Red Hat

CNF Certification Test failures

Table 1. Revision History

Version	Date	Who	Changes
1.0	September 7, 2023	David Rabkin	Initial Version

Table 2. Terminology

Acronym	Meaning
CNF	Containerized Network Function
OCP	OpenShift Container Platform
RHCOS	Red Hat Enterprise Linux CoreOS operating system
RHEL	Red Hat Enterprise Linux operating system

Overview

A major part of Telco partner certification is CNF Certification Test. These test cases are specifically designed to verify whether the deployment of the Telco partner's solution on Red Hat OpenShift follows the CNF Best Practices and the Operator Best Practices. By conducting these tests, we ensure that the implementation aligns with the recommended standards and guidelines for optimal performance and compatibility.

In the suite, there are 88 test cases, consisting of both mandatory and optional cases. These cases are divided among nine different suites.

Operators

We conducted the CNF Certification Test on over two hundred of Red Hat's operators on OCP 4.13. Consequently, we have detected an average of approximately thirty failures per operator. For additional details, please refer to the CNF Report for Operators on OCP 4.13 - September. You can use the operator name filter to narrow down your search.

Failures

The failures are categorized by operators in the CNF Report for Operators on OCP 4.13 - September. The report enables the filtering of failures based on specific operators.

The first priority should be addressing the most commonly required mandatory tests, see CNF Report for Operators on OCP 4.13 - September - Sorted.

	A	B
1	State	failed
2	Mandatory/Optional	Mandatory
3		
4	**Row Labels**	**Count of Failure Reason**
5	affiliated-certification-container-is-certified-digest	75
6	platform-alteration-base-image	75
7	platform-alteration-isredhat-release	75
8	access-control-pod-role-bindings	75
9	access-control-pod-service-account	75
10	affiliated-certification-operator-is-certified	73
11	access-control-container-host-port	44
12	access-control-pod-host-path	43
13	access-control-pod-host-pid	43
14	access-control-pod-host-network	42
15	access-control-sys-admin-capability-check	41
16	access-control-security-context-privilege-escalation	41
17	operator-install-status-no-privileges	39
18	lifecycle-pod-scheduling	26
19	lifecycle-liveness-probe	26
20	lifecycle-readiness-probe	26
21	access-control-cluster-role-bindings	26
22	lifecycle-pod-owner-type	26
23	lifecycle-startup-probe	26
24	lifecycle-pod-toleration-bypass	26
25	observability-termination-policy	26
26	access-control-pod-automount-service-account-token	26
27	lifecycle-image-pull-policy	26
28	access-control-requests-and-limits	26
29	access-control-projected-volume-service-account-token	26
30	lifecycle-container-startup	26
31	lifecycle-cpu-isolation	26
32	lifecycle-container-shutdown	26
33	access-control-ssh-daemons	14
34	platform-alteration-boot-params	2
35	networking-ocp-reserved-ports-usage	2
36	networking-icmpv4-connectivity	1
37	**Grand Total**	**1150**

Known Issues

A known bug exists in OCP 4.12, specifically within RHCOS 8.6, causing `platform-alteration-tainted-node-kernel` failures on one or more master nodes. Further details can be found in the Tainted Kernel Tech Preview. There is another known bug present in OCP 4.13. We should differentiate between taints originating from our side (ideally none) and those arising from the CNF under test.