

Release Notes

Published
2022-07-11

Cloud-Native Contrail Networking 22.1

Table of Contents

Introduction | 1

Features | 1

Supported Platforms | 5

Container Tags | 6

Known Behavior | 7

Requesting Technical Support | 8

Revision History | 10

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 22.1 of Cloud-Native Contrail Networking, which is the initial release for Cloud-Native Contrail Networking. They describe new features, limitations, platform compatibility requirements, and known problems.

Features

IN THIS SECTION

- [Advanced Virtual Networking | 2](#)
- [DPDK and SR-IOV | 3](#)
- [Services | 4](#)
- [Telemetry and Analytics | 4](#)

This release is the initial release of Cloud-Native Contrail Networking.

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

- **IP Fabric Forwarding and Fabric Source Network Address Translation**—Starting in Cloud-Native Contrail Networking Release 22.1, IP fabric forwarding and fabric source NAT can be used to provide access to the underlay network. IP fabric forwarding provides clusters running in the overlay network with a path to the underlay network through the external virtual network. Fabric source NAT allows a gateway device in a fabric to translate the source IP address of data plane node traffic exiting the fabric into a public-side IP address.

See [Enable IP Fabric Forwarding and Fabric Source NAT in Cloud-Native Contrail Networking](#).

- **Multiple Interfaces and Multus Support**—Starting in Cloud-Native Contrail Networking Release 22.1, Cloud-Native Contrail Networking supports multiple network interfaces for a pod within Kubernetes. The support for multiple network interfaces includes interoperability with Multus. Multus is a container network interface (CNI) plugin for Kubernetes that you can use to enable support for multiple network interfaces in a pod.

See [Enable Pods with Multiple Network Interfaces in Cloud-Native Contrail Networking](#).

- **IPv6 and IPv4 Dual-Stack Networking Support**—Starting in Contrail Networking Release 22.1, dual-stack (IPv4, IPv6) is supported for your Kubernetes (Kubeadm, Kubespray) clusters. The Cloud-Native Contrail Networking deployer creates an IPv6 network for the `podNetwork` and `serviceNetwork`. New pods have IPv6 and IPv4 addresses.

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

- **Kubernetes Network Policy Support** —Starting in Contrail Networking Release 22.1, the Cloud-Native Contrail Networking implementation of Kubernetes Network Policy is supported. Create and apply a `NetworkPolicy` resource to establish egress and ingress rules for your pods. See

See [Kubernetes Network Policy Support](#).

Advanced Virtual Networking

- **VirtualNetworkRouter Support**—Starting in Contrail Networking Release 22.1, the `VirtualNetworkRouter` (VNR) resource is supported. VNR establishes connectivity between virtual networks through route sharing between virtual networks.

See [Deploy VirtualNetworkRouter in Cloud-Native Contrail Networking](#).

- **Configure Inter-Virtual Networking with Route-Targets**—Starting in Contrail Networking Release 22.1, you can establish route-target communities by defining matching route-targets in a virtual network. Add route-targets to a `VirtualNetwork` resource to enable your virtual networks to exchange VRF routing tables.

See [Configure Inter-Virtual Network Routing Through Route Targets](#).

- **IPAM for Pod Networking**. Unlike previous releases, IPAM implementation is done through the `Subnet` and `SubnetPool` resources. These resources enable you to configure IPv4 and IPv6 address allocation in your cluster.

See [Configure IPAM for Pod Networking](#).

- **Support for Isolated Namespaces**— Starting in Contrail Networking Release 22.1, you can configure isolated namespaces on pods in a Kubernetes cluster. An isolated namespace enables you to run

customer-specific applications that you want to keep private. You can create an isolated namespace to isolate a pod from other pods, without explicitly configuring a network policy.

See [Create an Isolated Namespace](#).

- **Allowed Address Pairs Support on Interfaces**—Starting in Contrail Networking Release 22.1, Cloud-Native Contrail Networking supports allowed address pairs (AAPs). Allowed address pairs allows you to add additional IP/MAC (CIDR) addresses to the guest interface (`VirtualMachineInterface`) by using a secondary IP address.

See [Configure Allowed Address Pairs](#).

- **Packet-Based Forwarding on Virtual Interfaces**— Starting in Contrail Networking Release 22.1, you can enable packet-based forwarding on virtual interfaces. In packet mode, the virtual interface processes traffic on a per-packet basis and ignores all flow information. Packet mode is stateless, meaning that the virtual interface does not subsequently keep track of session information or go through traffic analysis to determine how a session is established.

See [Enable Packet-Based Forwarding on Virtual Interfaces](#).

- **Reverse Path Forwarding on Virtual Interfaces**—Starting in Contrail Networking Release 22.1, reverse path forwarding (RPF) is supported on virtual interfaces. RPF is a source address validation tool that uses the IP routing table to verify whether the source IP address of an incoming packet is from a valid path.

See [Configure Reverse Path Forwarding on Virtual Interfaces](#).

- **VLAN Subinterface Support on Virtual Interfaces**—Starting in Contrail Networking Release 22.1, you can use VLAN subinterfaces to route traffic to multiple VLANs for your services.

See [Enable VLAN Subinterface Support on Virtual Interfaces](#).

DPDK and SR-IOV

- **Deploy Kubevirt DPDK Dataplane Support for VMs**—Starting in Contrail Networking Release 22.1, your Kubernetes cluster supports container and VM workloads simultaneously with Kubevirt. Like container workloads, Kubevirt enables your VMs to take advantage of DPDK with `vhostuser` interface types.

See [Deploy Kubevirt DPDK Dataplane Support for VMs](#).

.

- **DPDK Interfaces for Optimal Container Networking**—Starting in Contrail Networking Release 22.1, DPDK interfaces (Vhost user protocol, virtio interface), are supported for container networking. Deploy a DPDK vRouter in your cluster to support DPDK, non-DPDK, and hybrid workloads.

See [Deploy DPDK vRouter for Optimal Container Networking](#).

- **Kubernetes Ingress Support**—Starting in Contrail Networking Release 22.1, Kubernetes Ingress Controller is supported. Use a validated ingress service (HAProxy, NGINX, Contour) to perform load balancing for your pods and services.
See [Kubernetes Ingress Support](#).

Services

- **Display Microservice Status**—Starting in Contrail Networking Release 22.1, you can use ContrailStatus, a kubectl plugin, to display the status information of Contrail Networking services in the three different planes (configuration, control, and data). In addition to the usual containers in a specific service, init (initialization) container status within the service and the relative software status, such as BGP and XMPP in control_controller are also visible.
See [Display Microservice Status in Cloud-Native Contrail Networking](#).
- **NodePort Service Support**—Starting in Contrail Networking Release 22.1, Kubernetes NodePort service is implemented using the InstanceIP resource and FloatingIP resource, both of which are similar to the ClusterIP service. NodePort service exposes a service on each node's IP address at a static port and maps the static port on each node with a port of the application on the pod.
See [NodePort Service Support in Cloud-Native Contrail Networking](#).
- **LoadBalancer Service Support**— Starting in Contrail Networking Release 22.1, the Kubernetes LoadBalancer service is supported. The LoadBalancer service allocates the IP address from an external virtual network. If you have external IPs that route to one or more cluster nodes, the LoadBalancer services can be exposed on those external IPs. Any requests received through the provisioned external IP is ECMP load-balanced across all backend pods in the cluster.
See [Create a LoadBalancer Service](#).
- **BGP as a Service (BGPaaS)**—Starting in Cloud-Native Contrail Networking Release 22.1, BGP as a Service (BGPaaS) is supported. BGPaaS provides the network support for BGP to operate within a virtual network in cloud networking environments using Cloud-Native Contrail Networking.
See [Enable BGP as a Service in Cloud-Native Contrail](#).

Telemetry and Analytics

- **Contrail Networking Analytics**—Analytics is an optional feature set in Contrail Networking Release 22.1. Analytics is packaged separately from the Contrail Networking core CNI components and has its own installation procedure. The package consists of a combination of open-source software and

Juniper developed software. The analytics features are categorized into the following high-level functional areas; metrics, flow and session records, Sandesh User Visible Entities (UVE), logs, and introspect.

See [Contrail Networking Analytics](#).

- **Alerts**—The Contrail Networking Release 22.1 analytics solution installs a set of predefined alert rules. You can also define your own custom alert rules. Generated alerts are stored as records in Prometheus and viewed in the Grafana UI. Integration with external systems, such as PagerDuty, OpsGenie, email, and so on for alert notification is supported with the AlertManager component. See [Contrail Networking Analytics](#).
- **vRouter Session Analytics**—Starting in Contrail Networking Release 22.1, the collection, storage, and query for vRouter traffic is supported. Contrail Networking collects user visible entities (UVEs) and traffic information (session) for traffic analysis and troubleshooting. The collector module provides the function of storing these objects and provides APIs to access the collected information. The following components are installed in the Contrail cluster in the contrail namespace (NS); Collector microservice, InfluxDB, Fluentd, and OpenSearch. See [vRouter Session Analytics in Contrail Networking](#).
- **Centralized Logging**—Starting in Contrail Networking 22.1, instead of browsing through individual log files, logs from all components of Contrail Networking are collected and available to the administrator in a centralized location. Centralized logging also provides the ability to correlate the log files from multiple software components. For security, there is strict logging of all create, read, update, and delete (CRUD) actions performed by any administrator, with individual access credentials so individuals can be identified. AWS OpenSearch Stack, an open source log collector and analyzer framework, provides out-of-box log collection and analysis functionality. See [Centralized Logging](#).

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 22.1.

Table 1: Supported Orchestration Platforms

Cloud-Native Contrail Release	Orchestrator Release	Deployment Tool	Operating System, Kernel, and Key Components Version
22.1	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 22.1.

Table 2: Container Tag—Release 22.1

Orchestrator Platform	Container Tag
Kubernetes 1.22.3, Kubernetes 1.23.5, OpenShift 4.8.39	22.1.0.93

Known Behavior

IN THIS SECTION

- [General Routing | 7](#)
- [General Features | 7](#)
- [Kubernetes | 8](#)
- [DPDK and SR-IOV | 8](#)

This section lists known limitations with Cloud-Native Contrail Networking Release 22.1.

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.
- CN2-4634: Configuring a local ASN parameter in a BGPRouter object interferes with the operation of a peer ASN parameter.
Workaround: Do not configure the local ASN field. Use the peer ASN field to configure a BGP peer.

General Features

- CN2-5166: When upgrading a CNI, sometimes Contour's load balance envoy readiness check fails. This is due to a bug in Contour. See: [Envoy Pod Issue with Contour](#).

Workaround: Restart Contour.

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.

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.

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

- 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.