

# Release Notes

Published  
2022-09-13

Cloud-Native Contrail Networking 22.2

---

# Table of Contents

[Introduction](#) | 1

[Features](#) | 1

[Supported Platforms](#) | 3

[Container Tags](#) | 4

[Known Behavior](#) | 5

[Resolved Issues](#) | 7

[Requesting Technical Support](#) | 7

[Revision History](#) | 9

# Introduction

Juniper Networks Cloud-Native Contrail Networking is a cloud-native software defined networking (SDN) solution that provides high-performance networking to Kubernetes-orchestrated environments. Cloud-Native Contrail automates the creation and management of virtualized networks to connect, isolate, and secure cloud workloads and services seamlessly across cloud networks. Contrail Networking delivers federated multi-cluster networking in Kubernetes-orchestrated environments, providing a networking solution that supports both virtualized network functions (VNFs) and containerized network functions (CNFs).

These release notes accompany Release 22.2 of Cloud-Native Contrail Networking. See: [Cloud-Native Contrail Networking, Release 22](#). This document describes new features, limitations, platform compatibility requirements, known behavior, and resolved issues.

## Features

### IN THIS SECTION

- [Kubernetes and Contrail | 1](#)
- [DPDK and SR-IOV | 2](#)
- [Cluster Security | 2](#)
- [Telemetry and Analytics | 3](#)
- [Tech Preview | 3](#)

This section highlights the key features introduced with Cloud-Native Contrail Networking Release 22.2. A brief description of each new feature follows.

## Kubernetes and Contrail

**Lens Extension**—Starting in Cloud-Native Contrail Networking Release 22.2, CN2 Extension for Lens adds custom visualizations and functionality to accelerate development workflows for all the

technologies and services that integrate with Kubernetes. CN2 Extension for Lens is a plug-in uploaded directly to the Lens UI.

See [Lens Install with CN2 Extension](#).

**Contrail Etcd Database (OpenShift)**—Starting in Cloud-Native Contrail Networking Release 22.2, Contrail uses its own etcd database on an OpenShift installation by default. In an Upstream Kubernetes installation, Contrail continues to use the main Kubernetes etcd database.

**Back Up and Restore of Contrail Etcd Database (OpenShift)**—Starting in Cloud-Native Contrail Networking Release 22.2, Contrail supports back up and restore of its own etcd database. This applies to Contrail running on an OpenShift installation only.

See [Back Up and Restore Contrail Etcd](#).

**Preflight and Postflight Checks (Upstream)**—Starting in Cloud-Native Contrail Networking Release 22.2, Contrail supports preflight and postflight checks using a custom controller. This applies to Contrail running on an Upstream Kubernetes installation only. When running on an OpenShift installation, OpenShift provides its own preflight and postflight checks.

See [Run Preflight and Postflight Checks in Release 22.2](#).

## DPDK and SR-IOV

**Custom Kubernetes Scheduler**—Starting in Cloud-Native Contrail Networking Release 22.2, Contrail supports custom scheduling plugins that extend the scheduling capabilities of the default Kubernetes scheduler. As a result of these plugins (Filter, Score, NormalizeScore), the Kubernetes scheduler schedules pods on DPDK nodes based on a 32 Virtual Machine Interface (VMI) limit.

See [Control Pod Scheduling on DPDK Nodes](#).

## Cluster Security

**Encrypting Secret Data at Rest**—Starting in Cloud-Native Contrail Networking Release 22.2, Contrail automatically encrypts secret data at rest in your Kubernetes cluster and encrypts any password that you configure. A secret is an object that contains a small amount of sensitive data such as a password, a token, or a key. Data at rest encryption is a cybersecurity practice of encrypting stored data to prevent unauthorized access.

See the Kubernetes documentation [Encrypting Secret Data at Rest](#) for detailed information.

# Telemetry and Analytics

**Port-Based Traffic Mirroring**—In Cloud-Native Contrail Networking Release 22.2, port mirroring sends network traffic from defined ports to a network analyzer where you can monitor and analyze the data.

[Port-Based Mirroring.](#)

## Tech Preview

**Introducing Tech Preview Features**—Starting in Cloud-Native Contrail Networking Release 22.2, Tech Previews are introduced. Tech Previews give you the ability to test functionality and provide feedback during the development process of innovations that are not final production features.

[Juniper CN2 Technology Previews \(Tech Previews\).](#)

**Configurable Categories of Metrics Collection and Reporting**—To provide more flexibility in the telemetry export component, Cloud-Native Contrail Networking Release 22.2 introduces a new Kubernetes custom resource: MetricGroup. MetricGroup allows you to enable or disable selected metrics for exporting.

[Configurable Categories of Metrics Collection and Reporting \(Tech Preview\).](#)

**HA Prometheus Support with Thanos (Upstream)**—Starting in Cloud-Native Contrail Networking Release 22.2, Contrail supports High Availability (HA) for Prometheus by using Thanos. Thanos is a set of open source components that integrate seamlessly with Prometheus to provide a highly available metric system. This applies to Prometheus running on Upstream Kubernetes only. Prometheus running on OpenShift already supports high availability.

See [Install Contrail Analytics](#).

## Supported Platforms

The following table lists the orchestrator releases and the corresponding operating systems and other software components versions supported in Cloud-Native Contrail Networking Release 22.2.

**Table 1: Supported Orchestration Platforms**

Cloud-Native Contrail Release	Orchestrator Release	Deployment Tool	Operating System, Kernel, and Key Components Version
22.2	Kubernetes 1.22.3	Ansible	Ubuntu 20.04.3—Linux Kernel Version 5.4.0-97-generic
	Kubernetes 1.23.5	Ansible	Ubuntu 20.04.3—Linux Kernel Version 5.4.0-97-generic
	OpenShift 4.8.39	Redhat Openshift AI	RHEL CoreOS 4.8.39 — Linux 4.18.0-305.45.1.el8_4.x86_64

## Container Tags

Container tags are needed to identify the image files to download from the Contrail Container Registry during a Contrail Networking installation or upgrade.

This table provides the container tag name for the image files for Cloud-Native Contrail Networking Release 22.2.

**Table 2: Container Tag—Release 22.2**

Orchestrator Platform	Container Tag
Kubernetes 1.22.3, Kubernetes 1.23.5, OpenShift 4.8.39	22.2.0.93

# Known Behavior

## IN THIS SECTION

- [General Routing | 5](#)
- [General Features | 5](#)
- [Redhat Openshift | 6](#)
- [Kubernetes | 6](#)
- [DPDK and SR-IOV | 7](#)

This section lists known limitations with Cloud-Native Contrail Networking Release 22.2.

## General Routing

- CN2-3234: When a flow matches an ingress network policy, the egress network policy is also allowed. The network policy in Cloud-Native Contrail Networking behaves differently than standard Kubernetes behavior.
- CN2-3429: When fabric source NAT is enabled in an isolated namespace, traffic flows between pods in isolated namespaces and between pods in isolated and non-isolated namespaces.  
Workaround: Do not configure fabric source NAT on an isolated namespace.
- CN2-3256: All cSRX workloads with subinterfaces are not compatible with Cloud-Native Contrail Networking.

## General Features

- CN2-6327: When interface mirroring is enabled with the **juniperheader** option, only egress packets are mirrored.  
Disable the **juniperheader** option to mirror both egress and ingress packets.

# Redhat Openshift

- CN2-5289: In an Openshift VRRP deployment, with a separate management network and control and data network, the CNI takes a long time to come up. This issue is due to traffic NATing issues as described in [Red Hat Bugzilla: Bug 2070318](#).
- CN2-5349: In Openshift deployments, sometimes the vRouter agent core appears causing the Openshift services to not work properly.

Workaround: Reboot the nodes one time before onboarding workloads.

- CN2-6205: When updating OCP from version 4.8.39 to 4.9.31, dual-stack clusters fail. See [Red Hat Bugzilla: Bug 2085335](#).

Workaround: Delete the secrets: `etcd-serving-metrics-ocp*`, `etcd-serving-ocp*`, `etcd-serving-ocp*`, and then perform the update.

# Kubernetes

- CN2-4642: In Cloud-Native Contrail Networking, the network policy uses the reserved tags "application" and "namespace". These tags conflict with Contrail's reserved resources.
- Workaround: Do not use application and namespace labels to identify the pod and namespace resources.
- CN2-5201: In scaled environments, we recommend that you refer to the node tuning parameters of the corresponding distribution. For example, for Openshift, follow the instructions [Using the Node Tuning Operator](#).

- CN2-5902: If a service label is shared between a working pod and non-working (terminating) pods, creating a service fails.

Workaround: Remove the service label association from the non-working pods.

- CN2-6325: You cannot use Docker as a container runtime with Kubernetes 1.20. Docker as a container runtime is now deprecated in Kubernetes.

Workaround: Use the CRI-O container engine or containerd as runtimes.



# DPDK and SR-IOV

- CN2-5916: When four interfaces are configured in a bond interface on an X710 NIC, an mbuf leak with traffic drop is observed.

Workaround: Limit two interfaces in a bond configuration for X710 NICs.

## Resolved Issues

You can research limitations that are resolved with this release at: [Resolved Issues in Cloud-Native Contrail Networking, Release 22.2](#).

Use your Juniper Support login credentials to view the list. If you do not have a Juniper Support account, you can register for one [here](#).

## Requesting Technical Support

### IN THIS SECTION

- [Self-Help Online Tools and Resources | 8](#)
- [Creating a Service Request with JTAC | 8](#)

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.

- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://supportportal.juniper.net/>.

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

## Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://support.juniper.net/support/requesting-support/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

# Revision History

- 22 June 2022—Revision 2
- 02 May 2022—Revision 1, initial release

---

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2022 Juniper Networks, Inc. All rights reserved.