Introduction

› The Akraino TSC has discussed the Release 3 requirements in the face-to-face meeting (see the following two slides)
› This presentation is a proposal for the mandatory tests in Release 3
› Again, the tests are mandatory only as relevant
2020 Priorities for the Community

4. Automated validation of Akraino Projects
   
   • **Goal:**
     
     • Minimum mandated tests defined and voted by the TSC and exercised in R3
     • Promote adoption of validation project as part of blueprint testing
     • Need minimum commitment/contribution from each BP
       • Minimum BP to contribute test cases/code related to each BP
     • Requesting sub-committee chairs to assist on this exercise
   
   • **Recent Progress:**
     
     • Deployment of Blueprint Validation User Interface (UI) to view validation test logs
     • Integrating security tests
   
   • **Action Item:**
     
     1. Validation project to present which test are ready and can be a mandated tests
     2. TSC to vote on the mandated tests by March
2020 Priorities for the Community

4. Automated validation of Akraino Projects
   • Goal:
     • Minimum mandated tests defined and voted by the TSC and exercised in R3
     • Promote adoption of validation project as part of blueprint testing
     • Need minimum commitment/contribution from each BP
       • Minimum BP to contribute test cases/code related to each BP
     • Requesting sub-committee chairs to assist on this exercise

   • Recent Progress:
     • Deployment of Blueprint Validation User Interface (UI) to view validation test logs
     • Integrating security tests

   • Action Item:
     1. Validation project to present which test are ready and can be a mandated tests
     2. TSC to vote on the mandated tests by March
Proposal

For Incubation projects (that have been in R1 and R2):
› Redfish
› Kubernetes Conformance 1.17
› Lynis
› Vuls
› Kubehunter

For Mature projects additionally:
› HA tests: etcd_ha, ha/*, ceph_service
Open questions

› Do we still need the OpenStack tests?
› What to do with Linux Testing Project?
› Is Kubernetes Conformance 1.17 ok for all?
› What to do with the results of Lynis/Vuls/Kubehunter?
Summary

- Docker
  - Docker Bench for Security
- Hardware
  - Bios_version
  - HPE_baremetal
  - Redfish
- Helm
  - Helm_chart
  - Helm_repository
- K8s
  - Conformance
  - Etcd_ha
  - HA
    - Ha_calico_dns_proxy
    - Ha_etcd_api_ctl_sch
    - Ha_services
    - Ha_worker
  - Kube-hunter
- Networking
  - Helloworld
- OpenStack
  - Ceph_service
  - Tempest
- Os
  - Cyclictest
  - Ltp (Linux Testing Project)
  - Lynis
  - Vuls
Docker Bench for Security

› https://github.com/docker/docker-bench-security

“The Docker Bench for Security is a script that checks for dozens of common best-practices around deploying Docker containers in production”
Redfish

› https://github.com/DMTF/Redfish-Usecase-Checkers
  › “collection of python3 tools to exercise and validate common use cases for Redfish”
› https://github.com/DMTF/Redfish-Test-Framework
  › “a python3 tool and a model for organizing and running a set of Redfish interoperability tests against a target system”
› There was a bug (https://github.com/DMTF/Redfish-Tacklebox/issues/22) that prevented running Redfish tests in Release 2
  › Fixed in 1.0.2
Helm_chart

› Tests to validate Helm charts available in chart repositories
› Does
  › helm fetch ${chart} -d ${CHARTDIR}
  › helm lint ${CHARTDIR}/${file}
Helm_repository

› Tests to validate Helm chart repositories
› *** Test Cases ***
› Chart Storing
  › Upload Chart to Repository
  › Chart Upload Should Have Succeeded
  › Update Repository Info
  › Find Chart In Repository
  › Chart Should Be Available
  › Inspect Chart
  › Chart Should Be Accessible
› Upload Already Uploaded Chart
  › Upload Chart to Repository
  › Chart Upload Should Have Failed
› Chart Removal
  › Delete Chart
  › Chart Delete Should Have Succeeded
  › Update Repository Info
  › Find Chart In Repository
  › Chart Should Not Be Available
› Delete Already Deleted Chart
  › Delete Chart
  › Chart Delete Should Have Failed
k8s/conformance

- [https://github.com/heptio/sonobuoy](https://github.com/heptio/sonobuoy)
- "Sonobuoy is a diagnostic tool that makes it easier to understand the state of a Kubernetes cluster by running a set of Kubernetes conformance tests and other plugins in an accessible and non-destructive manner"
- Specified on [https://github.com/cncf/k8s-conformance](https://github.com/cncf/k8s-conformance)
- Supports the current release and 2 minor versions before
k8s/etcd_ha

› Verify the recovery and health of etcd cluster

› *** Test Cases ***
› Failure Of Etcd Node
› Retrieve Etcd Config
› Etcd Cluster Should Be Healthy
› Delete Etcd Node
› Wait For Etcd Node To Recover
› Etcd Cluster Should Be Healthy
HA/*

› “Hand-made” test cases for high availability
› Documentation:
  › HA test cases for calico, coredns and haproxy
  › HA tests: etcd, api-server, controller-manager, scheduler
  › HA services tests: docker and kubelet
  › Run HA Test - Fail Control Plane
Kube-hunter

› https://pypi.org/project/kube-hunter/
› “kube-hunter hunts for security weaknesses in Kubernetes clusters. The tool was developed to increase awareness and visibility for security issues in Kubernetes environments”
› Steps:
  › Cluster Remote Scanning
  › Node Remote Scanning
  › Inside-a-Pod Scanning
OpenStack/ceph_service

› Tests the Ceph service
› Test cases:
   › Failure Of Single Monitor And Manager
   › Failure Of Two Monitors And Managers
   › Failure Of Single Object Storage Daemon
   › Failure Of Two Object Storage Daemons
OpenStack/Tempest

- [https://docs.openstack.org/tempest/latest/](https://docs.openstack.org/tempest/latest/)
- Tempest is a set of integration tests. Tempest has batteries of tests for OpenStack API validation, scenarios, and other specific tests useful in validating an OpenStack deployment
- Bluval uses test list from [https://refstack.openstack.org/api/v1/guidelines/$REFSTACK_TARGET/tests?target=platform&type=required&alias=true&flag=false](https://refstack.openstack.org/api/v1/guidelines/$REFSTACK_TARGET/tests?target=platform&type=required&alias=true&flag=false)
- These tests defined by OpenStack Interoperability Working Group to be mandatory
Cyclic-test

- “Cyclic-test accurately and repeatedly measures the difference between a thread's intended wake-up time and the time at which it actually wakes up in order to provide statistics about the system's latencies. It can measure latencies in real-time systems caused by the hardware, the firmware, and the operating system.”
- No pass/fail
- No Docker container but can be run with bluval if installed
LTP (Linux Testing Project)

› https://github.com/linux-test-project/ltp
› The LTP testsuite contains a collection of tools for testing the Linux kernel and related features
› Runs as a native executable and needs superuser rights for some tests
Lynis

› https://github.com/CISOfy/lynis or https://cisofy.com/lynis/
› “A battle-tested security tool for systems running Linux, macOS, or Unix-based operating system. It performs an extensive health scan of your systems to support system hardening and compliance testing”
› Gives a report with
  › Time of an action/event
  › Reason(s) why a test failed or was skipped
  › Output of (internal) tests
  › Suggestions about configuration options or how to fix/improve things
  › Threat/impact score
Vuls

› https://vuls.io/
› “Agentless Vulnerability Scanner for Linux/FreeBSD. Vuls is open-source, agent-less vulnerability scanner based on information from NVD, OVAL, etc”
› Downloads a database of known vulnerabilities which can become large
<table>
<thead>
<tr>
<th>Test</th>
<th>Release 2 status</th>
<th>Comments</th>
<th>Release 3?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Docker Bench for Security</td>
<td>-</td>
<td></td>
<td>Recommended (no clear pass/fail criteria) -&gt; security team could look at this?</td>
</tr>
<tr>
<td>Redfish</td>
<td>Planned but had bug</td>
<td>Works now</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Helm chart, helm repository</td>
<td>-</td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>k8s/conformance</td>
<td>Mandatory</td>
<td>Uses k8s version 1.16</td>
<td>Upgrade to 1.17, can support others (tell us!)</td>
</tr>
<tr>
<td>etcd_ha</td>
<td>-</td>
<td></td>
<td>Recommended/Mandatory for maturity</td>
</tr>
<tr>
<td>ha/*</td>
<td>-</td>
<td></td>
<td>Recommended/Mandatory for maturity</td>
</tr>
<tr>
<td>ceph_service</td>
<td>-</td>
<td></td>
<td>Recommended/Mandatory for maturity</td>
</tr>
<tr>
<td>OpenStack/Tempest</td>
<td>Mandatory</td>
<td>Uses Refstack version 2019.06</td>
<td>Is anyone using OpenStack?</td>
</tr>
</tbody>
</table>
### Summary

<table>
<thead>
<tr>
<th>Test</th>
<th>Release 2 status</th>
<th>Comments</th>
<th>Release 3?</th>
</tr>
</thead>
<tbody>
<tr>
<td>cyclic test</td>
<td>-</td>
<td>Not pass/fail</td>
<td>Optional</td>
</tr>
<tr>
<td>Linux Testing Project</td>
<td>Mandatory</td>
<td>Only system calls, takes 45 minutes. Needs sudo</td>
<td>Optional</td>
</tr>
<tr>
<td>Lynis</td>
<td>Mandatory security test?</td>
<td>Gives a report of findings, needs to be quantified</td>
<td>Mandatory to run but no pass/fail -&gt; security group can decide</td>
</tr>
<tr>
<td>Vuls</td>
<td>Mandatory security test?</td>
<td>Only Ubuntu is currently supported in bluval</td>
<td>Mandatory to run but no pass/fail -&gt; security group can decide</td>
</tr>
<tr>
<td>Kubehunter</td>
<td>-</td>
<td>K8s vulnerability checking</td>
<td>Recommended (ask security group for comments)</td>
</tr>
</tbody>
</table>