

# Release Notes for Contrail Release 3.0

**Release 3.0**  
**March 2016**

## **Contents**

Introduction .....	2
New and Changed Features .....	2
Support for Data Plane Development Kit (DPDK) .....	3
Support for Single Root I/O Virtualization (SR-IOV) .....	3
Support for BGP as a Service .....	3
Ability to Select Customized Hash Field for ECMP Load Balancing .....	3
Support for Service Instance Health Check .....	4
VMware vCenter as Compute Mode .....	4
Ability to Configure PCI-Passthrough and SR-IOV Interface for vCenter Integration .....	4
Enhancements to Contrail Alerts .....	4
Enhancements to the Loadbalancing Feature .....	5
Ability to Configure Virtual Networks for Hub and Spoke Topology .....	5
Ability to Use Physical Network Functions in Contrail Service Chains .....	5
Server Manager Lite Replaces fab Command Provisioning .....	6
Ability to Configure Transport Layer Security-Based XMPP .....	6
Support for IPv6 in the Service Chain .....	6
Service Chain Route Reorigination .....	6
Generation of Heat Templates .....	7
Using Port-Tuples for VM Ports .....	7
Section .....	?
Supported Platforms .....	7
Known Issues .....	8
Upgrading Contrail Software from Release 2.21 or Greater to Release 3.0 .....	12
Documentation Feedback .....	15
Requesting Technical Support .....	15
Self-Help Online Tools and Resources .....	15
Opening a Case with JTAC .....	16
Revision History .....	16

## 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 3.0 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 [http://www.juniper.net/techpubs/en\\_US/contrail3.00/information-products/topic-collections/release-notes/index.html](http://www.juniper.net/techpubs/en_US/contrail3.00/information-products/topic-collections/release-notes/index.html).

## New and Changed Features

---

The features listed in this section are new or changed as of Contrail Release 3.0. A brief description of each new feature is included.

- [Support for Data Plane Development Kit \(DPDK\) on page 3](#)
- [Support for Single Root I/O Virtualization \(SR-IOV\) on page 3](#)
- [Support for BGP as a Service on page 3](#)
- [Ability to Select Customized Hash Field for ECMP Load Balancing on page 3](#)
- [Support for Service Instance Health Check on page 4](#)
- [VMware vCenter as Compute Mode on page 4](#)
- [Ability to Configure PCI-Passthrough and SR-IOV Interface for vCenter Integration on page 4](#)
- [Enhancements to Contrail Alerts on page 4](#)
- [Enhancements to the Loadbalancing Feature on page 5](#)
- [Ability to Configure Virtual Networks for Hub and Spoke Topology on page 5](#)
- [Ability to Use Physical Network Functions in Contrail Service Chains on page 5](#)
- [Server Manager Lite Replaces fab Command Provisioning on page 6](#)
- [Ability to Configure Transport Layer Security-Based XMPP on page 6](#)
- [Support for IPv6 in the Service Chain on page 6](#)
- [Service Chain Route Reorigination on page 6](#)
- [Generation of Heat Templates on page 7](#)
- [Using Port-Tuples for VM Ports on page 7](#)
- [Section on page ?](#)

## Support for Data Plane Development Kit (DPDK)

Contrail 3.0 and later supports Data Plane Development Kit (DPDK). DPDK is an open source set of libraries and drivers for fast packet processing. DPDK enables fast packet processing by allowing network interface cards (NICs) to send direct memory access (DMA) packets directly into an application's address space, allowing the application to poll for packets, thereby avoiding the overhead of interrupts from the NIC. Integrating with DPDK allows a Contrail vRouter to process more packets per second than is possible when it runs as a kernel module.

See *Configuring Data Plane Development Kit (DPDK) Integrated with Contrail vRouter*.

## Support for Single Root I/O Virtualization (SR-IOV)

Contrail 3.0 and later supports single root I/O virtualization (SR-IOV). SR-IOV is an interface extension of the PCI Express (PCIe) specification. SR-IOV allows a device, such as a network adapter, to separate access to its resources among various hardware functions. For example, the DPDK library has drivers that run in user space for several NICs. However, if the application runs inside a virtual machine, it does not see the physical NIC unless SR-IOV is enabled on the NIC.

See *Configuring Single Root I/O Virtualization (SR-IOV)*.

## Support for BGP as a Service

The BGP as a service (BGPaaS) feature allows a guest virtual machine (VM) to place routes in its own virtual routing and forwarding (VRF) instance using BGP.

Using BGPaaS with Contrail requires the guest VM to have connectivity to the control node and to be able to advertise routes into the VRF instance.

With the BGPaaS feature:

- The vRouter agent is able to accept BGP connections from the VMs and proxy them to the control node.
- The vRouter agent always selects one of the control nodes that it is using as an XMPP server.

See *BGP as a Service*.

## Ability to Select Customized Hash Field for ECMP Load Balancing

Starting with Contrail Release 3.0, it is possible to configure the set of fields used to hash upon during equal-cost multipath (ECMP) load balancing.

Earlier versions of Contrail had this set of fields fixed to the standard 5-tuple set of: source L3 address, destination L3 address, L4 protocol, L4 SourcePort, and L4 DestinationPort.

With the custom hash feature, users can configure an exact subset of fields to hash upon when choosing the forwarding path among a set of eligible ECMP candidates.

Custom hash is useful whenever packets originating from a particular source and addressed to a particular destination must go through the same set of service instances during transit. This might be required if source, destination, or transit nodes maintain a certain state based on the flow, and the state behavior could be used for subsequent new flows as well, between the same pair of source and destination addresses. In such cases, subsequent flows must follow the same set of service nodes that the initial flow followed.

See *Customized Hash Field Selection for ECMP Load Balancing*.

## Support for Service Instance Health Check

In Contrail Release 3.0 and greater, a service instance health check is used to determine the liveness of a service provided by a VM, checking whether the service is operationally up or down. The vRouter agent uses ping and an HTTP URL to the link-local address to check the liveness of the interface.

If the health check determines that a service is no longer operational, it removes the routes for the VM, thereby disabling forwarding packets to the VM.

See *Service Instance Health Check*.

## VMware vCenter as Compute Mode

It is possible to integrate VMware vCenter with Contrail with OpenStack orchestrator, using the vCenter as Compute mode. In the vCenter as compute mode, the vCenter cluster is represented as a compute node under OpenStack.

See *VMWare vCenter Integration with Contrail OpenStack: vCenter as Compute*.

## Ability to Configure PCI-Passthrough and SR-IOV Interface for vCenter Integration

The user can configure PCI pass-through and SR-IOV interfaces.

PCI pass-through is a virtualization technique in which a physical PCI (Peripheral Component Interconnect ) device is directly connected to a virtual machine, bypassing the hypervisor. Drivers in the VM can directly access the PCI device, resulting in a high rate of data transfer.

A single root I/O virtualization (SR-IOV) interface allows a network adapter device to separate access to its resources among various hardware functions.

See *Configuring PCI-Passthrough and SR-IOV Interface for vCenter Integration* .

## Enhancements to Contrail Alerts

Starting with Contrail 3.0 and greater, Contrail alerts are provided on a per-user visible entity (UVE) basis.

Contrail analytics raise or clear alerts using Python-coded rules that examine the contents of the UVE and the configuration of the object. Some rules are built in. Others can be added using Python *stevedore* plugins.

See *Contrail Alerts*.

## Enhancements to the Loadbalancing Feature

Contrail Release 3.0 and later supports new LBaaS features. The provider field specified in the pool configuration determines which loadbalancer drivers are selected. The loadbalancer driver selected is responsible for configuring the external hardware or virtual machine loadbalancer.

Contrail currently supports the following loadbalancer drivers:

- HAProxy
- A10 Networks
- F5 Networks

Starting with Contrail 3.0, the Neutron LBaaS plugin creates required configuration objects (such as pool, VIP, members, and monitor) in the Contrail API server, instead of within the Neutron plugin context, as in previous releases.

This method of configuration has the following benefits:

- Configuration objects can be created in multiple ways: from Neutron, from virtual controller APIs, or from the Contrail UI.
- The loadbalancer driver can make inline calls, such as REST or SUDS, to configure the external loadbalancer device.
- The loadbalancer driver can use Contrail service monitor infrastructure, such as database, logging, and API server.

See *Using Loadbalancers in Contrail 3.0 and Greater*.

## Ability to Configure Virtual Networks for Hub and Spoke Topology

As of Contrail Release 3.0, hub and spoke topology can be used to ensure that virtual machines (VMs) don't communicate with each other directly; their communication is only allowed indirectly by means of a designated hub virtual network. The VMs are configured in spoke VNs.

This is useful for enabling VMs in a spoke VN to communicate by means of a policy or firewall, where the firewall exists in a hub site.

See *Configuring Virtual Networks for Hub and Spoke Topology*.

## Ability to Use Physical Network Functions in Contrail Service Chains

Contrail Release 3.0 and greater supports service appliance-based physical network functions devices (PNFs) in service chains, enabling the creation of service chains that include a combination of virtual network functions (VNFs) and PNFs. The PNFs are also supported with Contrail Device Manager.

See *Using Physical Network Functions in Contrail Service Chains* and *Example: Adding a Physical Network Function Device to a Service Chain*.

## Server Manager Lite Replaces fab Command Provisioning

Server Manager Lite (SM-Lite), is a streamlined version of the Server Manager software that does not include the reimage function.

SM-Lite supports the Server Manager provisioning, monitoring, inventory, and webui functions. SM-Lite is intended to replace fab command provisioning. It allows easy deployment of Contrail provisioning and enables developers to work in isolated environments for Contrail provisioning. SM-Lite eliminates installation and configuration of DHCP, DNS, and Cobbler services. Additionally, SM-Lite installation set up scripts are enhanced to reduce installation time. SM-Lite provides a single command to install SM-Lite and provision a Contrail cluster.

See *Installing and Using Server Manager Lite*.

## Ability to Configure Transport Layer Security-Based XMPP

In the Contrail environment, the Transport Layer Security (TLS) protocol is used for certificate exchange, mutual authentication, and negotiating ciphers to secure the stream from potential tampering and eavesdropping. Starting with Contrail 3.0, Transport Layer Security (TLS)-based XMPP can be used to secure all Extensible Messaging and Presence Protocol (XMPP)-based communication that occurs in the Contrail environment.

Secure XMPP is based on *RFC 6120, Extensible Messaging and Presence Protocol (XMPP): Core*. See *Configuring Transport Layer Security-Based XMPP in Contrail*.

## Support for IPv6 in the Service Chain

In Contrail release 2.22 and earlier, support for IPv6 overlay networks in Contrail is limited to basic routing only.

Contrail release 3.0 and later support for IPv6 overlay networks includes the following:

- Policy, security groups, and flow
- ECMP
- Service chaining

For more information, see *IPv6 Support*.

## Service Chain Route Reorigination

The service chaining feature allows the operator to insert dynamic services to control the traffic between two virtual networks. The service chaining works on a basic rule of next-hop stitching.

Route reorigination can be used for Contrail service chains, enabling the route for the VM in the Right VN to be added to the routing table for the Left VN, with the next hop modified to ensure that the traffic is sent by means of the left interface of the service chain. Service chain route reorigination is accomplished by means of:

- **Route aggregation**

Enables publishing an aggregated route as the service chain route, rather than publishing every route of each VM (/32).

- **Path attribute modification for reoriginated routes**

Enables the operator to control which service chain is used for traffic between two networks when two service chains with identical services are connected between the same two VNs.

- **Control to enable and disable reorigination of the route**

Enables the operator to stop reorigination of a route as the service chain route, for example, when static routes are configured on service VM interfaces.

See *Service Chain Route Reorigination*.

## Generation of Heat Templates

With Contrail Release 3.0, contrail-heat resources and templates are auto-generated, resulting in a number of changes to the heat configuration and use of templates. As a result, the templates from release R2.X are no longer compatible with the new templates.

Use the following link to understand the template changes, learn how to access the new templates, and use the new template configurations.

See [Generating Heat Resources and Templates](#).

## Using Port-Tuples for VM Ports

Contrail can use port-tuples for ports when launching VM services. The user can create ports and bind those ports to a service instance, versus previous versions in which the service monitor daemon used the VM object to bind service instances to ports. and the heat engine knew only about the service instance object. The VM, ports, and similar objects created by the service monitor daemon were not visible to heat.

With the new use of port-tuples, all objects created are visible to the heat-engine and managed directly by heat.

Use the following link to learn about the new object called PortTuple, which is used to contain all the ports of a VM.

See [Using Port Tuples for VM Ports](#).

## Supported Platforms

---

Contrail Networking Release 3.0 is supported on the OpenStack Juno and Kilo releases, on the following operating system versions:

- Ubuntu 14.04.2
- Centos 7.2
- RHOSP7
- vCenter 5.5

- vCenter is limited to Ubuntu 14.04.2 (Linux kernel version: 3.13.0-40-generic).
- vCenter 6.0 is also supported as Beta.

Contrail Cloud Release 3.0 is only supported on Ubuntu 14.04.2, and is no longer supported on Ubuntu 12.04 or Centos 6.x.

Additionally, Openstack Icehouse is no longer supported.

Following is the supported Linux kernel version for each distribution supported on Contrail Release 3.0.

- CentOS 7.1 — Linux kernel version 3.10.0-229.el7
- Ubuntu 14.04.2 — Linux kernel version 3.13.0-40-generic
- Red Hat 7.1 — Linux kernel version 3.10.0-229.el7
- vCenter 5.5 — vRouter VM on Ubuntu 14.04 kernel version 3.13.0-40-generic

## Known Issues

---

This section lists known limitations with this release. Bug numbers are listed and can be researched in [Launchpad.net](https://bugs.launchpad.net/juniperopenstack/r3.0) at <https://bugs.launchpad.net/juniperopenstack/r3.0>.

- 1556532: Unable to add Contrail 2.20 package from Server Manager 3.0.
- 1551229: In the Server Manager Lite UI, the monitoring details are not populated, although the corresponding daemon is running. A workaround is described in the bug.
- 1555319: In the Server Manager Lite UI, when trying to provision a target that has a bond interface, which requires an IP address in the UI, the provision does not complete. When the bond interface is not supported in the UI, the alternative is to configure with JSON.
- 1546613 The fab **add\_vrouter\_node** is missing **nova.conf** parameters on the controller. The user is required to use the command on openstack nodes as indicated.
- 1423813: Contrail DNS could be exploited to launch DDoS attacks. The workaround indicated in this bug to guard against such attacks should be deployed.
- 1551600: Collector hangs in the Zookeeper client. A workaround is specified in the bug.
- 1551405: The upgrade script is not re-entrant. If it fails the first time, then when it runs second time, the updated conf files may get overwritten and services might show as down in the contrail-status and might not work as expected. The workaround is to update the upgrade script when a failure occurs, before it is run the second time.
- 1550888: The **contrail-tor-agent** process of the vrouter node UVE is the controller of TORs. The status of **contrail-tor-agent** connectivity to its TOR is not reflected in its NodeStatus.process\_status data. Consequently, neither contrail-status nor the Contrail UI, will reflect the failure when there is no connection to the TOR. It needs to be manually looked into on the Details page by using the Advanced tab of the corresponding vrouter node.



- 1551050: UI showing BGP peer down alarms for BGPaaS clients. The Monitor > Control nodes incorrectly shows 'BGP peer mismatch' alarms if a BGPaaS object is attached to a VML.
- 1551503: In multi-controller clusters, if there is a control node failure, the memory utilization of the vRouter agent running on the compute that has the BGPaaS VM can grow unchecked, with the aAgent eventually holding 100% of the memory. The workaround is to the, restart vRouter agent.
- 1551576: In multi controller clusters, the BGP peering session between the BGPaaS VM and the control node can sometimes fail to come up after one of the active control nodes goes down.
- 1551107: The following steps are needed for mirroring:
  1. Create a separate virtual network to launch the mirroring service VM.
  2. Disable RPF check for the created virtual network.
- 1550059: The Cassandra database might become corrupted after power cycling the node without shutting down Cassandra.
- 1549160: Active flows are created for intra-VN traffic with random source IP. Source IP validation is not performed for L2 forwarded traffic.
- 1549454: Changes to the service chain in a policy disrupts route leaking for several minutes.
- 1550479: Quotas set in the **api-server** are not reflected in the Contrail UI.
- 1549786: The WebUI is getting logged out if a default project is selected in Monitor Page.
- 1549568: With a DPDK-enabled router, a router crash might occur if SNAT is used with MTU greater than 8k.
- 1547782: With DPDK enabled, the MTU on the vhost0 interface cannot be set higher than 8K.
- 1496609: For a control node to participate properly in high availability, all the control nodes must have a unique priority. When adding a new control node to an already-provisioned high availability-enabled cluster, the uniqueness in the priority across the control node is not automatic.

You need to adjust the values to ensure uniqueness as follows:

  1. Stop the keepalived process using the **service keepalived stop** command
  2. Edit the **/etc/keepalived/keepalived.conf** file in all the control nodes and modify the priority under the **vrrp\_instance INTERNAL\*** and **vrrp\_instance EXTERNAL\*** configuration section, so that all the control nodes have unique values.
  3. Start the keepalived process using the **service keepalived start** command.
- 1495697: When you add a new control node using the **fab install\_new\_contrail** command to a cluster that is already provisioned, there is a possibility that the command might fail due to a timing issue. Even though this command reports failure, it actually does

everything as expected. You can proceed using the **fab join\_cluster** command as the next step for adding a new control node.

- 1465744: Contrail/MX interop when a VM is using SNAT to reach a bare metal server floating IP address. This happens only in cases where a SNAT instance and destination Floating IP address are on the same compute node.
- 1466731: A QFX Series switch does not handle transient duplicate VxLAN IDs for two different VNs. If a VN is deleted and added quickly, the TOR switch may go into a bad state.
- 1484600: When a device is moved from one QFX Series switch to another Series switch, the MAC address is not learned on the switch for a period of up to 12 minutes.
- 1486387: If you configure compute and config services in the same node, you must use the **fab setup\_nova\_aggregate** command after the node is rebooted. If the command is not used, **setup\_nova\_aggregate** will never get executed.
- 1403348: If you attach and then detach a security group, the transparent firewall service interface does not have an internal security group.
- 1447401: On multiple VMs in a Docker cluster, the VMs invariably end up on only one compute node.
- 1455944: When creating Nova instances in Docker containers, the user-data script is not executed.
- 1458794: DNS configuration in Docker container is wrong. A Docker instance does not learn the DNS address provided by the vRouter.
- 1546965: LBaaS and SNAT are not supported with IPv6.
- 1460241: If you create twelve virtual routers attached to a single logical router and then clear the router, Neutron experiences an error.
- 1461791: When servers in a cluster are reimaged with an ESX ISO image, only one server is successfully reimaged, all other servers in that cluster will be re-imaging in a loop.
- 1463622: If you create multiple compute nodes and multiple virtual machines, return traffic from server to client converges on a single label. Eventually, all the flows converge on one VM on each compute node.
- 1465372: If a bare metal server and an SNAT instance are attached to a public network and a packet is sent from the network namespace (netns) instance to the bare metal server, it gets Layer 3 lookups rather than a bridge table lookup.
- 1468420: If you create thousands of virtual machine interfaces and logical interfaces with a thousand virtual networks, and then push the configuration using the device manager, the configuration might get repeatedly added and deleted on the MX Series router.
- 1492979: Broadcast routes are always programmed with the EVPN as the next hop, so even if there is no MX Series router to flood the traffic, it is still programmed in the composite next hop.

The vRouter replicates the traffic for the EVPN next hop and eventually the traffic is discarded. This causes the drop statistics count to increase.

- 1469341: The vCenter setup does not use the svc-monitor. The **contrail-svc-monitor** status needs to be removed from the **contrail-status** command output.
- 1485754: When a virtual network is extended to a physical router, the Device Manager allocates an IP address for the IRB interface. If the virtual network to physical router association is broken, the Device Manager tries to free the allocated IP address. This call fails. As a result, the IP address that was previously allocated is no longer available in the free pool.
- 1551405: Upon upgrade from 2.2x build to 3.0 build, the status of **contrail-analytics-api** might display as down in contrail-status output, and there will not be **contrail-alarm-gen** service status, as in the following:

```
== Contrail Analytics ==
supervisor-analytics: active
contrail-analytics-api initializing (UvePartitions:UVE-Aggregation connection
down)
contrail-analytics-nodemgr active
contrail-collector active
contrail-query-engine active
contrail-snmp-collector active
contrail-topology active
```

The workaround is to create:

**/etc/contrail/supervisord\_analytics\_files/contrail-alarm-gen.ini** and restart supervisor-analytics on all analytics nodes.

## Upgrading Contrail Software from Release 2.21 or Greater to Release 3.0

---

Use the following procedure to upgrade an installation of Contrail software from one release to a more recent release. This procedure is valid for Contrail Release 2.21 and later.



**NOTE:** If you are installing Contrail for the first time, refer to the full documentation and installation instructions in *Installing the Operating System and Contrail Packages*.

Instructions are given for both CentOS and Ubuntu versions. The only Ubuntu versions supported for upgrading are Ubuntu 12.04 and 14.04.2.

To upgrade Contrail software from Contrail Release 2.21 or later:

1. Download the **contrail-install-packages-x.xx-xxx.xxx.noarch.rpm | deb** file from <http://www.juniper.net/support/downloads/?p=contrail#sw> and copy it to the **/tmp** directory on the config node, as follows:

**CentOS :** `scp <id@server>:/path/to/contrail-install-packages-x.xx-xxx.xxx.noarch.rpm /tmp`

**Ubuntu :** `scp <id@server>:/path/to/contrail-install-packages-x.xx-xx~havana_all.deb /tmp`



**NOTE:** The variables **xxx.-xxx** and so on represent the release and build numbers that are present in the name of the installation packages that you download.

2. Install the **contrail-install-packages**, using the correct command for your operating system:

**CentOS:** `yum localinstall /tmp/contrail-install-packages-x.xx-xxx.xxx.noarch.rpm`

**Ubuntu:** `dpkg -i /tmp/contrail-install-packages_x.xx-xxx~icehouse_all.deb`

3. Set up the local repository by running the **setup.sh**:

`cd /opt/contrail/contrail_packages; ./setup.sh`

4. Ensure that the **testbed.py** file that was used to set up the cluster with Contrail is intact in the **/opt/contrail/utils/fabfile/testbeds/** directory.

- Ensure that the **testbed.py** file has been set up with a combined **control\_data** section (required in Contrail Release 1.10 and later).

See *Setting Up the Testbed Definitions File*.

5. In release packages prior to Contrail Release 3.0, the packaged Cassandra version is 1.2.11. In the 3.0 release, the packaged Cassandra version is 2.1.9. Upgrading Cassandra

from 1.2.11 to 2.1.9 is not supported by Cassandra. For more information, refer to [DataStax Upgrade Guide, Cassandra 2.1.x restrictions](#).

Consequently, during the Contrail upgrade procedure (**fab upgrade\_contrail**), the Cassandra SSTables are upgraded, which takes a long time if the Cassandra data is huge (usually because the Contrail Analytics keyspace is huge).

There is an option to minimize upgrade down time by dropping the Contrail Analytics keyspace before the upgrade, by issuing the following fab command:

**fab drop\_analytics\_keyspace**

6. Upgrade the software, using the correct set of commands to match your operating system and vRouter, as described in the following:

Change directory to the **utils** folder:

**cd /opt/contrail/utils; \**

Select the correct upgrade procedure from the following to match your operating system and vRouter. In the following, *<from>* refers to the currently installed release number, such as 2.0, 2.01, 2.1, or 2.2:

*CentOS Upgrade Procedure:*

**fab upgrade\_contrail:<from>,/tmp/contrail-install-packages-x.xx-xxx.xxx.noarch.rpm;**

*Ubuntu 12.04 Procedure:*

**fab upgrade\_contrail:<from>,/tmp/contrail-install-packages-x.xx-xxx-icehouse\_all.deb;**

*Ubuntu 14.04 Upgrade, Two Procedures:*

There are two different upgrade procedures for the upgrade to Contrail Release 3.0, depending on which vRouter (**contrail-vrouter-3.13.0-35-generic** or **contrail-vrouter-dkms**) is installed in your current setup.

In Contrail Release 3.0 and later, the recommended kernel version for an Ubuntu 14.04-based system is 3.13.0-40. Both procedures can use the command **fab upgrade\_kernel\_all** to upgrade the kernel.

**Ubuntu 14.04 Upgrade Procedure For a System With  
contrail-vrouter-3.13.0-35-generic:**

Use the following upgrade procedure for Contrail Release 3.0 systems based on Ubuntu 14.04 with the **contrail-vrouter-3.13.0-35-generic** installed. The command sequence upgrades the kernel version and also reboots the compute nodes when finished.

```
fab install_pkg_all:/tmp/contrail-install-packages-x.xx-xxx~icehouse_all.deb;
```

```
fab migrate_compute_kernel;
```

```
fab upgrade_contrail:<from>,/tmp/contrail-install-packages-x.xx-xxx~icehouse_all.deb;
```

```
fab upgrade_kernel_all;
```

```
fab restart_openstack_compute;
```

**Ubuntu 14.04 Upgrade Procedure For System with contrail-vrouter-dkms:**

Use the following upgrade procedure for Contrail Release 3.0 systems based on Ubuntu 14.04 with **contrail-vrouter-dkms** installed. The command sequence upgrades the kernel version and also reboots the compute nodes when finished.

```
fab upgrade_contrail:  
<from>,/tmp/contrail-install-packages-x.xx-xxx~icehouse_all.deb;
```

All nodes in the cluster can be upgraded to kernel version 3.13.0-40 by using the following **fab** command:

```
fab upgrade_kernel_all
```

7. *(For Contrail Storage option, only.)*

Contrail Storage has its own packages.

To upgrade Contrail Storage, download the file:

```
contrail-storage-packages_x.x-xx*.deb
```

from <http://www.juniper.net/support/downloads/?p=contrail#sw>

and copy it to the **/tmp** directory on the config node, as follows:

```
Ubuntu: scp <id@server>:/path/to/contrail-storage-packages_x.x-xx*.deb /tmp
```



**NOTE:** Use only Icehouse packages (for example, **contrail-storage-packages\_2.0-22~icehouse\_all.deb**) because OpenStack Havana is no longer supported.

---

Use the following statement to upgrade the software:

```
cd /opt/contrail/utlis; \
```

```
Ubuntu: fab
```

```
upgrade_storage:<from>,/tmp/contrail-storage-packages_2.0-22~icehouse_all.deb;
```

## Documentation Feedback

---

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

---

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:  
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

## Revision History

---

December, 2015—Revision 1, Contrail 2.22

October, 2015—Revision 1, Contrail 2.21

August 2015—Revision 1, Contrail 2.20

April 2014—Revision 1, Contrail 1.05

18 March 2014—Revision 1, Contrail 1.04

January 2014—Revision 1, Contrail 1.03

21 October 2013—Revision 1, Contrail 1.02

16 September 2013—Revision 1, Contrail 1.0

Copyright © 2015, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.