

Contrail Release 3.1 Release Notes

Release 3.1
August 2016

Contents

Introduction	2
New and Changed Features	2
Service Chain Version 2 with Port Tuple	2
Support for BGP as a Service Version 2	3
Quality of Service in Contrail	3
Multiqueue Virtio Interfaces in Virtual Machines	4
Contrail Global Controller	4
Support for OpenStack Load -Balancing as a Service Version 2.0 APIs	4
Role- and Resource-Based Access Control	4
Support for Heat Version 2 Resources and Port Tuple	5
Analytics Updates	5
Layer 3 Service Chaining for vCenter-Only	5
Support for Service Chain Health-Check	6
Using Gateway Mode to Support Remote Instances (Experimental)	6
Keystone Version 3	6
HTTPS Access to APIs	7
Enhancements to Transport Layer Security-Based XMPP	7
Passwords Do Not Display in Logs	7
Supported Platforms	7
Known Behavior	8
Resolved Issues	11
Deprecated Items	11
Additional Steps for CentOS 7.2 Installation	11
Upgrading Contrail Software	12
Documentation Feedback	14
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 3.1 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/contrail3.1/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 3.1. A brief description of each new feature is included.

- [Service Chain Version 2 with Port Tuple on page 2](#)
- [Support for BGP as a Service Version 2 on page 3](#)
- [Quality of Service in Contrail on page 3](#)
- [Multiqueue Virtio Interfaces in Virtual Machines on page 4](#)
- [Contrail Global Controller on page 4](#)
- [Support for OpenStack Load -Balancing as a Service Version 2.0 APIs on page 4](#)
- [Role- and Resource-Based Access Control on page 4](#)
- [Support for Heat Version 2 Resources and Port Tuple on page 5](#)
- [Analytics Updates on page 5](#)
- [Layer 3 Service Chaining for vCenter-Only on page 5](#)
- [Support for Service Chain Health-Check on page 6](#)
- [Using Gateway Mode to Support Remote Instances \(Experimental\) on page 6](#)
- [Keystone Version 3 on page 6](#)
- [HTTPS Access to APIs on page 7](#)
- [Enhancements to Transport Layer Security-Based XMPP on page 7](#)
- [Passwords Do Not Display in Logs on page 7](#)

Service Chain Version 2 with Port Tuple

This release of Contrail provides a port-tuple object for use with service instances. In previous versions of Contrail, when a service instance is created for a virtual machine (VM)-based service, the service monitor creates one or more VM objects and creates a port for each VM object. Each VM object is a placeholder for binding a service instance to a port.

Using the VM object as a placeholder doesn't add value beyond binding information between the service instance object and the port objects. By using a port-tuple object, the service instance can be linked directly to the port objects, eliminating the need to create a VM object. With a port-tuple object, the user can create ports and pass the port information when creating a service instance. This simplifies the implementation of service instance VM objects, and also allows integration with Heat templates.

With Contrail service templates Version 2, the user can create ports and bind them to a VM-based service instance, by means of a port-tuple object. All objects created with the Version 2 service template are visible to the Contrail Heat engine, and are managed by Heat.

See [Service Chain Version 2 with Port Tuple](#).

Support for BGP as a Service Version 2

With this release, the following features have been added to BGPaaS:

- All BGPaaS sessions are configured to have bidirectional exchange of routes.
- If inet6 routes are being advertised to the tenant VM, they are advertised with the IPv6 subnet's default gateway address as the BGP next hop.
- If multiple tenant VMs in the same virtual network have BGPaaS sessions and they use eBGP, standard loop prevention rules prevent routes advertised by one tenant VM from being advertised to other tenant VMs.

See [BGP as a Service in Contrail Release 3.1](#).

Quality of Service in Contrail

Quality of service (QoS) in networking provides the ability to control reliability, bandwidth, latency, and other traffic management features. Network traffic can be marked with QoS bits (DSCP, 802.1p, and MPLS EXP) that intermediate network switches and routers can use to provide service guarantees.

The Contrail QoS model has the following features:

- All packet forwarding devices, such as vRouter and the gateway, combine to form a system.
- Interfaces to the system are the ports from which the system sends and receives packets, such as tap interfaces and physical ports.
- Fabric interfaces are where the overlay traffic is tunneled.
- QoS is applied at the ingress to the system, for example, upon traffic from the interfaces to the fabric.

DPDK compute nodes do not support QoS rate-limiting.

See [Quality of Service in Contrail](#).

Multiqueue Virtio Interfaces in Virtual Machines

OpenStack Liberty supports the ability to create VMs with multiple queues on their virtio interfaces. Virtio is a Linux platform for I/O virtualization, providing a common set of I/O virtualization drivers. Multiqueue virtio is an approach that enables the processing of packet sending and receiving to be scaled to the number of available virtual CPUs (vCPUs) of a guest, through the use of multiple queues.

See [Multiqueue Virtio Interfaces in Virtual Machines](#).

Contrail Global Controller

Contrail Release 3.1 provides support for a global controller. The global controller provides a seamless controller experience across multiple regions in a cloud environment by helping manage multiple OpenStack installations, each having its own Keystone, Neutron, Nova, and so on. High availability is provided by using separate failure domains by region.

To handle the resource burdens when connecting and configuring servers and virtual machines over multiple, different regions, the global controller has the following main responsibilities:

- Resource identifier management
- Multiple location resource provisioning

See [Contrail Global Controller](#).

Support for OpenStack Load -Balancing as a Service Version 2.0 APIs

The OpenStack Load -Balancing as a Service (LBaaS) Version 2.0 extension enables tenants to manage load balancers for VMs, for example, load-balancing client traffic from a network to application services, such as VMs, on the same network. The LBaaS Version 2.0 extension is used to create and manage load balancers, listeners, pools, members of a pool, and health monitors, and to view the status of a resource.

For LBaaS v2.0, the Contrail controller 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.

For more information about OpenStack v2.0 APIs, refer to the section *LBaaS 2.0 (STABLE) (lbaas, loadbalancers, listeners, health_monitors, pools, members)*, at <http://developer.openstack.org/api-ref-networking-v2-ext.html>.

LBaaS v2.0 also allows users to listen to multiple ports for the same virtual IP, by decoupling the virtual IP address from the port.

See [Support for OpenStack LBaaS Version 2.0 APIs](#).

Role- and Resource-Based Access Control

Contrail Release 3.1 and later provides role- and resource-based access control (RBAC) with API operation-level access control.

The RBAC implementation relies on user credentials obtained from Keystone from a token present in an API request. Credentials include user, role, tenant, domain names, and corresponding UUIDs.

API-level access is controlled by a list of rules. The attachment points for the rules are domain and project. Resource-level access is controlled by permissions embedded in the object.

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

Support for Heat Version 2 Resources and Port Tuple

With Contrail service templates Version 2, the user can create ports and bind them to a virtual machine (VM)-based service instance, by means of a port-tuple object. All objects created with the Version 2 service template are directly visible to the Contrail Heat engine, and are directly managed by Heat.

Starting with Contrail Release 3.0.2, Contrail Heat resources and templates are autogenerated from the Contrail schema, using Heat Version 2 resources. Contrail Release 3.0.2 is the minimum required version for using Heat with Contrail in 3.x releases. The Contrail Heat Version 2 resources are of the following hierarchy:

OS::ContrailV2::<ResourceName>.

See [Using the Contrail Heat Template](#).

Analytics Updates

This release includes the following updates to Contrail analytics:

- User configuration of alarms, based on UVEs.
- User-defined log statistic.
- Node memory and CPU information added for all node types.
- Role- and resource-based access control for the Contrail analytics API.

See:

- [User Configuration for Analytics Alarms and Log Statistics](#)
- [Node Memory and CPU Information](#)
- [Role- and Resource-Based Access Control for the Contrail Analytics API](#)

Layer 3 Service Chaining for vCenter-Only

Service chaining for Layer 3 services for vCenter-only systems is supported, only by means of port-tuples.

This feature allows the user to configure service chaining Version 2 in the vCenter-only mode of operation. Both in-network and in-network-nat service chains are supported. Not supported is service chain Version 1.

Support for Service Chain Health-Check

Monitoring and checking the health of a service chain or a service VM is supported. The following modes are supported for service monitoring for the service instance health check:

- **link-local**—A local check for the service VM on the vRouter where the VM is running. In this case, the source IP of the packet is the service chain IP.
- **end-to-end**—A remote address or URL is provided for a service health check through a chain of services. In end-to-end service health check, the destination of the health check probe is allowed to be outside the service instance. However, the health check probe must be reachable through the interface of the service instance where the health check is attached. The end-to-end health check probe is transmitted all the way to the actual destination outside the service instance. The response to that probe is received and processed by the service health check to evaluate the status.

Restrictions include:

- This check is applicable for a chain where the services are not scaled out.
- When this mode is configured, a new health check IP is allocated and used as the source IP of the packet.
- The health check IP is allocated per **virtual-machine-interface** of the service VM where the health check is attached.
- The agent relies on the **service-health-check-ip** flag to use as the source IP.

See [Service Instance Health Check](#).

Using Gateway Mode to Support Remote Instances (Experimental)

Extending virtual instances running non-Openstack clusters or extending bare metal servers into Contrail virtual networks can be achieved using OVSDDB protocol.

Additionally, starting with Contrail Release 3.1, an experimental mode has been added to enable you to configure a Contrail compute node to run in gateway mode to support remote instances.

See [Using Gateway Mode to Support Remote Instances](#).

Keystone Version 3

Beta support is provided for Keystone Version 3 in Contrail Cloud with OpenStack Mitaka.

To enable Keystone V3, add the following configuration to **testbed.py** during fab setup:

```
env.keystone = {  
    'version': 'v3'  
}
```

Keystone V3 has the following features in Contrail Cloud:

- Enables multi-domain support in Horizon. Non-default domains can be created and a user can log in to Horizon in a non-default domain.



NOTE: The default domain is also the cloud-admin domain. An **admin** user is added to the default domain with an **admin** role.

- Keystone is configured to use **policy.v3cloudsample.json** as the policy file.
- Enables multi-domain support in Contrail UI.
- Various OpenStack services, such as Nova, Neutron, Glance, Heat, and the like, use Keystone V3 endpoints to talk to Keystone.
- Various Contrail services, such as API server, use Keystone V3 endpoints to talk to Keystone.

HTTPS Access to APIs

HTTPS access to REST APIs is supported. For more information on Fabric (fab) provisioning, see

<https://github.com/Juniper/contrail-fabric-utils/wiki/Provisioning-Keystone,-apiserver-and-neutron-with-SSL>.

Enhancements to Transport Layer Security-Based XMPP

TLS-based XMPP is supported on the Server Manager in Contrail Release 3.1. For more information, see

<https://bugs.launchpad.net/juniperopenstack/trunk/+bug/1522597/comments/28>.

Passwords Do Not Display in Logs

For security, Contrail system logs do not display passwords.

Supported Platforms

Contrail Release 3.1 is supported on the OpenStack Kilo and Liberty releases, on the following operating system versions:

- Ubuntu 14.04.4
- CentOS 7.2
- Red Hat Enterprise Linux (RHEL) 7.2 (RHOSP8)
- VMware vCenter 5.5, 6.0

Contrail Release 3.1 is also supported on OpenStack Mitaka on Ubuntu 14.04.4.

Following is the supported Linux kernel version for each distribution supported on Contrail Release 3.1.

- 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—Ubuntu 14.04.4 kernel version 3.13.0-85-generic



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

Known Behavior

This section lists known limitations with this release. Bug numbers are listed and can be researched in [Launchpad.net](https://launchpad.net) at <https://goo.gl/5OkS7i>.

- 1613159 Using Server Manager with a high availability setup on OpenStack Mitaka, provisioning can get stuck at config_started, due to a Keystone conflict among Openstack nodes. A workaround is provided in the bug text.
- 1611451 Service chain IPv6 doesn't follow IPv6 AAP-IP when AAP has both IPv4 and IPv6 addresses.
- 1610813 Server Manager provisioning of a high availability cluster hangs at u'openstack' due to Heat encryption key- related issue.
- 1610671 The AlarmAndList rule is not working.
- 1610489 For vCenter-only setup, fab upgrade_contrail from 2.21.2 to 3.1.0.0 fails @ upgrade_config.
- 1609768 In Contrail WebUI, setting global share permissions doesn't work while creating a VN.
- 1609683 Creation of service chain with Heat fails with authorization failure in OpenStack Mitaka.
- 1609154 On a cluster with a large number of VMIs, selecting all projects and all networks logs out the user.
- 1607701 WebUI icons are not loading in Internet Explorer 11.
- 1607485 For vCenter-only setup, the service svc-monitor failed after reboot of controller.
- 1606448 Fabric-based QoS configuration is not supported. No remarking is done while forwarding the received tunneled packet to a virtual instance interface.
- 1605466 Using Keystone v3, domains are not shown under the identity tab in Horizon.
- 1605409 The config node in a high availability cluster lost its management IP and took an external VIP after using setup_storage_interface.
- 1603666 Using RBAC, for a user with only 'read' permission, the Nova boot command was allowed.
- 1603337 With Server Manager, contrail-discovery failed in one of the config nodes. A workaround is provided in the bug text.

- 1595885 Server Manager needs provision support for Keystone V3.
- 1592125 Connection setup latency shoots up as the flow table nears full capacity.
- 1590643 The internal_vip is being set instead of contrail_internal_vip in /etc/cinder/cinder.conf on openstack nodes.
- 1589082 For a Server Manager upgrade, provision fails with a conflict of mysql root password.
- 1588643 Sometimes the ceilometer-api is not able to connect to mongo-db.
- 1588182 For DPDK, Link Aggregation Control Protocol (LACP) does not work on A bond interface on SR-IOV VFs.
- 1586246 The flow export rate is much higher than what is configured.
- 1584224 All TCP connections are dropped after 10 mins of sustained 25k flows per second.
- 1584210 The TCP flow setup performance degrades at 24k flows per second.
- 1580520 Using OpenStack Liberty, the python-pyvmmomi package is missing. This affects only the vCenter-as-compute feature.
- 1576507 Using BGPaaS, observe a TCP ACK war on a BGP session after control node failover and agent restart.
- 1575442 Using DPDK, the vRouter does not come up with bond mode active standby.
- 1560725 Using OpenStack Liberty, Nova compute failed to connect libvirt.
- 1551502 Using vCenter, the testbed.py needs modifications when upgrading from a 2.2x release to Release 3.x.
- 1551409 Deleting a port-tuple doesn't remove associated properties from the VMI.
- 1551408 Service instance delete shouldn't be allowed when port-tuples are attached.
- 1551280 A virtual MAC address is not getting copied in the allowed_address_pairs configuration of a service instance.
- 1550612 Using SR-IOV, and configuring more than 32 virtual functions per physical function, the VM is going to an error state.
- 1548801 The Discovery server shows the XMPP server usage count as 3 for a vrouter-agent.
- 1544935 The IPv6 router SNAT is not working for IPv6.
- 1543108 The XMPP server is not doing load balancing and auto load balancing.
- 1538825 After an Incomplete project deletion and readdition, the UI stopped displaying service instances.
- 1518137 After ESXi maintenance mode recovery, upon powerup of 200 guest VMs, can observe that a virtual network IP is not assigned from Contrail DHCP.
- 1496609 For high availability add or delete a node, the keepalived priority configuration for the node should be regenerated.

- 1493687 There are some vRouter fragments handling issues and limitations.
- 1480501 For Server Manager, with high availability configuration, a storage provision failure occurred due to wrong port 5005 in /usr/bin/ceph-rest-api.
- 1469296 Using Device Manager, overlapping subnets are not supported for a bare metal server and FIP scenario.
- 1468474 Upon ToR agent switchover there is BUM and ARP traffic loss.
- 1468420 Using Device Manager, only partial configurations are applied on an MX when pushing 16k FIPs.
- 1465744 Contrail and MX interoperability failing when a VM is going via SNAT to bare metal server FIP.
- 1458794 The DNS configuration in a Docker container is wrong.
- 1454813 With vCenter, using the same dvswitch or dv_port group name in a multiple DC setup vCenter fails.
- 1447401 Using Docker, VMs are not load balanced across compute nodes.
- 1423813 Contrail vDNS: DNS DDOS exposure.
- 1412162 Using OVSDDB, if the configuration leads to a commit error state, there is no way to recover.
- 1412162 For OVSDDB, if configuration leads to commit error state there is no point of recovery.
- 1385740 Network policies with multiple subnets are not handled by the Contrail UI Network Policy editor.
- 1372360 Creating an lb-pool should not set the status of the pool to ACTIVE.
- 1369725 When a FIP is associated with a VIP, clicking on the instance details of the FIP shows an error.
- 1369688 Some LBaaS Neutron commands are not working.
- 1366292 The redis-server is not restarted automatically upon kill.
- 1352822 Routing works even when the Neutron router attribute admin_state_up is set to False.
- 1352657 Using Neutron, max_dns_nameservers per subnet is not supported.
- 1351979 Updating allowed_address_pairs without any value or with the action clear results in internal server error.
- 1351929 The quota defaults for security group, router, security group rule, and floating IP are not the same as in stock OpenStack.
- 1351144 Contrail has a divergence in behavior from Neutron with regard to floating IPs and Layer 3 routers.
- 1350460 On a Neutron Layer 3 router, an extra route is not supported.

Resolved Issues

You can research limitations that are resolved with this release in Launchpad at:

<https://goo.gl/xwWd3f>.

Deprecated Items

The following features are supported for the final time in Release 3.1 and will not be supported in future releases.

- Heat support for service chaining Version 1.
- LBaaS F5 API is supported only on OpenStack Kilo and only up to Contrail Release 3.1.
- LBaaS Version 1 APIs are not supported in OpenStack Mitaka and later.
- Keystone Version 2 will not be supported beyond Contrail Release 3.1.

Additional Steps for CentOS 7.2 Installation

The default kernel version in CentOS 7.2 is 3.10.0-327. The recommended kernel version is 3.10.0-327.10.1. During installation of Contrail on CentOS 7.2, use the following command to change the kernel version to 3.10.0-327.10.1, before using the **install_contrail** command:

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

Upgrading Contrail Software

Use the following procedure to upgrade an installation of Contrail software from one release to a more recent release. This procedure is valid for upgrading Contrail Release 3.0.0.0 and later to Contrail Release 3.1.2.0.



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 14.04.4.

To upgrade Contrail software from Contrail Releases 3.0.0.0 and later to Release 3.1.2.0:

1. Download the **contrail-install-packages-x.x.x.x-xx 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.x.x.x-xxnoarch.rpm /tmp`

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



NOTE: The variables **x.x.x.x-xx** 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.x.x.x-xx.noarch.rpm`

Ubuntu: `dpkg -i /tmp/contrail-install-packages_x.x.x.x-xx~_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.

See *Setting Up the Testbed Definitions File*.

5. The **fab upgrade_contrail** command sequence enables upgrading Cassandra from 2.1.9 to 2.2.5. 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 3.0.3.2, 3.1.1.0, and so on:

CentOS Upgrade Procedure:

fab upgrade_contrail:<from>,/tmp/contrail-install-packages-x.x.x.x-xxnoarch.rpm;

Ubuntu 14.04 Upgrade, Two Procedures:

There are two different upgrade procedures for the upgrade to Contrail Release 3.1.2.0, depending on which vRouter (**3.13.0-X-generic** or **contrail-vrouter-dkms**) is installed in your current setup.

In Contrail Release 3.1.2.0, the recommended kernel version for an Ubuntu 14.04-based system is 3.13.0-100. 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-X-generic:**

Use the following upgrade procedure for Contrail systems based on Ubuntu 14.04 without the **contrail-vrouter-3.13.0-100-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.x.x.x-xx~<openstack_version>_all.deb;

fab migrate_compute_kernel;

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

All nodes in the cluster can be upgraded to kernel version 3.13.0-100 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.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.x.x-xx*.deb /tmp
```

Use the following statement to upgrade the software:

```
cd /opt/contrail/utils; \
```

```
Ubuntu: fab
```

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