

Release Notes

Published
2023-04-13

Release Notes: Cloud-Native Contrail Networking 23.1

Table of Contents

Introduction | 1

New Features | 1

Supported Platforms | 4

Container Tags | 5

Known Limitations | 6

Resolved Issues | 10

Requesting Technical Support | 10

Revision History | 11

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 23.1 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.

New Features

IN THIS SECTION

- [CN2 on Amazon EKS | 2](#)
- [CN2 on OpenShift | 2](#)
- [CN2 Apstra Integration | 2](#)
- [Configure Kubernetes | 2](#)
- [Security | 3](#)
- [Advanced Virtual Networking | 3](#)
- [Services | 4](#)

This section highlights the key features introduced in CN2 Release 23.1. A brief description of each new feature follows.

CN2 on Amazon EKS

- **Multi-cluster CN2**—CN2 Release 23.1 supports multi-cluster CN2 on Amazon EKS. In a multi-cluster CN2 deployment, the central cluster provides the networking and CNI for the distributed workload clusters.

See [Install Multi-Cluster CN2 on Amazon EKS](#).

- **VPC to CN2 Communication in AWS EKS**—Starting in CN2 Release 23.1, you can access a Kubernetes workload from an AWS VPC. Release 23.1 introduces a gateway service instance (GSI), which is a collection of Amazon Web Service (AWS) and Kubernetes resources that work together to seamlessly interconnect CN2 with VPC and external networks.

See [VPC to CN2 Communication in AWS EKS](#).

CN2 on OpenShift

- **OpenShift 4.12**—CN2 Release 23.1 supports OpenShift 4.12.

See [Upgrade OpenShift](#).

CN2 Apstra Integration

- **Extend Virtual Networks to Apstra**—Starting in CN2 Release 23.1, you can extend virtual networks from your Kubernetes cluster to the data center fabric managed by Apstra

See [Extend Virtual Networks to Apstra](#).

Configure Kubernetes

- **Pod Scheduling**—CN2 23.1 supports network-aware pod scheduling using contrail-scheduler. This feature enhances the Kubernetes pod scheduler with plugins that analyze the network metrics of a node before scheduling pods.

See [Pod Scheduling](#).

Security

- **Namespace Security Policies**—Starting in Release 23.1, CN2 supports Namespace security policies. Namespace security policies allows you to define policies from a source endpoint to a destination endpoint within a namespace, or to an external IP address.

See [Security Policies](#).

Advanced Virtual Networking

- **Customize Virtual Networks for Pod Deployments, Services, and Namespaces**—Starting in CN2 Release 23.1, you can apply a custom default network for pod Deployments, services, and namespaces. Pods and services that use a custom network are isolated from other networks. This feature also supports environments with Multus CNI enabled.

See [Customize Virtual Networks for Pod Deployments, Services, and Namespaces](#).

- **EVPN Networking**—CN2 Release 23.1 supports EVPN-VXLAN Networking using Type 5 routes. The Type 5 route, also called the IP prefix route, enables inter-virtual network connectivity in CN2.

See [EVPN Networking](#).

- **Static Routes**—Starting in CN2 23.1, you can configure static routes for your cluster. This release introduces RouteTable and InterfaceRouteTable CRs that configure static routes for a virtual network or VMI.

See [Static Routes](#).

- **IPv4 and IPv6 Dual-Stack Networking**—CN2 Release 23.1 supports dual-stack networking for services. Release 22.4 supported dual-stack networking for pods, but 23.1 enables you to assign IP addresses to services from an IPv4 or IPv6 network.

See [IPv4 and IPv6 Dual-Stack Networking](#).

Services

- **Floating IP/DNAT for IPv6 Addresses**— CN2 23.1 supports floating IP (DNAT) functionality for IPv6 addresses. Your back-end pod VMIs are mapped to an IPv6 floating IP. The vRouter performs DNAT and routes traffic to the next hop, or the translated destination address (back end pod VMI) from external networks to your back-end pod VMIs.

See [FloatingIP/DNAT for IPv6 Addresses](#).

Supported Platforms

The following table lists the orchestrator platforms and software versions supported in CN2 Release 23.1.

Table 1: Supported Orchestration Platforms for CN2 Release 23.1

Orchestrator Release	Runtime Version	Operating System, Kernel and Key Components Versions
Kubernetes 1.25.5	containerd, crio	Ubuntu 20.04—Linux Kernel version 5.4.0-135-generic
	containerd, crio	Ubuntu 22.04—Linux Kernel version 5.15.0-67-generic
Kubernetes 1.23.9	containerd, crio	Ubuntu 20.04.3—Linux Kernel version 5.4.0-135-generic
	containerd, crio	Ubuntu 22.04—Linux Kernel version 5.15.0-67-generic
Kubernetes 1.24.3	containerd, crio	Ubuntu 20.04.3—Linux Kernel version 5.4.0-135-generic
	containerd, crio	Ubuntu 22.04—Linux Kernel version 5.15.0-67-generic

Table 1: Supported Orchestration Platforms for CN2 Release 23.1 (Continued)

Orchestrator Release	Runtime Version	Operating System, Kernel and Key Components Versions
Red Hat OpenShift 4.8.39	crio	RHEL 8.4—Linux Kernel 4.18.0-305.45.1.el8_4.x86_64
Red Hat OpenShift 4.10.31	crio	RHEL 8.4—Linux Kernel 4.18.0-348.23.1.el8_5.x86_64
Red Hat OpenShift 4.12.0	crio	RHEL 8.6—Linux Kernel 4.18.0-305.62.1.el8_4.x86_64
Amazon EKS v1.24.10-eks-48e63af	containerd	Kernel 5.10.167-147.601.amzn2.x86_64

- Apstra version: 4.1.2-269
- DPDK version: 21.11
- Kubevirt version: 0.58.0-jnpr

NOTE: See [CN2 Tested Integrations](#) for integrations fully tested and validated by Juniper, including tested NICs and other software components.

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. To obtain access credentials to the registry or if you have any questions about file locations within the registry, send an email to: contrail-registry@juniper.net.

The following table provides the container tag name for the image files for CN2 Release 23.1.

Table 2: Container Tag—Release 23.1

Orchestrator Platform	Container Tag
<ul style="list-style-type: none"> • Kubernetes 1.25.5, 1.23.9, 1.24.3 • Red Hat OpenShift 4.12.0, 4.10.31, 4.8.39 • Amazon EKS v1.24.10-eks-48e63af 	23.1.0.282

Known Limitations

IN THIS SECTION

- [General Routing | 6](#)
- [General Features | 7](#)
- [Red Hat OpenShift | 8](#)
- [CN2 Apstra Integration | 8](#)
- [CN2 and Kubernetes | 9](#)
- [Security | 9](#)

This section describes the issues and limitations present in Cloud-Native Contrail Networking (CN2) Release 23.1.

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.

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 get 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 $2 }' | sed 's://')Revision History
for slave in "${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

```

- CN2-13314: The gateway service instance (GSI) does not work with a 4-byte ASN.

Workaround: Use a 2-byte ASN when connecting workloads through the GSI service.

Red Hat OpenShift

- CN2-7787: The Kubevirt deployment in Openshift 4.10 fails intermittently.

See [Red Hat OCPBUGS-2535](#) for a workaround.

- CN2-13011: Red Hat OCP backup and restore fails.

See Red Hat <https://access.redhat.com/solutions/6964756> for a workaround.

CN2 Apstra Integration

- CN2-13607: In a CN2 Apstra deployment, Apstra takes several minutes to create a virtual network.

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.

- CN2-10351: Kubevirt v0.58.0 does not support imagePullSecret, required for pulling images from the secure registry: 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 CN2 Release 23.1.](#)

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 | 11](#)
- [Creating a Service Request with JTAC | 11](#)

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

- 30 March 2023—Revision 5

- 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 © 2023 Juniper Networks, Inc. All rights reserved.