

Contrail Release 3.0.3.0 Release Notes

Release 3.0.3.0
September 2016

Contents

Introduction	2
New and Changed Features	2
Role- and Resource-Based Access Control	2
Secured Access for Contrail Analytics API	2
Passwords Do Not Display in Logs	3
Alarm Severity Updates	3
Supported Platforms	3
Known Behavior	4
Resolved Issues	4
Upgrading Contrail Software from Release 2.21 or Later to Release 3.0.3.0	5
Documentation Feedback	7
Requesting Technical Support	8
Self-Help Online Tools and Resources	8
Opening a Case with JTAC	9
Revision History	9

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 Network Functions Virtualization (NFV) use cases.

These release notes include new features, known issues, resolved items, and upgrade instructions for Contrail Release 3.0.3.0, 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 the [Release Notes for Contrail Release 3.0](#).

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

New and Changed Features

This section lists new features in Contrail Release 3.0.3.0:

- [Role- and Resource-Based Access Control on page 2](#)
- [Secured Access for Contrail Analytics API on page 2](#)
- [Passwords Do Not Display in Logs on page 3](#)
- [Alarm Severity Updates on page 3](#)

Role- and Resource-Based Access Control

This release provides role and resource-based access control (RBAC) to Contrail APIs and objects.

The RBAC implementation relies on user credentials obtained from Keystone from a token present in an API request. Credentials include user, role, tenant and domain information. API-level access is controlled by a list of rules. The attachment points for the rules are **global-system-config**, domain, and project. Resource-level access is controlled by permissions embedded in the object.

See [Role- and Resource-Based Access Control](#).

Secured Access for Contrail Analytics API

This release provides Contrail Analytics API access for the cloud-admin user only. Based on the user role, **contrail-analytics-api** allows access only for the **cloud-admin** user and reject the request for other users. The **contrail-analytics-api** provides access without an authorization token for users of local analytics nodes, such as **contrail-logs**, **contrail-stats**, and **contrail-flows** scripts.

See [Role- and Resource-Based Access Control for the Contrail Analytics API](#).

Passwords Do Not Display in Logs

For security, Contrail system logs do not display passwords.

Alarm Severity Updates

Previously, the severity of an alarm ranged from 0 (highest) through 7 (lowest). Starting with this release, alarms have the following severity:

- 0 — Critical
- 1 — Major
- 2 — Minor

Supported Platforms

Contrail Release 3.0.3.0 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.



NOTE: vCener-as-compute is *NOT* supported on Liberty.

Following is the supported Linux kernel version for each distribution supported on Contrail Release 3.0.3.0:

- 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



NOTE: vCenter-as-compute is *NOT* supported on Liberty.

Always use the recommended kernel version with Contrail nodes. If the kernel version of your Ubuntu system is different from the required version, the following Fabric task installs the required version, as an upgrade or as a downgrade:

```
cd /opt/contrail/utils; fab upgrade_kernel_all
```

Known Behavior

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

- 1480501: For Server Manager, with high availability configuration, storage provision failure occurs due to wrong port 5005 in `/usr/bin/ceph-rest-api` service.
- 1575649: On a standalone Server Manager Web UI, clicking on **Alarms** displays a `ECONNREFUSED` error.
- 1600020: While setting up vCenter-as-Compute, the **fab add_vcenter_compute_node** step finishes successfully but displays the following warning message:

setup-vcenter-plugin: error: unrecognized arguments: --keystone_version v2.0

This causes incomplete programming of the vCenter compute node.

- 1620928: Contrail 3.0.3 includes a new qemu version (2.3) for OpenStack Kilo. When upgrading to 3.0.3 from earlier releases using **fab** commands, the qemu version is not upgraded. However, a fresh install of Contrail 3.0.3 will install the newer qemu version.
- 1622754: OpenStack administrator must restrict launch of a VM in Nova policy.json based on user project and role to prevent read-only users from launching a VM.
- 1623695: User should create **network-ipam** in their own tenant configuration instead of using the default **network-ipam** for which the user doesn't have permissions.
- 1624148: Service instance automatically created by the system on behalf of a user will not be visible in the UI.
- 1626761: If a cluster is upgraded from a contrail release without barbican support to 3.0.3.0, for example, when upgrading from releases before 3.0.2.0 to 3.0.3.0, in order to use barbican service, execute the `/opt/contrail/bin/contrail-keystone-setup.sh` script once after upgrade on the OpenStack node.
- 1627203: In a 3.0.2.0 cluster, if SRIOV is configured in any of the computes, upgrade to 3.0.3.0 and make the following change in `/etc/nova/nova.conf` (in all OpenStack nodes) and restart the nova-scheduler service:
 - Replace **scheduler_default_filters = PciPassthroughFilter** with the following:
scheduler_default_filters = RetryFilter, AvailabilityZoneFilter, RamFilter, DiskFilter, ComputeFilter, ComputeCapabilitiesFilter, ImagePropertiesFilter, ServerGroupAntiAffinityFilter, ServerGroupAffinityFilter, PciPassthroughFilter

Resolved Issues

You can research limitations that are fixed with this release in Launchpad at <http://bit.ly/2cRMBGE>.

Upgrading Contrail Software from Release 2.21 or Later to Release 3.0.3.0

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 version supported for upgrading is Ubuntu 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~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/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 14.04 Upgrade, Two Procedures:

There are two different upgrade procedures for the upgrade to Contrail Release 3.0.3.0, 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. For both procedures, the command **fab upgrade_kernel_all** installs the correct kernel version, as an upgrade or as a downgrade.

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 a 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

October 2016—Revision 2, Contrail 3.0.3.0

September 2016—Revision 1, Contrail 3.0.3.0

Copyright © 2017, 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.