OCI certification updates

OCI Runtime and OCI Image

Hi, I'm Alban

Alban Crequy
CTO @ Kinvolk

alban@kinvolk.io

OCI certification updates

- Spec and tools repositories
- Monthly GitHub activity
- Testing different runtimes
- Updated tests & new tests

OCI specs and tests

OCI	Spec	Tests
Runtime	github.com/opencontainers/runtime-spec	github.com/opencontainers/runtime-tools
Image	github.com/opencontainers/image-spec	github.com/opencontainers/image-tools
Distribution	github.com/opencontainers/distribution-spec	

Runtime monthly activity

runtime-spec

> Excluding merges, **1 author** has pushed **1 commit** to master and **1 commit** to all branches. On master, **11 files** have changed and there have been **198 additions** and **7 deletions**.

runtime-tools

> Excluding merges, **4 authors** have pushed **17 commits** to master and **17 commits** to all branches. On master, **65 files** have changed and there have been **1,928 additions** and **1,314 deletions**.

Image monthly activity

image-spec

none

image-tools

none

Distribution monthly activity

distribution-spec

Excluding merges, **29 authors** have pushed **78 commits** to master and **78 commits** to all branches. On master, **11 files** have changed and there have been **5,939 additions** and **4 deletions**.

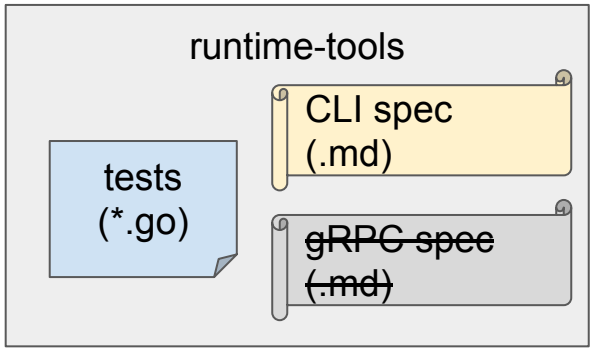
~~distribution-tools~~

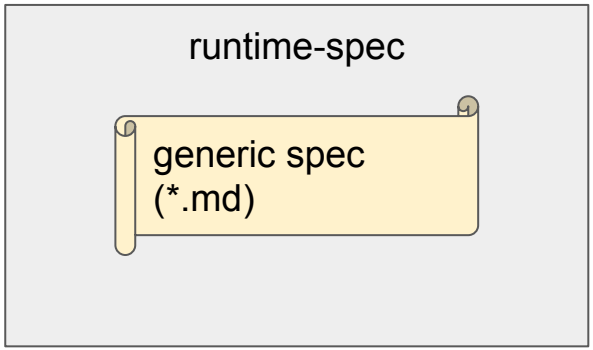
Testing OCI runtimes

- Running the tests manually:
  - All the tests

    ```
    $ sudo make RUNTIME=runc localvalidation
    ```
  - Choosing one test

    ```
    $ sudo RUNTIME=runc validation/hostname.t
    ```





Testing OCI runtimes

- Running the tests manually:
  - All the tests

    ```
    $ sudo make RUNTIME=runc localvalidation
    ```
  - Choosing one test

    ```
    $ sudo RUNTIME=runc validation/hostname.t
    ```
- Running tests in CI:

runc	**crun**	**bwrap-oci**
PR for Travis runc#1758 (pending review)	PR for Travis crun#3 (merged but then removed)	Blocked by bwrap-oci#18 (operations create & start missing)

Testing runc

alban commented 12 days ago Contributor

I rebased this PR and this ran the tests on Travis again. The tests show the following errors:

Issues in runc:

- [ ] validation/delete.t: #1774
- [ ] validation/linux_rootfs_propagation_shared.t: #1755

Limitation of the TravisCI platform

- [ ] validation/linux_cgroups_blkio.t
- [ ] validation/linux_cgroups_relative_blkio.t

Bug in the certification tests:

- [ ] validation/linux_masked_paths.t
- [ ] validation/linux_readonly_paths.t
- [ ] validation/start.t

To investigate:

- [ ] validation/linux_rootfs_propagation_unbindable.t
- [ ] validation/linux_seccomp.t
- [ ] validation/misc_props.t
- [ ] validation/process_capabilities_fail.t

▶ Details

Testing other implementations

- runc
  - Some issues reported
    - rootfsPropagation, state, hooks
- crun
  - Minor issue fixed (cmd params)
- bwrap-oci (Bubblewrap)
  - Blocked by create|start issue
- railcar
  - Blocked by seccomp issue
- spawn-oci (systemd-nspawn)
  - Does not exist yet

- docker, containerd, CRI-O
  - Use runc internally but don’t expose the CLI interface
- rkt
  - Issues for supporting the OCI Runtime & Image spec
  - Issue for using runc at the app-level

Scope of OCI runtime certification

- Containerd, docker = high level runtimes, use runc but don’t expose OCI interfaces
- https://github.com/opencontainers/certification/issues/36
- Ideas from that issue:
  - Expose the OCI interface. Does not make much sense technically.
  - Certify when they use an unmodified version of runc + sign agreement that they do
  - Building a test/mock runc and check that they call it correctly + log that they exercice different features
  - Run a container that gives a report
- Priority: continue tests for runc-like first (IMHO)

Updates in runtime-tools since March 2018

```
$ git shortlog --no-merges  -sne \
          d2b5e631979a4a6afe56d29198ac357806e128d4..origin/master

    15  W. Trevor King <wking@tremily.us>
    14  Zhou Hao <zhouhao@cn.fujitsu.com>
    10  Alban Crequy <alban@kinvolk.io>
     4  梁辰晔 (Liang Chenye) <liangchenye@huawei.com>
     3  Vincent Batts <vbatts@hashbangbash.com>
     1  Dongsu Park <dongsu@kinvolk.io>

 82 files changed, 2731 insertions(+), 1589 deletions(-)
```

(but some PRs are in progress...)

Updates: TAP

- TAP refactoring
  - Some error messages were wrong
  - Fix output (incorrect numbering)
  - Granular output
  - More precise errors with reference to the spec
  - Developer documentation

```
ok 208 - has a file at default symlink path "/dev/stdin"
  ---
  {
    "level": "MUST",
    "path": "/dev/stdin",
    "reference": "https://github.com/opencontainers/runtime-spec/blob/v1.0.0/runtime-linux.md#de
  }
  ...
```

Updates: misc fixes & refactoring

- Misc refactoring to support tests
  - Update Gentoo base for the process running in the container
- Updates in cmd/runtimetest to support tests
  - Tests for RW/RO
  - Tests for propagation mounts
- Updates in the ‘generate/’ library to support tests
  - Process-username, UID/GID
  - seccomp
- Improve support for other platforms (linux, solaris, windows)

Updates: updated tests

- Test updates:
  - rlimits: more complete tests
  - fixed UID mappings for user namespace
  - Fix RO test and remove RW test (when it’s not part of the spec)
- New tests:
  - Capabilities
  - process_user
  - hooks stdin test
  - ConfigUpdatesWithoutAffect
  - annotations
  - delete

Scope of OCI Image certification

- Issue https://github.com/opencontainers/certification/issues/35
- What should we certify?
  - Certify a specific image, e.g. image of Redis v2
    - Previous work & PRs are about this
  - Certify a OCI runtime (conversion OCI image -> OCI bundle)
  - Certify Registry services (we would need progress on distribution-spec)
  - Certify builders (“docker-build”, buildah...)
- Discussion from that issue:
  - Having tests for the conversion (OCI image -> OCI bundle) would be useful.
  - The spec is giving a lot of freedom. So, certifying that is tricky with edge cases.
- Or, just wait until the OCI distribution spec progresses a bit...

Questions / discussion