

# Release Notes: Cloud-Native Contrail Networking 22.4

## IN THIS GUIDE

- [Introduction | 1](#)
- [Features | 2](#)
- [Supported Platforms | 4](#)
- [Container Tags | 5](#)
- [Known Issues | 6](#)
- [Resolved Issues | 9](#)
- [Requesting Technical Support | 9](#)
- [Revision History | 10](#)

## Introduction

Juniper Cloud-Native Contrail® Networking (CN2) is a cloud-native SDN solution that provides advanced networking capabilities to containerized cloud networking environments. CN2 is optimized for Kubernetes-orchestrated environments and can be used to connect, isolate, and secure cloud workloads and services seamlessly across private, public, and hybrid clouds.

These release notes accompany Release 22.4 of CN2. They describe new features, limitations, platform compatibility requirements, known behavior, and resolved issues in CN2.

See the [Cloud-Native Contrail Networking \(CN2\)](#) page for a complete list of all CN2 documentation.

# Features

## IN THIS SECTION

- [CN2 on Amazon EKS | 2](#)
- [Cluster Security | 2](#)
- [Advanced Virtual Networking | 3](#)
- [Services | 3](#)
- [DPDK | 3](#)
- [CN2 Apstra Integration | 4](#)
- [Tech Previews for 22.4 | 4](#)

This section highlights the key features introduced with Juniper Cloud-Native Contrail Networking (CN2) Release 22.4. A brief description of each new feature follows.

## CN2 on Amazon EKS

- **CN2 on Amazon EKS**—Starting in Cloud-Native Contrail Networking Release 22.4, you can run CN2 CNI on an Amazon EKS cluster. Amazon EKS is an industry-leading managed Kubernetes service. To support ease of installation, release 22.4 makes available Terraform manifests that you can use to create a greenfield Amazon EKS cluster together with a CN2 CNI.

See the [Installation and Life Cycle Management Guide for Amazon EKS](#).

## Cluster Security

**Configure Management and Control Plane Authentication with TLS Encryption**—Starting in Cloud-Native Contrail Networking Release 22.4, you can configure TLS encryption on the Contrail control plane and vRouter. The TLS protocol is used for certificate exchange, mutual authentication, and negotiating ciphers to secure the stream from potential tampering and eavesdropping. You can use TLS-based XMPP to secure all XMPP communication that occurs in the networking environment.

See [Configure Management and Control Plane Authentication with TLS Encryption](#).

# Advanced Virtual Networking

- **Deploy a Custom Default Pod Network**— Starting in Cloud-Native Contrail Networking release 22.4, you can create pods with individual Custom Pod Networks on a per-namespace or per-pod basis. Instead of a shared Classless Interdomain Routing (CIDR), you can designate a Custom Default Pod Network for each new pod within a Network Attachment Definition (NAD) or Virtual Network.

See [Deploy a Custom Default Pod Network](#).

- **EVPN Networking Support**— Starting in Cloud-Native Contrail Networking release 22.4, you can establish connectivity between a CN2 virtual network and an EVPN-VXLAN-signalled service using Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) for virtual networks. Release 22.4 supports EVPN-VXLAN forwarding using Type2 network prefixes with virtual networks utilizing forwarding mode L2 and L2\_L3.

See [EVPN Networking Support](#).

- **vRouter Interface Health Check**—In Cloud-Native Contrail Networking Release 22.4 and 22.3, two attributes (`targetIpList` and `targetIpAll`) related to VMI health check are configurable but not supported. Documentation modified to reflect this.

See [vRouter Interface Health Check](#).

## Services

**Configure ClusterIP Service by Assigning Endpoints**—Cloud-Native Contrail Networking Release 22.4 and Release 22.2 support the ClusterIP service to work with manually assigned endpoints without adding a selector in the service.

See [Configure ClusterIP Service by Assigning Endpoints](#).

## DPDK

**DPDK on OpenShift Cluster Node**—Starting in Cloud-Native Contrail Networking Release 22.4, you can run CN2 with a DPDK data plane on an OpenShift cluster node. DPDK can provide a higher performance data path in certain circumstances versus a kernel mode data path.

See [Installing with User-Managed Networking](#).

# CN2 Apstra Integration

**CN2 Apstra Integration for SR-IOV-Based Workloads**—Starting in Release 22.4, you can extend virtual networks in Cloud-Native Contrail Networking to an Apstra-managed fabric for SR-IOV-enabled networks. The SR-IOV technology enables the physical NIC to be split into several virtual functions. These virtual NICs or virtual functions can transmit and receive packets directly as opposed to going through the vRouter. When you create workloads on SR-IOV servers and attach virtual functions to the pods, the workloads use the fabric underlay directly.

See [CN2 Apstra Integration for SR-IOV Based Workloads](#).

## Tech Previews for 22.4

**Introducing Tech Preview Features**—Starting in Cloud-Native Contrail Networking Release 22.2, Tech Previews were 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 \(Tech Previews\)](#).

## 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 22.4.

**Table 1: Supported Orchestration Platforms for Release 22.4**

Orchestrator Release	Deployment Tool	Operating System, Kernel, and Key Components Version
Kubernetes 1.23.9	Ansible	Ubuntu 20.04.3—Linux Kernel Version 5.4.0-135-generic
Kubernetes 1.24.3	Ansible	Ubuntu 20.04.3—Linux Kernel Version 5.4.0-135-generic
Kubernetes 1.25.0	Ansible	Ubuntu 20.04.3—Linux Kernel Version 5.4.0-135-generic

**Table 1: Supported Orchestration Platforms for Release 22.4 (Continued)**

Orchestrator Release	Deployment Tool	Operating System, Kernel, and Key Components Version
Red Hat OpenShift 4.8.39	Red Hat OpenShift AI	RHEL CoreOS 4.8.39 – Linux 4.18.0-305.19.1.el8_4.x86_64
Red Hat OpenShift 4.10.31	Red Hat OpenShift AI	RHEL CoreOS 4.10.31 – Linux Kernel 4.18.0-305.62.1.el8_4.x86_64

**NOTE:** Apstra integration with CN2 was tested against Apstra version 4.0.2-142.  
 DPDK integration with CN2 was tested against DPDK version 21.11.

## 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.

The procedures to access the Contrail Container Registry are provided directly by Juniper Networks. The location of the files in the Contrail Container Registry changed for the CN2 software starting in Release 22.4. Email [contrail-registry@juniper.net](mailto:contrail-registry@juniper.net) to obtain access credentials to the registry or if you have any questions about file locations within the registry.

The following table provides the container tag name for the image files for CN2 Release 22.4.

**Table 2: Container Tag—Release 22.4**

Orchestrator Platform	Container Tag
Kubernetes 1.23.9, Kubernetes 1.24.3, Kubernetes 1.25.0, OpenShift 4.8.39, OpenShift 4.10.31	22.4.0.284

# Known Issues

## IN THIS SECTION

- [General Routing | 6](#)
- [General Features | 6](#)
- [Redhat OpenShift | 7](#)
- [CN2 and Kubernetes | 8](#)
- [Security | 8](#)

This section lists the known issues in Cloud-Native Contrail Networking (CN2) Release 22.4.

## General Routing

- 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.
- CN2-10038: The maximum number of virtual interfaces (VIFs) you can attach to a DPDK vRouter is 64. This includes the VIF used by the compute service pods running on the compute node.

## General Features

- CN2-3256: cSRX workloads with sub-interfaces are not compatible with CN2.
- CN2-6327: When interface mirroring is enabled with the **juniperheader** option, only egress packets are mirrored.  
Workaround: Disable the **juniperheader** option to mirror both egress and ingress packets.
- CN2-8729: If the nodeSelector field is not populated to run on a single node, the postflight check might show some error messages for UDP test. Also, ping and TCP tests will fail.  
Workaround: In the contrail-readiness-postflight.yaml file, populate the nodeSelector field to run on a single node.
- CN2-5916: When four interfaces are configured in a bond interface on an X710 NIC, an mbuf leak with traffic drop occurs.

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

- CN2-10346: When restarting a vRouter pod on kernel-mode nodes where vhost0 is installed onto bond interfaces, the bond IP address might gets assigned to a bond secondary interface instead of a bond primary interface.

Run the following script for the workaround:

```
Bond-patch.txt
text · 982 B

#!/bin/bash

set -x

slave_list=$(ip addr show | grep SLAVE | awk '{ print $2 }' | sed 's:////')
for slave in "${slave_list[@]"; do
    IFS=' '
    bond=$(ip addr show dev ${slave} | grep SLAVE | awk -F'master ' '{print $2}' | awk -F' ' '{print $1}')
    IFS=$'\n'
    route_list=$(ip route show | grep ${slave})
    for route in "${route_list[@]"; do
        echo "route: ${route}"
        new_route=$(echo ${route} | sed "s/${slave}/${bond}/g")
        route_cmd=$(echo "ip route replace ${new_route}" | sed -e 's|["'\''"]||g')
        eval ${route_cmd}
    done
    ipv4=$(ip addr show dev ${slave} | grep 'inet ' | awk '{ print $2 }')
    ipv6=$(ip addr show dev ${slave} | grep 'inet6 ' | awk '{ print $2 }')
    echo "slave: '${slave}', bond: '${bond}', ipv4: '${ipv4}', ipv6: '${ipv6}'"
    if [[ -n "$ipv4" ]]; then
        ip addr del ${ipv4} dev ${slave}
        ip addr add ${ipv4} dev ${bond}
    fi
    if [[ -n "$ipv6" ]]; then
        ip addr del ${ipv6} dev ${slave}
        ip addr add ${ipv6} dev ${bond}
    fi
fi
```

## Redhat OpenShift

- CN2-7787: The Kubevirt deployment in Openshift 4.10 fails intermittently. See the [Red Hat OCPBUGS-2535](#) for information.

# CN2 and Kubernetes

- CN2-4822: You can not configure BGPaaS objects on nodes that host the Contrail controller and worker nodes on same physical host.
- Workaround: None. Production deployments run the Kubernetes worker nodes and controller in different physical hosts.
- CN2-8728: When you deploy CN2 on AWS EC2 instances, running Kubernetes service traffic and Contrail datapath traffic on different interfaces is not supported.

Workaround: Do not deploy Kubernetes and data traffic on the same interface in AWS.

- CN2-9276: The custom default pod network does not support environments where Multus is installed. This includes Red Hat's OpenShift Container Platform and any Kubernetes distribution where Multus was manually installed.
- CN2-10010: If you create more pods in a subnet than the number of available IP addresses, the usable IPs are blocked from the subnet when other active pods are deleted.

Workaround: Delete the pods that failed to release the blocked IPs.

- CN2-10351: Kubevirt v0.58.0 does not support imagePullSecret, required for pulling images from the secure registry: [enterprise-hub.juniper.net/contrail-container-prod/](https://enterprise-hub.juniper.net/contrail-container-prod/).

Following these steps for the workaround:

1. Install Docker.
2. Create a local insecure registry.
3. Restart Docker.
4. Download the required containers. The containers are located at [Release Userspace CNI - dpdk vhostuser interface support Juniper/kubevirt](#). These containers are stored as Assets.
5. Load the containers.
6. Tag and push the containers to the new insecure registry.
7. Download operator.yaml and cr.yaml.
8. Modify the kubevirt-operator.yaml to use your insecure registry.

## Security

- CN2-4642: In CN2, the network policy uses the reserved tags application and namespace. These tags conflict with Contrail's reserved resources.



Workaround: Do not use the application and namespace labels to identify the pod and namespace resources.

- CN2-10012: If the network policy has a deny-all rule, removing it by updating the policy does not work.

Workaround: Delete the policy and re-add it again.

## Resolved Issues

You can research limitations that are resolved with this release at: [Resolved Issues in Cloud-Native Contrail Networking 22.4](#).

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 | 9](#)
- [Creating a Service Request with JTAC | 10](#)

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

- 19 December 2022—Revision 4
- 23 September 2022—Revision 3
- 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.