Date: *July 15th, 2014*
Submitted by: Rob Hirschfeld and Joshua McKenty

Topic: **DefCore**

Executive Summary:

DefCore has made significant progress delivering the first artifacts of the progress including an advisory Havana Capabilities definition for approval today. We've also had to make adjustments that impact schedule including owning Designated Sections (instead of the TC as expected) and challenges adapting Tempest to Refstack needs.

Proposed Board Actions:

1. **Approve Havana Advisory Core Definition (Capabilities & Tests List)**
2. **Reconsider guidance about "do not reveal" vendor names ("pass only")**
3. **Schedule special meeting about Designated Sections (September)**

Proposed Implementation:

- Board approves the following capabilities as *advisory* Havana Core:
  - compute-servers
  - volume
  - compute-volume
  - compute-quotas
  - compute-flavors
  - images-v1
  - compute-auth
  - images-v2
  - objectstore-object
  - compute-keypairs
  - compute-servers-metadata
  - objectstore-container
  - volume-snapshots
  - compute-images
  - compute-floating-ips
  - compute-instance-actions
- The tests included in each capability are defined in https://github.com/stackforge/refstack/tree/master/defcore and may be adjusted based on review by DefCore.
- At this time, no designated sections have been determined. This work will be reviewed and approved at the requested special Board meeting in September.

Background Information / Reason for Board Consideration:

This is part of the ongoing operation of the DefCore process. Approving the Havana capabilities is part of the expected timeline. If approved, DefCore remains on target to present official Ice House core capabilities and designated sections at the Paris board meeting. If not approved, DefCore will have to adjust the timeline based on board direction.

Overall, community reaction to the DefCore process has been positive. While unexpected, the TC asking the Board to own designated sections does not compromise the process. We need to validate TC acceptance of the process with this change; however, there is reason to expect approval since the change matches their own recommendation.

Previous Restrictions: Anonymous Data Only

At the Atlanta Summit, DefCore and Refstack agreed that we would adjust the upload expectations to only take “pass” results and treat all skip or fail results as “no data.” This change greatly reduces the risk of leaking secure data from error logs and also improves the positive perception of results. Specifically, results will collect have positive results. These results will be compared to the required core set to determine “core” or “not core.” No additional information is needed.

We believe this simplification addresses the board’s earlier concern about flagging vendor results. At this time, we’d like the board to soften earlier guidance and allow vendors to optionally claim their results.

Financial, Legal Implications:

The DefCore process is loosely coupled to a recommended change in the bylaws. This relatively minor change will shift from a “project defined” core to one that is more process and test oriented. Since this change requires substantial community participation to pass, it is vital that we have strong support from the Board and TC.

However, the Bylaws change as proposed is primarily cosmetic. The Capabilities-based definition of Core *could* be rolled out to govern the commercial trademark licenses without this Bylaw change. The purpose of the change is to remove confusing language and accommodate the more flexible “designated sections” concept.

Rather than embedding the current DefCore process into the Bylaws, we propose a bylaws change that references the DefCore process as an appendix (attached as Addendum 2). Updates to this process would be by a simple majority of the Board.

Foundation Impacts

The Foundation staff must remain engaged in the DefCore process. The process will have an impact in updating license agreements, vendor engagement and trademark rollouts. In addition, the DefCore deliverables need to account for the pre-summit frenzy for announcements.

The Board should be aware that vendors will want to apply Ice House criteria and designated sections at least 3 weeks before the summit.

Issues / Discussion Topics

In discussion, we've learned that there are some import points to clarify:

1. DefCore is for commercial use of the brand only
2. "core" requires projects having BOTH the required capability & designated code
3. if a project lacks a required capability then we don't consider designated code

Here topics to review:

- Discuss alignment with TC regarding DefCore process and bylaws changes
- Challenges with Refstack cross dependencies on Tempest
    - testing issues on Tempest & configuration
- Discuss designated sections on "hot items" > Swift, Keystone

DefCore believes that Swift has required capabilities; however, we also recognize that 1) it is not modular code in Havana and 2) there are several commercial implementations of OpenStack that use alternatives to Swift but could/would pass the capabilities test.

To be addressed in September, the critical question for Havana Swift comes down to these choices:

1. keep the required capabilities and say no designated sections: vendors are OK
2. keep the required capabilities and all designated: vendors cannot claim OpenStack
3. drop the required capabilities and all designated: vendors are OpenStack w/o Swift

Reminder: designated sections can change release to release.

Related Materials:

Reference Materials:

- Havana Capabilities: https://wiki.openstack.org/w/images/e/e3/DefCore_Capabilities_Scoring.pdf
- Addendum 1: DefCore Process Flow
- Addendum 2: DefCore Process draft for Bylaws
- https://etherpad.openstack.org/p/DefCoreLighthouse.Bylaws1
- TC Scoring: https://review.openstack.org/#/c/100721/3/resolutions/20140617-defcore-capabilities-scoring.rst

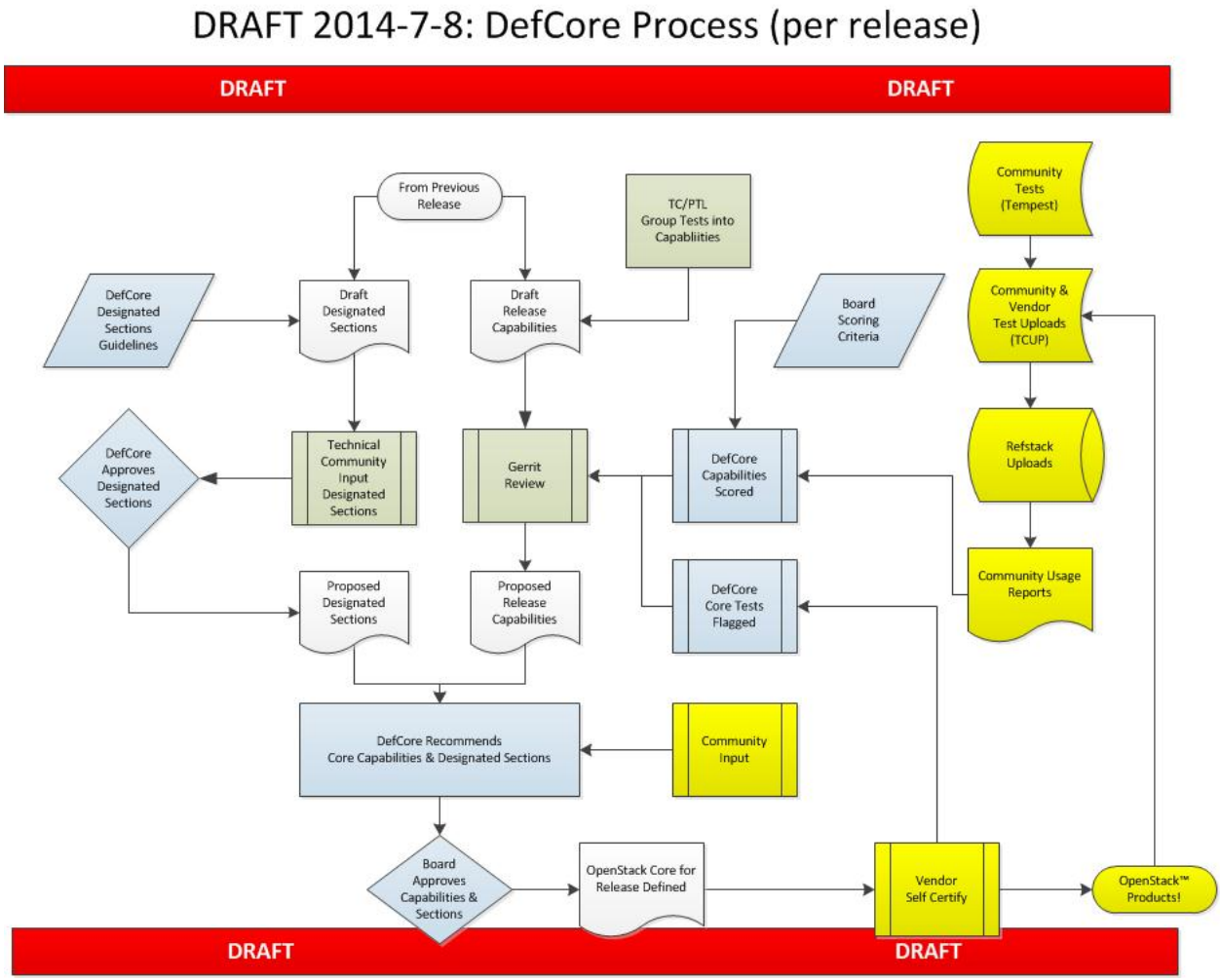
Addendum 1: DefCore Process Flow (per release)

The following flow chart reflects the latest thinking on the DefCore process based on the TC request for the Board to “own” designated sections.

> Note: in Lighthouse.F2F we added the concept of “flagging” tests so that we have a process where Vendors can raise concerns about required tests that do not produce valid or reproducible results.

Key:

- white = documents
- blue = board/defcore actions
- green = technical community
- yellow = communty
- ovals - start/end



Addendum 2: DefCore Process (to be included in the updated Bylaws by reference)

Today's core definitions are tightly coupled to individual projects.
Tomorrow's core definitions will be individual capabilities of different projects.

DEFINITION: **Certification for commercial use of the OpenStack mark requires passing tests of capabilities, and including designated sections of code.**

A. TESTS

1. All tempest tests for OpenStack must be grouped into capabilities.
1. Tests that don't pass in trunk (or that can only be passed by certain configurations) can be "flagged" by DefCore, and will be skipped.
1. These capabilities are scored by the DefCore committee during each release cycle, using board-approved criteria.
1. The board defines the criteria for this scoring and may adjust relative importance of criteria with each release.
1. The board defines the cut-off score for determining that a capability is core
1. Capabilities that surpass the cutoff score are considered "core capabilities".
1. In each core capability, all non-flagged tests must pass in any OpenStack product or service that uses the mark
1. Capabilities will not be depricated without with at least 1 release notice

B. DESIGNATED SECTIONS

1. The DefCore committee will identify sections of code to be "designated" which must be used in OpenStack products and services.
1. The Board will ratify these designated sections.
1. Designated sections only apply to projects that have some core capabilities.
1. Designated sections will not be increased without at least 1 release notice

C. ACTIVITIES(Work Flow?)

1. Criteria changes are managed by the DefCore committee and ratified by Board vote and posted on the OpenStack Wiki
1. Designated Sections changes are managed by the TC as Gerrit proposals
1. Capabilities changes are managed via Gerrit reviews
1. all tests are categorized into a capability by the PTL through Gerrit patch of the JSON file
1. tests are flagged-to-skip by approval of patches to the refstack json (by the Board as a slate vote)
1. Tests are unflagged through the same mechanism (by action of the DefCore committee)
1. DefCore changes to flagged to skip tests, criteria are to be ratified by the Board

D. GRIEVANCES

1. Test Issues > via Gerrit to Capabilities list
1. Criteria Issues > via DefCore mailing list & meetings
1. Designated Sections > via DefCore processes
1. Compliance Violations > same as trademark issues
2. Capabilities scores -> Community forums and roundtables during matrix review / also through Gerrit

E. PUBLISHING

1. The DefCore committee will manage content of a community website (currently at http://RefStack.org) and publish:
1. The DefCore principles
1. The current and historical scoring criteria
1. The categorization of tests into capabilities
1. The current and historical scored matrixes of capabilities
1. The scorecards of licensed products and services
1. Only "pass" tests will be reported in the process
1. OpenStack retains the right to be the official source of the results, and will copyright the RefStack and DefCore materials to support this.

F. TIMELINES:

1. Vendors will anonymously self-certify their products and services under the DefCore program for the Juno release.
1. In the "K" release, the Vendor's scorecards will be made public on the RefStack website.
1. Process modifications will be applied to future releases.