OCI AND REGCLIENT

Cloud Native Luxembourg
Brandon Mitchell 2024-02-13

WHOAMI

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

OCI SPECS

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

REGISTRIES

- Registries implement the distribution-spec
- API and a bit of metadata/management on top of a data store
- Built on Merkle Trees and Content Addressability

BLOBS

- Lowest level data structure
- Opaque data (json, tar, gif, binary, etc)
- Named by the hash of its content

BLOB: CONTENT ADDRESSABILITY

```
$ regctl blob get ocidir://output/regctl \
    sha256:a0bbcef6dfea17bb0c9d6753e708f87... \
  | sha256sum
a0bbcef6dfea17bb0c9d6753e708f87...  -
```

BLOB: CONFIG

```
$ regctl blob get ocidir://output/regctl \
    sha256:a0bbcef6dfea17bb0c9d6753e708f87... \
  | jq .
{
  "created": "2023-11-09T19:36:19Z",
  "architecture": "amd64",
  "os": "linux",
  "config": {
    "User": "appuser",
    "Env": [
      "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin..."
    ],
    "Entrypoint": [
      "/regctl"
    ],
```

BLOB: LAYERS

```
$ regctl blob get ocidir://output/regctl \
    sha256:8d45cbeb0e9342913c7a1f5212daec96... \
  | tar -tvzf -
drwxr-xr-x 0/0               0 2023-11-09 14:36 etc/
-rw-r--r-- 0/0             720 2023-11-09 14:36 etc/group
-rw-r--r-- 0/0            1229 2023-11-09 14:36 etc/passwd
```

MANIFESTS

- JSON data structures parsed by registries
- Image manifests identify a blob for the config, and a list of blobs for layers
- Index manifests contain a list of manifests
- Each reference to content is a descriptor
  - JSON structure with: media type, digest, size

IMAGE MANIFEST

```
{
 "mediaType": "application/vnd.oci.image.manifest.v1+json",
 "config": {
  "mediaType": "application/vnd.oci.image.config.v1+json",
  "digest": "sha256:a0bbcef6dfea17bb0c9d6753e708f87be31...",
  "size": 3101
 },
 "layers": [
  {
   "mediaType": "application/vnd.oci.image.layer.v1.tar+gzip",
   "digest": "sha256:77cc5d38ae6cd88138627ad233e9701b7...",
   "size": 92
  },
...
 ],
```

INDEX MANIFEST

```
{
 "mediaType": "application/vnd.oci.image.index.v1+json",
 "manifests": [
  {
   "mediaType": "application/vnd.oci.image.manifest.v1+json",
   "digest": "sha256:d301bbb0aab4c166de121bf1b999b1cad02...",
   "size": 1298,
   "platform": {
     "architecture": "amd64",
     "os": "linux"
   }
  },
  ...
 ],
 "annotations": {
```

ARTIFACTS

- Manifests that do not package a runnable container image
- Image manifest is overloaded to serve artifacts
- Differentiate with config media type
- Defined an empty JSON blob to fill in required fields
- Added an "artifactType" field for artifacts without a config blob

ARTIFACT

```
{
  "mediaType": "application/vnd.oci.image.manifest.v1+json",
  "artifactType": "application/spdx+json",
  "config": {
    "mediaType": "application/vnd.oci.empty.v1+json",
    "digest": "sha256:44136fa355b3678a1146ad16f7e8649e9...",
    "size": 2
  },
  "layers": [
    {
      "mediaType": "application/spdx+json",
      "digest": "sha256:0dbd95a7a958019dbdc3c62e423bcc7...",
      "size": 17415
    }
  ],
```

TAGS

- Named pointer to a manifest digest in a repository
- Designed to be human readable
- Mutable: "v1" today may be different from last week
- Non-exclusive: "v1" and "v1.2.3" may point to the same digest

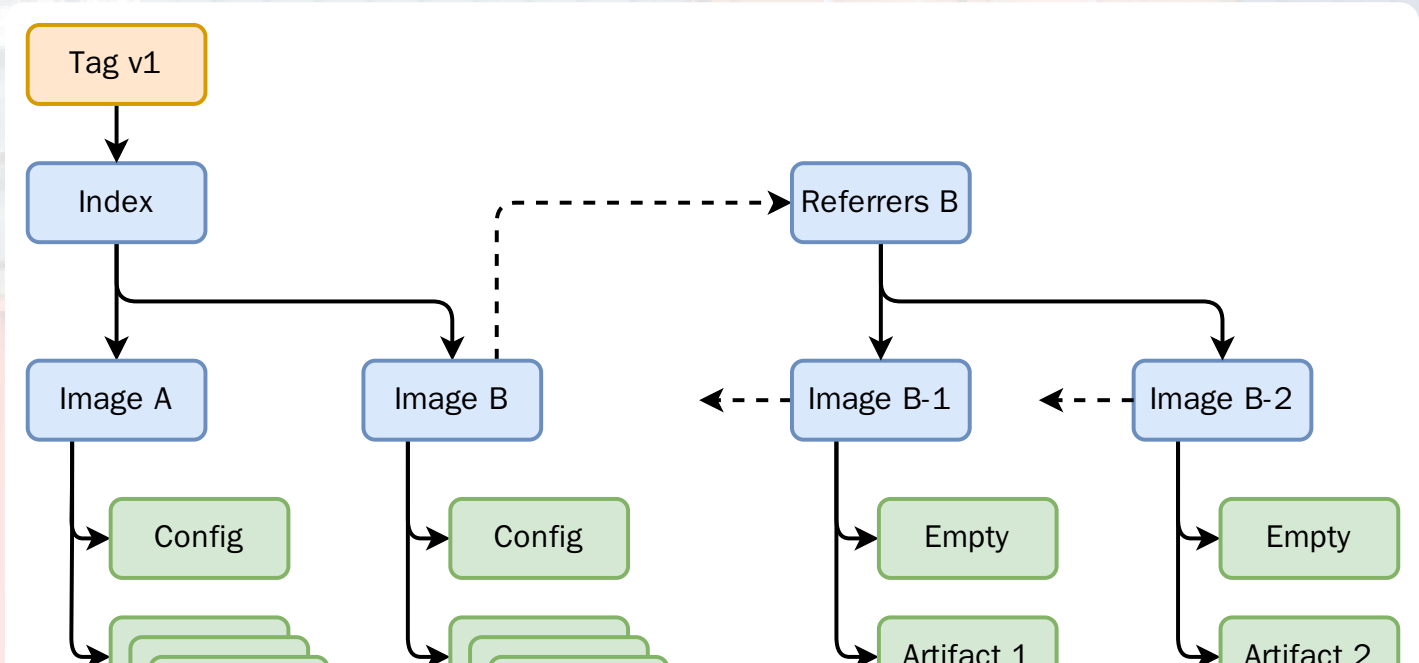
REFERRERS

- New API discovering loose relationships between manifests
- Associate signatures, attestations, SBOMs, etc, with an image
- Subject descriptor in a manifest may reference another manifest
- Referrers API returns an index of all manifests with a

REFERRERS FALLBACK

- Image and Index manifests are extended
  - Added the "subject" and "artifactType" fields
  - New fields should be ignored by old tools
- Client tooling falls back to managing a Tag
  - Tag is formatted `sha256-1234...`
  - Response is an Index manifest

DATA STRUCTURE



OCI LAYOUT

- Filesystem definition for a repository
- Uses and index to reference the manifests/tags
- Filenames for content addressability
- Useful for air-gap, CI pipelines, and scanners

OCI ECOSYSTEM

- Build tooling: buildkit, buildah, kaniko, buildpacks
- Runtimes: containerd/runc, podman, crun, wasm
- Applications: Helm, Flux, sigstore/cosign, notation
- Clients: crane, ORAS, regclient, skopeo

REGCLIENT

- Go client library
- regctl: CLI for regclient
- regsync: tool for maintaining mirrors
- regbot: Lua based scripting

REGCTL: QUERY

```
regctl tag ls
regctl image digest
regctl manifest get

regctl image config
regctl blob get
regctl artifact list
regctl artifact get
regctl image get-file
regctl blob get-file
```

REGCTL: COPY

```
regctl image copy
regctl image import
regctl image export
```

REGCTL: CREATE

```
regctl index create

regctl index add
regctl index rm
regctl artifact put
regctl manifest put
regctl blob put
```

REGCTL: DELETE

```
regctl manifest rm
regctl tag rm
```

REGCTL: COMPARE

```
regctl manifest diff
regctl blob diff-config
regctl blob diff-layer
```

REGCTL: MODIFY

```
regctl image mod
```

REGSYNC

- Managed with a yaml config
- Schedule updates by cron or frequency
- Concurrency
- Backup before overwriting
- Filtering tags (in or out)
- Monitoring rate limits (Docker Hub)

```yaml
sync:
  - source: busybox:latest
    target: registry:5000/library/busybox:latest
    type: image
    backup: "bkup-{{.Ref.Tag}}"
  - source: alpine

    target: registry:5000/library/alpine
    type: repository
    tags:
      allow:
      - "latest"
      - "3"
      - "3.\\d+"
```

REGBOT

- Lua interface to various regclient APIs
- Allows scripting for retention policies
- Can also be used for more complex image copy commands

```
scripts:
  - script: |
      ref = reference.new("registry:5000/regclient/example")
      tagExp = "^ci%-%d+$"
      imageLabel = "org.opencontainers.image.created"
      cutoff = os.date("!%Y-%m-%d", os.time() - (86400*30))
      tags = table.sort(tag.ls(ref))

      for k, t in pairs(tags) do
        if string.match(t, tagExp) then
          ref:tag(t)
          ic = image.config(ref)
          if ic.Config.Labels[imageLabel] < cutoff then
            tag.delete(ref)
          end ...
```


DEMO

USEFUL LINKS

- github.com/opencontainers/image-spec
- github.com/opencontainers/distribution-spec
- github.com/regclient/regclient/
- github.com/olareg/olareg

THANK YOU

- Brandon Mitchell
- GitHub: sudo-bmitch
- Mastodon: @bmitch@fosstodon.org
- Twitter: @sudo_bmitch