

Contrail Release 4.1.5

Published
2023-11-02

RELEASE

Table of Contents

[Introduction](#)

[New and Changed Features](#)

[Supported Platforms Contrail 4.1](#)

[Known Behavior](#)

[Resolved Issues](#)

[Upgrade Procedure for RHOSP-based Contrail 4.1.4.1 to Contrail 4.1.5](#)

[Upgrade Procedure for RHOSP-based Contrail 4.1.3 or 4.1.4 to Contrail 4.1.4.1](#)

[Upgrade Procedure for Ubuntu-based Contrail 4.1.3 to Contrail 4.1.4 Using Juju with Netronome SmartNIC](#)

[Deploying Contrail Release 4.1 with Netronome SmartNICs by Using Juju](#)

[Upgrading Contrail 4.0 to 4.1](#)

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 4.1.5 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/contrail4.1/information-products/topic-collections/release-notes/index.html.

New and Changed Features

IN THIS SECTION

- [New and Changed Features in Contrail Release 4.1.5 | 2](#)
- [New and Changed Features in Contrail Release 4.1.4.1 | 2](#)
- [New and Changed Features in Contrail Release 4.1.4 | 2](#)
- [New and Changed Features in Contrail Release 4.1.3 | 2](#)
- [New and Changed Features in Contrail Release 4.1.2 | 2](#)
- [New and Changed Features in Contrail Release 4.1.1 | 3](#)
- [New and Changed Features in Contrail Release 4.1 | 3](#)

The features and enhancements listed in this section are new or changed as of Contrail Release 4.1. A brief description of each new feature is included.

New and Changed Features in Contrail Release 4.1.5

There are no new features in Contrail Release 4.1.5.

New and Changed Features in Contrail Release 4.1.4.1

There are no new features in Contrail Release 4.1.4.1.

New and Changed Features in Contrail Release 4.1.4

There are no new features in Contrail Release 4.1.4.

New and Changed Features in Contrail Release 4.1.3

There are no new features in Contrail Release 4.1.3.

New and Changed Features in Contrail Release 4.1.2

The feature listed in this section is new as of Contrail Release 4.1.2.

Support for SmartNIC from Netronome

Contrail Release 4.1.2 supports Netronome SmartNIC. You can use Juju to deploy Contrail Release 4.1.2 and later with Netronome SmartNICs. The Netronome SmartNIC improves Contrail SDN performance, by saving host resources and providing a stable, high-performance infrastructure.

The Netronome SmartNIC has all server-side networking features, such as overlay networking based on MPLS over UDP/GRE and VXLAN. It supports DPDK, SR-IOV, and Express Virtio (XVIO) for data plane acceleration.

New and Changed Features in Contrail Release 4.1.1

The feature listed in this section is new as of Contrail Release 4.1.1.

Support for Flat Provider Network on SR-IOV Virtual Functions

Contrail Release 4.1.1 supports configuration of VLAN ID 0 on single-root I/O virtualization (SR-IOV) virtual functions to allow multiple VLAN traffic to a virtual machine (VM) running over a single SR-IOV interface.

Support for SR-IOV, DPDK and vRouter on RHEL

Contrail Release 4.1.1 supports SR-IOV, Data Plane Developer Kit (DPDK) and the Contrail vRouter kernel module on Red Hat Enterprise Linux (RHEL) operating systems.

New and Changed Features in Contrail Release 4.1

The features listed in this section are new as of Contrail Release 4.1.

Using Huge Pages to Facilitate vRouter Hash Table Handling

To facilitate vRouter handling of flow and bridge tables at bootup, Contrail Release 4.1 requires the user to enable huge pages (1G in Linux), so that sufficient contiguous memory is available to the vrouter module. Huge page allocation and usage for the vrouter is in the kernel space. Enable huge pages at installation to use this feature.

Simple Underlay Connectivity without Gateway

For simple enterprise use cases and public cloud environments, it is possible to directly route packets using the IP fabric network without using an SDN gateway.

The following features can be enabled when using this method:

- Network policy support for IP fabric
- Security groups for VMs and containers on IP fabric
- Security groups for vhost0 interface, to protect compute node or bare metal server applications
- Support for service chaining, if policy dictates that traffic goes through a service chain.

See [Simple Underlay Connectivity without Gateway](#).

Contrail Support for SR-IOV on RHEL

Starting in Release 4.1, Contrail supports single root I/O virtualization (SR-IOV) on Red Hat Enterprise Linux (RHEL) operating systems. Contrail Release 3.0 through Release 4.0 supported SR-IOV on Ubuntu systems only.

For more information, see [Configuring Single Root I/O Virtualization \(SR-IOV\)](#).

Bidirectional Forwarding and Detection Health Check over Virtual Machine Interfaces

Contrail Release 4.1 supports BFD-based health check for VMIs.

Health check for VMIs is already supported in earlier releases as poll-based checks with ping and curl commands. When enabled, these health checks run periodically, once every few seconds. Consequently, failure detection times can be quite large and are always in seconds.

Health checks based on the BFD protocol can provide failure detection and recovery in sub-second intervals, because applications are notified immediately upon BFD session state changes.

See [Service Instance Health Checks](#).

Bidirectional Forwarding and Detection Health Check for BGPaaS

Contrail Release 4.1 adds support for BFD-based health check for BGP as a Service (BGPaaS) sessions.

The BFD-based health check over VMIs, also introduced in Contrail Release 4.1, cannot be directly used for a BGPaaS session, because the session shares a tenant destination address over a set of VMIs, with only one VMI active at any given time.

When configured, any time a BFD-for-BGP session is detected as down by the health checker, corresponding logs and alarms are generated.

To enable this health check, configure the `ServiceHealthCheckType` property and associate it with a `bgp-as-a-service` configuration object. This can also be accomplished in the Contrail WebUI.

See [Service Instance Health Checks](#).

Health Check of Transparent Service Chain

Contrail Release 4.1 enhances service chain redundancy by implementing an end-to-end health check for the transparent service chain. The service health check monitors the status of the service chain and if there is a failure, the control node no longer considers the service chain as a valid next hop, triggering traffic failover.

A segment-based health check is used to verify the health of a single instance in a transparent service chain. The user creates a service-health-check object, with type `segment-based`, and attaches it to either the left or right interface of the service instance. The service health-check packet is injected to the interface to which it is attached. When the packet comes out of the other interface, a reply packet is injected on that interface. If health check requests fail after 30-second retries, the service instance is considered unhealthy and the service VLAN routes of the left and right interfaces are removed. When the agent receives health-check replies successfully, it adds the retracted routes back on both interfaces, which triggers the control node to start reoriginating routes to other service instances on that service chain.

See [Service Instance Health Checks](#).

More Efficient Flow Queries

Flow queries are now analyzed on a 7-tuple basis, enabling more efficient flow queries by focusing on elements more important for analysis, and de-emphasizing lesser elements. More efficient queries enable load reduction and allow application of security policy.

An enhanced security framework is implemented to manage connectivity between workloads, or VMIs. Each VMI is tagged with the attributes of Deployment, App, Tier, and Site, and the user specifies security policies for VMIs using the values of these tags.

The existing `FlowLogData` is replaced by `SessionEndpointData`, and a `SessionAggregate` map provides statistics about the flow sessions and the security tags. Session data can belong to either `Sampled` or `Logged` Flows. `SessionAggregates` are sent to configurable destinations, including collector, local log, and syslog.

RBAC for Analytics API and WebUI—Beta

Role-based access control (RBAC) for analytics API provides the ability to access UVE and query information based on the permissions of the user for the UVE or queried object. Previously, the analytics API supported authenticated access only for the cloud-admin role. However, to display network monitoring for tenant pages in the UI, the analytics API now supports RBAC (similar to that of the config API) so that tenants can view information about the networks for which they have the read permissions. Tenants will not be able to view system logs and flow logs, which are only viewable by the cloud-admin role. A non-admin user will be able to see only non-global UVEs.

In the `/etc/contrail/contrail-analytics-api.conf`, the section `DEFAULTS`, the parameter `aaa_mode` now supports `rbac` as one of the values.

See [Role-Based Access Control for Analytics](#).

Security Policy Enhancements

As the Contrail environment has grown and become more complex, it has become harder to achieve desired security results with the existing network policy and security group constructs. The Contrail network policies have been tied to routing, making it difficult to express security policies for environments such as cross sectioning between categories, or having a multi-tier application supporting development and production environment workloads with no cross environment traffic.

Contrail 4.1 introduces new firewall security policy objects, including the following enhancements:

- Routing and policy decoupling—introducing new firewall policy objects, which decouples policy from routing.
- Multi dimension segmentation—segment traffic and add security features, based on multiple dimensions of entities, such as Application, Tier, Deployment, Site, UserGroup.
- Policy portability—security policies can be ported to different environments, such as ‘from development to production’, ‘from pci-complaint to production’, ‘to bare metal environment’ and ‘to container environment’.

See [Security Policy Enhancements](#).

Allocation of Service Instance IP

In service chaining version 2, for scaling up, the `contrail-svc-monitor` allocates a service instance IP address from the same subnet currently in use. If the scaling is not required, the IP is wasted, from a limited pool of IPs.

Starting with Contrail 4.1, any new service instance allocates IPs from a different subnet, by using a fixed value for ther IP, allocated from 0.0.0.0/8 and ::ffff/104 for IPv4 and IPv6.

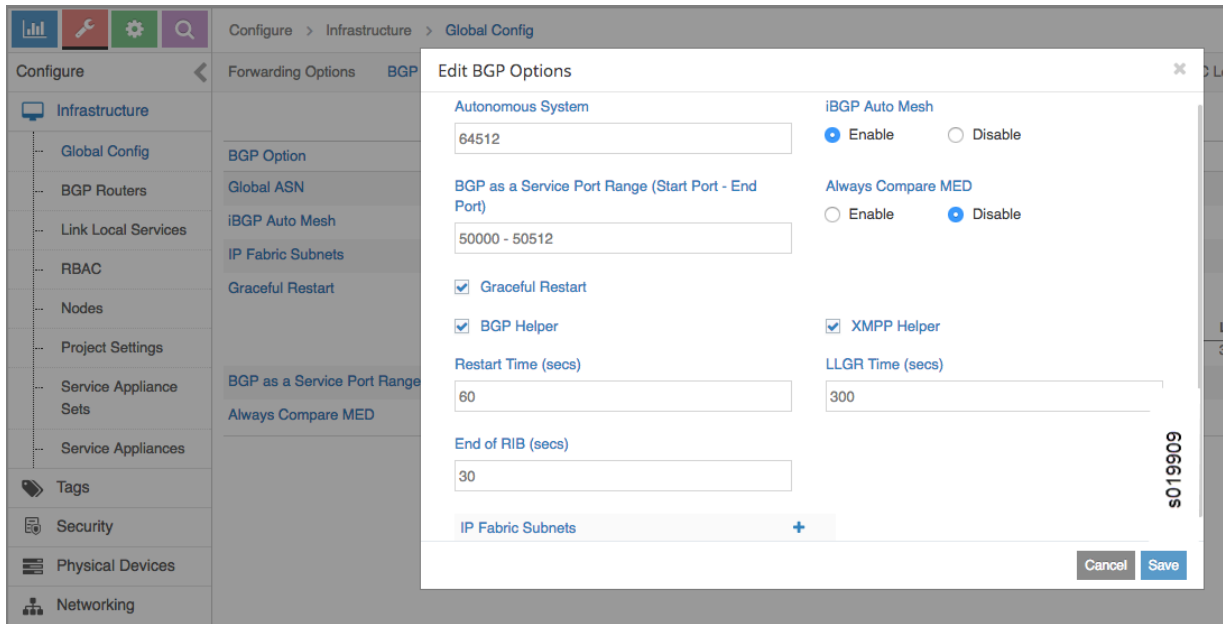
Existing service instances retain use of the previous method of allocating IPs; new instances make use of the new allocation method.

Long-Lived Graceful Restart for XMPP

Contrail Release 4.1 introduces support for long-lived graceful restart (LLGR) with XMPP helper mode. Previous versions of Contrail provided only the BGP helper mode. Graceful restart and long-lived graceful restart can be enabled using the Contrail web UI or by using the `provision_control` script.

In the web UI, you can control the helper modes at **Configure > Infrastructure Global Config > Edit BGP Options**, see [Figure 1 on page 7](#).

Figure 1: Edit BGP Options Page



The helper modes can also be enabled via schema, and can be disabled selectively in a Contrail control node for BGP or XMPP sessions by configuring `gr_helper_disable` in the `/etc/contrail/contrail-control.conf` configuration file.

For more information, see [Configuring Graceful Restart and Long-lived Graceful Restart](#).

Proxy Encryption of Interactions of vRouter and Nova API

OpenStack allows VMs to access metadata by sending an HTTP request to the link local address 169.254.169.254. The request is proxied to Nova API and HTTP header fields are added, which Nova uses to identify the source instance and respond with appropriate metadata. In Contrail, the vRouter is the proxy, trapping the metadata requests, adding the header fields, and sending the requests to the Nova API server. Previously, these requests were not encrypted, posing a security risk.

In Contrail 4.1, SSL is used to encrypt the HTTP interactions between the Contrail vRouter and Nova API.

To enable this encryption on the Nova side, add the following configuration in the default section of the `nova.conf` file.

```
enabled_ssl_apis = metadata
nova_metadata_protocol = https
nova_metadata_insecure = False
ssl_cert_file = cert.pem
```

```
ssl_key_file = privkey.pem
ssl_ca_file = cacert.pem
```

To enable this encryption on the Contrail vrouter agent, add the following configuration in the METADATA section of `contrail-vrouter-agent.conf`.

```
metadata_use_ssl = True
metadata_client_cert = client_cert.pem
metadata_client_key = client_key.pem
metadata_ca_cert = cacert.pem
```

Contrail provisioning is updated to populate the configuration files and to copy the certificate files to the appropriate paths.

Contrail EVPN-VXLAN Support Using QFX Series Switches

Contrail Release 4.1 enables you to use Ethernet VPN (EVPN) with Virtual Extensible LAN protocol (VXLAN) encapsulation when you have an environment that includes both virtual and bare metal devices. MX Series routers use EVPN-VXLAN encapsulation to provide both Layer 2 and Layer 3 connectivity for end stations within a Contrail virtual network (VN).

Two types of encapsulation methods are used in virtual networks:

- MPLS-over-GRE (generic routing encapsulation) is used for Layer 3 overlay virtual network routing between Contrail and MX Series routers.
- EVPN-VXLAN is used for Layer 2 overlay virtual network connectivity between virtual machines on Contrail, bare-metal servers attached to QFX Series switches, and their respective Layer 3 gateway configured on the QFX Series switch. Subsequently, inter-VXLAN routing between virtual machines and bare-metal servers, and between bare-metal servers on different VXLAN network identifiers (VNIs), is performed on the QFX Series switch.

For more information, see [EVPN-VXLAN Support for Bare Metal Devices and QFX Device Configuration](#).

Supported Platforms Contrail 4.1

[Table 1 on page 9](#) lists the operating system versions and the corresponding Linux or Ubuntu kernel versions supported by Contrail Release 4.1.

Table 1: Supported Platforms

Contrail Release	Orchestrator Release	Operating System and Kernel Versions
Contrail Release 4.1.5	OpenStack Newton	<ul style="list-style-type: none"> • RHEL7.5—Linux Kernel Version 3.10.0-862.14.4 (RHOSP 10.0) [Satellite content synced on Oct 29, 2018] • RHEL7.7—Linux Kernel Version 3.10.0-1062.12.1 (RHOSP 10.0.14) [Satellite content synced on May 20, 2020]
	OpenStack Ocata	<ul style="list-style-type: none"> • Ubuntu 16.04.6 - Linux Kernel Version 4.15.0-112-generic
Contrail Release 4.1.4.1	OpenStack Newton	<ul style="list-style-type: none"> • RHEL7.5—Linux Kernel Version 3.10.0-862.14.4 (RHOSP 10.0) • RHEL7.7—Linux Kernel Version 3.10.0-1062.9.1 (RHOSP 10.0.14)
Contrail Release 4.1.4	OpenStack Ocata	<ul style="list-style-type: none"> • Ubuntu 16.04.2—Linux kernel version 4.4.0-165-generic • VMware vCenter 6.0, 6.5—Ubuntu 16.04.2 kernel version 4.4.0-62-generic
	OpenStack Newton	<ul style="list-style-type: none"> • RHEL7.7—Linux Kernel Version 3.10.0-1062.1.2 (RHOSP 10.0.12) • Ubuntu 16.04.2—Linux kernel version 4.4.0-165-generic
	OpenStack Mitaka	<ul style="list-style-type: none"> • Ubuntu 14.04.5—Linux kernel versions 3.13.0-171-generic

Table 1: Supported Platforms *(Continued)*

Contrail Release	Orchestrator Release	Operating System and Kernel Versions
Contrail Release 4.1.3	OpenStack Ocata	<ul style="list-style-type: none"> • RHEL 7.5—Linux kernel version 3.10.0-862.11.6 and Linux kernel version 3.10.0-957 (RHOSP11) • Ubuntu 16.04.2—Linux kernel version 4.4.0-116-generic • VMware vCenter 6.0, 6.5—Ubuntu 16.04.2 kernel version 4.4.0-62-generic
	OpenStack Newton	<ul style="list-style-type: none"> • RHEL 7.5—Linux kernel version 3.10.0-862.11.6 • RHEL 7.6—Linux kernel version 3.10.0-957 (RHOSP10) • Ubuntu 16.04.2—Linux kernel version 4.4.0-116-generic
	OpenStack Mitaka	<ul style="list-style-type: none"> • Ubuntu 14.04.5—Linux kernel versions 3.13.0-142-generic and 4.4.0-116-generic
Contrail Release 4.1.2	Kubernetes 1.7.5	<ul style="list-style-type: none"> • Ubuntu 16.04.2—Linux kernel version 4.4.0-116-generic
	OpenStack Ocata	<ul style="list-style-type: none"> • RHEL 7.5—Linux kernel version 3.10.0-862.11.6 and Linux kernel version 3.10.0-957 (RHOSP11) • Ubuntu 16.04.2—Linux kernel version 4.4.0-116-generic • VMware vCenter 6.0, 6.5—Ubuntu 16.04.2 kernel version 4.4.0-62-generic
	OpenStack Newton	<ul style="list-style-type: none"> • RHEL 7.5—Linux kernel version 3.10.0-862.11.6 • Ubuntu 16.04.2—Linux kernel version 4.4.0-116-generic

Table 1: Supported Platforms *(Continued)*

Contrail Release	Orchestrator Release	Operating System and Kernel Versions
	OpenStack Mitaka	<ul style="list-style-type: none"> • Ubuntu 14.04.5—Linux kernel versions 3.13.0-142-generic and 4.4.0-116-generic
Contrail Release 4.1.1	Kubernetes 1.7.5	<ul style="list-style-type: none"> • Ubuntu 16.04.2—Linux kernel version 4.4.0-116-generic
	OpenShift 3.6	<ul style="list-style-type: none"> • RHEL 7.5—Linux kernel version 3.10.0-862.3.2
	OpenStack Ocata	<ul style="list-style-type: none"> • RHEL 7.5—Linux kernel version 3.10.0-862.3.2 (RHOSP11) • Ubuntu 16.04.2—Linux kernel version 4.4.0-116-generic • VMware vCenter 6.0, 6.5—Ubuntu 16.04.2 kernel version 4.4.0-62-generic
	OpenStack Newton	<ul style="list-style-type: none"> • RHEL 7.5—Linux kernel version 3.10.0-862.3.2 (RHOSP10) • Ubuntu 16.04.2—Linux kernel version 4.4.0-116-generic
	OpenStack Mitaka	<ul style="list-style-type: none"> • Ubuntu 14.04.5—Linux kernel versions 3.13.0-142-generic and 4.4.0-116-generic
Contrail Release 4.1	Kubernetes 1.7.5	<ul style="list-style-type: none"> • Ubuntu 16.04.2—Linux kernel version 4.4.0-62-generic
	OpenShift 3.6	<ul style="list-style-type: none"> • RHEL 7.4—Linux kernel version 3.10.0-693

Table 1: Supported Platforms *(Continued)*

Contrail Release	Orchestrator Release	Operating System and Kernel Versions
	OpenStack Ocata	<ul style="list-style-type: none"> • RHEL 7.4—Linux kernel version 3.10.0-693 (RHOSP11) • Ubuntu 16.04.2—Linux kernel version 4.4.0-62-generic • VMware vCenter 6.0, 6.5—Ubuntu 16.04.2 kernel version 4.4.0-62-generic
	OpenStack Newton	<ul style="list-style-type: none"> • RHEL 7.4—Linux kernel version 3.10.0-693 (RHOSP10) • Ubuntu 16.04.2—Linux kernel version 4.4.0-62-generic
	OpenStack Mitaka	<ul style="list-style-type: none"> • Ubuntu 14.04.5—Linux kernel versions 3.13.0-110-generic and 4.4.0-34-generic

NOTE: In Contrail Release 4.0 and later, if the stock kernel version of your Ubuntu system is other than the required version, you can upgrade the kernel for all nodes in the cluster by using the following parameter in `cluster.json` for Server Manager or SM-Lite provisioning or `testbed.py`.

```
{
  "cluster" : [{
    "parameters" : {
      "provisioning" : {
        "contrail" : {
          "kernel_upgrade" : true
        }
      }
    }
  }]
}
```

Known Behavior

IN THIS SECTION

- [Known Behavior in Contrail Release 4.1.5 | 13](#)
- [Known Behavior in Contrail Release 4.1.4.1 | 15](#)
- [Known Behavior in Contrail Release 4.1.4 | 17](#)
- [Known Behavior in Contrail Release 4.1.3 | 19](#)
- [Known Behavior in Contrail Release 4.1.2 | 21](#)
- [Known Behavior in Contrail Release 4.1.1 | 23](#)
- [Known Behavior in Contrail Release 4.1 | 26](#)

This section lists known limitations with this release.

Known Behavior in Contrail Release 4.1.5

- CEM-16030 Contrail Installation on Red Hat environment has a dependency on net-snmp package version 48. The repository should provide the following files during the installation.

```
net-snmp-5.7.2-48.el7.x86_64.rpm
net-snmp-agent-libs-5.7.2-48.el7.x86_64.rpm
net-snmp-libs-5.7.2-48.el7.x86_64.rpm
net-snmp-python-5.7.2-48.el7.x86_64.rpm
net-snmp-utils-5.7.2-48.el7.x86_64.rpm
```

- CEM 10726 Reboot the compute nodes manually after a kernel upgrade.
- JCB-1681680 / JCB-161567 When the DPDK vRouter fragments packets before sending them on the wire, the reassembly of the fragments on the receiver might time out in some cases.
- 1694343 / JCB-177784 In DPDK vRouter use-cases (SNAT, LBaaS) that require netns to be launched, do not set Jumbo frames. Use MTU <= 1500 bytes.

- 1711256 Project isolation is not supported in nested mode. In nested mode, Namespaces-isolation results in a virtual-network creation and doesn't create a new project.
- 1716308/ JCB-184771 When the head fragment is received in the vRouter, the head fragment is enqueued to the assembler immediately upon arrival. 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. If agent does not write flow action by the time the assembler releases fragments to the flow module, fragments get enqueued in the hold queue. As a maximum of only three fragments are enqueued in the hold queue, rest of the fragments from the assembler get dropped in the flow module. This leads to the whole packet being dropped on the receive side leading to the first packet loss.
- 1718807 / JCB-186624 In OVSDB case, the routes are exported from the ToR Agent where the SG is appropriately updated so that inter-virtual network traffic doesn't require any explicit SG to be configured for it to pass. When TOR is peering with control node, this SG has to be explicitly configured and this behavior is expected.
- 1720990 / JCB-195914 With policy-based mirroring with ECMP destinations, one of the destination vRouter drops packet with invalid NH.
- 1724357 / JCB-215307 While provisioning a RHOSP10 cluster with DPDK nodes, the DPDK node power state goes offline during introspection stage. As a workaround, delete the DPDK nodes from Ironic configuration and add them with the right configuration.

1. `ironic node-delete node-name`

2. Create a JSON file configuration as shown in the following example for all DPDK nodes:

```
{
  "nodes": [
    {
      "mac": [
        "90:e2:ba:4c:67:3d"
      ],
      "name": "compute3-dpdk",
      "capabilities": "profile:compute-dpdk",
      "pm_user": "admin",
      "pm_addr": "10.87.122.164",
      "pm_password": "admin",
      "pm_type": "pxe_ipmitool"
    }
  ]
}
```



```
]
}
```

3. `openstack baremetal import --json path to .json`
 4. `openstack baremetal introspection bulk start`
- 1728802 / JCB-166617 Session logging: Incorrect VN information seen for sessions on transparent SI VMs. As a workaround, ensure that VLAN NH inherits the policy status from its associated interface.
 - 1796812 In Netronome based Smart NIC deployments, launching a VM directly using net-ids is not supported. Port-ids need to be used instead.

Known Behavior in Contrail Release 4.1.4.1

- CEM-13620 While deploying RHOSP 10, under rare scenarios, contrail-named service will stay down. As a one-time workaround, restart the service using `service contrail-named restart` command from the command prompt.
- CEM 10126 When three analytics db nodes are configured, the Cassandra service on one of the analytics db nodes is down after provisioning. This was observed rarely during testing. The cassandra service on the other two analytics db nodes are functional and active. As a workaround, restart the 'contrail-database' service.
- CEM 10158 On a Red Hat 7.7 OSP10 scale cluster, Keystone is not issuing tokens, causing OpenStack commands to fail. This is attributed to the following Red Hat KBs and it is recommended to deploy the cluster as per the following documentation from Red Hat.
 - <https://access.redhat.com/solutions/2262771>
 - <https://access.redhat.com/solutions/3451691>
- CEM 10311 After provisioning, sometimes the kafka server does not come up due to `ZooKeeperClientTimeoutException`. This happens if kafka tries to connect to zookeeper before it is up. As a workaround, restart kafka once zookeeper is up.
- CEM 10726 Reboot the compute nodes manually after a kernel upgrade.
- JCB-1681680 / JCB-161567 When the DPDK vRouter fragments packets before sending them on the wire, the reassembly of the fragments on the receiver might time out in some cases.
- 1694343 / JCB-177784 In DPDK vRouter use-cases (SNAT, LBaaS) that require netns to be launched, do not set Jumbo frames. Use MTU <= 1500 bytes.

- 1711256 Project isolation is not supported in nested mode. In nested mode, Namespaces-isolation results in a virtual-network creation and doesn't create a new project.
- 1716308/ JCB-184771 When the head fragment is received in the vRouter, the head fragment is enqueued to the assembler immediately upon arrival. 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. If agent does not write flow action by the time the assembler releases fragments to the flow module, fragments get enqueued in the hold queue. As a maximum of only three fragments are enqueued in the hold queue, rest of the fragments from the assembler get dropped in the flow module. This leads to the whole packet being dropped on the receive side leading to the first packet loss.
- 1718807 / JCB-186624 In OVSD case, the routes are exported from the ToR Agent where the SG is appropriately updated so that inter-virtual network traffic doesn't require any explicit SG to be configured for it to pass. When TOR is peering with control node, this SG has to be explicitly configured and this behavior is expected.
- 1720990 / JCB-195914 With policy-based mirroring with ECMP destinations, one of the destination vRouter drops packet with invalid NH.
- 1724357 / JCB-215307 While provisioning a RHOSP10 cluster with DPDK nodes, the DPDK node power state goes offline during introspection stage. As a workaround, delete the DPDK nodes from Ironic configuration and add them with the right configuration.

1. `ironic node-delete node-name`

2. Create a JSON file configuration as shown in the following example for all DPDK nodes:

```
{
  "nodes": [
    {
      "mac": [
        "90:e2:ba:4c:67:3d"
      ],
      "name": "compute3-dpdk",
      "capabilities": "profile:compute-dpdk",
      "pm_user": "admin",
      "pm_addr": "10.87.122.164",
      "pm_password": "admin",
      "pm_type": "pxe_ipmitool"
    }
  ]
}
```

```
]
}
```

3. `openstack baremetal import --json path to .json`
 4. `openstack baremetal introspection bulk start`
- 1728802 / JCB-166617 Session logging: Incorrect VN information seen for sessions on transparent SI VMs. As a workaround, ensure that VLAN NH inherits the policy status from its associated interface.
 - 1796812 In Netronome based Smart NIC deployments, launching a VM directly using net-ids is not supported. Port-ids need to be used instead.

Known Behavior in Contrail Release 4.1.4

- CEM 10126 When three analytics db nodes are configured, the cassandra service on one of the analytics db nodes is down after provisioning. This was observed rarely during testing. The cassandra service on the other two analytics db nodes are functional and active. As a workaround, restart the 'contrail-database' service.
- CEM 10158 On a Red Hat 7.7 OSP10 scale cluster, Keystone is not issuing tokens, causing OpenStack commands to fail. This is attributed to the following Red Hat KBs and it is recommended to deploy the cluster as per the following documentation from Red Hat.
 - <https://access.redhat.com/solutions/2262771>
 - <https://access.redhat.com/solutions/3451691>
- CEM 10311 After provisioning, sometimes the kafka server does not come up due to ZooKeeperClientTimeoutException. This happens if kafka tries to connect to zookeeper before it is up. As a workaround, restart kafka once zookeeper is up.
- CEM 10726 Reboot the compute nodes manually after a kernel upgrade.
- JCB-1681680 / JCB-161567 When the DPDK vRouter fragments packets before sending them on the wire, the reassembly of the fragments on the receiver might time out in some cases.
- 1694343 / JCB-177784 In DPDK vRouter use-cases (SNAT, LBaaS) that require netns to be launched, do not set Jumbo frames. Use MTU <= 1500 bytes.
- 1711256 Project isolation is not supported in nested mode. In nested mode, Namespaces-isolation results in a virtual-network creation and doesn't create a new project.

- 1716308/ JCB-184771 When the head fragment is received in the vRouter, the head fragment is enqueued to the assembler immediately upon arrival. 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. If agent does not write flow action by the time the assembler releases fragments to the flow module, fragments get enqueued in the hold queue. As a maximum of only three fragments are enqueued in the hold queue, rest of the fragments from the assembler get dropped in the flow module. This leads to the whole packet being dropped on the receive side leading to the first packet loss.
- 1718807 / JCB-186624 In OVSDDB case, the routes are exported from the ToR Agent where the SG is appropriately updated so that inter-virtual network traffic doesn't require any explicit SG to be configured for it to pass. When TOR is peering with control node, this SG has to be explicitly configured and this behavior is expected.
- 1720990 / JCB-195914 With policy-based mirroring with ECMP destinations, one of the destination vRouter drops packet with invalid NH.
- 1724357 / JCB-215307 While provisioning a RHOSP10 cluster with DPDK nodes, the DPDK node power state goes offline during introspection stage. As a workaround, delete the DPDK nodes from Ironic configuration and add them with the right configuration.

1. `ironic node-delete node-name`

2. Create a JSON file configuration as shown in the following example for all DPDK nodes:

```
{
  "nodes": [
    {
      "mac": [
        "90:e2:ba:4c:67:3d"
      ],
      "name": "compute3-dpdk",
      "capabilities": "profile:compute-dpdk",
      "pm_user": "admin",
      "pm_addr": "10.87.122.164",
      "pm_password": "admin",
      "pm_type": "pxe_ipmitool"
    }
  ]
}
```

3. `openstack baremetal import --json path to .json`

4. openstack baremetal introspection bulk start

- 1728802 / JCB-166617 Session logging: Incorrect VN information seen for sessions on transparent SI VMIs. As a workaround, ensure that VLAN NH inherits the policy status from its associated interface.
- 1796812 In Netronome based Smart NIC deployments, launching a VM directly using net-ids is not supported. Port-ids need to be used instead.

Known Behavior in Contrail Release 4.1.3

- Redhat BZ 1684271: Installation of Contrail Release 4.1.3 release on Red Hat 7.6 does not work. Contrail Release 4.1.3 is tested on Red Hat 7.5.
- 1797358 In a Netronome based Smart NIC deployment, gateway less forwarding feature does not work with nfp_p1 interface. This works with nfp_p0 interface.
- 1796812 In Netronome based Smart NIC deployments, launching a VM directly using net-ids is not supported. Port-ids need to be used instead.
- 1681680 When the DPDK vRouter fragments packets before sending them on the wire, the reassembly of the fragments on the receiver might time out in some cases.
- 1694343 In DPDK vRouter use-cases (SNAT, LBaaS) that require `netns` to be launched, do not set Jumbo frames. Use `MTU <= 1500` bytes.
- 1705795 On an RHOSP10 provisioned cluster, if the vrouter-agent gets restarted, vhost0 interface does not come up. The `service supervisor-vrouter restart` command brings the service back online.
- 1709974 TSN support in RHOSP-based clusters are supported upto RHOSP10. As a workaround, deploy the stack with computes and DPDK first. Then change the `VrouterPhysicalInterface`, add the TSN nodes, and update the stack.
- 1711256 Project isolation is not supported in nested mode. In nested mode, Namespaces-isolation results in a virtual-network creation and doesn't create a new project.
- 1716308 When the head fragment is received in the vRouter, the head fragment is enqueued to the assembler immediately upon arrival. 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. If agent does not write flow action by the time the assembler releases fragments to the flow module, fragments get enqueued in the hold queue. As a maximum of only three fragments are enqueued in the hold queue, rest of the fragments from the assembler get dropped in the flow module. This leads to the whole packet being dropped on the receive side leading to the first packet loss.

- 1718807 In OVSDDB case, the routes are exported from the ToR Agent where the SG is appropriately updated so that inter-virtual network traffic doesn't require any explicit SG to be configured for it to pass. When TOR is peering with control node, this SG has to be explicitly configured and this behavior is expected.
- 1720990 With policy-based mirroring with ECMP destinations, one of the destination vRouter drops packet with invalid NH.
- 1721620 VNC API sends an update of all subfields in a field, like `virtual_network_properties` and not the updated subfields, like `allow_transit` of `vn_properties` alone, hence matching against all the subfields due to which you might not be able to update a subfield. As a workaround, perform the following steps:
 1. Delete the attributes which are not updated from the field class. For example, all the attributes of `virtual_network_properties` except `allow_transit`.
 2. Call `vn_obj.set_virtual_network_properties()`.
 3. Use RestApi or Contrail-UI instead of `vnc_api`.
- 1724357 While provisioning a RHOSP10 cluster with DPDK nodes, the DPDK node power state goes offline during introspection stage. As a workaround, delete the DPDK nodes from Ironic configuration and add them with the right configuration.
 1. `ironic node-delete node-name`
 2. Create a JSON file configuration as shown in the following example for all DPDK nodes:

```
{
  "nodes": [
    {
      "mac": [
        "90:e2:ba:4c:67:3d"
      ],
      "name": "compute3-dpdk",
      "capabilities": "profile:compute-dpdk",
      "pm_user": "admin",
      "pm_addr": "10.87.122.164",
      "pm_password": "admin",
      "pm_type": "pxe_ipmitool"
    }
  ]
}
```

3. `openstack baremetal import --json path to .json`

4. `openstack baremetal introspection bulk start`

- 1728802 Session logging: Incorrect VN information seen for sessions on transparent SI VMIs. As a workaround, ensure that VLAN NH inherits the policy status from its associated interface.
- 1729059 You must use Ansible version 2.3 to install Contrail using `contrail-ansible` for Kubernetes and OpenShift deployments.
- 1735057 When bringing up Contrail cluster on Red Hat container, manually install `docker-py` on all the target nodes.
- To install Pip, use the following command:

```
wget https://bootstrap.pypa.io/get-pip.py
python get-pip.py
```

- To install `docker-py`, use the following command:

```
pip install docker-py
```

Known Behavior in Contrail Release 4.1.2

- 1794702 - vRouter crashes if network policy contains large number of Community Tags. Recommended number for 4.1.2 code is less than 50.
- 1797358 - In a Netronome based Smart NIC deployment, gateway less forwarding feature does not work with `nfp_p1` interface. This works with `nfp_p0` interface.
- 1796812 - In Netronome based Smart NIC deployments, Launching a VM directly using `net-ids` is not supported. `Port-ids` need to be used instead.
- 1681680 When the DPDK vRouter fragments packets before sending them on the wire, the reassembly of the fragments on the receiver might time out in some cases.
- 1694343 In DPDK vRouter use-cases (SNAT, LBaaS) that require `netns` to be launched, do not set Jumbo frames. Use `MTU <= 1500` bytes.
- 1705795 On an RHOSP10 provisioned cluster, if the `vrouter-agent` gets restarted, `vhost0` interface does not come up. The service `supervisor-vrouter` restart command brings the service back online.

- 1709974 TSN support in RHOSP-based clusters are supported upto RHOSP10. As a workaround, deploy the stack with computes and DPDK first. Then change the `VrouterPhysicalInterface`, add the TSN nodes, and update the stack.
- 1711256 Project isolation is not supported in nested mode. In nested mode, Namespaces-isolation results in a virtual-network creation and doesn't create a new project.
- 1716308 When the head fragment is received in the vRouter, the head fragment is enqueued to the assembler immediately upon arrival. 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. If agent does not write flow action by the time the assembler releases fragments to the flow module, fragments get enqueued in the hold queue. As a maximum of only three fragments are enqueued in the hold queue, rest of the fragments from the assembler get dropped in the flow module. This leads to the whole packet being dropped on the receive side leading to the first packet loss.
- 1718807 In OVSD case, the routes are exported from the ToR Agent where the SG is appropriately updated so that inter-virtual network traffic doesn't require any explicit SG to be configured for it to pass. When TOR is peering with control node, this SG has to be explicitly configured and this behavior is expected.
- 1720990 With policy-based mirroring with ECMP destinations, one of the destination vRouter drops packet with invalid NH.
- 1721620 VNC API sends an update of all subfields in a field, like `virtual_network_properties` and not the updated subfields, like `allow_transit` of `vn_properties` alone, hence matching against all the subfields due to which you might not be able to update a subfield. As a workaround, perform the following steps:
 1. Delete the attributes which are not updated from the field class. For example, all the attributes of `virtual_network_properties` except `allow_transit`.
 2. Call `vn_obj.set_virtual_network_properties()`.
 3. Use RestApi or Contrail-UI instead of `vnc_api`.
- 1724357 While provisioning a RHOSP10 cluster with DPDK nodes, the DPDK node power state goes offline during introspection stage. As a workaround, delete the DPDK nodes from Ironic configuration and add them with the right configuration.
 1. `ironic node-delete node-name`
 2. Create a JSON file configuration as shown in the following example for all DPDK nodes:

```
{
  "nodes": [
```



```
{
  "mac": [
    "90:e2:ba:4c:67:3d"
  ],
  "name": "compute3-dpdk",
  "capabilities": "profile:compute-dpdk",
  "pm_user": "admin",
  "pm_addr": "10.87.122.164",
  "pm_password": "admin",
  "pm_type": "pxe_ipmitool"
}
]
```

3. `openstack baremetal import --json path to .json`

4. `openstack baremetal introspection bulk start`

- 1728802 Session logging: Incorrect VN information seen for sessions on transparent SI VMIs. As a workaround, ensure that VLAN NH inherits the policy status from its associated interface.
- 1729059 You must use Ansible version 2.3 to install Contrail using `contrail-ansible` for Kubernetes and OpenShift deployments.
- 1735057 When bringing up Contrail cluster on Red Hat container, manually install `docker-py` on all the target nodes.
 - To install Pip, use the following command:

```
wget https://bootstrap.pypa.io/get-pip.py
python get-pip.py
```

- To install `docker-py`, use the following command:

```
pip install docker-py
```

Known Behavior in Contrail Release 4.1.1

- 1681680 When the DPDK vRouter fragments packets before sending them on the wire, the reassembly of the fragments on the receiver might time out in some cases.

- 1694343 In DPDK vRouter use-cases (SNAT, LBaaS) that require netns to be launched, do not set Jumbo frames. Use MTU <= 1500 bytes.
- 1705795 On an RHOSP10 provisioned cluster, if the vrouter-agent gets restarted, vhost0 interface does not come up. The service supervisor-vrouter restart command brings the service back online.
- 1709974 TSN support in RHOSP-based clusters are supported upto RHOSP10. As a workaround, deploy the stack with computes and DPDK first. Then change the VrouterPhysicalInterface, add the TSN nodes, and update the stack.
- 1711256 Project isolation is not supported in nested mode. In nested mode, Namespaces-isolation results in a virtual-network creation and doesn't create a new project.
- 1716297 Provisioning fails for OpenStack HA with SMLite on Ocata.
- 1716308 When the head fragment is received in the vRouter, the head fragment is enqueued to the assembler immediately upon arrival. 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. If agent does not write flow action by the time the assembler releases fragments to the flow module, fragments get enqueued in the hold queue. As a maximum of only three fragments are enqueued in the hold queue, rest of the fragments from the assembler get dropped in the flow module. This leads to the whole packet being dropped on the receive side leading to the first packet loss.
- 1718807 In OVSDDB case, the routes are exported from the ToR Agent where the SG is appropriately updated so that inter-virtual network traffic doesn't require any explicit SG to be configured for it to pass. When TOR is peering with control node, this SG has to be explicitly configured and this behavior is expected.
- 1720990 With policy-based mirroring with ECMP destinations, one of the destination vRouter drops packet with invalid NH.
- 1721564 Contrail Ocata: ansible_hostname does not handle "-" in hostname. As a workaround, copy the cert and key files with the expected name without the "-" in the same path as **/etc/contrail_smgr/puppet/ssl/**.
- 1721620 VNC API sends an update of all subfields in a field, like virtual_network_properties and not the updated subfields, like allow_transit of vn_properties alone, hence matching against all the subfields due to which you might not be able to update a subfield. As a workaround, perform the following steps:
 1. Delete the attributes which are not updated from the field class. For example, all the attributes of virtual_network_properties except allow_transit.
 2. Call vn_obj.set_virtual_network_properties().
 3. Use RestApi or Contrail-UI instead of vnc_api.

- 1724357 While provisioning a RHOSP10 cluster with DPDK nodes, the DPDK node power state goes offline during introspection stage. As a workaround, delete the DPDK nodes from Ironic configuration and add them with the right configuration.

1. `ironic node-delete node-name`

2. Create a JSON file configuration as shown in the following example for all DPDK nodes:

```
{
  "nodes": [
    {
      "mac": [
        "90:e2:ba:4c:67:3d"
      ],
      "name": "compute3-dpdk",
      "capabilities": "profile:compute-dpdk",
      "pm_user": "admin",
      "pm_addr": "10.87.122.164",
      "pm_password": "admin",
      "pm_type": "pxe_ipmitool"
    }
  ]
}
```

3. `openstack baremetal import --json path to .json`

4. `openstack baremetal introspection bulk start`

- 1728802 Session logging: Incorrect VN information seen for sessions on transparent SI VMIs. As a workaround, ensure that VLAN NH inherits the policy status from its associated interface.
- 1729059 You must use Ansible version 2.3 to install Contrail using `contrail-ansible` for Kubernetes and OpenShift deployments.
- 1735057 When bringing up Contrail cluster on Red Hat container, manually install `docker-py` on all the target nodes.
- To install Pip, use the following command:

```
wget https://bootstrap.pypa.io/get-pip.py
python get-pip.py
```

- To install docker-py, use the following command:

```
pip install docker-py
```

Known Behavior in Contrail Release 4.1

- 1735874 Kubernetes: Analytics services fail when 3 node HA setup is brought up using single yaml.
- 1681680 When the DPDK vRouter fragments packets before sending them on the wire, the reassembly of the fragments on the receiver might time out in some cases.
- 1694343 In DPDK vRouter use-cases (SNAT, LBaaS) that require `netns` to be launched, do not set Jumbo frames. Use `MTU <= 1500` bytes.
- 1705795 On an RHOSP10 provisioned cluster, if the `vrouter-agent` gets restarted, `vhost0` interface does not come up. The service `supervisor-vrouter restart` command brings the service back online.
- 1709974 TSN support in RHOSP-based clusters are supported upto RHOSP10. As a workaround, deploy the stack with computes and DPDK first. Then change the `VrouterPhysicalInterface`, add the TSN nodes, and update the stack.
- 1711256 Project isolation is not supported in nested mode. In nested mode, `Namespaces-isolation` results in a virtual-network creation and doesn't create a new project.
- 1716297 Provisioning fails for OpenStack HA with SMLite on Ocata.
- 1716308 When the head fragment is received in the vRouter, the head fragment is enqueued to the assembler immediately upon arrival. 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. If agent does not write flow action by the time the assembler releases fragments to the flow module, fragments get enqueued in the hold queue. As a maximum of only three fragments are enqueued in the hold queue, rest of the fragments from the assembler get dropped in the flow module. This leads to the whole packet being dropped on the receive side leading to the first packet loss.
- 1718807 In OVSD case, the routes are exported from the ToR Agent where the SG is appropriately updated so that inter-virtual network traffic doesn't require any explicit SG to be configured for it to pass. When TOR is peering with control node, this SG has to be explicitly configured and this behavior is expected.
- 1719430 While upgrading OpenShift cluster from build 31 to 32 in Redhat base OS, contrail kube-manager fails to come up for permission due to an issue with **contrail-kube-manager.log**. As a

workaround, change the permission of the log file inside **contrail-kube-manager** docker and restart the service.

- 1720118 Configuration of Allowed Address Pair (AAP) with prefix length less than 24 is not allowed.
- 1720990 With policy-based mirroring with ECMP destinations, one of the destination vRouter drops packet with invalid NH.
- 1721564 Contrail Ocata: ansible_hostname does not handle "-" in hostname. As a workaround, copy the cert and key files with the expected name without the "-" in the same path as **/etc/contrail_smgr/puppet/ssl/**.
- 1721620 VNC API sends an update of all subfields in a field, like virtual_network_properties and not the updated subfields, like allow_transit of vn_properties alone, hence matching against all the subfields due to which you might not be able to update a subfield. As a workaround, perform the following steps:
 1. Delete the attributes which are not updated from the field class. For example, all the attributes of virtual_network_properties except allow_transit.
 2. Call vn_obj.set_virtual_network_properties().
 3. Use RestApi or Contrail-UI instead of vnc_api.
- 1722877 There is no automated provisioning method through director for SRIOV.
- 1724357 While provisioning a RHOSP10 cluster with DPDK nodes, the DPDK node power state goes offline during introspection stage. As a workaround, delete the DPDK nodes from Ironic configuration and add them with the right configuration.
 1. ironic node-delete *node-name*
 2. Create a JSON file configuration as shown in the following example for all DPDK nodes:

```
{
  "nodes": [
    {
      "mac": [
        "90:e2:ba:4c:67:3d"
      ],
      "name": "compute3-dpdk",
      "capabilities": "profile:compute-dpdk",
      "pm_user": "admin",
      "pm_addr": "10.87.122.164",
      "pm_password": "admin",
      "pm_type": "pxe_ipmitool"
    }
  ]
}
```

```
    }
  ]
}
```

3. `openstack baremetal import --json path to .json`

4. `openstack baremetal introspection bulk start`

- 1728802 Session logging: Incorrect VN information seen for sessions on transparent SI VMIs. As a workaround, ensure that VLAN NH inherits the policy status from its associated interface.
- 1729059 You must use Ansible version 2.3 to install Contrail using `contrail-ansible` for Kubernetes and OpenShift deployments.
- 1733684 ContrailSecurity: Addressgroup match performs the OR function of both subnet and label rather than the AND function.
- 1734110 Provisioning SSL for metadata fetch does not work if the OpenStack SKU is Ocata.
- 1734790 In RBAC-enabled deployments, SM-Lite doesn't enable RBAC in `api-paste.ini` for Neutron. As a workaround, after provisioning the cluster, manually update `/etc/neutron/api-paste.ini` as described in [RBAC](#).
- 1735054 RBAC for analytics alarms doesn't work.
- 1735057 When bringing up Contrail cluster on Red Hat container, manually install `docker-py` on all the target nodes.
 - To install Pip, use the following command:

```
wget https://bootstrap.pypa.io/get-pip.py
python get-pip.py
```

- To install `docker-py`, use the following command:

```
pip install docker-py
```

- 1735081 While deploying using Contrail Networking package, the dependency for `liblua5.3-0` must be resolved explicitly by the user.
- 1735590 In Kubernetes and OpenShift-based deployments when we create SNAT router and extend cluster-network to that SNAT router host is losing all connectivity.

As a workaround, if you want to use the SNAT feature in Contrail, disassociate the ip-fabric-cluster-network-default policy and delete it.

- 1773294 In a RHOSP deployment incase of DPDK vRouter crash the vRouter does not restart itself. As a workaround, use the service supervisor-vrouter restart command.

Resolved Issues

IN THIS SECTION

- [Resolved Issues in Contrail Release 4.1.5 | 29](#)
- [Resolved Issues in Contrail Release 4.1.4.1 | 31](#)
- [Resolved Issues in Contrail Release 4.1.4 | 31](#)
- [Resolved Issues in Contrail Release 4.1.3 | 33](#)
- [Resolved Issues in Contrail Release 4.1.2 | 33](#)
- [Resolved Issues in Contrail Release 4.1.1 | 33](#)
- [Resolved Issues in Contrail Release 4.1 | 33](#)

This section lists limitations that are resolved with this release.

Resolved Issues in Contrail Release 4.1.5

- CEM-4956 Wrong format for route_table_refs in body JSON when adding two routes to the VN.
- CEM-6191 VM in paused state after stop/start as some interfaces are not created by qemu.
- CEM-6861 4.1.4 dpdk vrouter LACP bond member link failing after compute reboots.
- CEM-7202 VM-to-VM IPERF poor throughput observed after upgrading Contrail 4.1.2 to 4.1.3.
- CEM-7918 Online vRouter shown as down in the Contrail Web UI.
- CEM-9129 Spawning 10 VMs simultaneously in OpenStack using Rally leads to RefsExistError.
- CEM-9285 vRouter crashes and does not restart.

- CEM-9850 Contrail 4.1.2 Network disappeared from OpenStack after setting allowed address pair on vRouter ports.
- CEM-10284 vRouter's systemd file uses mount namespaces which leads to problems.
- CEM-10354 Contrail 4.1.4.0-52.el7: After Nova stop/start of vSRX, some BGPaaS session do not work, and vRouter agent memory keeps increasing.
- CEM-10897 Unable to reach the VM from the second DC gateway.
- CEM-10907 vrouter-agent crashes on 4.1.4 binaries and does not recover automatically.
- CEM-11051 Running VM gets one interface in VRF 65535.
- CEM-11131 VTEP destination MAC address is not taken into account when using port mirroring towards an external physical probe.
- CEM-11151 DPDK vRouter agent intermittently times out causing outage to VNFs
- CEM-11181 VM goes into paused state on start and stop.
- CEM-11421 Missing prefixes in vRouter forwarding table.
- CEM-11226 Health check stops working after VM reboot.
- CEM-12013 4.1.3 - Significance of "opscenter" user on Contrail nodes.
- CEM-12128 Contrail processes not coming up because 8082 port is not getting binded in controller processes.
- CEM-12782 vRouter agent and DPDK agent restart - segmentation fault on DPDK.
- CEM-12969 Contrail 4.1.4.0-52.el7 - After Nova stop/start of vSRX agent memory keeps increasing
- CEM-13568 Agent crash in FlowHandler::IsL3ModeFlow.
- CEM-14035 Leading white spaces in AAP address configuration causes VMI to not be visible from OpenStack side
- CEM-14072 VMs stuck in paused state when restarted after upgrade from release 4.1.3 to 4.1.4.1.
- CEM-14439 Errors in Contrail regarding WSGI server whenever we query any network resources like OpenStack network list.
- CEM-14572 contrail-api service in initializing status.
- CEM-15515 4.1.3: Contrail Web Interface is not showing fixed IP for ports belonging to one specific tenant.
- CEM-16029 Wrong vrouter.ko copied in OSP10 env when multi-kernels are packaged.

- CEM-16030 Red Hat updated the net-snmp package to version 48. We need to package version 48 for analytics services to work.
- CEM-16257 vRouter crash related to restart of VM on a remote compute.
- CEM-16355 RHOSP-7.5+R4.1.5 deployment failed at step-4 dpdk/kernel provisioning with a Libvirt puppet code error.
- CEM-17067 Upgrade of release 4.1.4.1 to 4.1.5 failed on compute node due to a hostname issue.
- CEM-17147 vRouter - Fragment table entries are not ageing out after 400 days.

Resolved Issues in Contrail Release 4.1.4.1

- CEM-10075 Issue when restarting a VM with 1800 BGPaaS sessions and 900 BFD sessions.
- CEM-11421 Missing prefixes in vRouter forwarding table.

Resolved Issues in Contrail Release 4.1.4

- JCB-181802 Adding security rules in parallel to security group results in some rules not being present in the security group.
- JCB-218976 When updating a security group in parallel to add/delete multiple rules, a lost update problem leads to undefined behavior.
- JCB-219237 object_read() with fields filter is not honored.
- CEM-11114 [DPDK] 4.1.2.0/RHOSP10 Tenant VMs stuck in Pause state after compute node reboots.
- CEM-10973 Upgrading from release 4.1.3 to 4.1.4 using Juju: After controller upgrade, contrail status is inactive (disabled on boot).
- CEM-10799 One of the VMs in paused state after start / stop of instances.
- CEM-10798 Agent crash in NextHop::GetType().
- CEM-10694 API takes longer to respond for query than previous releases. Heat test execution failing due to api timeout.
- CEM-10603 Post_virtual_network_delete_failed.

- CEM-10423 Upgrading from release 4.1.3 to 4.1.4: contrail-analytics-api in initializing state due to Redis-UVe:connection down.
- CEM-10075 Issue when restarting a VM with 1800 BGPaaS sessions and 900 BFD sessions.
- CEM-10039 Juju + Netronome : vRouter provisioning with kernel version 4.4.0-166 is failing.
- CEM-9968 RHOSP-4-1-4: DPDK compute vRouter agent stuck in initializing state.
- CEM-9950 RHOSP-4-1-4-OSP10-contrail-database is inactive after deployment.
- CEM-9923 vRouter keeps restarting because of segfault, causing Logical Router outages.
- CEM-9813 Enabling healthchecks for native LBaaS driver leads to vRouter crash.
- CEM-9676 RHOSP-deployment fails due to net-snmp package version, it needs 5.7.2-43 version package.
- CEM-9541 Production VM suddenly loses connectivity (Interface down Contrail + VM).
- CEM-9204 contrail-collector crashes in rare cases where vector move operation reads bad memory.
- CEM-9078 Extra DHCP Options does not work properly for dhcp-lease-time.
- CEM-8919 Misalignment between UIs and schema.
- CEM-8756 VNC API timeouts too long if API server is down.
- CEM-8595 Fabric configuration (including vxlan and vlan) was removed by Contrail.
- CEM-8450 HA availability failure with Analytics nodes (4.1.3).
- CEM-8439 OOO Remove strip for DPDK(contrail-router-dpdk) binary.
- CEM-8327 db_json_exim.py fails to export the DB.
- CEM-8228 The same internal RTs are assigned to different Routing Instances after upgrading from Contrail 4.1.2 to 4.1.3.
- CEM-7469 Spawning simultaneously 10 VMs in openstack using rally leads to RefsExistError.
- CEM-7384 OpenStack security group rule list returns rules from all groups.
- CEM-7232 failed to delete VN due to missing zk path.
- CEM-6205 DPDK vRouter, VMs stuck in paused state and VIF interfaces not being created.
- CEM-5800 VM stuck in powering state after a reboot after applying hotfix 4.1.4 (4.1.4.0-32.el7). Some tap interfaces are still created in client mode.

- CEM-5343 Memory leak issue with 5.0.1 and 4.1.3 kmod vRouter.
- CEM-5251 On DPDK nodes, prevent flood of duplicate packets, when disabling a link w/in a bonded pair
- CEM-4567 Issue in authentication context of all the Contrail Heat resources.
- CEM-4115 dpdk nodes are showing vrouter-agent in initializing state.
- CEM-3187 agent core at bgp peer deletion when control node is restarted.

Resolved Issues in Contrail Release 4.1.3

Contrail Release 4.1.3 addresses issues in BFD health check and stability issues in the vRouter.

Resolved Issues in Contrail Release 4.1.2

You can research limitations that are resolved with Contrail Release 4.1.2 in Launchpad at:

<https://launchpad.net/juniperopenstack/+milestone/r4.1.2.0> .

Resolved Issues in Contrail Release 4.1.1

You can research limitations that are resolved with Contrail Release 4.1.1 in Launchpad at:

<https://launchpad.net/juniperopenstack/+milestone/r4.1.1.0> .

Resolved Issues in Contrail Release 4.1

You can research limitations that are resolved with Contrail Release 4.1 in Launchpad at:

<https://launchpad.net/juniperopenstack/+milestone/r4.1.0.0-fcs> .

Upgrade Procedure for RHOSP-based Contrail

4.1.4.1 to Contrail 4.1.5

IN THIS SECTION

- Prerequisites | 34
- Post-Installation | 35
- Net-SNMP Package Requirements | 35
- Acquire the Software | 36
- Preparing the Environment | 36
- Upgrade the Contrail Heat Templates | 41
- Modify the Yum Update Script for TripleO Puppet | 42
- Update the Overcloud Deployment Plan | 43
- Upgrade the Overcloud | 44
- Upgrade Cautions | 45

This section presents the steps to upgrade a RHOSP-based Contrail deployment from Contrail version 4.1.4.1 to Contrail version 4.1.5.

Prerequisites

Ensure you have a cloud up and running with RHOSP10 and Contrail 4.1.4.1 before you proceed with the upgrade procedure. See the [Release Notes for Contrail Release 4.1](#) if you need instructions for other Contrail Networking 4.1 upgrade procedures.

This procedure has been validated with the following Contrail, Red Hat, and OpenStack versions.

Table 2: Pre-Installation Software Versions

Contrail Version	Red Hat Version	OpenStack Version
4.1.4.1	RHEL 7.5 (3.10.0-862.14.4.el7.x86_64)	RHOSP10 (packages dated October 29, 2018)
4.1.4.1	RHEL-7.7-kernel-3.10.0-1062.12.1.el7.x86_64	RHOSP10 (packages dated May 20,2020)

This procedure has been validated in environments where the RHEL version is unchanged during the procedure only. Do not upgrade or downgrade your RHEL version while performing this procedure.

Post-Installation

After the installation, you'll have a cloud networking running RHOSP10 and Contrail 4.1.5. The Red Hat Enterprise Linux (RHEL) kernel version will remain at 7.5 or 7.7—whichever version was running in your pre-installation environment—during this procedure.

[Table 3 on page 35](#) summarizes the validated post-installation software combinations.

Table 3: Post Installation Supported Software Combinations Summary

Contrail Version	Red Hat Version	OpenStack Version
4.1.5	RHEL-7.7-kernel-3.10.0-1062.12.1.el7.x86_64	RHOSP10 (packages dated May 20,2020)
4.1.5	RHEL 7.5 (3.10.0-862.14.4.el7.x86_64)	RHOSP10 (packages dated October 29, 2018)

Net-SNMP Package Requirements

Contrail version R4.1.5 supports net-snmp package version 5.7.2-48 to support SNMP in most environments.

The net-snmp are provided by Red Hat, with the exception of the *net-snmp-python-5.7.2-48.el7.x86_64.rpm* package which is provided in the Contrail repository.

Table 4 on page 36 summarizes the net-snmp depend packages and their associated repository locations.

Table 4: Net-SNMP Depend Packages (version 43)

Net-SNMP Depend Packages	Initial Repository
<i>net-snmp-5.7.2-48.el7.x86_64.rpm</i>	Red Hat Satellite
<i>net-snmp-agent-libs-5.7.2-48.el7.x86_64.rpm</i>	Red Hat Satellite
<i>net-snmp-libs-5.7.2-48.el7.x86_64.rpm</i>	Red Hat Satellite
<i>net-snmp-python-5.7.2-48.el7.x86_64.rpm</i>	Contrail
<i>net-snmp-utils-5.7.2-48.el7.x86_64.rpm</i>	Red Hat Satellite

If you need to replace the SNMP packages, run the `createrepo` command to create the repository and complete the update.

Acquire the Software

To download the software images for this procedure:

1. Go to the [Juniper Networks Support site for Contrail](#).
2. Select **OS** as *Contrail* and **Version** as *4.1.5*. Download the images that apply to your environment.

Preparing the Environment

1. Log in to the undercloud as the stack user.

```
$ su - stack
```

2. Update the Contrail repositories.

- Backup the Contrail 4.1.4.1 packages to a repository with a different name.

In this example, the Contrail 4.1.4.1 packages are moved to a repository named *contrail-R4-1-4-1*.

```
[stack@undercloud ~]$ cd /var/www/html/
[stack@undercloud html]$ sudo mv contrail/ contrail-R4-1-4-1
```

- Create a new repository directory to store the Contrail 4.1.5 packages:

```
[stack@undercloud html]$ sudo mkdir contrail
```

3. Copy the downloaded file—in the provided sample, the file is *contrail-install-packages_4.1.5.0-70-newton_redhat7*—to the Contrail repository created in Step 2.

NOTE: This step assumes that you've already downloaded the Contrail software. See ["Acquire the Software" on page 36](#).

```
[stack@undercloud contrail]$ ls -lrt
total 377104
-rw-r--r--. 1 root root 386151602 Aug 5 06:58 contrail-install-packages_4.1.5.0-70-
newton_redhat7
```

4. Untar the downloaded tgz file.

```
[stack@undercloud contrail]$ sudo tar -xvf contrail-install-packages_4.1.5.0-70-
newton_redhat7
```

5. Ensure your satellite has a supported net-snmp package setup. The net-snmp packages in the Contrail repository and the satellite repository must match. See ["Net-SNMP Package Requirements" on page 35](#).
6. Create a repository in the new directory:

```
[stack@undercloud contrail]$ pwd
/var/www/html/contrail
```

```
[stack@undercloud contrail]$ sudo createrepo .
```

If the **createrepo** command is not available, download the createrepo package from Red Hat (Red Hat subscription required).

7. (Clusters deployed using Swift Puppet files only) If your Contrail 4.1 cluster was deployed using Swift Puppet, perform these steps:

- a. Remove overcloud artifacts from the undercloud:

```
[stack@undercloud ~]$ swift delete overcloud-artifacts
puppet-modules.tgz
overcloud-artifacts
```

- b. Delete the *deployments-artifacts.yaml* file if the file is present.

```
[stack@undercloud ~]$ ls /home/stack/.tripleo/environments/deployment-artifacts.yaml
[stack@undercloud ~]$ rm -rf /home/stack/.tripleo/environments/deployment-artifacts.yaml
```

- c. Clean the repositories and confirm that all repositories are available.

```
[stack@undercloud ~]$ sudo yum clean all
[stack@undercloud ~]$ sudo yum repolist
```

NOTE: The undercloud is often updated at this point of the Contrail Networking upgrade procedure. The undercloud does not need to be updated for this procedure since the RHEL and RHOSP versions are unchanged.

8. Ensure the undercloud has the latest Contrail R4.1.5 contrail packages:

```
[stack@undercloud ~]$ rpm -qa | grep contrail

puppet-contrail-4.1.5.0-70.el7.noarch
contrail-tripleo-heat-templates-4.1.5.0-70.el7.noarch
contrail-tripleo-puppet-4.1.5.0-70.el7.noarch
python-gevent-1.1rc5-1contrail1.el7.x86_64
```


9. Review the **ironic node-list** output to confirm the following statuses for each package::

- **Power state** is *power on*.
- **Provision State** is *active*.
- **Maintenance** is *False*.

```
[stack@undercloud ~]$ ironic node-list
```

+-----+-----+-----+			
Name	Power	Provisioning	Maintenance
	State	State	
+-----+-----+-----+			
controller-3	power on	active	False
compute-5c5s35	power on	active	False
contrail-controller1	power on	active	False
contrail-analytics1	power on	active	False
contrail-controller-3	power on	active	False
contrail-controller-2	power on	active	False
contrail-analytics-database1	power on	active	False
controller-2	power on	active	False
controller1	power on	active	False
compute-5c5s37	power on	active	False
compute-5c5s36	power on	active	False
contrail-analytics-2	power on	active	False
contrail-analytics-3	power on	active	False
compute-5c5s38	power on	active	False
contrail-analytics-database-3	power on	active	False
contrail-analytics-database-2	power on	active	False
+-----+-----+-----+			

NOTE: This output presentation has been modified for readability. The *UUID* and *Instance UUID* fields were removed as part of this modification.

10. Verify that all OpenStack servers are in the Active state.

```
[stack@undercloud ~]$ openstack server list
```

+-----+-----+	
Name	Status
+-----+-----+	

```
| overcloud-contrailanalytics-2-4-1-4-7-7 | ACTIVE |
| overcloud-controller-0-4-1-4-7-7 | ACTIVE |
| overcloud-contrailanalytics-0-4-1-4-7-7 | ACTIVE |
| overcloud-contrailanalyticsdatabase-2-4-1-4-7-7 | ACTIVE |
| overcloud-contrailanalytics-1-4-1-4-7-7 | ACTIVE |
| overcloud-contrailanalyticsdatabase-0-4-1-4-7-7 | ACTIVE |
| overcloud-contrailcontroller-1-4-1-4-7-7 | ACTIVE |
| overcloud-contrailanalyticsdatabase-1-4-1-4-7-7 | ACTIVE |
| overcloud-contrailcontroller-2-4-1-4-7-7 | ACTIVE |
| overcloud-contrailcontroller-0-4-1-4-7-7 | ACTIVE |
| compute-0-4-1-4-rhel-7-7 | ACTIVE |
| overcloud-contraildpdk-0-4-1-4-7-7 | ACTIVE |
| overcloud-contraildpdk-1-4-1-4-7-7 | ACTIVE |
| compute-1-4-1-4-rhel-7-7 | ACTIVE |
+-----+-----+
```

NOTE: This output presentation has been modified for readability. The *ID*, *Image Name*, and *Networks* fields were removed as part of this modification.

NOTE: Overcloud packages are often downloaded from the Contrail satellite at this point of other Contrail upgrade procedures. The overcloud is not upgraded in this procedure so these steps do not need to be performed.

11. Observe the contrail-status on all Contrail nodes. All services in the Contrail nodes, except the controller (OpenStack), should be up and running before proceeding with the upgrade.

```
[stack@undercloud ~]$ source stackrc
[stack@undercloud ~]$ for i in $(nova list | grep contrail | awk '{print $12}' | cut -d '=' -f2); do ssh heat-admin@$i sudo contrail-status; done
```

The Contrail repository must be enabled on all overcloud nodes.

12. Ensure that all overcloud node contrail repository pointers are properly pointing to the contrail repository.

Contrail Analytics Example:

```
[root@overcloud-contrailanalytics-0 heat-admin]# cat /etc/yum.repos.d/contrail.repo
[Contrail]
name=Contrail Repo
baseurl=http://192.168.24.1/contrail
enabled=1
gpgcheck=0
protect=1
metadata_expire=30
```

13. Before proceeding with the upgrade, consider performing the following tasks to optimize your results:

- Clean the yum cache on all overcloud virtual machines.
- Disable the subscriptions from the satellite to ensure new packages are not accidentally loaded during the procedure.
- Synch the satellites to the desired satellite repo end date, which is either the *Oct 29, 2018* or *May 5, 2020* end date depending on your RHEL version.

Upgrade the Contrail Heat Templates

You must copy the new Contrail Heat templates package to the undercloud node, while retaining a copy of the Heat templates that were used for the existing deployment.

1. Make a copy of all of the Heat templates that were used for deployment and save the copies, because the existing files will be overwritten by the new versions. The templates to copy are of the form `contrail-services.yaml`, `contrail-net.yaml`, and so on.

NOTE: Red Hat does not support changing IP address of the existing cluster as a part of upgrade. Do not change IP address of the cluster while creating new tripleo-heat-templates

2. Copy the new `contrail-tripleo-heat` templates to the undercloud node.

```
sudo cp -r /usr/share/contrail-tripleo-heat-templates/environments/contrail /home/stack/
tripleo-heat-templates/environments/
```

```
sudo cp -r /usr/share/contrail-tripleo-heat-templates/puppet/services/network/* /home/stack/
tripleo-heat-templates/puppet/services/network
```

NOTE: The directory `/home/stack/tripleo-heat-templates` is user defined, it can be *User Defined-directory* `>/openstack-tripleo-heat-templates`

Modify the Yum Update Script for TripleO Puppet

The following Puppet commands must be added to the `yum_update` script before starting the upgrade. The script is located at:

`/home/stack/tripleo-heat-templates/extraconfig/tasks/yum_update.sh`

1. Update the following Puppet commands in the `yum_update.sh` after the line `"echo -n "false" > $heat_outputs_path.update_managed_packages"`.

Refer to the following patch for details regarding the exact placement of the commands patch:

https://github.com/Juniper/contrail-tripleo-heat-templates/blob/stable/newton/environments/contrail/yum_updates.patch

```
yum install -y contrail-tripleo-puppet puppet-contrail
```

```
rsync -a /usr/share/contrail-tripleo-puppet/ /usr/share/openstack-puppet/modules/tripleo/
```

2. Update the fields `*contrail version` and `*contrail repo` in `contrail-services.yaml`.

Default parameter for `contrailVersion` is 4.

Filename: `/home/stack/tripleo-heat-templates/environments/contrail/contrail-services.yaml`.

Add the following parameters:

ContrailVersion: 4

ContrailRepo : *<location of the contrail repo>*

NOTE: `/home/stack/tripleo-heat-templates` directory is user defined and it can be the directory name under stack user.

The Contrail Repo is often a URL in the `http://<IP-address>/<directory>` format.

For example:

```
ContrailRepo: http://192.168.24.1/contrail
```

Update the Overcloud Deployment Plan

1. Update the current plan by re-running the command used for cloud deployment and adding the suffix `-update-plan-only`.

```
openstack overcloud deploy -update-plan-only
```

Example:

```
openstack overcloud deploy --update-plan-only --templates /home/stack/tripleo-heat-templates/ \
  --roles-file /home/stack/tripleo-heat-templates/environments/contrail/roles_data.yaml \
  -e /home/stack/tripleo-heat-templates/environments/puppet-pacemaker.yaml \
  -e /home/stack/tripleo-heat-templates/environments/contrail/contrail-services.yaml \
  -e /home/stack/tripleo-heat-templates/environments/contrail/network-isolation.yaml \
  -e /home/stack/tripleo-heat-templates/environments/contrail/contrail-net.yaml \
  -e /home/stack/tripleo-heat-templates/environments/ips-from-pool-all.yaml \
  -e /home/stack/tripleo-heat-templates/environments/network-management.yaml \
  -e /home/stack/tripleo-heat-templates/extraconfig/pre_deploy/rhel-registration/environment-
  rhel-registration.yaml \
  -e /home/stack/tripleo-heat-templates/extraconfig/pre_deploy/rhel-registration/rhel-
  registration-resource-registry.yaml \
  --libvirt-type qemu
```

2. Make a copy of the existing deploy script to the `update-stack.sh`. The `update-stack.sh` is the script used to update the overcloud plan, and it references the same templates that were used to deploy the stack. All files used for the overcloud update should be identical to the files used for deployment, except `contrail-services` file that was updated with the latest `contrail-version` and `contrail-repo`.

```
cp deploy.sh update-stack.sh
```

3. Update the deployment plan.

```
./update-stack.sh
```

Example:

```
[stack@undercloud ~]$ ./update-stack.sh
  Removing the current plan files
  Uploading new plan files
  Started Mistral Workflow. Execution ID: 998a1b40--a034-8cff453acfb1
  Plan updated
  Deploying templates in the directory /tmp/tripleoclient-JulIde/tripleo-heat-templates
  Overcloud Endpoint: http://10.0.0.35:5000/v2.0
  Overcloud Deployed
```

Upgrade the Overcloud



CAUTION: The steps in this section are service disrupting, and should only be performed within a maintenance window.

1. Update the overcloud stack.

```
$ openstack overcloud update stack -i overcloud
on_breakpoint: [u'overcloud-contrailanalyticsdatabase-0']
Breakpoint reached, continue? Regexp or Enter=proceed (will clear
4386bdc7-5087-4a4d-865c-0b0181ce9345), no=cancel update, C-c=quit interactive mode:
IN_PROGRESS
IN_PROGRESS
IN_PROGRESS
IN_PROGRESS
IN_PROGRESS
COMPLETE
update finished with status COMPLETE
```

2. Verify the overcloud stack status, the contrail-status, and the contrail-version after the upgrade.

Overcloud Stack Status

```
[stack@undercloud ~]$ openstack stack list
+-----+-----+-----+-----+
| Name | Status | Updated |
```

Stack Name	Stack Status	Creation Time	Updated Time
overcloud	UPDATE_COMPLETE	2020-03-17T23:30:26Z	2020-08-05T22:40:01Z

NOTE: The **openstack stack list** output presentation has been modified for readability. The *ID* field was removed as part of this modification.

Contrail Stack Status

```
sudo for i in $(nova list | grep contrail | awk '{print $12}' | cut -d '=' -f2); do ssh heat-admin@$i sudo contrail-status; done
```

Contrail Version Check

```
for i in $(nova list | grep contrail | awk '{print $12}' | cut -d '=' -f2); do ssh heat-admin@$i sudo contrail-version; ssh heat-admin@$i sudo contrail-status -d ; done
```

Upgrade Cautions



CAUTION: The steps to perform the overcloud upgrade are service disrupting, and should only be performed within a maintenance window.

Contrail-Named Services Remains Down After Upgrade

In rare cases, the contrail-named service stays down after an upgrade.

Workaround: Restart the service once using the *service contrail-named restart* command.

To identify and respond to this issue:

```
overcloud-contrailcontroller-1 contrail]# service contrail-named status -d
contrail-named          FATAL      Exited too quickly (process log may have details)
[root@overcloud-contrailcontroller-1 contrail]#
```

```
[root@overcloud-contrailcontroller-1 contrail]# service contrail-named restart
```

Upgrade Procedure for RHOSP-based Contrail 4.1.3 or 4.1.4 to Contrail 4.1.4.1

IN THIS SECTION

- [Prerequisites | 46](#)
- [Post-Installation | 47](#)
- [Net-SNMP Package Requirements | 47](#)
- [Acquire the Software | 49](#)
- [Preparing the Environment | 49](#)
- [Upgrade the Contrail Heat Templates | 53](#)
- [Modify the Yum Update Script for TripleO Puppet | 54](#)
- [Update the Overcloud Deployment Plan | 55](#)
- [Upgrade the Overcloud | 56](#)
- [Upgrade Cautions | 57](#)

This section presents the steps to upgrade a RHOSP-based Contrail deployment from Contrail version 4.1.3 or 4.1.4 to Contrail version 4.1.4.1.

Prerequisites

Ensure you have a cloud up and running with RHOSP10 and Contrail 4.1.3 or Contrail 4.1.4 before you proceed with the upgrade procedure.

This procedure has been validated with the following Contrail, Red Hat, and OpenStack versions.

Table 5: Pre-Installation Software Versions

Contrail Version	Red Hat Version	OpenStack Version
4.1.4	RHEL 7.5 (3.10.0-862.14.4.el7.x86_64)	RHOSP10 (packages dated October 29, 2018)
4.1.3	RHEL 7.5 (3.10.0-862.11.6.el7.x86_64)	RHOSP10 (packages dated October 29, 2018)

Post-Installation

After the installation, you'll have a cloud networking running RHOSP10 and Contrail 4.1.4.1. The Red Hat Enterprise Linux (RHEL) kernel version remains at 7.5 during this procedure.

[Table 6 on page 47](#) summarizes the post-installation software versions.

Table 6: Post Installation Software Summary

Contrail Version	Red Hat Version	OpenStack Version
4.1.4.1	RHEL 7.5 (3.10.0-862.14.4.el7.x86_64)	RHOSP10 (packages dated October 29, 2018)

Net-SNMP Package Requirements

Contrail version R4.1.4.1 supports net-snmp package version 5.7.2-43 to support SNMP in most environments.

The net-snmp packages come from Red Hat, with the exception of the *net-snmp-python-5.7.2-43.el7.x86_64.rpm* package which is provided in the Contrail repository.

[Table 7 on page 48](#) summarizes the net-snmp depend packages and their associated repository locations.

Table 7: Net-SNMP Depend Packages (version 43)

Net-SNMP Depend Packages	Initial Repository
<i>net-snmp-5.7.2-43.el7.x86_64.rpm</i>	Red Hat Satellite
<i>net-snmp-agent-libs-5.7.2-43.el7.x86_64.rpm</i>	Red Hat Satellite
<i>net-snmp-libs-5.7.2-43.el7.x86_64.rpm</i>	Red Hat Satellite
<i>net-snmp-python-5.7.2-43.el7.x86_64.rpm</i>	Contrail
<i>net-snmp-utils-5.7.2-43.el7.x86_64.rpm</i>	Red Hat Satellite

If you are working in an environment with devices that have dependencies on older net SNMP packages, replace the net SNMP packages with the following version 37-based SNMP packages.

Table 8: Net-SNMP Depend Packages (version 37)

Net-SNMP Depend Packages	Initial Repository
<i>net-snmp-5.7.2-37.el7.x86_64.rpm</i>	Red Hat Satellite
<i>net-snmp-agent-libs-5.7.2-37.el7.x86_64.rpm</i>	Red Hat Satellite
<i>net-snmp-libs-5.7.2-37.el7.x86_64.rpm</i>	Red Hat Satellite
<i>net-snmp-python-5.7.2-37.el7.x86_64.rpm</i>	Contrail
<i>net-snmp-utils-5.7.2-37.el7.x86_64.rpm</i>	Red Hat Satellite

If you need to replace the SNMP packages, run the `createrepo` command to create the repository and complete the update.

Acquire the Software

To download the software images for this procedure:

1. Go to the [Juniper Networks Support site for Contrail](#).
2. Select **OS** as *Contrail* and **Version** as *4.1.4*. Download the images that apply to your environment.

Preparing the Environment

1. Log in to the undercloud as the stack user.

```
$ su - stack
```

2. Update the Contrail repositories.

- Backup the Contrail 4.1.3 or 4.1.4 packages to a repository with a different name.

In this example, the Contrail 4.1.3 packages are moved to a repository named *contrail-R4-1-3*.

```
[stack@undercloud ~]$ cd /var/www/html/
[stack@undercloud html]$ sudo mv contrail/ contrail-R4-1-3
```

- Create a new repository directory to store the Contrail 4.1.4.1 packages:

```
[stack@undercloud html]$ sudo mkdir contrail
```

3. Copy the downloaded file—in the provided sample, the file is *contrail-install-packages_4.1.4.1-10-newton.tgz*—to the Contrail repository created in Step 2.

NOTE: This step assumes that you've already downloaded the Contrail software. See ["Acquire the Software" on page 49](#).

```
[stack@undercloud contrail]$ ls -lrt
total 377104
-rw-r--r--. 1 root root 386151602 Mar 14 06:58 contrail-install-packages_4.1.4.1-10-
newton.tgz
```

4. Untar the downloaded tgz file.

```
[stack@undercloud contrail]$ sudo tar -xvf contrail-install-packages_4.1.4.1-10-newton.tgz
```

5. Ensure your satellite has a supported net-snmp package setup. The net-snmp packages in the Contrail repository and the satellite repository must match. See ["Net-SNMP Package Requirements" on page 47](#).
6. Create a repository in the new directory:

```
[stack@undercloud contrail]$ pwd
/var/www/html/contrail

[stack@undercloud contrail]$ sudo createrepo .
```

If the **createrepo** command is not available, download the createrepo package from Red Hat (Red Hat subscription required).

7. (Clusters deployed using Swift Puppet files only) If your Contrail 4.1 cluster was deployed using Swift Puppet, perform these steps:
 - a. Remove overcloud artifacts from the undercloud:

```
[stack@undercloud ~]$ swift delete overcloud-artifacts
puppet-modules.tgz
overcloud-artifacts
```

- b. Delete the *deployments-artifacts.yaml* file if the file is present.

```
[stack@undercloud ~]$ ls /home/stack/.tripleo/environments/deployment-artifacts.yaml
[stack@undercloud ~]$ rm -rf /home/stack/.tripleo/environments/deployment-artifacts.yaml
```

- c. Clean the repositories and confirm that all repositories are available.

```
[stack@undercloud ~]$ sudo yum clean all
[stack@undercloud ~]$ sudo yum repolist
```

NOTE: The undercloud is often updated at this point of the Contrail Networking upgrade procedure. The undercloud does not need to be updated for this procedure since the RHEL and RHOSP versions are unchanged.

8. Ensure the undercloud has the latest Contrail R4.1.4.1 contrail packages:

```
[stack@undercloud ~]$ rpm -qa | grep contrail

puppet-contrail-4.1.4.1-10.el7.noarch
contrail-tripleo-heat-templates-4.1.4.1-10.el7.noarch
contrail-tripleo-puppet-4.1.4.1-10.el7.noarch
python-gevent-1.1rc5-1contrail1.el7.x86_64
```

9. Review the **ironic node-list** output to confirm the following statuses for each package::

- **Power state** is *power on*.
- **Provision State** is *active*.
- **Maintenance** is *False*.

```
[stack@undercloud ~]$ ironic node-list
```

Name	Power State	Provisioning State	Maintenance
controller-3	power on	active	False
compute-5c5s35	power on	active	False
contrail-controller1	power on	active	False
contrail-analytics1	power on	active	False
contrail-controller-3	power on	active	False
contrail-controller-2	power on	active	False
contrail-analytics-database1	power on	active	False
controller-2	power on	active	False
controller1	power on	active	False
compute-5c5s37	power on	active	False
compute-5c5s36	power on	active	False
contrail-analytics-2	power on	active	False
contrail-analytics-3	power on	active	False
compute-5c5s38	power on	active	False

contrail-analytics-database-3	power on	active	False	
contrail-analytics-database-2	power on	active	False	

NOTE: This output presentation has been modified for readability. The *UUID* and *Instance UUID* fields were removed as part of this modification.

10. Verify that all OpenStack servers are in the Active state.

```
[stack@undercloud ~]$ openstack server list
```

Name	Status
overcloud-contrailanalytics-2-4-1-4-7-7	ACTIVE
overcloud-controller-0-4-1-4-7-7	ACTIVE
overcloud-contrailanalytics-0-4-1-4-7-7	ACTIVE
overcloud-contrailanalyticsdatabase-2-4-1-4-7-7	ACTIVE
overcloud-contrailanalytics-1-4-1-4-7-7	ACTIVE
overcloud-contrailanalyticsdatabase-0-4-1-4-7-7	ACTIVE
overcloud-contrailcontroller-1-4-1-4-7-7	ACTIVE
overcloud-contrailanalyticsdatabase-1-4-1-4-7-7	ACTIVE
overcloud-contrailcontroller-2-4-1-4-7-7	ACTIVE
overcloud-contrailcontroller-0-4-1-4-7-7	ACTIVE
compute-0-4-1-4-rhel-7-7	ACTIVE
overcloud-contraildpdk-0-4-1-4-7-7	ACTIVE
overcloud-contraildpdk-1-4-1-4-7-7	ACTIVE
compute-1-4-1-4-rhel-7-7	ACTIVE

NOTE: This output presentation has been modified for readability. The *ID*, *Image Name*, and *Networks* fields were removed as part of this modification.

NOTE: Overcloud packages are often downloaded from the Contrail satellite at this point of other Contrail upgrade procedures. The overcloud is not upgraded in this procedure so these steps do not need to be performed.

11. Observe the contrail-status on all Contrail nodes. All services in the Contrail nodes, except the controller (OpenStack), should be up and running before proceeding with the upgrade.

```
[stack@undercloud ~]$ source stackrc
[stack@undercloud ~]$ for i in $(nova list | grep contrail | awk '{print $12}' | cut -d '=' -f2); do ssh heat-admin@$i sudo contrail-status; done
```

The Contrail repository must be enabled on all overcloud nodes.

12. Ensure that all overcloud node contrail repository pointers are properly pointing to the contrail repository.

Contrail Analytics Example:

```
[root@overcloud-contrailanalytics-0 heat-admin]# cat /etc/yum.repos.d/contrail.repo
[Contrail]
name=Contrail Repo
baseurl=http://192.168.24.1/contrail
enabled=1
gpgcheck=0
protect=1
metadata_expire=30
```

13. Before proceeding with the upgrade, consider performing the following tasks to optimize your results:
 - Clean the yum cache on all overcloud virtual machines.
 - Disable the subscriptions from the satellite to ensure new packages are not accidentally loaded during the procedure.
 - Synch the satellites to the *Oct 29, 2018* satellite repo end date.

Upgrade the Contrail Heat Templates

You must copy the new Contrail Heat templates package to the undercloud node, while retaining a copy of the Heat templates that were used for the existing deployment.

1. Make a copy of all of the Heat templates that were used for deployment and save the copies, because the existing files will be overwritten by the new versions. The templates to copy are of the form `contrail-services.yaml`, `contrail-net.yaml`, and so on.

NOTE: Red Hat does not support changing IP address of the existing cluster as a part of upgrade. Do not change IP address of the cluster while creating new tripleo-heat-templates

2. Copy the new contrail-tripleo-heat templates to the undercloud node.

```
sudo cp -r /usr/share/contrail-tripleo-heat-templates/environments/contrail /home/stack/
tripleo-heat-templates/environments/

sudo cp -r /usr/share/contrail-tripleo-heat-templates/puppet/services/network/* /home/stack/
tripleo-heat-templates/puppet/services/network
```

NOTE: The directory /home/stack/tripleo-heat-templates is user defined, it can be *User Defined-directory>/openstack-tripleo-heat-templates*

Modify the Yum Update Script for TripleO Puppet

The following Puppet commands must be added to the `yum_update` script before starting the upgrade. The script is located at:

/home/stack/tripleo-heat-templates/extraconfig/tasks/yum_update.sh

1. Update the following Puppet commands in the `yum_update.sh` after the line “echo -n "false" > \$heat_outputs_path.update_managed_packages”.

Refer to the following patch for details regarding the exact placement of the commands patch:

https://github.com/Juniper/contrail-tripleo-heat-templates/blob/stable/newton/environments/contrail/yum_updates.patch

```
yum install -y contrail-tripleo-puppet puppet-contrail
```

```
rsync -a /usr/share/contrail-tripleo-puppet/ /usr/share/openstack-puppet/modules/tripleo/
```

2. Update the fields `*contrail version` and `*contrail repo` in `contrail-services.yaml`.

Default parameter for `contrailVersion` is 4.

Filename: **/home/stack/tripleo-heat-templates/environments/contrail/contrail-services.yaml**.

Add the following parameters:

ContrailVersion: 4

ContrailRepo : *<location of the contrail repo>*

NOTE: `/home/stack/tripleo-heat-templates` directory is user defined and it can be the directory name under stack user.

Update the Overcloud Deployment Plan

1. Update the current plan by re-running the command used for cloud deployment and adding the suffix `-update-plan-only`.

```
openstack overcloud deploy -update-plan-only
```

Example:

```
openstack overcloud deploy --update-plan-only --templates /home/stack/tripleo-heat-templates/ \
  \
  --roles-file /home/stack/tripleo-heat-templates/environments/contrail/roles_data.yaml \
  -e /home/stack/tripleo-heat-templates/environments/puppet-pacemaker.yaml \
  -e /home/stack/tripleo-heat-templates/environments/contrail/contrail-services.yaml \
  -e /home/stack/tripleo-heat-templates/environments/contrail/network-isolation.yaml \
  -e /home/stack/tripleo-heat-templates/environments/contrail/contrail-net.yaml \
  -e /home/stack/tripleo-heat-templates/environments/ips-from-pool-all.yaml \
  -e /home/stack/tripleo-heat-templates/environments/network-management.yaml \
  -e /home/stack/tripleo-heat-templates/extraconfig/pre_deploy/rhel-registration/environment- \
  rhel-registration.yaml \
  -e /home/stack/tripleo-heat-templates/extraconfig/pre_deploy/rhel-registration/rhel- \
  registration-resource-registry.yaml \
  --libvirt-type qemu
```

2. Make a copy of the existing deploy script to the `update-stack.sh`. The `update-stack.sh` is the script used to update the overcloud plan, and it references the same templates that were used to deploy the stack. All files used for the overcloud update should be identical to the files used for deployment, except `contrail-services` file that was updated with the latest `contrail-version` and `contrail-repo`.

```
cp deploy.sh update-stack.sh
```

3. Update the deployment plan.

```
./update-stack.sh
```

Example:

```
[stack@undercloud ~]$ ./update-stack.sh
  Removing the current plan files
  Uploading new plan files
  Started Mistral Workflow. Execution ID: 998a1b40--a034-8cff453acfb1
  Plan updated
  Deploying templates in the directory /tmp/tripleoclient-JulIde/tripleo-heat-templates
  Overcloud Endpoint: http://10.0.0.35:5000/v2.0
  Overcloud Deployed
```

Upgrade the Overcloud



CAUTION: The steps in this section are service disrupting, and should only be performed within a maintenance window.

1. Update the overcloud stack.

```
$ openstack overcloud update stack -i overcloud
on_breakpoint: [u'overcloud-contrailanalyticsdatabase-0']
Breakpoint reached, continue? Regexp or Enter=proceed (will clear
4386bdc7-5087-4a4d-865c-0b0181ce9345), no=cancel update, C-c=quit interactive mode:
IN_PROGRESS
IN_PROGRESS
IN_PROGRESS
IN_PROGRESS
IN_PROGRESS
COMPLETE
update finished with status COMPLETE
```

2. Verify the overcloud stack status, the contrail-status, and the contrail-version after the upgrade.

Overcloud Stack Status

```
[stack@undercloud ~]$ openstack stack list
```

Stack Name	Stack Status	Creation Time	Updated Time
overcloud	UPDATE_COMPLETE	2020-03-17T23:30:26Z	2020-03-17T22:40:01Z

NOTE: The `openstack stack list` output presentation has been modified for readability. The `ID` field was removed as part of this modification.

Contrail Stack Status

```
sudo for i in $(nova list | grep contrail | awk '{print $12}' | cut -d '=' -f2); do ssh heat-admin@$i sudo contrail-status; done
```

Contrail Version Check

```
for i in $(nova list | grep contrail | awk '{print $12}' | cut -d '=' -f2); do ssh heat-admin@$i sudo contrail-version; ssh heat-admin@$i sudo contrail-status -d ; done
```

Upgrade Cautions



CAUTION: The steps to perform the overcloud upgrade are service disrupting, and should only be performed within a maintenance window.

Contrail-Named Services Remains Down After Upgrade

In rare cases, the contrail-named service stays down after an upgrade.

Workaround: Restart the service once using the `service contrail-named restart` command.

To identify and respond to this issue:

```
overcloud-contrailcontroller-1 contrail]# service contrail-named status -d
contrail-named          FATAL    Exited too quickly (process log may have details)
[root@overcloud-contrailcontroller-1 contrail]#

[root@overcloud-contrailcontroller-1 contrail]# service contrail-named restart
```

Upgrade Procedure for Ubuntu-based Contrail 4.1.3 to Contrail 4.1.4 Using Juju with Netronome SmartNIC

IN THIS SECTION

- [Prerequisites | 58](#)
- [Acquire the Software | 59](#)
- [Attach Contrail Packages using Juju | 59](#)
- [Upgrade the Contrail Clusters | 60](#)

This section presents the steps to upgrade from an Ubuntu-16.04-based Contrail deployment from Contrail version 4.1.3 to Contrail version 4.1.4 using Juju charms.

Prerequisites

These instructions assume that these requirements for installing Contrail Release 4.1.3 are already present in your environment:

- **MaaS Server**—MaaS version 2.3 is installed on this server. This procedure was tested using MaaS version 2.3.5.

- Juju Controller—Juju version 2.3 is installed, and the Juju controller is bootstrapped on a VM or a bare metal server. This procedure was tested using Juju version 2.3.7-xenial-amd64.
- A repository to get Netronome, patched Openstack packages, and Contrail vRouter packages is operational.
- A Contrail Controller using Ubuntu 16.04 xenial is operational.
- A Contrail cluster with one or more compute nodes using Agilio SmartNICs.

Acquire the Software

To acquire the Contrail 4.1.4 software images to perform this procedure:

1. Go to the [Juniper Networks Support site for Contrail](#).
2. Select **OS** as *Contrail* and **Version** as *4.1.4* from the drop-down menus.
3. Download the *contrail-cloud-docker_4.1.4.0-63-ocata_xenial.tgz* file.
4. Extract the following images from the *contrail-cloud-docker_4.1.4.0-63-ocata_xenial.tgz* file:
 - Contrail Analytics package: *contrail-analytics-ubuntu16.04-4.1.4.0-63.tar.gz*.
 - Contrail Analytics Database package: *contrail-analyticsdb-ubuntu16.04-4.1.4.0-63.tar.gz*.
 - Contrail Controller package: *contrail-controller-ubuntu16.04-4.1.4.0-63.tar.gz*

The images need to be extracted because the Contrail Analytics, Contrail Analytics Database, and Contrail Controller packages must be upgraded individually to perform this upgrade.

Attach Contrail Packages using Juju

The Contrail Controller, Contrail Analytics, and Contrail Analytics DB packages need to be attached using Juju to perform this upgrade.

To attach these software packages into Juju:

1. Attach the Contrail Controller, Contrail Analytics, & Contrail Analytics DB packages into Juju:

```
juju attach contrail-analytics contrail-analytics=/home/jenkins/docker/contrail-analytics-ubuntu16.04-4.1.4.0-63.tar.gz
```

```
juju attach contrail-controller contrail-controller=/home/jenkins/docker/contrail-controller-ubuntu16.04-4.1.4.0-63.tar.gz
juju attach contrail-analyticsdb contrail-analyticsdb=/home/jenkins/docker/contrail-analyticsdb-ubuntu16.04-4.1.4.0-63.tar.gz
```

2. Check status of the software image attachments into Juju using the `juju status` command.

Wait for the `juju status` command output to indicate that the upgrade is successful. The output in the `juju status` should indicate that all processes are *Active* and all machine states are *started*.

Upgrade the Contrail Clusters

This section provides the steps to update the Contrail clusters for this upgrade.

It includes the following sections:

Upgrade the Contrail Controllers

The Contrail controllers must be upgraded one by one to complete this procedure.

To upgrade the Contrail controllers:

1. SSH into the Contrail controller server and decommission the Contrail controller from the Cassandra cluster:

```
sudo docker exec -it contrail-controller /usr/bin/nodetool decommission
```

2. Remove the Contrail Controller container:

```
sudo docker rm -f contrail-controller
```

3. Update the hooks to the Contrail Controller from the Juju Controller:

```
juju run --application contrail-controller hooks/update-status
```

4. Wait for the Contrail status for all packages on the upgrading node to change to *active*. This step can take up to 10 minutes.

Enter the **contrail-status** command to check status. All packages in the *Contrail Control* section of the output must move to the *active* state before proceeding.

5. Check Juju status by entering the `juju status` command.

All Contrail components in this output should be in the *active* state.

6. After each controller update, check the controllers to make sure the databases are consistent across all controllers:

- Enter the **nodetool describecluster** command. Confirm that the *schema version* output is identical on all 3 controllers.
- Enter the **echo stat | nc localhost 2181** command. The *node count* output should be identical on all 3 controllers.
- Ensure that the **contrail-status** output is *active* for all components in all 3 controllers.

If your upgrade is not successful after 15 minutes, retry steps 1 through 5.

If you need to decommission a node that is not upgrading successfully, use the **nodetool remove node *node-ID*** command.

7. Repeat steps 1 through 6 for all other Contrail controller nodes.

Upgrade Contrail Analytics Nodes

To upgrade the Contrail Analytics nodes:

1. SSH into the first Contrail Analytics node and remove the Contrail Analytics container:

```
sudo docker rm -f contrail-analytics
```

2. Confirm Juju status using the `juju status` command.

The output in the `juju status` should indicate that all processes are *Active* and all machine states are *started*.

3. From the MaaS server, update hooks to the Contrail Analytics controller:

```
juju run --application contrail-analytics/0 hooks/update-status
```

4. Wait for the Contrail status for all packages on the upgrading node to change to *active*. This step can take up to 10 minutes.

Enter the **contrail-status** command to check status. All packages in the *Contrail Analytics* section of the output must move to the *active* state before proceeding.

5. Repeat steps 1 through 4 for all other Contrail Analytics nodes.

Upgrade Analytics Database Nodes

To upgrade the Contrail Analytics database nodes:

1. SSH into a Contrail analytics database server and decommission the node from the Cassandra cluster:

```
sudo docker exec -it contrail-analyticsdb /usr/bin/nodetool decommission
```

2. Remove the AnalyticsDB container:

```
sudo docker rm -f contrail-analyticsdb
```

3. From the Juju controller, update the hooks to the Contrail Analytics DB controller:

```
juju run --application contrail-analyticsdb hooks/update-status
```

4. Wait for the Contrail status for all packages on the upgrading node to change to *active*. This step can take up to 10 minutes.

Enter the **contrail-status** command to check status. All packages in the *Contrail Database* section of the output must move to the *active* state before proceeding.

5. Check Juju status by entering the `juju status` command.

All Contrail components in this output should be in the *active* state.

6. After each analytics database node update, check the nodes to ensure the databases are consistent inside the contrail analytics database containers:

- Enter the **nodetool describecluster** command. Confirm that the *schema version* output is identical on all 3 nodes.
- Enter the **echo stat | nc localhost 2181** command. The *node count* output should be identical on all 3 nodes.
- Ensure that the **contrail-status** output is *active* for all components in all 3 contrail analytics db nodes.

If your upgrade is not successful after 15 minutes, retry steps 1 through 5.

If you need to decommission a node that is not upgrading successfully, use the **nodetool removemode *node-ID*** command.

7. Repeat steps 1 through 6 for all other Contrail Analytics database nodes.

Updating the Neutron Plugin and the vRouter Agent

The process for updating the neutron plugin and the vRouter agent is different for compute nodes than it is for other nodes.

This section covers both procedures and includes these sections:

Updating the Neutron Plugin and the vRouter Agent on Non-Compute Nodes

Use this procedure to update the Neutron Plugin and the vRouter agent on all non-compute nodes in your environment:

NOTE: This procedure assumes that the APT Get repository was created during the previous installation, and that the latest Contrail packages can be placed into the repository.

1. SSH into the Neutron API plugin unit.
2. From the Neutron API plugin unit, get the latest APT Get update:

```
sudo apt-get update
```

3. Upgrade APT GET:

```
sudo apt-get upgrade
```

NOTE: This step shows how to upgrade APT get for all packages. You can also manually update the neutron-plugin-contrail and python-contrail packages to complete this step, if you'd rather not perform the complete upgrade. This procedure does not provide the steps to manually update these packages.

4. Restart the Neutron service:

```
sudo systemctl restart neutron-server.service
```

Updating the Neutron Plugin and the vRouter Agent on Compute Nodes

Use this procedure to update the Neutron Plugin and the vRouter agent on all compute devices in your environment:

NOTE: This procedure assumes that the APT Get repository was created during the previous installation, and that the latest Contrail packages can be placed into the repository.

1. SSH into the Neutron API plugin unit.
2. From the Neutron API plugin unit, get the latest APT Get update:

```
sudo apt-get update
```

3. Upgrade APT GET:

```
sudo apt-get upgrade
```

NOTE: This step shows how to upgrade APT get for all packages. You can also manually update the following packages to complete this step:

- contrail-lib
- contrail-nodemgr
- contrail-setup
- contrail-utils
- contrail-vrouter-agent
- contrail-vrouter-common

- contrail-vrouter-dkms
- contrail-vrouter-init
- contrail-vrouter-utils
- python-contrail
- python-contrail-vrouter-api
- python-opencontrail-vrouter-netns

This procedure does not provide the steps to manually update these packages.

4. Upgrade the vRouter agent and, if using Netronome SmartNICs, the netronome plugin.

- If you are performing this procedure on a compute node without a Netronome SmartNIC:

NOTE: The network connection over the vhost is down while this procedure is performed. Traffic will be lost.

a. Stop the Contrail vRouter agent:

```
sudo systemctl stop contrail-vrouter-agent
```

b. Remove the Contrail vRouter module:

```
sudo rmmod vrouter
```

c. Insert the vRouter module:

```
sudo insmod /lib/modules/4.4.0-116-generic/updates/dkms/vrouter.ko
```

d. Activate the vhost:

```
sudo ifup vhost0
```

- e. Restart the Contrail vRouter agent:

```
sudo systemctl start contrail-vrouter-agent
```

- If you are performing this procedure on a compute node with a Netronome SmartNIC:

NOTE: The network connection over the vhost is down while this procedure is performed. Traffic will be lost.

- a. Stop the Contrail vRouter agent:

```
sudo systemctl stop contrail-vrouter-agent
```

- b. Stop the Virtio forwarder module:

```
sudo systemctl stop virtio-forwarder
```

- c. Stop the vRouter control module:

```
sudo /opt/netronome/bin/ns-vrouter-ctl stop
```

- d. Restart the Virtio forwarder module:

```
sudo systemctl start virtio-forwarder
```

- e. Restart the Contrail vRouter agent:

```
sudo /opt/netronome/bin/ns-vrouter-ctl start
```

- f. Activate the vhost:

```
sudo ifup vhost0
```

- g. Restart the Contrail vRouter agent:

```
sudo systemctl start contrail-vrouter-agent
```

5. Verify Contrail status:

```
sudo contrail-status
```

All packages in the *Contrail vRouter* section of the output should be in the *active* state. This step can take several minutes.

RELATED DOCUMENTATION

| [Deploying Contrail Release 4.1 with Netronome SmartNICs by Using Juju](#)

Deploying Contrail Release 4.1 with Netronome SmartNICs by Using Juju

IN THIS SECTION

- [Deploying Contrail Release 4.1 with Netronome SmartNIC | 68](#)
- [Launching a VM after Deploying Contrail Release 4.1 with Netronome SmartNIC | 70](#)
- [Caveats | 71](#)

Prerequisites

Make sure that the following requirements are met:

- MaaS Server (if the cloud type is maas)—Install MaaS and Juju on this server
- Juju Controller—Bootstrap the Juju controller. This can be on a VM or a bare metal server.
- A repository—To get Netronome and patched OpenStack packages. The repository can be a virtual machine.

- Contrail controller—Use Ubuntu 16.04 xenial
- OpenStack—OpenStack can be on the same node as contrail-controller. Use the patched packages to support virtio-forwarder
- Compute node with Agilio SmartNIC—Use Ubuntu16.04 xenial

Deploying Contrail Release 4.1 with Netronome SmartNIC

Follow these steps to deploy Contrail Release 4.1 with Netronome SmartNIC:

1. Download the Netronome build package (Agilio vRouter r4.1.2—release notes build 82—(2018/10/25)) from <https://support.netronome.com> .
2. Download the Contrail package (contrail-networking-docker_4.1.2.0-<build>_xenial.tgz) at <https://support.juniper.net/support/downloads/?p=contrail#sw> .

NOTE: You must use Ubuntu 16.04 Xenial for the deployment.

3. Run the following script to rename the NFP interfaces.

```
Extract Netronome build tar file - > Netronome_R4.1.2_build_<build_nr>_Juju/Maas-
Commissioningscript/
00-maas-01-dagilio
```

Ubuntu-16.04-ga (kernel-4.4) package does not contain NFP driver. So the NFP driver needs to be installed separately. If deployed using MaaS, run the following command in the `/etc/maas/preseeds/curtin_userdata` directory to install the NFP driver.

```
netronome_01_driver_add_target: curtin in-target -- bash -c '[[ "$(lspci -Dnnd
19ee:4000)" ]] && aptget install --quiet --assume-yes agilio-nfp-driver-dkms agilio-nic-
firmware || true'
```

The sample **bundle.yaml** file for the deployment is available in the Netronome .tar file in the following path:

Netronome_R4.1.2_build_26_Juju/agilio-vrouter/ example-docker-ocata-agilio-bundle.yaml

4. Change the Kernel options setting for enabling Huge Pages as shown below:

```
kernel_opts='intel_iommu=on iommu=pt default_hugepagesz=2M hugepagesz=2M
hugepages=<nr_hugepages>'
```

5. Enable hardware acceleration by installing the following Agilio packages.

```
agilio-nfp-driver-dkms, agilio-nic-firmware
```

6. Bootstrap Juju controller.
7. Run the following command to clone Contrail Charm from Github.

```
git clone https://github.com/Juniper/contrail-charms
```

8. Agilio-vrouter uses virtio-forwarder as vnic-type to enable hardware acceleration. You need to patch OpenStack packages to use virtio-forwarder as vnic-type. For this, you need to specify the location of the patched OpenStack packages in the **bundle.yaml** file.

The following are the patched OpenStack Charm packages to be picked from the local directory.

```
charm: ./charm-nova-cloud-controller, charm: ./charm-neutron-api
charm: ./charm-nova-compute, charm: ./agilio-vrouter
```

You can find the patches in <https://drive.google.com/drive/folders/1XtFA3rEkYeXl13xAqTrwHD6jO8JcIBWI>.

Use the following script provided in the Netronome build tar file:

```
Extract Netronome_R4.1_build_<build_nr>.tar-> debs/package_builder -> ./create-
openstackpackages.sh
```

9. Deploy the cluster using the following command.

```
juju deploy ./bundle.yaml
```

10. Run the following commands to attach the Contrail packages to Juju.

```
juju attach contrail-controller contrail-controller=contrail-controller.tar.gz
juju attach contrail-analytics contrail-analytics=contrail-analytics.tar.gz
juju attach contrail-analyticsdb contrail-analyticsdb.tar.gz
```

11. Use the following commands to view the status or to log into any of the contrail/openstack units after deployment:

```
openstack units after the deployment:
juju status
```

12. Identify the name of the unit or IP address from the `juju status` output:

```
ssh into contrail-controller:
Juju ssh accel-nova-compute/0 B0 is unit number
```

You can find the logs in the `/var/log/juju` directory of the unit.

If logs do not indicate failure of any of the above steps, and all the units are deployed and are ready for use, make sure that `contrail-api` is reachable from `neutron-server`. If control data subnet is not same as the subnet used for the provisioning, you may need to configure a static route.

Launching a VM after Deploying Contrail Release 4.1 with Netronome SmartNIC

Follow these steps to launch a VM after deployment.

1. Create a flavour with the following metadata for spawning hardware accelerated VMs.

```
--property hw:mem_page_size = 2048 or --property hw:mem_page_size = 1048576
```


In this release, spawning a VM without creating a port is not supported. You need to create a port with `virtio-forwarder` as `vnic-type`. Then you need to use this port to launch a hardware accelerated VM.

```
vnic_type virtio-forwarder
```

2. Use OpenStack dashboard or nova boot to spawn the VM.

Caveats

This section lists the known issues with Netronome SmartNIC deployment.

- `nfp_p1` interface is not recommended to be used because of the following issue:
<https://bugs.launchpad.net/juniperopenstack/trunk/+bug/1797358>
- Launching a VM directly using `net-ids` is not supported. You need to use `port-ids`. See <https://bugs.launchpad.net/juniperopenstack/r4.1/+bug/1796812> for more information.

Upgrading Contrail 4.0 to 4.1

IN THIS SECTION

- [Upgrade Assumptions | 71](#)
- [Upgrade Procedure | 72](#)

This section provides the process for upgrading an existing Contrail Release 4.0 system to Contrail Release 4.1.

Upgrade Assumptions

This upgrade procedure assumes the following.

- The initial cluster (4.0.x) was provisioned using Server Manager.
- The OpenStack SKU is the same in the “from” and “to” versions.
- A backup has been made of the analytics database, see *Backing Up Contrail Databases Using JSON Format*.

Upgrade Procedure

1. Make a backup of the analytics database, because the upgrade procedure removes the analytics database information, see *Backing Up Contrail Databases Using JSON Format*.
2. Add the new Contrail 4.1 Debian image to the Server Manager JSON used for provisioning.

```
server-manager add image -f contrail_image.json
```

3. Upgrade the cluster by reprovisioning the cluster with the new image.

- For an all-in-one, single-node demo system:

```
server-manager provision--cluster_id <all_in_one_cluster> combined_image_mainline
```

- For a multinode system:

```
server-manager provision --cluster_id <multi_node> combined_image_mainline
```

4. Monitor progress of the provisioning by observing cluster status or log entries.

- Cluster status: `server-manager display server --cluster_id <cluster_id> --select "id,ip_address,roles,status"`
- Log entries: `/var/log/contrail-server-manager/debug.log`

NOTE: Log entries from the previous version are lost in the upgrade process.

For more upgrade instructions, see:

- [Upgrade Procedure for RHOSP-based Contrail 4.1.3 to Contrail 4.1.4](#)
- [Upgrade Procedure for RHOSP-based Contrail 4.1.2 to Contrail 4.1.3](#)
- [Upgrade Procedure for RHOSP-based Contrail 4.1.1 to Contrail 4.1.2](#)
- [Upgrade Procedure for RHOSP-based Contrail 3.2.x to Contrail 4.1](#)

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.