

Contrail Release 1907

Published
2025-08-18

RELEASE

Table of Contents

Introduction

New and Changed Features

Supported Platforms Contrail 1907

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 1907 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/contrail5.1/information-products /topic-collections/ release-notes/index.html.

New and Changed Features

IN THIS SECTION

- [Configure Assisted Replication on Datacenter Devices | 2](#)
- [Upgrade Devices During ZTP | 2](#)
- [Configure Hostnames for Datacenter Devices During ZTP | 2](#)
- [Support for Return Material Authorization | 3](#)
- [Topology View in Contrail Command | 3](#)
- [Upgrade Contrail Networking using Red Hat Fast Forward Upgrade Procedure | 3](#)

The features listed in this section are new or changed as of Contrail Release 1907. A brief description of each new feature is included.

Configure Assisted Replication on Datacenter Devices

Starting with Contrail Networking Release 1907, you can configure assisted replication and assign the roles AR-Replicator and AR-Client to the QFX10000 devices in a datacenter. An AR-Replicator is a network virtualization overlay (NVO) device or a provider edge (PE) device that can replicate ingress broadcast, unknown unicast, and multicast (BUM) traffic received through an overlay tunnel to other overlay tunnels and local attachment circuits. An AR-Client is a device that supports assisted replication and sends BUM traffic only to AR-Replicator.

Assisted replication feature optimizes the replication of BUM traffic received from the CE interfaces by replicating BUM traffic towards a single EVPN core Replicator PE (a QFX10000 device) rather than sending BUM traffic to all PE devices for replication. This reduces the load on the PEs and improves bandwidth utilization in the network.

You can configure the AR-Client role to MX Series, QFX10000 and QFX5000 devices as spine or leaf and the AR-Replicator role to QFX10000 devices as spine or leaf.



NOTE: To configure AR-Client and AR-Replicator roles, the MX Series, QFX10000, and QFX5000 devices must be running Junos OS Release 18.4 R2 or later.

For more information, see [Assisted Replication of Broadcast, Unknown Unicast, and Multicast Traffic](#).

Upgrade Devices During ZTP

Starting with Contrail Release 1907, you can upgrade devices during the zero touch provisioning (ZTP) process. Before you start with the ZTP process, ensure that you have already uploaded the necessary images files.

For more information, see [Providing Intent Driven Automation Capabilities on Physical Network Elements](#).

Configure Hostnames for Datacenter Devices During ZTP

Starting with Contrail Release 1907, you can configure hostnames for all devices during Greenfield onboarding of devices in a Contrail datacenter. The hostnames are specified in the YAML file that lists the devices for zero touch provisioning (ZTP). When configured, the hostname is assigned to the physical router object in the database and the device is displayed with the configured hostname in the

Contrail Command UI. If the hostname attribute is not specified, the device serial number is used as the hostname, by default. Prior to release 1907, the device serial number was used as the hostname.

For more information, see [Provisioning Fabric Devices Using End-to-End ZTP](#).

Support for Return Material Authorization

Starting with Contrail Release 1907, Contrail Networking supports Return Material Authorization (RMA). You can create an RMA for a device after a Juniper Technical Assistance Center (JTAC) engineer has confirmed that the device is defective and has to be replaced or repaired. After you move a device to RMA state, the device cannot be configured and can be removed from the network. You can then replace the device that is in RMA state with a new device.

For more information, see [Return Material Authorization](#).

Topology View in Contrail Command

Contrail Command UI provides visual representation of the network topology. All devices within a fabric are displayed in a single view. The Topology view supports basic manipulations such as dragging nodes, zooming in and out, fitting to view, in addition to having different layout visualizations.

For more information, see [Viewing the Network Topology](#).

Upgrade Contrail Networking using Red Hat Fast Forward Upgrade Procedure

Starting with Contrail Release 1907, you can use a combined procedure to upgrade Red Hat OpenStack Platform (RHOSP) from RHOSP 10 to RHOSP 13 by leveraging Red Hat Fast Forward Upgrade (FFU) procedure while simultaneously upgrading Contrail Networking from Release 4.1.x to Release 1907. The procedure leverages the In-Service Software Upgrade (ISSU) procedure from Contrail Networking to minimize the downtime.

For more information, see [Upgrading Contrail Networking Release 3.x or 4.x with RHOSP10 to Contrail Networking Release 1907 with RHOSP13](#).

Supported Platforms Contrail 1907

Table 1 on page 4 lists the orchestrator releases and the corresponding operating systems and kernel versions supported by Contrail Release 1907.

Table 1: Supported Platforms

Contrail Release	Orchestrator Release	Deployment Tool	Operating System, Kernel, and Key Components Version
Contrail Release 1907	Kubernetes 1.12	Ansible	<ul style="list-style-type: none"> CentOS 7.6—Linux Kernel Version 3.10.0-957.21.3 Docker version: 18.06.0-ce
	OpenShift 3.11	Ansible	<ul style="list-style-type: none"> RHEL7.6—Linux Kernel Version 3.10.0-957.21.3
	OpenStack Rocky	Ansible	<ul style="list-style-type: none"> CentOS 7.6—Linux Kernel Version 3.10.0-957.21.3 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
	OpenStack Queens	Ansible	<ul style="list-style-type: none"> CentOS 7.6—Linux Kernel Version 3.10.0-957.21.3 Ansible version: 2.5.2 Docker version: 18.03.1-ce

Table 1: Supported Platforms *(Continued)*

Contrail Release	Orchestrator Release	Deployment Tool	Operating System, Kernel, and Key Components Version
		Juju Charms	<ul style="list-style-type: none"> Ubuntu 18.04.2—Linux Kernel Version 4.15.0-48-generic MaaS Version: 2.4.2
		Helm	<ul style="list-style-type: none"> Ubuntu 16.04.3—Linux Kernel Version 4.4.0-112-generic Docker version: 17.03.2-ce Helm version: 2.7.2 Kubernetes version: 1.9.3
	Red Hat OpenStack Platform 13	RHOSP 13 director	<ul style="list-style-type: none"> RHEL7.6—Linux Kernel Version 3.10.0-957.21.3
	VMware vCenter 6.7	Ansible	<ul style="list-style-type: none"> ESX version 6.5 CentOS VM version running vRouter: CentOS 7.5—Linux Kernel Version 3.10.0-862.9.1

[Table 2 on page 5](#) lists the AppFormix release to use with Contrail Release 1907.

Table 2: AppFormix Release

Contrail Release	AppFormix Release
Contrail Release 1907	2.9.11

Known Behavior

This section lists known limitations with this release.

- CEM-7054 In Contrail Fabric deployments, it was observed that in rare scenarios the node profile for devices cannot be accessed. If this happens, restarting the Config API container will recover from the issue.
- CEM-6379 Restarting Schema Transformer service can cause traffic disruption in BMS connected to Fabric Leafs.
- 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-5402 Though the APIs allow 4 byte ASN, the backend code only support 2 byte ASN. Do not use 4 byte ASN in API integrations.
- 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-5287 Multicloud Provision may fail in add_tunnel routes, if the initial subcluster extension is rerun .If the initial subcluster extension fails user need to delete the subcluster and extend it again.
- 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-5283 For all-in-one cluster, where vrouter and openstack roles exist on the same node, "enable_haproxy" must not be enabled (set to 'yes') in the ansible yaml file. This is because of multicast traffic restrictions when vrouter is running.
- 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: YYYYYYYYYYYY
    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. Workaround is to 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 need 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-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-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.