DISTRIBUTABLE LAYERS

- These were included for Windows images
- No longer needed by Microsoft so their use is discouraged

ZSTD COMPRESSION

- Alternative to gzip compression for image layers
- May use less CPU and compress to a smaller size

MULTIPLE MATCHING PLATFORMS

- When an Index has multiple entries that clients cannot differentiate
- Clients pick the first matching entry
- Gives ability to introduce new features while supporting existing runtimes

REGISTRY API EXTENSIONS

- Allows registries to add custom APIs
- Will not conflict with future OCI APIs
- Register to avoid conflicting with other registries

RESUMABLE CHUNKED UPLOAD

- Allows an interrupted blob push to be resumed
- Needed to push large blobs on flaky networks

WARNING HEADER

- Registries can return a header on requests that client tooling should show
- Deprecation notices, security alerts, any non-fatal notification

ANONYMOUS BLOB MOUNTS

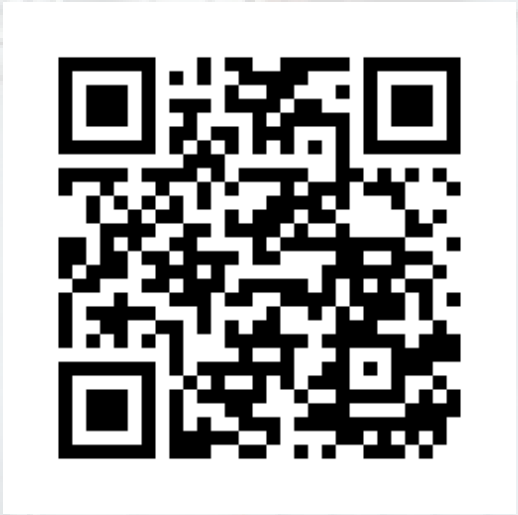
- Pushing an image can "mount" layers from another repository
- That blob "mount" no longer requires the source repository

SUMMARY

- Artifacts, Subject
- Data Field
- Maximum Size
- Deprecated Non-distributable Layers
- zstd Compression

- Referrers API
- Registry API Extensions
- Resumable Chunked Uploads
- Warning Header
- Anonymous Blob Mounts

THANK YOU



- Brandon Mitchell
- GitHub: sudo-bmitch
- Mastodon: fosstodon.org/@bmitch
- github.com/opencontainers

github.com/sudo-bmitch/presentations