

Contrail Release 1908

Published
2025-08-18

RELEASE

Table of Contents

Introduction

New and Changed Features

Supported Platforms Contrail Release 1908

Known Behavior

Introduction

Juniper Networks Contrail is an open, standards-based software solution that delivers network virtualization and service automation for federated cloud networks. It provides self-service provisioning, improves network troubleshooting and diagnostics, and enables service chaining for dynamic application environments across enterprise virtual private cloud (VPC), managed Infrastructure as a Service (IaaS), and Networks Functions Virtualization (NFV) use cases.

These release notes accompany Release 1908 of Juniper Networks Contrail. They describe new features, limitations, and known problems.

These release notes are displayed on the Juniper Networks Contrail Documentation Web page at https://www.juniper.net/documentation/en_US/contrail19/information-products /topic-collections/ release-notes/index.html.

New and Changed Features

IN THIS SECTION

- [Configure Storm Control on Interfaces | 2](#)
- [Support for Port Profiles | 2](#)
- [Support for Enterprise Style Configuration for QFX Devices During Fabric Creation | 3](#)
- [Support for 4 Byte AS Number in Contrail Release 1908 | 3](#)
- [Encryption Support for Redis Traffic | 4](#)
- [Support for Contrail Networking Deployment with Kubernetes Using Juju Charms | 4](#)
- [Support for Adding DHCP Server Information | 5](#)
- [Support for Device Image Upgrade after RMA | 5](#)
- [Support for Netronome SmartNIC vRouter | 5](#)

The features listed in this section are new or changed as of Contrail Release 1908. A brief description of each new feature is included.

Configure Storm Control on Interfaces

Starting with Contrail Networking Release 1908, when Contrail manages a datacenter fabric, you can configure storm control on the access logical interfaces of a datacenter fabric managed by Contrail.

A traffic storm is generated when messages are broadcast on a network and each message prompts a receiving node to respond by broadcasting its own copy of the messages on the network. This, in turn, prompts further replications, creating a snowball effect. The network is suddenly flooded with packets, creating unnecessary traffic that leads to poor network performance or even a complete loss of network service. Storm control enables the switch to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level—called the *storm control level*—is exceeded, thus preventing packets from proliferating and degrading the LAN. As an alternative to having the switch drop packets, you can configure it to shut down interfaces or temporarily disable interfaces when the storm control level is exceeded.

To enable storm control on an interface, you must first create a storm control profile, and then attach it to a port profile. You can then apply the port profile to an interface or a virtual port group (VPG). In a greenfield deployment with enterprise style configuration, you can configure storm control on a device after Contrail command is set up and all devices discovered. You can create port profiles and storm control profiles from the **Overlay > Port Profiles** page.

Storm control profile feature is supported only on QFX5000 and QFX10000 series devices.

For more information, see [Configure Storm Control on Interfaces](#).

Support for Port Profiles

Starting with Contrail Networking Release 1908, you can define port profiles for the interfaces on a datacenter fabric. A port profile functions like a container that can support multiple port-related configurations, and allows you to apply those configuration by attaching them to the port profile. You can then apply the port profile on an interface or a virtual port group. In Contrail Networking Release 1908, you can attach only storm control profiles to port profiles.

To delete a port profile, you must first detach the port profile from the virtual port group or the instance.

For more information, see [Configure Storm Control on Interfaces](#).

Support for Enterprise Style Configuration for QFX Devices During Fabric Creation

Contrail Release 1908 enables you to select enterprise style of configuration for the CRB-Access role on QFX Series switches.

With the enterprise style of configuration, any VLAN being provisioned in an EVPN VXLAN fabric maps to a Virtual Extensible LAN Network Identifier (VNI) in a 1:1 ratio. For more information, see [Configuring EVPN VXLAN Fabric with Multitenant Networking Services](#).

You can select the **VLAN-ID Fabric Wide Significance** check box in the **Infrastructure > Fabrics > Create > New Fabric > Provision** and **Infrastructure > Fabrics > Create > Existing Fabric > Provision** pages to enable enterprise style of configuration. De-select the check box to enable service provider style of configuration. The check box is selected by default since enterprise style is the default setting. Once configured, you can modify the enterprise style setting to service provider style of configuration. However, you cannot modify the service provider style to enterprise style of configuration without having to recreate the fabric.

For more information, see [Create a Fabric](#).

Support for 4 Byte AS Number in Contrail Release 1908

Contrail 1908 supports 4-byte or 32-bit Autonomous System (AS) numbers in BGP as specified in RFC 6793. The provision for 4-byte AS numbers is introduced to avoid exhaustion of AS numbers. You can now set an AS number in the range 1-4294967295. The default AS number is 64512.

To start using AS value in the 4-byte range:

1. Navigate to **Infrastructure > Cluster > Advanced Options** page.

The **Global Config** tab is displayed, which lists all system configuration information.

2. Click the **Edit** icon.

The **Edit System Configuration** dialog box is displayed.

3. Select **Enabled** option button under **4 Byte ASN** field.

To disable 4-byte ASN range, select **Disabled**.

You can now assign 2-byte or 16-bit AS number in the range 1-65535.

To assign 4-byte value in **Route Target(s)** field:

1. Navigate to **Overlay > Virtual Networks > Edit Virtual Network** page to edit existing virtual network.

Navigate to **Overlay > Virtual Networks > Create Virtual Network** page to create a new virtual network.

2. Click **Routing, Bridging and Policies**.

Route Target(s) field is displayed. Click **+Add**.

In **Route Target(s)** section, you can now assign a 4-byte value in the range of 1-4,294,967,295 in the **ASN** field, when **4 Byte ASN** is enabled in **Global Config**. If you assign the **ASN** field a 4-byte value, you must assign a 2-byte value in the range of 0-65,535 in the **Target** field. You can also assign a 2-byte value in the range of 1-65,535 in the **ASN** field, when **4 Byte ASN** is disabled in **Global Config**. If you assign the **ASN** field a 2-byte value, you must assign a 4-byte value in the range of 0-4,294,967,295 in the **Target** field.

You can also add suffix *L* or *l* (*lower-case L*) at the end of a value in the **ASN** field to assign the value in 4-byte range. Even if the value provided in the **ASN** field is in the range of 1-65,535, adding *L* or *l* (*lower-case L*) at the end of the value assigns it in 4-byte range. If you assign the **ASN** field a value in the 4-byte range, you must enter a value in the range of 0-65,535 in the **Target** field .

Encryption Support for Redis Traffic

Contrail Release 1908 supports an SSL encrypted tunneling program called stunnel to secure Redis traffic. The stunnel is used to route traffic between Redis clients and servers. SSL encryption in the stunnel acts as a layer of security when Contrail analytics client processes connect to a Redis instance server. In releases prior to Contrail Release 1908, connection requests sent from contrail-analytics clients to Redis server sometimes posed security threats since Redis did not support encryption. The stunnel feature is supported in Contrail Release 1908 only when Contrail is deployed with Red Hat OpenStack Platform (RHOSP).

Support for Contrail Networking Deployment with Kubernetes Using Juju Charms

Starting in Contrail Release 1908, you can deploy Contrail Networking with Kubernetes by using Juju Charms. Juju helps you deploy, configure, and efficiently manage applications on private clouds and public clouds. A Charm is a module containing a collection of scripts and metadata and is used with Juju to deploy Contrail. Juju Charms helps reduce the complexity of deploying Contrail Networking by providing a simple way to deploy, configure, scale, and manage Contrail operations.

Starting with Release 1908, Contrail Networking supports the following charms:

- `contrail-kubernetes-master`

- `contrail-kubernetes-node`

For more information, see [Installing Contrail with Kubernetes by Using Juju Charms](#).

Support for Adding DHCP Server Information

Starting in Contrail Release 1908, tenant administrators can define a set of DHCP server IP addresses while configuring virtual networks and logical routers on a multi-tenant data center fabric. In earlier releases, a Contrail services node (CSN) is used to provide DHCP and Domain Name System (DNS) services to bare metal servers. With Contrail Release 1908, you can directly add DHCP server information by adding the server IP address in the **Overlay > Logical Router > Create Logical Router** page of the Contrail Command user interface (UI). However, Contrail Networking does not support the use of a DHCP server and a CSN at the same time. When you use a DHCP server, you must not provision a CSN and must remove existing CSNs.

For more information, see [Adding DHCP Server Information](#).

Support for Device Image Upgrade after RMA

Starting with Contrail Release 1908, Contrail Networking supports device image upgrade after the Return Material Authorization (RMA) process. Contrail Release 1907 supported Return Material Authorization (RMA). With Contrail Release 1908, after you replace a device in RMA state with a new device, the new device is upgraded to the device image version specified during the initial ZTP onboarding process.

For more information on RMA, see the [Return Material Authorization](#) topic.

For more information on ZTP onboarding process, see the **Provisioning Option - New Fabric** section of the [Create a Fabric](#) topic.

Support for Netronome SmartNIC vRouter

Contrail Networking Release 1908 supports Netronome Agilio CX for Contrail Networking deployment with Red Hat OpenStack Platform Director (RHOSPd) 13 environment. This feature will enable increased packets per second (PPS) capacity of Contrail vRouter datapath allowing applications to reach their full processing capacity. Additionally, it allows to reclaim CPU cores from Contrail vRouter off-loading permitting more VMs and VNFs to be deployed per server.

For more information, see [Using Netronome SmartNIC vRouter with Contrail Networking](#).

Supported Platforms Contrail Release 1908

Table 1 on page 6 lists the orchestrator releases and the corresponding operating systems and kernel versions supported by Contrail Release 1908.

Table 1: Supported Platforms

Contrail Release	Orchestrator Release	Deployment Tool	Operating System, Kernel, and Key Components Version
Contrail Release 1908	Kubernetes 1.12	Ansible	<ul style="list-style-type: none"> CentOS 7.6—Linux Kernel Version 3.10.0-957.27.2 Docker version: 18.06.0-ce
	OpenShift 3.11	Ansible	<ul style="list-style-type: none"> RHEL7.6—Linux Kernel Version 3.10.0-957.27.2
	OpenStack Rocky	Ansible	<ul style="list-style-type: none"> CentOS 7.6—Linux Kernel Version 3.10.0-957.27.2 Ansible version: 2.5.2 Docker version: 18.03.1-ce
		Ansible	<ul style="list-style-type: none"> Ubuntu-16.04.5 - Linux Kernel Version 4.15.0-45-generic
		Ansible	<ul style="list-style-type: none"> Ubuntu-18.04.2 - Linux Kernel Version 4.15.0-46-generic

Table 1: Supported Platforms (Continued)

Contrail Release	Orchestrator Release	Deployment Tool	Operating System, Kernel, and Key Components Version
	OpenStack Queens	Ansible	<ul style="list-style-type: none"> CentOS 7.6—Linux Kernel Version 3.10.0-957.27.2 <p>Ansible version: 2.5.2</p> <p>Docker version: 18.03.1-ce</p>
		Juju Charms	<ul style="list-style-type: none"> Ubuntu 18.04.2—Linux Kernel Version 4.15.0-48-generic <p>MaaS Version: 2.4.2</p>
		Helm	<ul style="list-style-type: none"> Ubuntu 16.04.3—Linux Kernel Version 4.4.0-112-generic <p>Docker version: 17.03.2-ce</p> <p>Helm version: 2.7.2</p> <p>Kubernetes version: 1.9.3</p>
	Red Hat OpenStack Platform 13	RHOSP 13 director	<ul style="list-style-type: none"> RHEL7.6—Linux Kernel Version 3.10.0-957.27.2
	VMware vCenter 6.7	Ansible	<ul style="list-style-type: none"> ESX version 6.5 <p>CentOS VM version running vRouter: CentOS 7.5—Linux Kernel Version 3.10.0-862.9.1</p>

[Table 2 on page 7](#) lists the AppFormix release to use with Contrail Release 1908.

Table 2: AppFormix Release

Contrail Release	AppFormix Release
------------------	-------------------

Known Behavior

This section lists known limitations with this release.

- CEM-8553 As a part of CEM-335, zookeeper path for system defined route targets are changed from `/id/bgp/route-targets` to `/id/bgp/route-targets/type0` and `/id/bgp/route-targets/type1-2`. During upgrade, schema transformer is restarted and when the Routing Instances are reinit, route targets from new path are added but some route targets from old path are not removed from the routing instances. Some Routing Instance have references to more than one system defined route target or route targets with IDs in target:<ASN>:8XXXXXX.

As a workaround, remove the incorrect route targets from routing instances by using the ref-update requests. Contact JTAC for help in fixing this issue.

- CEM-8149 BMS LCM with fabric set with `enterprise_style=True` is not supported. By default, `enterprise_style` is set to `False`. User should avoid using `enterprise_style=True` if the fabric object will onboard BMS LCM instance.
- CEM-8026 Contrail multicloud credentials are insecurely stored in release 1908. Contrail multicloud currently supports only clouds where provider is unique for all clouds. Only one cloud can exist within the same provider. To obtain credential files for Azure (`accessToken.json`, `azureProfile.json`) user must run the following command from the desktop terminal:

```
az login -tenant <enter_tenant_name>
```

For example:

```
az login --tenant contrailmirrorgmail.onmicrosoft.com
```

User must download AWS secret key and AWS access key to CSV and save it in two separate files (values only). Those files are needed during provisioning of Contrail multicloud.

- CEM-7943 4-byte ASN support cannot be enabled during provisioning. To configure 4-byte ASN, post provisioning, user must use new UI and rest-api to enable 4-Byte ASN and then configure 4-Byte ASN number.

- CEM-7874 User defined alarms may not be generated, when third stunnel/Redis service instance is down after the first two instances were restarted.
- CEM-5441 On a freshly provisioned Contrail + Appformix cluster, to enable the live data streaming the web sockets between Contrail UI and Appformix server need to be established. In release 1907 this needs to be triggered once by login to the Appformix UI.
- CEM-5334 The multi cloud gateway on the cloud will allow traffic from only a vRouter or Controller nodes to reach to the On-Prem cluster. So in case of deployment where the On-Prem open stack cluster need to be extended to the K8s cluster on the cloud, the k8s master must be defined in one of the vRouters on the cloud.
- CEM-5284 Cloud Compute/vrouter nodes will not be listed in the cluster-nodes/compute node page, all nodes/computes will be listed in the servers page
- CEM-5141 For deleting compute nodes, the UI workflow will not work. Instead, update the instances.yaml with "ENABLE_DESTROY: True" and "roles:" (leave it empty) and run the following playbooks.

```
ansible-playbook -i inventory/ -e orchestrator=openstack --tags nova playbooks/
install_openstack.yml
ansible-playbook -i inventory/ -e orchestrator=openstack playbooks/install_contrail.yml
```

For example:

```
global_configuration:
  ENABLE_DESTROY: True
  ...
  ...
instances:
  ...
  ...
  srvr5:
    provider: bms
    ip: 19x.xxx.x.55
    roles:
  ...
  ...
```

- CEM-5290 While adding AWS cloud to an already existing public cloud with Azure, the AWS credentials need to be manually added in Contrail-Command container. Perform the following steps to add AWS credentials manually.

1. Log in to the `contrail_command` container.

```
docker exec -it contrail_command bash
export CONTRAIL_CONFIG=/etc/contrail/contrail.yml
```

2. Get the public cloud UUID.

```
contrailcli list cloud
```

3. Use the following command to get the `cloud_user_refs` for the `<public_cloud_uuid>` public cloud UUID.

```
contrailcli show cloud <public_cloud_uuid> | grep -A 4 cloud_user_refs
cloud_user_refs:

  uuid: <cloud_user_ref>
  to:
  sol4-public-cloud-user-<cloud_user_ref>
  href: ""
```

4. Replace the UUID in the `cloud_user.yaml` with the `<cloud_user_ref>` UUID of your cluster.

```
cat <<EOF > cloud_user.yaml
resources:

  data:
    uuid: "<cloud_user_ref>"
    aws_credential:
      access_key: XXXXXXXX
      secret_key: YYYYYYYYYYYYYY
    kind: cloud_user
    operation: UPDATE
  EOF
```

5. Use the following command to sync the `cloud_user.yaml` file.

```
contrailcli sync cloud_user.yaml
```

6. Verify that the credentials are updated.

```
contrailcli show cloud_user <cloud_user_ref>
```



NOTE: The instance name or the hostname must be in lowercase so that it is consistent across all components.

- CEM-5282 When Azure cloud is extended to On-Prem cluster running on RHEL hosts, contrail-status shows vRouters running on Azure as initializing, though the services are up. This is due to the Red Hat issue <https://access.redhat.com/solutions/2766251>.
- CEM-5043 VNI update on a LR doesn't update the RouteTable. As a workaround, delete the LogicalRouter and create a new LogicalRouter with the new VNI.
- CEM-5042 Adding new subnet on an already provisioned VPC is not supported. If all the subnets are added during initial bringup of VPC, nodes can be added incrementally to the subnets anytime.
- CEM-5041 Provisioning of Region or VPC objects only on the cloud without any nodes is not supported. Add at least one node while provisioning Region/VPC.
- CEM-5024 Current multi cloud provisioning does not enable the On-prem TOR to exchange public cloud subnets with the On-Prem controllers. The user needs to add static routes on the controllers to all the public cloud subnets.
- CEM-4943 After deleting and reprovisioning public cloud infra, though the nodes get deleted from the cloud, the API server and Kubernetes will have stale entries for the deleted objects. To clean up the stale entries, run the following housekeeping scripts:
 1. Log in to the command container.
 2. Navigate to the **contrail-multi-cloud** folder.

```
cd /usr/share/contrail/contrail-multi-cloud/
```

3. Run the following script.

```
TF_STATE=/root/contrail-multi-cloud/terraform.tfstate INVENTORY=inventories/inventory.yml  
TOPOLOGY=/root/contrail-multi-cloud/topology.yml ./housekeeper.sh
```



NOTE: If you run the script after provisioning, ensure that TF_STATE is the backup file. For example:

```
TF_STATE=/root/contrail-multi-cloud/terraform.tfstate.backup
INVENTORY=inventories/inventory.yml TOPOLOGY=/root/contrail-multi-cloud/
topology.yml ./housekeeper.sh
```

- CEM-4941 The multicloud gateway on the public cloud cannot be shared across different subnets. Each subnet must have its own gateway.
- CEM-4865 Provisioning of Contrail Controllers on public cloud is not supported. Controllers need to be provisioned On-prem.
- CEM-4467 On DPDK computes, sometimes VM creation fails with "Connection is closed" error. The issue is not related to any of the contrail components. It is related to systemd-machined service in registering VMs. As a workaround, restart the systemd-machined service to fix the issue.
- CEM-4381 Contrail Fabric device manager tasks can fail if one or more Contrail API servers is down. Contrail-status on the Contrail config nodes can be used to determine if this situation occur.
- CEM-4370 After creating a PNF Service Instance, the fields like PNF eBGP ASN*, RP IP Address, PNF Left BGP Peer ASN*, Left Service VLAN*, PNF Right BGP Peer ASN*, Right Service VLAN* cannot be modified. If there is a need to modify these values, delete and re-create the Service Instance with intended values.
- CEM-4190 IPtables rules are not updated on MC-GW nodes. As a workaround, you must configure IPtables on the on-premise MC-GW nodes with INPUT and FORWARD and default ACCEPT policy.
- CEM-3959 BMS movement across TORs is not supported. To move BMS across TORs the whole VPG need to be moved. That means if there are more than one BMS associated to one VPG, and one of the BMS need to be moved, the whole VPG need to be deleted and re-configured as per the new association.
- CEM-3913 From release 1908, the Contrail services run as root user. However agent, dpdk and nodemgr services will still run as root as those services need root access to the system.
- CEM-3324 Users cannot provision Contrail Cluster entirely in Public cloud. Contrail Cluster need to be On-Prem and vRouters can be extended to public cloud.
- JCB-204796 In a Helm-based provisioned cluster, VM launch fails if MariaDB replication is set to >1.
- JCB-202874 After deleting a vRouter chart with DPDK, the NICS do not rebind to the host in Helm.
- JCB-190956 While creating ironic-provision, service address in the subnet must be pointing to openstack ironic node ip/kolla internal vip.

- JCB-187320 On a DPDK compute vif list -rate core-dumps with traffic.
- JCB-187287 High Availability provisioning of Kubernetes master is not supported.
- JCB-186493 When a snapshot of an active VM fails, shutdown the VM before generating the snapshot.
- JCB-184837 After provisioning Contrail by using a Helm-based provisioned cluster, restart nova-compute container.
- JCB-184776 When the vRouter receives the head fragment of an ICMPv6 packet, the head fragment is immediately enqueued to the assembler. The flow is created as hold flow and then trapped to the agent. If fragments corresponding to this head fragment are already in the assembler or if new fragments arrive immediately after the head fragment, the assembler releases them to flow module. Fragments get enqueued in the hold queue if agent does not write flow action by the time the assembler releases fragments to the flow module. A maximum of three fragments are enqueued in the hold queue at a time. The remaining fragments are dropped from the assembler to the flow module.

As a workaround, the head fragment is enqueued to assembler only after flow action is written by agent. If the flow is already present in non-hold state, it is immediately enqueued to assembler.

- JCB-177787 In DPDK vRouter use cases such as SNAT and LBaaS that require netns, jumbo MTU cannot be set. Maximum MTU allowed: <=1500.
- JCB-177541 When you receive an error message during Kolla provisioning, rerunning the code will not work. In order for the provisioning to work, restart provisioning from scratch.
- JCB-171466 Metadata SSL works only in HA deployment mode.
- JCB-163773 A false alarm for config service is generated when config and configdb services are installed on different nodes. Ignore the false alarm.
- JCB-162927 SR-IOV with DPDK co-existence deployment is not supported using contrail-helm-deployer.