Akraino Bluval

Tapio Tallgren, Juha Kosonen, Cristina Pauna, Ioakeim Samaras

March 31, 2020

Introduction

- The Blueprint validation tests are mandatory for Akraino Release 3 (see next slide)
- This presentation covers how to work with the tests
  - From command line
  - With CI
  - With Bluval UI
- The requirement is to make the results available
- Security tests are handled separately
- Again, only relevant tests are mandatory

AKRAINO EDGE STACK

Proposal

For Incubation projects (that have been in R1 and R2):

- Redfish
- Kubernetes Conformance 1.17
- Lynis
- Vuls
- Kubehunter
- OpenStack Tempest 2019.11

For Mature projects additionally:

- HA tests: etcd_ha, ha/*, ceph_service

AKRAINO EDGE STACK

Summary

- Docker
  - Docker Bench for Security
- Hardware
  - Bios_version
  - Hp_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

AKRAINO EDGE STACK

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”

```
# ------------------------------------------------------------------------------
# Docker Bench for Security v1.3.5
#
# Docker, Inc. (c) 2015-
#
# Checks for dozens of common best-practices around deploying Docker containers in production.
# Inspired by the CIS Docker Benchmark v1.2.0.
# ------------------------------------------------------------------------------

Initializing Tue Nov  5 10:27:42 UTC 2019


[INFO] 1 - Host Configuration

[INFO] 1.1 - General Configuration
[NOTE] 1.1.1  - Ensure the container host has been Hardened
[INFO] 1.1.2  - Ensure Docker is up to date
[INFO]        * Using 19.03.4, verify is it up to date as deemed necessary
[INFO]        * Your operating system vendor may provide support and security maintenance for Docker

[INFO] 1.2 - Linux Hosts Specific Configuration
[WARN] 1.2.1 - Ensure a separate partition for containers has been created
[INFO] 1.2.2  - Ensure only trusted users are allowed to control Docker daemon
[INFO]        * docker:x:998:
[WARN] 1.2.3  - Ensure auditing is configured for the Docker daemon
[WARN] 1.2.4  - Ensure auditing is configured for Docker files and directories - /var/lib/docker
[WARN] 1.2.5  - Ensure auditing is configured for Docker files and directories - /etc/docker
[WARN] 1.2.6  - Ensure auditing is configured for Docker files and directories - docker.service
[WARN] 1.2.7  - Ensure auditing is configured for Docker files and directories - docker.socket
[WARN] 1.2.8  - Ensure auditing is configured for Docker files and directories - /etc/default/docker
[INFO] 1.2.9  - Ensure auditing is configured for Docker files and directories - /etc/sysconfig/docker
[INFO]        * File not found
[INFO] 1.2.10  - Ensure auditing is configured for Docker files and directories - /etc/docker/daemon.json
[INFO]         * File not found
[WARN] 1.2.11  - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd
[INFO] 1.2.12  - Ensure auditing is configured for Docker files and directories - /usr/sbin/runc
[INFO]         * File not found


[INFO] 2 - Docker daemon configuration
[WARN] 2.1  - Ensure network traffic is restricted between containers on the default bridge
[PASS] 2.2  - Ensure the logging level is set to 'info'
[PASS] 2.3  - Ensure Docker is allowed to make changes to iptables
```

AKRAINO EDGE STACK

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

AKRAINO EDGE STACK

Helm_chart

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

AKRAINO EDGE STACK

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

AKRAINO EDGE STACK

k8s/conformance

- 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
- Supports the current release and 2 minor versions before

AKRAINO EDGE STACK

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

AKRAINO EDGE STACK

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

AKRAINO EDGE STACK

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

AKRAINO EDGE STACK

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

AKRAINO EDGE STACK

OpenStack/Tempest

- 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
- These tests defined by OpenStack Interoperability Working Group to be mandatory

AKRAINO EDGE STACK

Cyclictest

- https://wiki.linuxfoundation.org/realtime/documentation/howto/tools/cyclictest/start
- “Cyclictest 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

AKRAINO EDGE STACK

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

AKRAINO EDGE STACK

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

AKRAINO EDGE STACK

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

AKRAINO EDGE STACK

Summary

Test	Release 2 status	Comments	Release 3?
Docker Bench for Security	-		Recommended (no clear pass/fail criteria) -> security team could look at this?
Redfish	Planned but had bug	Works now	Mandatory
Helm chart, helm repository	-		Recommended
k8s/conformance	Mandatory	Uses k8s version 1.16	Upgrade to 1.17, can support others (tell us!)
etcd_ha	-		Recommended/Mandatory for maturity
ha/*	-		Recommended/Mandatory for maturity
ceph_service	-		Recommended/Mandatory for maturity
OpenStack/Tempest	Mandatory	Uses Refstack version 2019.06	Is anyone using OpenStack?

AKRAINO EDGE STACK

Summary

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

AKRAINO EDGE STACK