Smart Data Transaction for CPS Test Documentation

Introduction

This document describes the blueprint test environment for the Smart Data Transaction for CPS blueprint. The test results and logs are posted in the Akraino Nexus at the link below:

https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/

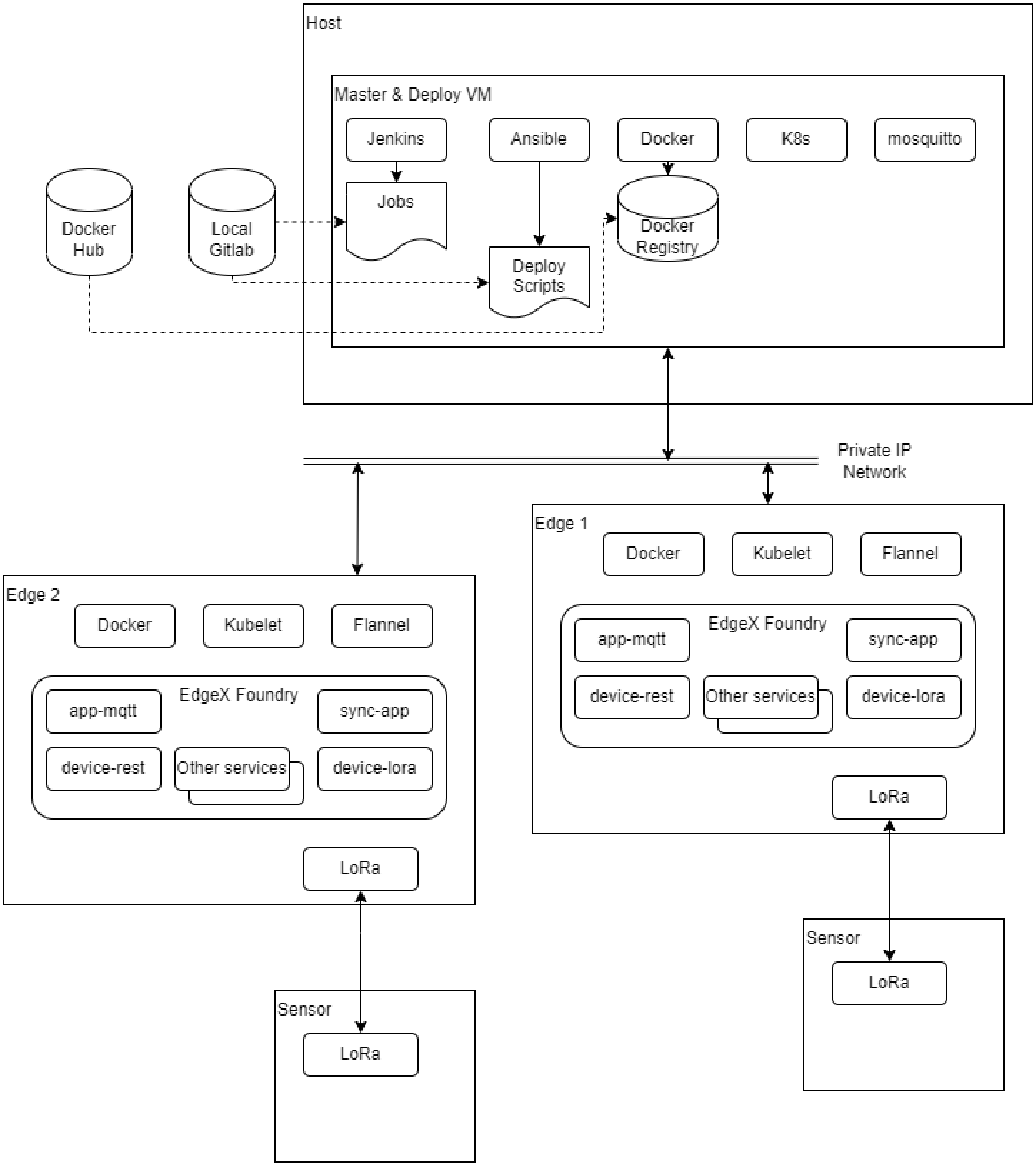
Akarino Test Group Information

N/A

Testing has been carried out at Fujitsu Limited labs without any Akraino Test Working Group resources.

Overall Test Architecture

Tests are carried out on the architecture shown in the diagram below.



Test Bed

The test bed consists of a VM running on x86 hardware, performing jump host/deploy and master node roles, two edge nodes on ARM64 (Jetson Nano) hardware, and two sensor nodes on ARM32 (Raspberry Pi) hardware.

Node Type	Count	Hardware	OS
Jump Host, Deploy/Master	1	Intel i5, 2 cores VM	Ubuntu 20.04
Edge	2	Jetson Nano, ARM Cortex-A57, 4 cores	Ubuntu 20.04

Sensor	2	Raspberry Pi 3, ARM Cortex-A53, 4 cores	Rasbian 11.1

A second VM is used to run the BluVal test framework components outside the system under test.

Test Framework

BluVal and additional tests are carried out using Robot Framework.

Traffic Generator

N/A

Test API description

CI/CD Regression Tests: Docker Private Registry

This set of test cases confirms the Docker private registry setup, population, and tear-down procedures.

The Test inputs

The test scripts and data are stored in the source repository's `cicd/tests/docker` directory.

Test Procedure

The test bed is placed in a state with the deploy and master node setup complete, but with Kubernetes, EdgeX, and the private registry not running.

Execute the test scripts:

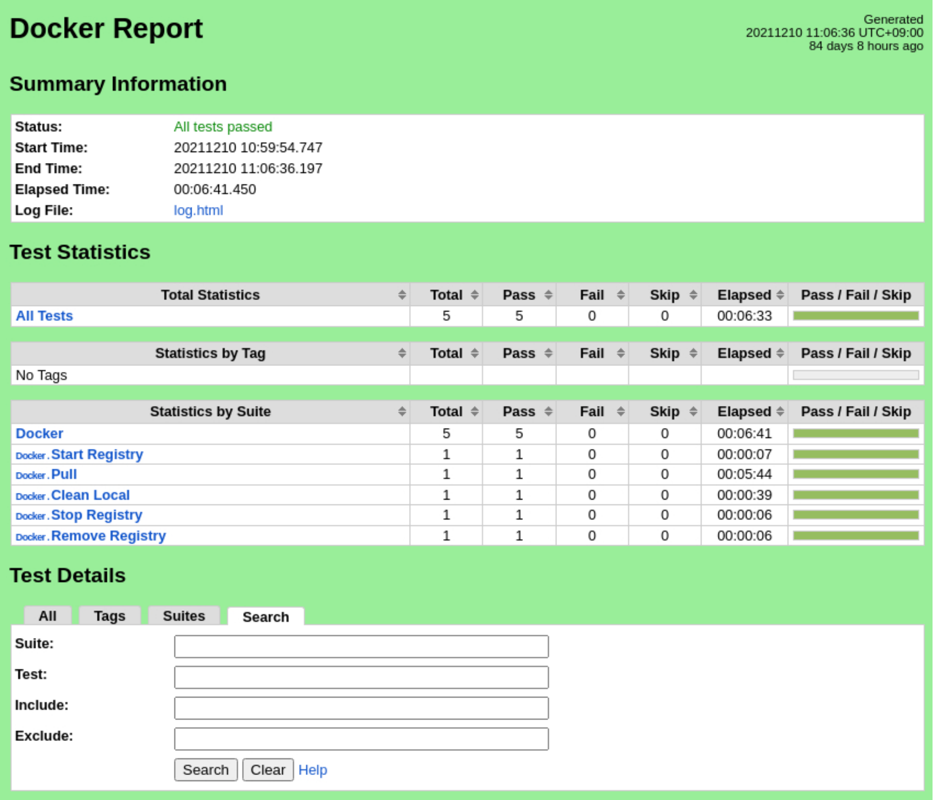
```
robot cicd/tests/docker
```

Expected output

The test script will start the registry, pull upstream images and populate the registry, clean images left over from the pull process, stop the registry, and remove the registry. The robot command should report success for all test cases.

Test Results

Nexus URL: https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/lfedge-docker/1/



Docker Report

Generated
20211210 11:06:36 UTC+09:00
84 days 8 hours ago

Summary Information

Status:	All tests passed
Start Time:	20211210 10:59:54.747
End Time:	20211210 11:06:36.197
Elapsed Time:	00:06:41.450
Log File:	log.html

Test Statistics

Total Statistics	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
All Tests	5	5	0	0	00:06:33	🟩

Statistics by Tag	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
No Tags						

Statistics by Suite	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
Docker	5	5	0	0	00:06:41	🟩
Docker.Start Registry	1	1	0	0	00:00:07	🟩
Docker.Pull	1	1	0	0	00:05:44	🟩
Docker.Clean Local	1	1	0	0	00:00:39	🟩
Docker.Stop Registry	1	1	0	0	00:00:06	🟩
Docker.Remove Registry	1	1	0	0	00:00:06	🟩

Test Details

Pass (5/5 test cases)

CI/CD Regression Tests: Node Setup

This set of test cases confirms the scripting to initialize master and edge nodes.

The Test inputs

The test scripts and data are stored in the source repository's `cicd/tests/install` directory.

Test Procedure

The test bed is place in a state where only the deploy node is initialized. No EdgeX or Kubernetes services are running. For a complete test, the master and edge nodes should not have any software installed that was not installed as part of the OS installation.

Execute the test scripts:

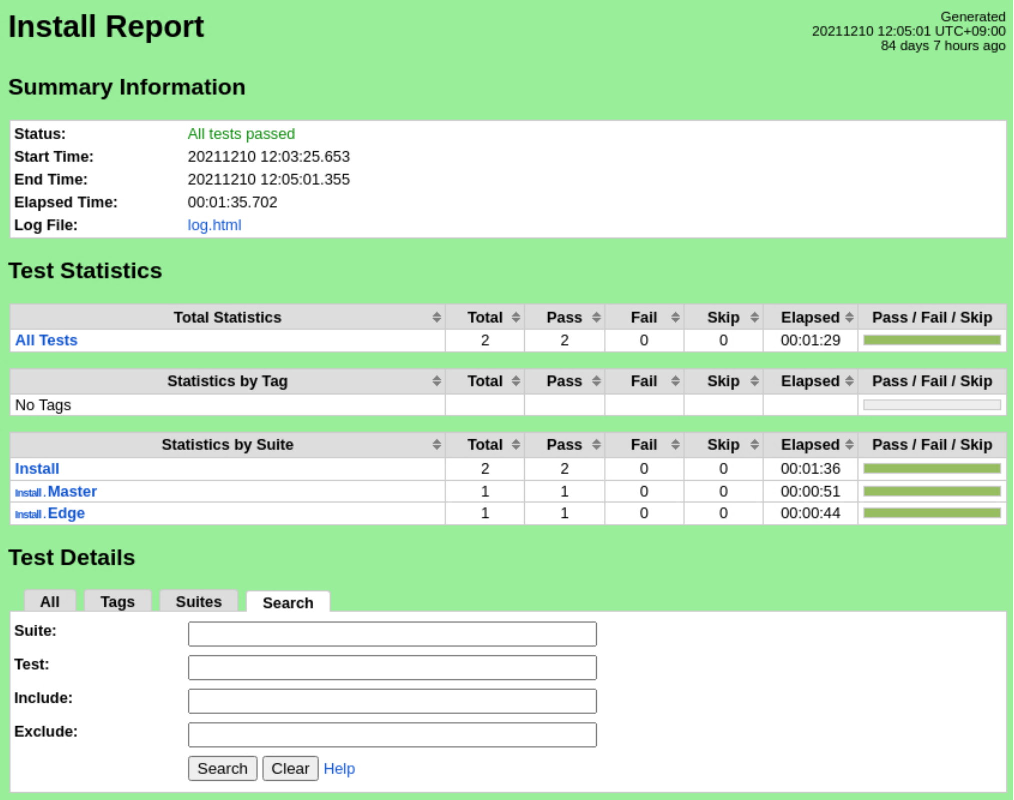
```
robot cicd/tests/install
```

Expected output

The test scripts will initialize the master and edge nodes and verify the required software is installed. The robot command should report success for all test cases.

Test Results

Nexus URL: https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/lfedge-install/1/



Install Report

Generated
20211210 12:05:01 UTC+09:00
84 days 7 hours ago

Summary Information

Status:	All tests passed
Start Time:	20211210 12:03:25.653
End Time:	20211210 12:05:01.355
Elapsed Time:	00:01:35.702
Log File:	log.html

Test Statistics

Total Statistics	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
All Tests	2	2	0	0	00:01:29	🟩

Statistics by Tag	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
No Tags						

Statistics by Suite	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
Install	2	2	0	0	00:01:36	🟩
Install . Master	1	1	0	0	00:00:51	🟩
Install . Edge	1	1	0	0	00:00:44	🟩

Test Details

Suite:

Test:

Include:

Exclude:

Pass (2/2 test cases)

CI/CD Regression Tests: Cluster Setup & Teardown

These test cases verify that the Kubernetes cluster can be initialized, edge nodes added to it and removed, and the cluster torn down.

The Test inputs

The test scripts and data are stored in the source repository's `cicd/tests/cluster` directory.

Test Procedure

The test bed is placed in a state where all nodes are prepared with required software and the Docker registry is running. The registry must be populated with the Kubernetes and Flannel images from upstream.

Execute the test scripts:

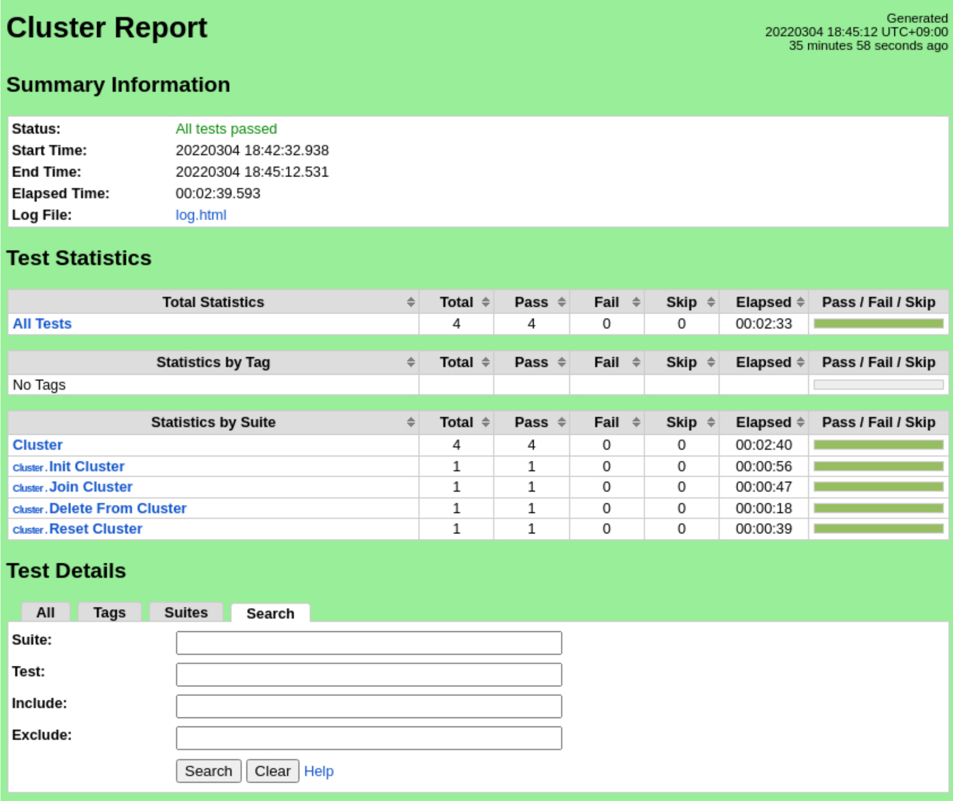
```
robot cicd/tests/cluster
```

Expected output

The test scripts will start the cluster, add all configured edge nodes, remove the edge nodes, and reset the cluster. The robot command should report success for all test cases.

Test Results

Nexus URL: https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/lfedge-cluster/7/



Cluster Report

Generated
20220304 18:45:12 UTC+09:00
35 minutes 58 seconds ago

Summary Information

Status:	All tests passed
Start Time:	20220304 18:42:32.938
End Time:	20220304 18:45:12.531
Elapsed Time:	00:02:39.593
Log File:	log.html

Test Statistics

Total Statistics	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
All Tests	4	4	0	0	00:02:33	🟩

Statistics by Tag	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
No Tags						□

Statistics by Suite	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
Cluster	4	4	0	0	00:02:40	🟩
Cluster.Init Cluster	1	1	0	0	00:00:56	🟩
Cluster.Join Cluster	1	1	0	0	00:00:47	🟩
Cluster.Delete From Cluster	1	1	0	0	00:00:18	🟩
Cluster.Reset Cluster	1	1	0	0	00:00:39	🟩

Test Details

Suite:

Test:

Include:

Exclude:

Pass (4/4 test cases)

CI/CD Regression Tests: EdgeX Services

These test cases verify that the EdgeX micro-services can be started and that MQTT messages are passed to the master node from the services.

The Test inputs

The test scripts and data are stored in the source repository's `cicd/tests/edgex` directory.

Test Procedure

The test bed is placed in a state where the cluster is initialized and all edge nodes have joined. The Docker registry and mosquitto MQTT broker must be running on the master node. The registry must be populated with all upstream images and custom images. Either the `device-lora` service should be enabled with `dht2lra` service running on the sensor nodes, or `device-virtual` should be enabled to provide readings.

Execute the test scripts:

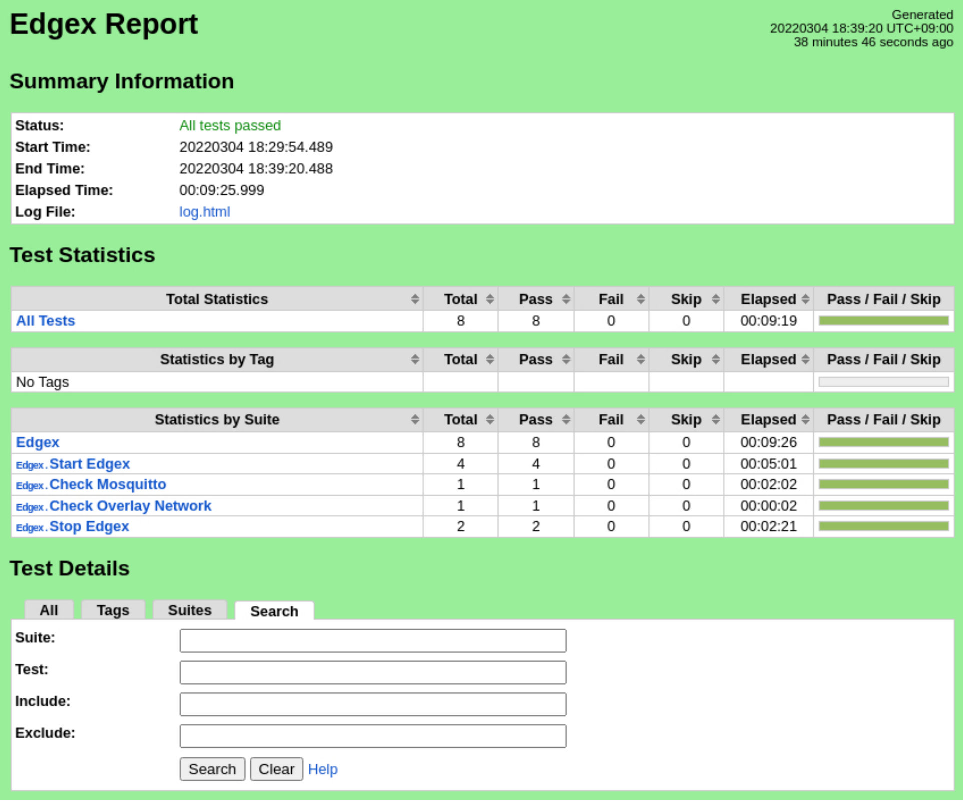
```
robot cicd/tests/edgex
```

Expected output

The test scripts will start the EdgeX micro-services on all edge nodes, confirm that MQTT messages are being delivered from the edge nodes, and stop the EdgeX micro-services. The robot command should report success for all test cases.

Test Results

Nexus URL: https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/edgex-install/7/



Edgex Report

Generated
20220304 18:39:20 UTC+09:00
38 minutes 46 seconds ago

Summary Information

Status:	All tests passed
Start Time:	20220304 18:29:54.489
End Time:	20220304 18:39:20.488
Elapsed Time:	00:09:25.999
Log File:	log.html

Test Statistics

Total Statistics	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
All Tests	8	8	0	0	00:09:19	🟩

Statistics by Tag	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
No Tags						

Statistics by Suite	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
Edgex	8	8	0	0	00:09:26	🟩
Edgex . Start Edgex	4	4	0	0	00:05:01	🟩
Edgex . Check Mosquitto	1	1	0	0	00:02:02	🟩
Edgex . Check Overlay Network	1	1	0	0	00:00:02	🟩
Edgex . Stop Edgex	2	2	0	0	00:02:21	🟩

Test Details

Suite:
Test:
Include:
Exclude:

Pass (8/8 test cases)

CI/CD Regression Tests: LoRa Device Service

These test cases verify that the LoRa device service can read sensor data over the LoRa communications channel.

The Test inputs

The test steps and data are contained in the scripts in the source repository `cicd/tests/lora` directory.

Test Procedure

The test bed is initialized to the point of having all EdgeX services running, with `device-lora` enabled.

The `dht2lra` service is started on the two sensor nodes.

Execute the test scripts:

```
robot cicd/tests/lora
```

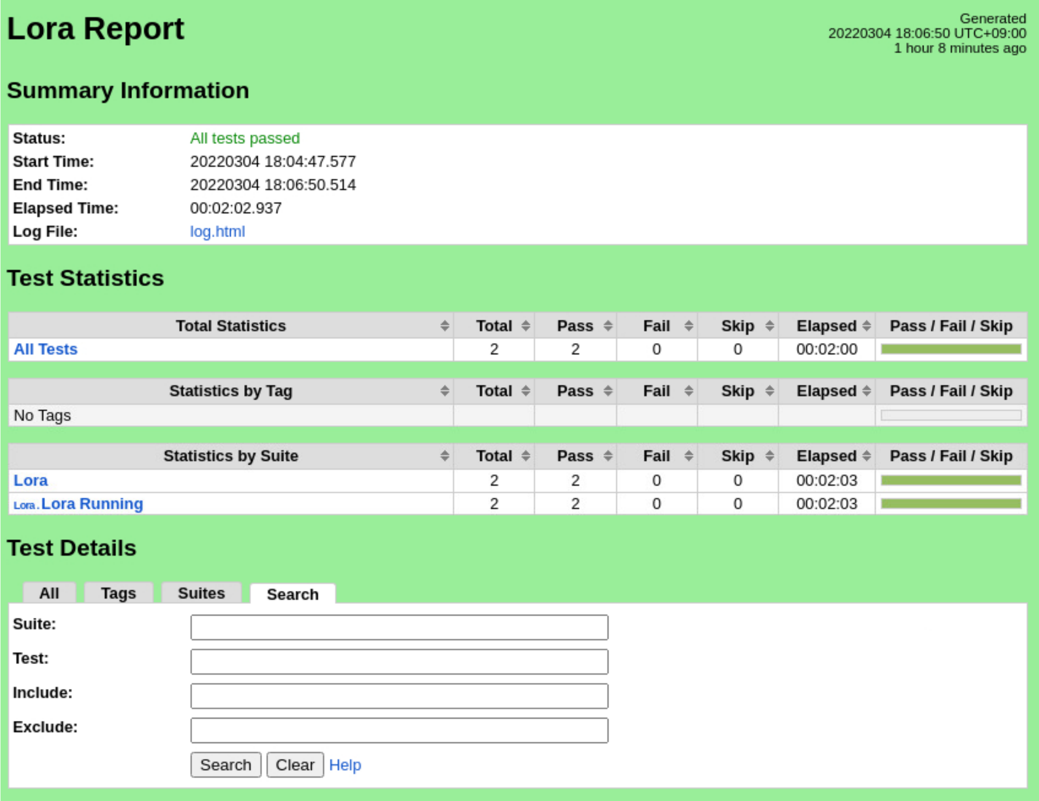
Expected output

The test cases will check if MQTT messages containing temperature data gathered from the sensor nodes are arriving at the master node on the topic for each each edge node, validating that the LoRa device support is functioning.

The Robot Framework should report success for all test cases.

Test Results

Nexus URL: https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/edgex-lora/3/



Lora Report

Generated
20220304 18:06:50 UTC+09:00
1 hour 8 minutes ago

Summary Information

Status:	All tests passed
Start Time:	20220304 18:04:47.577
End Time:	20220304 18:06:50.514
Elapsed Time:	00:02:02.937
Log File:	log.html

Test Statistics

Total Statistics	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
All Tests	2	2	0	0	00:02:00	🟩

Statistics by Tag	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
No Tags						

Statistics by Suite	Total	Pass	Fail	Skip	Elapsed	Pass / Fail / Skip
Lora	2	2	0	0	00:02:03	🟩
Lora . Lora Running	2	2	0	0	00:02:03	🟩

Test Details

Suite:

Test:

Include:

Exclude:

Pass (2/2 test cases)

Feature Project Tests

N/A

BluVal Tests

BluVal tests for Lynis, Vuls, and Kube-Hunter were executed on the test bed.

The Test inputs

Bluval User Guide

Steps To Implement Security Scan Requirements

https://vuls.io/docs/en/tutorial-docker.html

Test Procedure

1. Deploy a Test VM
2. Copy the folder ~/.kube from Kubernetes master node to the Test VM
3. Create SSH Key to access Kubernetes master node

Vuls

We use Ubuntu 20.04, so we ran Vuls test as follows:

1. Create directory

```
$ mkdir ~/vuls
$ cd ~/vuls
$ mkdir go-cve-dictionary-log goval-dictionary-log gost-log
```

2. Fetch NVD

```
$ docker run --rm -it \
    -v $PWD:/go-cve-dictionary \
    -v $PWD/go-cve-dictionary-log:/var/log/go-cve-dictionary \
    vuls/go-cve-dictionary fetch nvd
```

3. Fetch OVAL

```
$ docker run --rm -it \
     -v $PWD:/goval-dictionary \
     -v $PWD/goval-dictionary-log:/var/log/goval-dictionary \
     vuls/goval-dictionary fetch ubuntu 16 17 18 19 20
```

4. Fetch gost

```
$ docker run --rm -i \
     -v $PWD:/gost \
     -v $PWD/gost-log:/var/log/gost \
     vuls/gost fetch ubuntu
```

5. Create config.toml

```
[servers]

[servers.master]
host = "192.168.51.22"
port = "22"
user = "test-user"
keyPath = "/root/.ssh/id_rsa" # path to ssh private key in docker
```

6. Start vuls container to run tests

```
$ docker run --rm -it \
    -v ~/.ssh:/root/.ssh:ro \
    -v $PWD:/vuls \
    -v $PWD/vuls-log:/var/log/vuls \
    -v /etc/localtime:/etc/localtime:ro \
    -v /etc/timezone:/etc/timezone:ro \
    vuls/vuls scan \
    -config=./config.toml
```

7. Get the report

```
$ docker run --rm -it \
     -v ~/.ssh:/root/.ssh:ro \
     -v $PWD:/vuls \
     -v $PWD/vuls-log:/var/log/vuls \
     -v /etc/localtime:/etc/localtime:ro \
     vuls/vuls report \
     -format-list \
     -config=./config.toml
```

Lynis/Kube-Hunter

1. Create ~/validation/bluval/bluval-sdtfc.yaml to customize the Test

```
blueprint:
    name: sdtfc
    layers:
        - os
        - k8s

    os: &os
        -
            name: lynis
            what: lynis
            optional: "False"
    k8s: &k8s
        -
            name: kube-hunter
            what: kube-hunter
            optional: "False"
```

2. Update ~/validation/bluval/volumes.yaml file

```
volumes:
    # location of the ssh key to access the cluster
    ssh_key_dir:
        local: '/home/ubuntu/.ssh'
        target: '/root/.ssh'
    # location of the k8s access files (config file, certificates, keys)
    kube_config_dir:
        local: '/home/ubuntu/kube'
        target: '/root/.kube/'
    # location of the customized variables.yaml
    custom_variables_file:
        local: '/home/ubuntu/validation/tests/variables.yaml'
        target: '/opt/akraino/validation/tests/variables.yaml'
    # location of the bluval-<blueprint>.yaml file
    blueprint_dir:
        local: '/home/ubuntu/validation/bluval'
        target: '/opt/akraino/validation/bluval'
    # location on where to store the results on the local jumpserver
    results_dir:
        local: '/home/ubuntu/results'
        target: '/opt/akraino/results'
    # location on where to store openrc file
    openrc:
        local: ''
        target: '/root/openrc'

# parameters that will be passed to the container at each layer
layers:
    # volumes mounted at all layers; volumes specific for a different layer are below
    common:
        - custom_variables_file
        - blueprint_dir
        - results_dir
    hardware:
        - ssh_key_dir
    os:
        - ssh_key_dir
    networking:
        - ssh_key_dir
    docker:
        - ssh_key_dir
    k8s:
        - ssh_key_dir
        - kube_config_dir
    k8s_networking:
        - ssh_key_dir
        - kube_config_dir
    openstack:
        - openrc
    sds:
    sdn:
    vim:
```

3. Update ~/validation/tests/variables.yaml file

```
### Input variables cluster's master host
host: <IP Address>             # cluster's master host address
username: <username>            # login name to connect to cluster
password: <password>         # login password to connect to cluster
ssh_keyfile: /root/.ssh/id_rsa        # Identity file for authentication
```

4. Run Blucon

```
$ bash validation/bluval/blucon.sh sdtfc
```

Expected output

BluVal tests should report success for all test cases.

Test Results

Vuls results (manual) Nexus URL: https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/sdt-vuls/2/

Lynis results (manual) Nexus URL: https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/sdt-lynis/3/

Kube-Hunter results Nexus URL: https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/sdt-bluval/2/

Vuls

Nexus URL: https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/sdt-vuls/2/

There are 17 CVEs with a CVSS score >= 9.0. These are exceptions requested here:

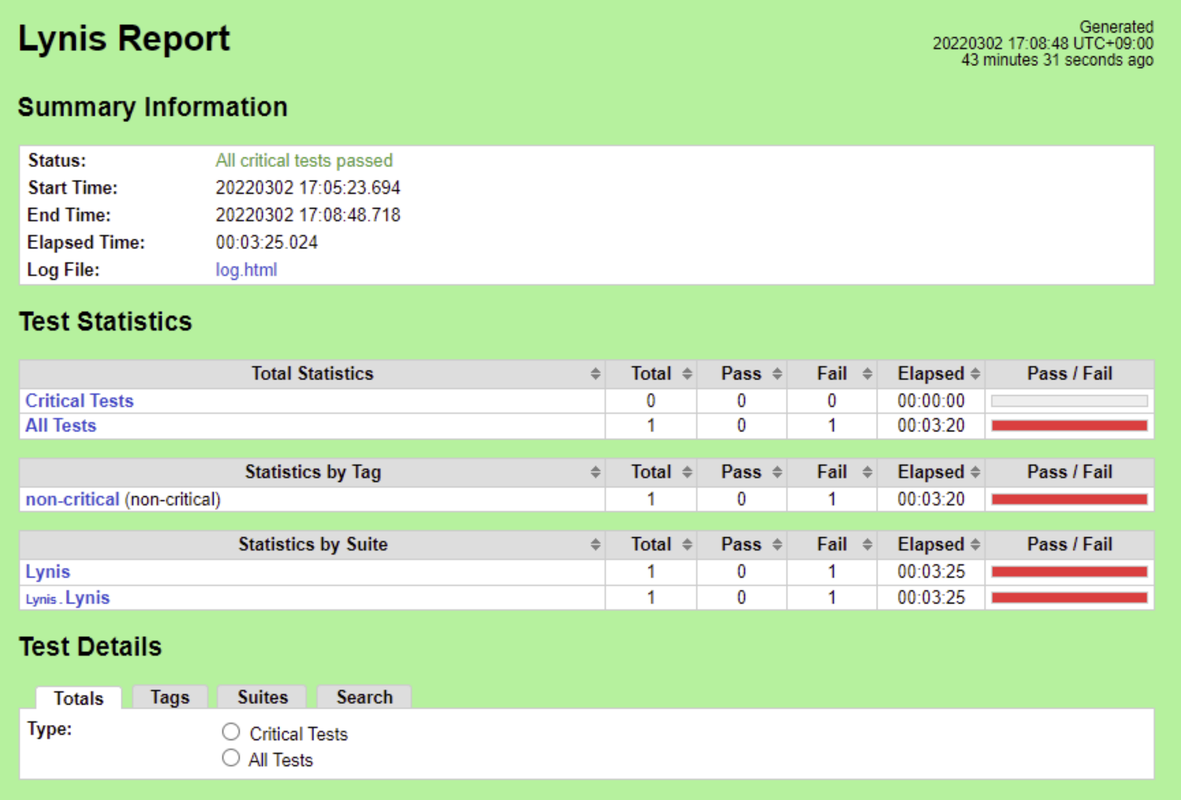
Release 6: Akraino CVE and KHV Vulnerability Exception Request

CVE-ID	CVSS	NVD	Fix/Notes
CVE-2016-1585	9.8	https://nvd.nist.gov/vuln/detail/CVE-2016-1585	No fix available
CVE-2021-20236	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-20236	No fix available (latest release of ZeroMQ for Ubuntu 20.04 is 4.3.2-2ubuntu1)
CVE-2021-31870	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-31870	No fix available (latest release of klibc for Ubuntu 20.04 is 2.0.7-1ubuntu5)
CVE-2021-31872	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-31872	No fix available (latest release of klibc for Ubuntu 20.04 is 2.0.7-1ubuntu5)
CVE-2021-31873	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-31873	No fix available (latest release of klibc for Ubuntu 20.04 is 2.0.7-1ubuntu5)
CVE-2021-33574	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-33574	Will not be fixed in Ubuntu stable releases
CVE-2021-45951	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-45951	No fix available (vendor disputed)
CVE-2021-45952	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-45952	No fix available (vendor disputed)
CVE-2021-45953	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-45953	No fix available (vendor disputed)
CVE-2021-45954	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-45954	No fix available (vendor disputed)
CVE-2021-45955	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-45955	No fix available (vendor disputed)
CVE-2021-45956	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-45956	No fix available (vendor disputed)
CVE-2021-45957	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-45957	No fix available (vendor disputed)
CVE-2022-23218	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-23218	Reported fixed in 2.31-0ubuntu9.7 (installed), but still reported by Vuls
CVE-2022-23219	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-23219	Reported fixed in 2.31-0ubuntu9.7 (installed), but still reported by Vuls
CVE-2016-9180	9.1	https://nvd.nist.gov/vuln/detail/CVE-2016-9180	No fix available
CVE-2021-35942	9.1	https://nvd.nist.gov/vuln/detail/CVE-2021-35942	Reported fixed in 2.31-0ubuntu9.7 (installed), but still reported by Vuls

Lynis

Nexus URL (run via Bluval, without fixes): https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/sdt-bluval/2/

Nexus URL (manual run, with fixes): https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/sdt-lynis/2/



Lynis Report

Generated
20220302 17:08:48 UTC+09:00
43 minutes 31 seconds ago

Summary Information

Status:	All critical tests passed
Start Time:	20220302 17:05:23.694
End Time:	20220302 17:08:48.718
Elapsed Time:	00:03:25.024
Log File:	log.html

Test Statistics

Total Statistics	Total	Pass	Fail	Elapsed	Pass / Fail
Critical Tests	0	0	0	00:00:00	
All Tests	1	0	1	00:03:20	🟥

Statistics by Tag	Total	Pass	Fail	Elapsed	Pass / Fail
non-critical (non-critical)	1	0	1	00:03:20	🟥

Statistics by Suite	Total	Pass	Fail	Elapsed	Pass / Fail
Lynis	1	0	1	00:03:25	🟥
Lynis . Lynis	1	0	1	00:03:25	🟥

Test Details

Type: ○ Critical Tests
○ All Tests

The initial results compare with the Lynis Incubation: PASS/FAIL Criteria, v1.0 as follows.

The Lynis Program Update test MUST pass with no errors.

```
2022-03-04 15:33:28 Test: Checking for program update...
2022-03-04 15:33:31 Current installed version  : 301
2022-03-04 15:33:31 Latest stable version      : 307
2022-03-04 15:33:31 Minimum required version   : 297
2022-03-04 15:33:31 Result: newer Lynis release available!
2022-03-04 15:33:31 Suggestion: Version of Lynis outdated, consider upgrading to the latest version [test:LYNIS] [details:-] [solution:-]
```

Fix: Download and run the latest Lynis directly on SUT.

Steps To Implement Security Scan Requirements#InstallandExecute

The following list of tests MUST complete as passing

No.	Test	Result	Fix
1	Test: Checking PASS_MAX_DAYS option in /etc/login.defs	Result: password minimum age is not configured Suggestion: Configure minimum password age in /etc/login.defs [test:AUTH-9286]	Set PASS_MAX_DAYS 180 in /etc/login.defs
2	Performing test ID AUTH-9328 (Default umask values)	Result: found umask 022, which could be improved Suggestion: Default umask in /etc/login.defs could be more strict like 027 [test:AUTH-9328]	Set UMASK 027 in /etc/login.defs
3	Performing test ID SSH-7440 (Check OpenSSH option: AllowUsers and AllowGroups)	Result: SSH has no specific user or group limitation. Most likely all valid users can SSH to this machine. Hardening: assigned partial number of hardening points (0 of 1).	Configure AllowUsers in /etc/ssh/sshd_config
4	Test: checking for file /etc/network/if-up.d/ntpdate	Test: checking for file /etc/network/if-up.d/ntpdate Result: file /etc/network/if-up.d/ntpdate does not exist ... Hardening: assigned maximum number of hardening points for this item (3).	OK
5	Performing test ID KRNL-6000 (Check sysctl key pairs in scan profile) : Following sub-tests required	N/A	N/A
5a	sysctl key fs.suid_dumpable contains equal expected and current value (0)	Result: sysctl key fs.suid_dumpable has a different value than expected in scan profile. Expected=0, Real=2	Set recommended value in /etc/sysctl.d/90-lynis-hardening.conf and disable apport in /etc/default/apport
5b	sysctl key kernel.dmesg_restrict contains equal expected and current value (1)	Result: sysctl key kernel.dmesg_restrict has a different value than expected in scan profile. Expected=1, Real=0	Set recommended value in /etc/sysctl.d/90-lynis-hardening.conf
5c	sysctl key net.ipv4.conf.default.accept_source_route contains equal expected and current value (0)	Result: sysctl key net.ipv4.conf.default.accept_source_route has a different value than expected in scan profile. Expected=0, Real=1	Set recommended value in /etc/sysctl.d/90-lynis-hardening.conf
6	Test: Check if one or more compilers can be found on the system	Result: found installed compiler. See top of logfile which compilers have been found or use /usr/bin/grep to filter on 'compiler' Hardening: assigned partial number of hardening points (1 of 3).	Uninstall gcc and remove /usr/bin/as (installed with binutils)

Results after the above fixes are as follows:

The Lynis Program Update test MUST pass with no errors.

```
2022-03-07 15:19:07 Test: Checking for program update...
2022-03-07 15:19:10 Current installed version : 308
2022-03-07 15:19:10 Latest stable version : 307
2022-03-07 15:19:10 No Lynis update available.
```

The following list of tests MUST complete as passing

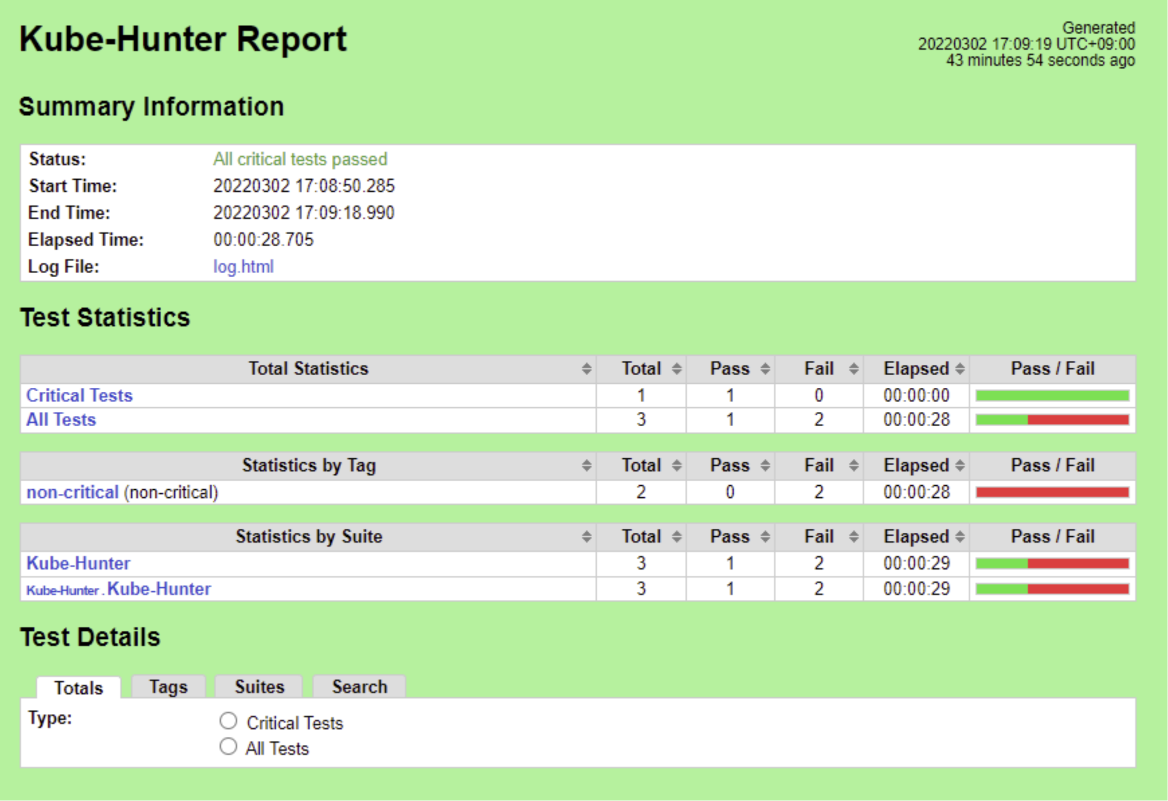
No.	Test	Result
1	Test: Checking PASS_MAX_DAYS option in /etc/login.defs	Result: max password age is 180 days Hardening: assigned maximum number of hardening points for this item (3).

2	Performing test ID AUTH-9328 (Default umask values)	Result: umask is 027, which is fine Hardening: assigned maximum number of hardening points for this item (2).
3	Performing test ID SSH-7440 (Check OpenSSH option: AllowUsers and AllowGroups)	Result: SSH is limited to a specific set of users, which is good Hardening: assigned maximum number of hardening points for this item (2).
5a	sysctl key fs.suid_dumpable contains equal expected and current value (0)	Result: sysctl key fs.suid_dumpable contains equal expected and current value (0) Hardening: assigned maximum number of hardening points for this item (1).
5b	sysctl key kernel.dmesg_restrict contains equal expected and current value (1)	Result: sysctl key kernel.dmesg_restrict contains equal expected and current value (1) Hardening: assigned maximum number of hardening points for this item (1).
5c	sysctl key net.ipv4.conf.default.accept_source_route contains equal expected and current value (0)	Result: sysctl key net.ipv4.conf.default.accept_source_route contains equal expected and current value (0) Hardening: assigned maximum number of hardening points for this item (1).
6	Test: Check if one or more compilers can be found on the system	Result: no compilers found Hardening: assigned maximum number of hardening points for this item (3).

The post-fix manual logs can be found at https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/sdt-lynis/3/.

Kube-Hunter

Nexus URL (with fixes): https://nexus.akraino.org/content/sites/logs/fujitsu/job/sdt/r6/sdt-bluval/2/



Kube-Hunter Report

Generated
20220302 17:09:19 UTC+09:00
43 minutes 54 seconds ago

Summary Information

Status:	All critical tests passed
Start Time:	20220302 17:08:50.285
End Time:	20220302 17:09:18.990
Elapsed Time:	00:00:28.705
Log File:	log.html

Test Statistics

Total Statistics	Total	Pass	Fail	Elapsed	Pass / Fail
Critical Tests	1	1	0	00:00:00	🟩
All Tests	3	1	2	00:00:28	🟩🟥

Statistics by Tag	Total	Pass	Fail	Elapsed	Pass / Fail
non-critical (non-critical)	2	0	2	00:00:28	🟥

Statistics by Suite	Total	Pass	Fail	Elapsed	Pass / Fail
Kube-Hunter	3	1	2	00:00:29	🟩🟥
Kube-Hunter . Kube-Hunter	3	1	2	00:00:29	🟩🟥

Test Details

Type: ○ Critical Tests
○ All Tests

There are 5 Vulnerabilities.

- KHV002
- KHV005
- KHV050
- CAP_NET_RAW Enabled
- Access to pod's secrets

Fix for KHV002

```
$ kubectl replace -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  annotations:
    rbac.authorization.kubernetes.io/autoupdate: "false"
  labels:
    kubernetes.io/bootstrapping: rbac-defaults
  name: system:public-info-viewer
rules:
- nonResourceURLs:
  - /healthz
  - /livez
  - /readyz
  verbs:
  - get
EOF
```

Fix for KHV005, KHV050, Access to pod's secrets

```
$ kubectl replace -f - <<EOF
apiVersion: v1
kind: ServiceAccount
metadata:
  name: default
  namespace: default
automountServiceAccountToken: false
EOF
```

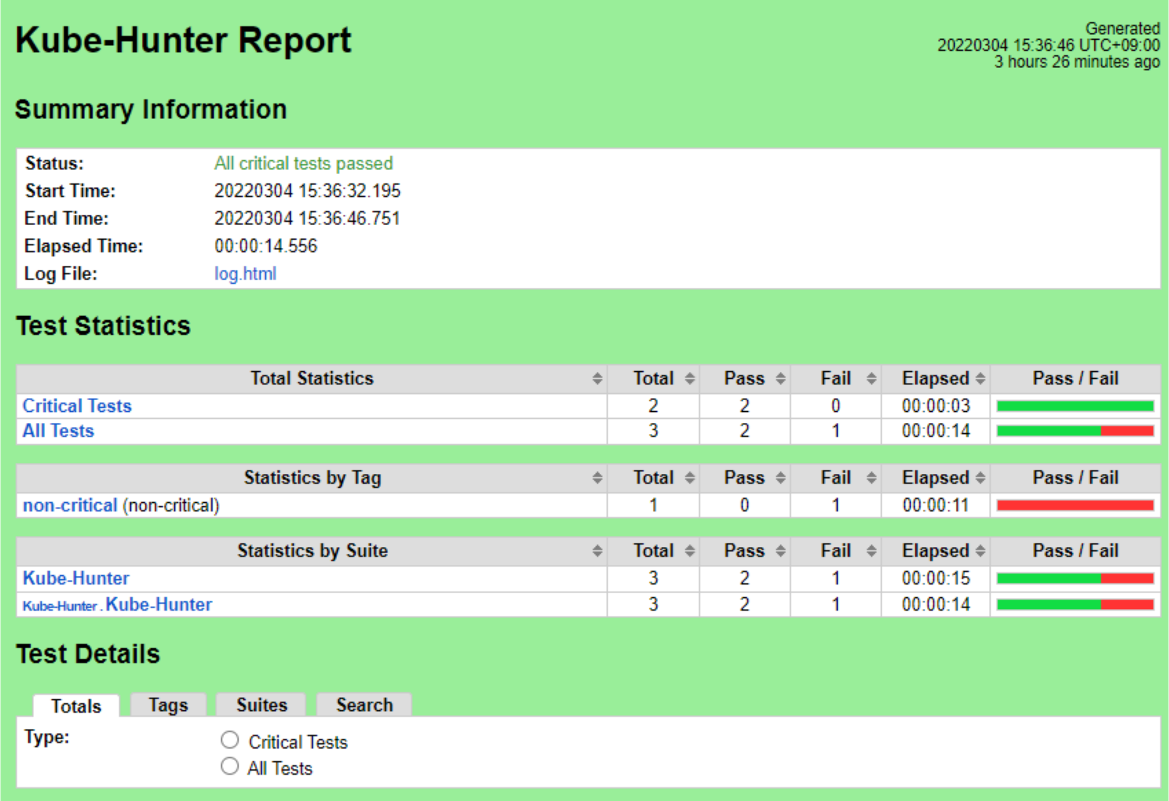
The above fixes are implemented in the Ansible playbook `deploy/playbook/init_cluster.yml` and configuration file `deploy/playbook/k8s/fix.yml`

Fix for CAP_NET_RAW Enabled:

Create a PodSecurityPolicy with requiredDropCapabilities: NET_RAW. The policy is shown below. The complete fix is implemented in the Ansible playbook `deploy/playbook/init_cluster.yml` and configuration files `deploy/playbook/k8s/default-psp.yml` and `deploy/playbook/k8s/system-psp.yml`, plus enabling PodSecurityPolicy checking in `deploy/playbook/k8s/config.yml`.

```
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: psp-baseline
spec:
  privileged: true
  allowPrivilegeEscalation: true
  allowedCapabilities:
  - IPC_LOCK
  - NET_ADMIN
  requiredDropCapabilities:
  - NET_RAW
  hostIPC: true
  hostNetwork: true
  hostPID: true
  hostPorts:
  - max: 65535
    min: 0
  readOnlyRootFilesystem: false
  fsGroup:
    rule: 'RunAsAny'
  runAsUser:
    rule: 'RunAsAny'
  seLinux:
    rule: 'RunAsAny'
  supplementalGroups:
    rule: 'RunAsAny'
  volumes:
  - '*'
```

Results after fixes are shown below:



Kube-Hunter Report

Generated
20220304 15:36:46 UTC+09:00
3 hours 26 minutes ago

Summary Information

Status:	All critical tests passed
Start Time:	20220304 15:36:32.195
End Time:	20220304 15:36:46.751
Elapsed Time:	00:00:14.556
Log File:	log.html

Test Statistics

Total Statistics	Total	Pass	Fail	Elapsed	Pass / Fail
Critical Tests	2	2	0	00:00:03	🟩
All Tests	3	2	1	00:00:14	🟩🟥

Statistics by Tag	Total	Pass	Fail	Elapsed	Pass / Fail
non-critical (non-critical)	1	0	1	00:00:11	🟥

Statistics by Suite	Total	Pass	Fail	Elapsed	Pass / Fail
Kube-Hunter	3	2	1	00:00:15	🟩🟥
Kube-Hunter . Kube-Hunter	3	2	1	00:00:14	🟩🟥

Test Details

Type: ○ Critical Tests
○ All Tests

Note that in spite of all Kube-Hunter vulnerabilities being fixed, the results still show one test failure. The "Inside-a-Pod Scanning" test case reports failure, apparently because the log ends with "Kube Hunter couldn't find any clusters" instead of "No vulnerabilities were found." Because vulnerabilities were detected and reported earlier by this test case, and those vulnerabilities are no longer reported, we believe this is a false negative, and may be caused by this issue: https://github.com/aquasecurity/kube-hunter/issues/358

Test Dashboards

Single pane view of how the test score looks like for the Blue print.

Total Tests	Test Executed	Pass	Fail	In Progress
26	26	24	2	0

*Vuls is counted as one test case.

*One Kube-Hunter failure is counted as a pass. See above.

Vuls and Lynis test cases are failing, an exception request is filed for Vuls-detected vulnerabilities that cannot be fixed. The Lynis results have been confirmed to pass the Incubation criteria.

Additional Testing

None at this time.

Bottlenecks/Errata

None at this time.