

Which Tool Mirrors a Cosign-Signed Image into a Private Registry?

2026-07-06

A verified, sourced comparison of `regctl`, `oras`, `skopeo`, `Zot`, `Harbor`, and `cosign copy` for mirroring a Cosign-signed container image into a private registry.

TL;DR

`regctl` is the most complete option — it exposes the legacy tag-based signature scheme and the modern OCI 1.1 referrers API as two separate, explicit flags. `oras cp -r` is the second choice, and the tool `cosign`'s own project points to now that `cosign copy` is deprecated. `oc-mirror v2` looks like it should be on this list but actually solves a different, unrelated signature problem.

The problem

Verifying a signature only works if the signature actually travels with the image. Anyone mirroring a Cosign-signed image into a private or air-gapped registry needs the copy step itself to carry the signature along, not just the layers — and that is not automatic. Some tools drop it silently, some need a config flag turned on first, and one widely-used tool solves a related but entirely different problem. [k8s-scale-app-rs](#) is the worked example throughout this post — its own container images are signed keylessly with `cosign`, carry an SBOM and SLSA build provenance, and its “[Verifying a published image](#)” section shows what verification actually checks. This post is about what happens *before* verification: getting the signature into the registry the verifier will actually query.

A short, sourced comparison, checked directly against each project's docs/source (as of July 2026):

A naming trap worth knowing first

Red Hat's `oc-mirror v2` — the tool for mirroring into disconnected OpenShift installs — has its own `--secure-policy/--remove-signatures/--registries.d` flags, but they implement Red Hat's older “simple signing” scheme: a `policy.json` plus GPG keys plus an external `sigstore: URL` (e.g. `mirror.openshift.com/pub/openshift-v4/signatures` for OpenShift release images). That predates, and has nothing to do with, the CNCF Sigstore project this post's `cosign` workflow uses — same word, unrelated mechanism. `oc-mirror v2` went GA in OpenShift 4.18 ([release notes](#)), but its `ImageSetConfiguration` API is still `v2alpha1`, and none of Red Hat's own walkthroughs for it touch Cosign-style signatures at all.

Tool comparison

Tool	Legacy tag-based signature (sha256- <digest>.sig)	OCI 1.1 refererrs (modern Cosign/SBOM/attestations)	Note
<code>regctl image copy</code>	<code>--digest-tags</code>	<code>--refererrs</code>	only tool here with separate, explicit flags for both schemes
<code>oras cp -r</code>	via <code>-r</code>	<code>-r</code> (marked "Preview")	<code>--from/to-distribution-spec</code> handles refererrs-tag vs. refererrs-API mismatches between registries
<code>skopeo copy</code>	opt-in	not supported	needs <code>use-sigstore-attachments: true</code> under the <code>default-docker</code> key in <code>registries.d</code> , on both source and destination
Zot registry <code>sync</code>	<code>syncLegacyCosignTags</code> (default true)	only with <code>preserveDigest: true</code>	without <code>preserveDigest</code> , Zot re-encodes Docker-format images to OCI on sync, which changes the digest and detaches the signature
<code>cosign copy</code>	yes	no	deprecated as of sigstore/cosign#4681 (merged 2026-02-04) — the tool itself now points to <code>oras copy -r</code> instead
<code>crane copy</code>	only incidentally, via <code>--all-tags</code>	no	plain manifest/layer copier, no signature awareness at all
Harbor replication	per Harbor's own docs, yes	open gap (goharbor/harbor#23210)	works for the legacy scheme; OCI 1.1 refererrs replication is not yet reliable

`regctl` is the only tool in this comparison that exposes both signature schemes as distinct, intentional flags rather than as a side effect of copying "everything." For a registry pair that already speaks the OCI 1.1 refererrs API end to end, `oras cp -r` is the other option worth checking — it's what the cosign project's own deprecation notice for `cosign copy` points to.

Example: mirroring with regctl

Here is an example command to mirror `k8s-scale-app-rs` itself, signature included, using `regctl`:

```
regctl image copy \  
  --digest-tags --referrers \  
  ghcr.io/git001/k8s-scale-app-rs:v1.0.0 \  
  my-private-registry.example.com/k8s-scale-app-rs:v1.0.0
```

Sources

- [sigstore/cosign PR #4681](#) — “Deprecate cosign copy”
- [sigstore/cosign#4335](#) — Complete OCI 1.1 Referrers API Support Across All Cosign Commands
- [sigstore/cosign#4564](#) — cosign verify fails after cosign copy (JFrog Artifactory)
- [podman-container-tools/skopeo#2061](#) — sigstore signature copying and use-sigstore-attachments
- [regctl image copy](#) reference
- [oras cp](#) command reference
- [goharbor/harbor#23210](#) — OCI 1.1 referrers not replicated
- [Zot registry: mirroring/sync](#) documentation
- [OpenShift Container Platform 4.18](#) release notes
- [openshift/oc-mirror](#) — signature-verification.md