

Contrail Release 3.0.2.0 Release Notes

Release 3.0.2.0
June 2016

Contents

Introduction	2
New and Changed Features	2
Support for SR-IOV VF as the Physical Interface of vRouter	2
Sending Flow Messages to the Contrail System Log	3
Beta Support for OpenStack LBaaS v2 APIs	4
New Port for Cassandra Database	4
Server Manager Passwords Changes	5
vCenter as a Compute Notes	5
Heat	6
Additional Platform Support	6
Supported Platforms	6
Known Behavior	6
Resolved Issues	9
Upgrading Contrail Software from Release 2.21 or Greater to Release 3.0.2.0	9
Documentation Feedback	11
Requesting Technical Support	12
Self-Help Online Tools and Resources	12
Opening a Case with JTAC	13
Revision History	13

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 include new features, known issues, resolved items, and upgrade instructions for Contrail Release 3.0.2.0, a maintenance release for Contrail Release 3.0.

For a full description of new features, limitations, and known problems for Contrail Release 3.0, refer to [Release Notes for Contrail Release 3.0](#).

For full documentation of all features, refer to [Contrail Release 3.0, Feature Guide](#).

New and Changed Features

This section lists new features in Contrail Release 3.0.2.0.

- [Support for SR-IOV VF as the Physical Interface of vRouter on page 2](#)
- [Sending Flow Messages to the Contrail System Log on page 3](#)
- [Beta Support for OpenStack LBaaS v2 APIs on page 4](#)
- [New Port for Cassandra Database on page 4](#)
- [Server Manager Passwords Changes on page 5](#)
- [vCenter as a Compute Notes on page 5](#)
- [Heat on page 6](#)
- [Additional Platform Support on page 6](#)

Support for SR-IOV VF as the Physical Interface of vRouter

Support for single root I/O virtualization (SR-IOV) virtual functions (VF) used as the physical router for vRouter is included in this release.

SR-IOV allows a network interface to separate the access to its resources across multiple PCI Express (PCIe) functions. The functions can be physical (PFs) or virtual (VFs).

The Contrail vRouter can use an SR-IOV VF as its physical interface. One VF on a network interface (NIC) can be used by vRouter, while the remaining VFs can be used by virtual machines on the same compute node. It is also possible to create a VLAN interface on a VF, and use that as the physical interface of the vRouter.

Alternatively, VFs from two different interfaces can be bonded together, and that bonded interface can be used as the physical interface of vRouter. It is also possible to create a VLAN on a bonded interface, like the one just described, and then use that bonded interface as the physical interface of vRouter.

To set up VFs for the physical interface of vRouter:

Include the **env.sriov** section in the `testbed.py` file, and use the following steps to define the SR-IOV VFs, so that the VFs are created during the provisioning of the cluster.

1. Create SR-IOV VFs on the compute nodes (**host1** and **host2**, in this example). VFs are usually identified with the following naming scheme: **p6p2_1**, **p6p2_2**, and so on. See the following example:

```
env.sriov = {

    host1 : [ {'interface' : 'p6p2', 'VF' : 7, 'physnets' : ['physnet1']} ],
    host2 : [ {'interface' : 'p6p2', 'VF' : 7, 'physnets' : ['physnet1']} ]

}
```

2. Specify the VF interfaces in the **control_data** section of the `testbed.py` file, with or without a VLAN, so that they can be used by vRouter. See the following example:

```
control_data = {

    host1 : { 'ip' : '10.x.x.100/2x', 'gw' : '10.x.x.254', 'device' : 'p6p2_1' },
    host2 : { 'ip' : '10.x.x.200/2x', 'gw' : '10.x.x.254', 'device' : 'p6p2_2' }

}
```

3. Optionally, for bonded interfaces (**bond0** in this example), specify the VFs in the **bond** section of the `testbed.py` file, with or without a VLAN. See the following example:

```
bond = {

    host1 : { 'name' : 'bond0', 'member' : ['p6p2_4', 'p6p1_5'], 'mode' : 'balance-xor' },
    host2 : { 'name' : 'bond0', 'member' : ['p6p2_2', 'p6p1_3'], 'mode' : 'balance-xor' }

}
```

Sending Flow Messages to the Contrail System Log

The **contrail-vrouter-agent** can be configured to send flow messages and other messages to the system log (syslog). To send flow messages to syslog, configure the following parameters in `/etc/contrail/contrail-vrouter-agent.conf`.

Parameters under the section **DEFAULT**:

- **log_flow=1**—Enables logging of all flow messages.
- **use_syslog=1**—Enables sending of all messages, including flow messages, to syslog.
- **syslog_facility=LOG_LOCAL0**—Enables sending messages from the **contrail-vrouter-agent** to the syslog, using the facility **LOCAL0**. You can configure **LOCAL0** to your required facility.
- **log_level=SYS_INFO**—Changes the logging level of **contrail-vrouter-agent** to **INFO**.

If syslog is enabled, flow messages are NOT sent to Contrail Analytics, because the two destinations are mutually exclusive.

Flow log sampling settings apply the same, regardless of the flow log destination specified. If sampling is enabled, the syslog messages will be sampled using the same rules that would apply to Contrail Analytics. If non-sampled flow data is required, sampling must be disabled by means of configuration settings.

Flow events for termination will include both the appropriate tear down fields and the appropriate set up fields.

The flow messages will be sent to the syslog with a severity of INFO.

The user can configure the remote system log (**rsyslog**) on the compute node to send syslog messages with facility LOCAL0, severity of INFO (and lesser), to the remote syslog server. Messages with higher severity than INFO can be logged to a local file to allow for debugging.

Flow messages appear in the syslog in a format similar to the following log example:

```
May 24 14:40:13 a7s10 contrail-vrouter-agent[29930]: 2016-05-24 Tue 14:40:13:921.098
PDT a7s10 [Thread 139724471654144, Pid 29930]: [SYS_INFO]: FlowLogDataObject:
flowdata= [ [ [ flowuuid = 7ea8bf8f-b827-496e-b93e-7622a0c8eeea direction_ing = 1
sourcevn = default-domain:mock-gen-test:vn8 sourceip = 1.0.0.9 destvn =
default-domain:mock-gen-test:vn58 destip = 1.0.0.59 protocol = 1 sport = -29520 dport =
20315 setup_time = 1464125225556930 bytes = 1035611592 packets = 2024830 diff_bytes
= 27240 diff_packets = 40 ], ] ]
```



NOTE: Several individual flow messages might be packed into a single syslog message for improved efficiency.

Beta Support for OpenStack LBaaS v2 APIs

Contrail Release 3.0.2.0 provides Beta-level support for the OpenStack LBaaS v2 APIs that are available in the Liberty release of OpenStack.

For LbaaS v2, the Contrail controller now aggregates the configuration by provider. For example, if **haproxy** is the provider, the controller generates the configuration for **haproxy** and eliminates the need to send all of the load balancer resources to the **vrouter-agent**; only the generated configuration is sent, as part of the service instance.

New Port for Cassandra Database

In previous versions, the **cassandra_server_list** used port 9160 as the Cassandra database port in configuration files. Starting with Contrail Release 3.0.2.0, the interface for services to the Cassandra database has been changed from Thrift to Cassandra Query Language (CQL). Consequently, the **cassandra_server_list** now uses port 9042 as the Cassandra connection port in the following configuration files:

- **/etc/contrail/contrail-collector.conf**
- **/etc/contrail/contrail-query-engine.conf**
- **/etc/contrail/contrail-analytics-api.conf**

Previous Configuration

```
cassandra_server_list=<ip1>:9160 <ip2>:9160 <ip3>:9160
```

New Configuration

```
cassandra_server_list=<ip1>:9042 <ip2>:9042 <ip3>:9042
```

Server Manager Passwords Changes

In the Server Manager server and cluster parameters are fields that represent the password for a host or a service. If a value for the password field is not explicitly provided, the Server Manager selects a default password.

The behavior of having a hardcoded default password could lead to a security hole. If an explicit password is not defined, an attacker could gain access using the known default passwords.

Starting with Contrail Release 3.0.2.0, a new feature is designed to curb such attacks by autogenerating passwords when the user doesn't explicitly specify the password. This makes the clusters provisioned by Server Manager secure.

The following fields now autogenerate a password whenever an explicit password is not provided.

- Previous Parameters:
 - mysql_root_password
 - keystone_password
 - heat_encryption_key
- New Parameters:
 - mysql:root_password
 - mysql:service_password
 - keystone:admin_password
 - heat_encryption_key

vCenter as a Compute Notes

Although Contrail Release 3.0.2.0 supports OpenStack Juno, Kilo, and Liberty, if you are using vCenter as a Compute, there is support only for Juno and Kilo.



NOTE: Contrail's support for VMware, vCenter as a Compute, leverages the VMware vSphere Distributed Switch (VDS). To use VDS, a customer must obtain a license from VMware.

Heat

Heat Version 1 support for service chains is deprecated, beginning with Contrail Release 3.0. With Release 3.0.2, **contrail-heat** resources and templates are automatically generated, using Heat Version 2 resources. Full details are available at: <https://github.com/Juniper/contrail-heat/wiki>.

Additional Platform Support

Contrail Release 3.0.2.0 adds support for the following platforms:

- OpenStack Liberty for Contrail Networking (no Server Manager provisioning at this time).
- Ubuntu 14.04.04, kernel 3-35-85 generic.

Supported Platforms

Contrail Release 3.0.2.0 is supported on the OpenStack Juno, Kilo, and Liberty RHOSP8 releases, on the following operating system versions:

- Ubuntu 14.04.4
- CentOS 7.2
- Red Hat Enterprise Linux (RHEL) 7.2
- VMware 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.

Following is the supported Linux kernel version for each distribution supported on Contrail Release 3.0.2.0.

- CentOS 7.2—kernel version 3.10.0-327.10.1
- Ubuntu 14.04.4—kernel version 3.13.0-85-generic
- Red Hat 7.2—kernel version 3.10.0-327.10.1
- vCenter 5.5—vRouter VM on Ubuntu 14.04 kernel version 3.13.0-40-generic

Known Behavior

The following are known behaviors in this release of Contrail. Bug numbers are listed and can be researched in [Launchpad](#).

- 1586203 If you are upgrading a Server Manager image and you have added Ubuntu images to the previous Server Manager database, you will need to delete and re-add those images before the new kickstart files will take effect.
- 1546965 An internal server error occurred while creating IPv6 VIP for LBaaS.

- 1544935 Router SNAT is not working for IPv6.
- 1560725 Nova compute failed to connect libvirt on Liberty.
- 1549786 The WebUI is getting logged out if the user selects a default project in Monitor Page.
- 1550612 SR-IOV: When configuring more than 32 VFs per PF, the VM goes into an error state.
- 1465744 The Contrail and MX device interoperability fails when a VM goes by means of SNAT to a bare metal (BMS) FIP.
- 1551408 A service instance delete shouldn't be allowed when port-tuples are attached.
- 1551409 Deleting a port-tuple doesn't remove associated properties from the VMI.
- 1552936 For the service monitor, the high availability mode needs to be set in IIP object parameters.
- 1351979 Updating **allowed_address_pairs** without any value or with the clear action throws an internal server error.
- 1370301 With the health monitor configured, the **lb-member-list** doesn't update when one of the members in the pool goes down.
- 1458794 The DNS configuration in a Docker container is wrong.
- 1461791 In Server Manager, reimage of servers is happening in a loop for ESX ISO, when reimaging a cluster.
- 1463786 For ToR scale, Delete All using the Web UI is failing.
- 1491791 ToR: There are 6 seconds of traffic loss during control node switch over.
- 1547198 There is inconsistency between ifmap and the api-server.
- 1573265 Flows go into and remain in a halt state randomly.
- 1575442 DPDK: The vRouter does not come up with a bond mode (active standby).
- 1576507 BGPaaS: A TCP ACK war occurs on a BGP session after a control node failover or agent restart.
- 1584210 TCP flow setup performance degrades at 24k flows per second.
- 1586246 The flow export rate is much higher than what is configured.
- 1588643 The **ceilometer-api** is not able to connect to **mongo-db**.
- 1496609 For high availability (HA) add or delete node, the keepalived priority configuration for the node should be regenerated.
- 1551502 For vCenter, the testbed.py needs modifications when the customer upgrades from Contrail Release 2.2x to Release 3.x.
- 1423813 The Contrail vDNS has DDOS exposure.
- 1551280 In Kilo, the vMAC is not getting copied in the AAP configuration of a service instance.

- 1538825 Web UI: After an incomplete project deletion and re-add, the UI stopped displaying service instances.
- 1567000 The availability zone is not working as expected in Contrail 3.0 from Horizon.
- 1403348 There is inconsistent behavior when attaching or detaching a security group from a service instance.
- 1412162 With Ubuntu Icehouse and OVSDDB, if a configuration leads to a commit error state, there is no point of recovery.
- 1454813 vCenter: Using the same dvswitch or dv_port group name in a multiple domain controller (DC) setup of vCenter fails.
- 1467028 A vCenter plugin took 2 minutes to establish mastership after a service restart in a 3 cfm setup.
- 1468420 Device Manager scaling: Only partial configurations are applied on an MX device, when pushing 16k FIPs.
- 1468474 A ToR agent switchover results in BUM/ARP traffic loss.
- 1469296 In Device Manager, overlapping subnets are not supported for a BMS and FIP scenario.
- 1492979 ToR-BMS: Broadcast traffic is getting replicated for an invalid EVPN next hop and discarded.
- 1580340 There are Liberty changes needed for vcenter-as-compute.
- 1580520 The python-pyvmomi package is missing.
- 1582116 The supervisord socket files should be in `/var/run` rather than in `/tmp`.
- 1588182 DPDK: Link Aggregation Control Protocol (LACP) does not work on a bond interface on SR-IOV VFs.
- 1332422 A VM can be created on a VN that is admin disabled.
- 1351929 The quota defaults for SG, router, SG rule, and floating ip are not the same as in the stock OpenStack.
- 1352822 Routing works even when the Neutron router attribute **admin_state_up** is set to False.
- 1367097 SNAT VNs that are created with a name `svc-snat-si_*` are not deleted upon deleting an external gateway configuration.
- 1447401 With Docker, VMs are not load balanced across computes.
- 1493687 There are vRouter fragment handling issues and limitations.
- 1548677 A health check failure doesn't withdraw advertised routes, in the case of multiple services in a chain.
- 1544787 There are steps to upgrade the VMDK in an existing setup in VMware.
- 1555772 A non-local service health check is failing.
- 1350460 For a Neutron L3 router, an extra route is not supported.

- 1352657 With Neutron, **max_dns_nameservers** per subnet is not supported.
- 1542552 VxLAN-encapsulated packets are dropped by the agent if an ECMP route exists to the source.
- 1402080 There is unequal distribution across OSDs.
- 1376872 Fab: Times on storage compute nodes are not in sync.
- 1413468 A Glance image download of a volume snapshot fails with a checksum error.

Resolved Issues

You can research limitations that are fixed with this release in Launchpad at <https://goo.gl/74A2bQ>.

Upgrading Contrail Software from Release 2.21 or Greater to Release 3.0.2.0

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 version supported for upgrading is Ubuntu 4.04.2.

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~kilo_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/utls/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 **utls** folder:

```
cd /opt/contrail/utls; \
```

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 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-3.13.0-40-generic** or **contrail-vrouter-dkms**) is installed in your current setup.

In Contrail Release 3.0.2.0 and later, the recommended kernel version for an Ubuntu 14.04-based system is 3.13.0-85. 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-3.13.0-40-generic:

Use the following upgrade procedure for Contrail Release 3.0 systems based on Ubuntu 14.04 with the **contrail-vrouter-3.13.0-40-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~kilo_all.deb;

fab migrate_compute_kernel;

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

All nodes in the cluster can be upgraded to kernel version 3.13.0-85 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
```

Use the following statement to upgrade the software:

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

```
Ubuntu: fab
```

```
upgrade_storage:<from>,/tmp/contrail-storage-packages_x.x.x-xx~kilo_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. 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

Copyright © 2016, 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.