



**KubeCon**



**CloudNativeCon**

**North America 2024**





KubeCon



CloudNativeCon

North America 2024

# What containerd 2.0 means for you

Samuel Karp, Google



KubeCon



CloudNativeCon

North America 2024

containerd 2.0 is now available!

# Agenda

- What's new
- What's changing
- Deprecations and removals
- Preparing to upgrade
- How you can remediate any issues
- Where to find help
- What's next
- Q&A



KubeCon



CloudNativeCon

North America 2024

# So what's new?

# New features, newly stable features, defaults

- Transfer service NOW STABLE
- Sandbox service (and sandboxed CRI) NOW STABLE
- Faster image extraction with igzip NEW
- Improved OTEL configuration NEW
- NRI enabled by default NEW
- Image verifier plugins NEW
- Plugin introspection NEW
- CDI enabled by default NEW
- CRI support for user namespaces NEW

# Highlight: Node Resource Interface (NRI)

- Akin to a mutating webhook, but for container configuration
  - Middleware between CRI and OCI
- Use cases
  - Injection (devices, network devices, OCI hooks)
  - Resource modification/management (ulimits, topology/NUMA, advanced QoS, SGX memory)
  - Policy enforcement
- Plugins can run in containers or as system services
- Enabled by default
- Community plugins
  - <https://github.com/containerd/nri/tree/main/plugins>
  - <https://github.com/containers/nri-plugins>

# Highlight: Image verifier plugins

- Exec-based plugins containerd invokes during image pull
- Policy enforcement use-cases
  - Container image signature verification
  - Trust for particular signers
  - Allow only specific registries/repositories
- Integrated with the Transfer service (not supported for legacy pulls)





KubeCon



CloudNativeCon

North America 2024

# Changes

(non-breaking)

- Go client library as a separate package
  - Now in [github.com/containerd/containerd/v2/client](https://github.com/containerd/containerd/v2/client)
- gRPC API is versioned separately from containerd
  - Go package [github.com/containerd/containerd/api](https://github.com/containerd/containerd/api)
- CRI registry properties are deprecated (but not removed)
  - `mirrors`, `auths`, and `configs` of `[plugins.\"io.containerd.grpc.v1.cri\".registry]`
  - Targeted for removal in 2.1
  - `auths` replaced by credential manager plugins
- Go-plugin (`*.so`) libraries are deprecated
  - Targeted for removal in 2.1
- Envelope type is changing
  - `types.Envelope` replaces `service.events.Envelope` and `ttrpc.events.Envelope`
  - Targeted for removal in a future release



KubeCon



CloudNativeCon

North America 2024

# Deprecations $\Rightarrow$ Removals

(breaking changes)



KubeCon



CloudNativeCon

North America 2024

Removals can be scary

But don't worry

We'll talk about how to prepare next

- Docker Schema 1 image support DISABLED BY DEFAULT
- CRI v1alpha2 API
- Default **LimitNOFILE** in systemd unit
- **io\_uring\_\*** syscalls in default seccomp profile
- **io.containerd.runtime.v1.linux** and **io.containerd.runc.v1**
- **containerd.io/restart.logpath** label
- AUFS snapshotter
- CRI+CNF release bundles



KubeCon



CloudNativeCon

North America 2024

# Preparing to upgrade

(finding out if you need to take action)

- Deprecation warnings exposed by containerd
  - Usage-based; warnings show up if usage is detected
  - If you see the warning, you should expect to take action
- Use `ctr deprecations list` to see warnings (optional: `--format json`)
- The `lastOccurrence` field records the last time the deprecated feature was used.\*
- Warnings are cleared when containerd is restarted
- Use at least containerd 1.7.12 or 1.6.27

\* Config-related warnings will show the time containerd started. The CRI v1alpha2 warning will show the first occurrence for containerd versions before 1.7.21 and 1.6.36.

# Deprecation warnings

- **ctr deprecations list**
- Supported in v1.7.12+, v1.6.27+
- For each warning, you can see
  - What is being removed
  - A suggestion for migration
  - When it was last used

```
→ containerd git:(v1.6.28) sudo ctr deprecations list --format json
```

```
[
  {
    "id": "io.containerd.deprecation/pull-schema-1-image",
    "message": "Schema 1 images will be deprecated in containerd v1.7 and removed in containerd v2.0. Since containerd v1.6.25, schema 1 images are identified by the \"io.containerd.image/converted-docker-schemal\" label.",
    "lastOccurrence": "2024-03-02T13:06:48.901759427Z"
  },
  {
    "id": "io.containerd.deprecation/runtime-runc-v1",
    "message": "The `io.containerd.runc.v1` runtime is deprecated since containerd v1.4 and removed in containerd v2.0. Use the `io.containerd.runc.v2` runtime instead.",
    "lastOccurrence": "2024-03-02T13:02:07.964720821Z"
  },
  {
    "id": "io.containerd.deprecation/runtime-v1",
    "message": "The `io.containerd.runtime.v1.linux` runtime is deprecated since containerd v1.4 and removed in containerd v2.0. Use the `io.containerd.runc.v2` runtime instead.",
    "lastOccurrence": "2024-03-02T13:03:47.795952561Z"
  }
]
```



1. Upgrade to the latest 1.7.x or 1.6.x release of containerd
  - a. (prefer at least 1.7.21 or 1.6.36)
2. Find your impact through deprecation warnings
3. Remediate the warnings
  - a. Config format v1 will be auto-migrated; you can convert fully later
4. Test to make sure no warnings reoccur (restart containerd or create new nodes)
5. Try upgrading to containerd 2.0 (test clusters are a good practice)
6. Upgrade when you are ready
  - containerd 1.6 will be supported until the next LTS
  - containerd 1.7 will transition to Extended support in 6 months

- Providers can integrate warnings into their systems for you
- Case study: Google Kubernetes Engine
  - containerd 2.0 is currently expected in GKE 1.33
  - Deprecation warnings exposed as Node Conditions
  - Recommendations surfaced in the Google Cloud console (coming soon)
  - Automatic upgrades to containerd 2.0 will be blocked if deprecated feature use is detected



KubeCon



CloudNativeCon

North America 2024

# Remediation

(selected highlights)

# Highlight: Docker Schema 1 images

- Media type:  
`application/vnd.docker.distribution.manifest.v1+prettyjws`
- Replaced by Docker schema 2 (2014) and OCI Images (2017)
- Most modern images are not schema 1
- containerd labels schema 1 images for you  
`ctr image list 'labels."io.containerd.image/converted-docker-schema1"'`
- containerd can convert for you; pull + push image to fix
- Schema 1 support can be re-enabled, but will be removed in 2.1

# Highlight: CRI v1alpha2

- CRI v1 replaced v1alpha2 in Kubernetes 1.23
- Kubelet should use the correct version
- Other workloads may still depend on v1alpha2
- Use containerd 1.7.21 and 1.6.36 for accurate warnings

# Highlight: Sandboxed CRI

- *Not* a deprecation
- Sandboxed CRI replaces legacy CRI
- Internal refactor of CRI support on top of the new Sandbox and Sandboxer abstractions
- Try it out in 1.7 with `ENABLE_CRI_SANDBOXES=true` in `containerd.service`

# The rest of the changes

- Most deprecations have direct replacements
- <https://containerd.io/releases/#deprecated-features>
- Deprecation warnings will also provide suggestions
- Most applications should degrade gracefully for **io\_uring** changes

- Guide to containerd 2.0:  
<https://github.com/containerd/containerd/blob/main/docs/containerd-2.0.md>
- Discussions: <https://github.com/containerd/containerd/discussions>
- Slack: **#containerd** on [cncf.slack.io](https://cncf.slack.io)
- Community meetings: [cncf.io/calendar](https://cncf.io/calendar) (2nd and 4th Thursdays)





KubeCon



CloudNativeCon

North America 2024

# What's next

(2.1 and beyond)

# What's next



KubeCon



CloudNativeCon

North America 2024

- 2.1 milestone:  
<https://github.com/containerd/containerd/milestone/48>
- OCI Image Volume Source (KEP-4639)
- Continuing improvements to Sandboxes/Sandboxers
- Image pull improvements (multi-part layer fetch)
- Integration for CRI with the Transfer service
- Credential manager plugins for Transfer service



KubeCon



CloudNativeCon

North America 2024

# containerd maintainer session “What’s going on in the containerd neighborhood”

2:55pm-3:30pm

Hyatt Regency | Level 4 | Regency Ballroom A

# Q&A

Join us on Slack:

`#containerd` and `#containerd-dev` at [slack.cncf.io](https://slack.cncf.io)

Community meetings on [cncf.io/calendar](https://cncf.io/calendar)

[github.com/containerd/containerd](https://github.com/containerd/containerd)

# A brief note before we finish –

Feedback provides valuable information to speakers (and I'd really appreciate yours)!

Feedback that is very helpful:

- Topics you were excited to learn about
- Suggestions for improving understanding and clarity

Please avoid comments unrelated to the talk subject or content  
(refer to the CNCF Code of Conduct)

Follow the QR code to leave session feedback!

