Contrail Release 5.1 Release Notes

Release 5.1
April 2019

Contents

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 5.1 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 https://www.juniper.net/documentation/en_US/contrail5.1/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 5.1. A brief description of each new feature is included.

Contrail All-In-One Cluster

Starting in Contrail Networking Release 5.1, Contrail supports deploying Contrail Command and All-In-One (AIO) Contrail Cluster using a single docker command without providing any configuration files. For more information, see Deploying Contrail Command and Contrail All-In-One Cluster.

BGPaaS Peer Zone Selection

Starting with Contrail Networking Release 5.1, to better support high availability (HA) architectures, BGPaaS supports control node zone selection, with options available to configure BGPaaS control node zone peers. This capability enables you to set up primary and secondary control node zones, which can have one or more control nodes.

For more information, see BGP as a Service.

Deploying Enterprise Multicloud with Contrail Command

Starting in Contrail Release 5.1, Contrail supports provisioning multi cloud with the Contrail Command UI. Contrail supports provisioning of Microsoft Azure and Amazon Web Services (AWS).

For more information, see Deploying Enterprise Multicloud with Contrail Command .

Installing Contrail with Mesos

Starting in Contrail Release 5.1, Contrail supports running Contrail with Mesosphere DC/OS. Contrail overlay and non-overlay network virtualization features are available in Apache Mesos environment.

For more information, see Installing Contrail with Mesos.

Importing Contrail Cluster data to Contrail Command by using TripleO

Starting in Contrail Release 5.1, Contrail supports the importing of Contrail Cluster data to Contrail Command server when provisioned using *OSPDirector/TripleO* Life Cycle Manager for RedHat OpenStack Orchestration.

For more information, see Importing Contrail Cluster Data using Contrail Command.

Importing Contrail Cluster data to Contrail Command by using Mesos

Starting in Contrail Release 5.1, Contrail supports the importing of Contrail Cluster data to Contrail Command server by provisioning *Mesos* orchestrator.

For more information, see Importing Contrail Cluster Data using Contrail Command.

Importing Contrail Cluster data to Contrail Command by using VMware vCenter

Starting in Contrail Release 5.1, Contrail supports the importing of Contrail Cluster data to Contrail Command server by using VMware vCenter orchestrator.

For more information, see Importing Contrail Cluster Data using Contrail Command.

Layer 3 PNF Service Chaining of Inter-LR Traffic

Starting with Contrail Release 5.1, Contrail provides layer 3 physical network functions (PNF) support to create service chains for inter-LR (logical router) traffic. Contrail Release 5.1 automates configuration of QFX10000 and SRX devices to allow movement of inter-LR traffic between bare metal servers through layer 3 PNF.

For more information, see Creating Layer 3 PNF Service Chains for Inter-LR Traffic.

Adding a New Compute Node to an Existing Containerized Contrail Cluster.

Starting in Contrail Release 5.1, Contrail supports the adding of a new compute node to the existing Contrail OpenStack cluster by configuring the **instances.yaml** file as well as by using the Contrail Command UI.

For more information, see Adding a New Compute Node to Existing Containerized Contrail Cluster.

Policy Generation Feature

The policy generation feature in Contrail Release 5.1 automates the creation of security policies based on observed traffic flows. When using policy generation, vRouter observes and forwards traffic between selected applications without enforcing any policies. Draft security policies are created based on observed inter and intra-application traffic and are called auto-generated policies. You can review and accept the auto-generated policies before enforcing them.

For more information, see Policy Generation.

PostgreSQL Support

Starting with Release 5.1, Contrail Controller supports PostgreSQL only. In earlier releases, Contrail Controller supported both MySQL and PostgreSQL.

For more information, see Installing Contrail Command.

Support for Edge Routed Bridging

Starting with Contrail Release 5.1, the edge-routed bridging (ERB) for QFX series switches feature configures the inter-VN unicast traffic routing to occur at the leaf (ToR) switches in an IP CLOS with underlay connectivity topology. The ERB feature introduces the **ERB-UCAST-Gateway** and **CRB-MCAST-Gateway** roles in release 5.1. ERB is supported on the following devices running only Junos OS release 18.1R3:

- QFX5110-48S
- QFX5110-32Q
- QFX10002-36Q
- QFX10002-72Q
- QFX10008
- QFX10016

For more information, see Edge Routed Bridging for QFX Series Switches.

Routing Policies Match on Extended Communities

Contrail Release 5.1 supports extended communities on the import routing policy function. Release 5.1 allows import routing policy terms to match on extended communities and import routing policy actions to add, set, and remove extended communities. Filtering routes based on extended communities prevent advertising unnecessary service interface and static routes from the control node.

For more information, see Creating a Routing Policy With External Communities in Contrail Command.

Support for OpenShift 3.11

Contrail Release 5.1 supports the installation of a standalone Red Hat OpenShift Container Platform version 3.11 cluster using ansible-openshift as the deployment tool.

For more information, see Installing a Standalone Red Hat OpenShift Container Platform 3.11 Cluster Using OpenShift Ansible Deployer.

Support for Kubernetes 1.12

Contrail Release 5.1 supports the following Kubernetes release 1.12 network policy features:

- Egress support for network policy
- Classless Interdomain Routing (CIDR) selector support for egress and ingress network policies

- Contrail-ansible-deployer provisioning

For more information, see Kubernetes Updates.

Auto-provisioning of IPtable Filtering Rules on Contrail Nodes

Contrail nodes are automatically configured with locally enforced firewall rules allowing access only to Contrail services.

Certificate Lifecycle Management Using Red Hat Identity Management

Contrail Release 5.1 supports using Transport Layer Security (TLS) with RHOSP to perform lifecycle management, including renewal, expiration, and revocation, of certificates using Red Hat Identity Management (IdM). Because IdM uses fully qualified domain names (FQDNs) to manage endpoints instead of IP addresses, Contrail services are also enhanced to use FQDNs.

For more information, see .

Support for Controlling the Maximum Flow Scale Supported on a Virtual Machine Interface

Starting in Contrail Release 5.1, you can configure the maximum number of flows (**max-flows**) on a virtual machine interface (VMI) and in a virtual network. In releases prior to Contrail Release 5.1, you can control the number of flows only at the virtual machine-level.

When you configure **max-flows** at the virtual network-level, the configuration is applied to every VMI within the virtual network. When you configure **max-flows** at the virtual machine interface-level, the configuration applies only to that VMI.

End to end Data Center ZTP and Contrail cluster provisioning using Contrail Command

Starting in Release 5.1, Contrail supports provisioning of Contrail Fabric with end to end ZTP using Contrail Command UI.

For more information, see Provisioning fabric devices with end to end ZTP.

Support for Data Center Interconnect

Starting in Contrail Release 5.1, you can automate data center interconnect (DCI) of two different data centers. Multiple tenants connected to a logical router in a data center can exchange routes with tenants connected to a logical router in another data center.

For more information, see Creating Data Center Interconnect.

Support for Deployment of a Standalone Kubernetes Cluster Using Contrail Command

Starting with Contrail Release 5.1, the Contrail Command UI supports the deployment of a standalone Kubernetes cluster. You can select the Kubernetes orchestrator type in the Contrail Command UI when deploying a cluster.

For more information, see Installing Standalone Kubernetes Contrail Cluster using the Contrail Command UI.

Support for AppFormix in Contrail Command

Starting with Contrail release 5.1, the following AppFormix features are supported in Contrail Command:

- Installing AppFormix using Contrail Command
- Configuring AppFormix Alarms using Contrail Command
- Configuring Instances in AppFormix
- Viewing Cluster Node Details and Metric Values

For more information, see the *Contrail Installation and Configuration Guide* and the *Contrail Analytics and Troubleshooting Guide*.

Support for Multiple Network Interfaces in Kubernetes

Starting in Contrail Release 5.1, you can allocate multiple network interfaces (multi-net) to a container managed by Kubernetes to enable the container to connect to multiple networks. You can specify the networks the container can connect to. This capability can be leveraged to apply service chaining to containerized network functions.

For more information, see Multiple Network Interfaces for Containers.

Support for Prefix-Based Fat Flow

Starting in Contrail Release 5.1, fat flows has been extended to prefix length. With the introduction of prefix-based fat flow, Contrail supports mask processing where you can create flows based on a group of subscribers. This provides a higher level of flow aggregation than single IP address-based fat flow by grouping all the flows for all the end devices sharing the same subnet into a common fat flow.

For more information, see Fat Flows.

Enable TLS Communication Between Analytics and Kafka

Starting with Contrail Release 5.1, Transport Layer Security (TLS) communication is enabled between Kafka brokers and Contrail analytics processes. **contrail-collector** and **contrail-alarm-gen** connects to Kafka for UVE processing. The User-Visible Entity (UVE) mechanism is used to aggregate and send the status information.

Support for Route Reflectors

Contrail Release 5.1 supports Route Reflector (RR) functionality in the Control node for for Internal Border Gateway Protocol (iBGP) peers. Route reflection is a BGP feature that enables BGP routers to acquire route information from one iBGP router and reflect or advertise the information to other iBGP peers in the same autonomous system (AS).

For more information, see Route Reflector Support in Contrail Control Node.

Support for Contrail on Windows Operating System

Contrail Release 5.1 supports overlay network virtualization for Windows Docker containers. Windows server 2016 supports containerization using Docker containers and Contrail components such as vRouter agent and the vRouter kernel module have been ported and qualified to run on Windows Server 2016. A Docker CNM plugin is added to process requests from the Docker daemon when a user creates or removes a network or an endpoint.

To install Contrail for Windows, you must have Windows Server 2016 and Docker EE 17.06.

For more information, see Understanding Contrail Deployment on Windows.

Generic Device Operations Commands

Contrail Release 5.1 and later enables you to run generic device operations commands on the devices in a network from the Contrail Command UI. You can run a specific generic device operations command on multiple devices at a time. A job template is defined in Contrail Command for each generic device operations command.

You can select a maximum of 20 devices at a time and run a generic device operational command to view information about those devices.

For more information, see Generic Device Operational Commands In Contrail Command.

Support for EVPN Multicast Type 6 Selective Multicast Ethernet Tag Routes

Contrail Release 5.1 supports EVPN Type 6 selective multicast Ethernet tag (SMET) route to selectively send or receive traffic based on the presence or absence of active receivers on a compute node. The EVPN Type-6 SMET route helps build and use multicast trees selectively on a per **<*, G>** basis.

Currently, all broadcast, unknown unicast, multicast (BUM) traffic is carried over the inclusive multicast ethernet tag (IMET) routes. This results in flooding all compute nodes irrespective of whether an active receiver is present or not on each of those compute-nodes.

For more information, see Support for EVPN Type 6 Selective Multicast Ethernet Tag Route

Support for MPLS L3VPN InterAS Option C

Contrail Release 5.1 supports L3VPN inter AS Option C, which is used to interconnect multi-AS backbones as described in RFC 4364.

For more information, see Support for L3VPN Inter AS Option C.

Support for Virtual Port Group

Starting with Contrail Release 5.1, you can create virtual port groups (VPG). A VPG is a group of one or more physical interfaces attached to one or more virtual machine interfaces (VMI). Each VMI object corresponds to a VLAN ID and is attached to a Virtual Network. You can create new virtual port group either when you create a virtual network

or by navigating to **Overlay > Virtual Port Group > Create Virtual Port Group** from Contrail Command.

For more information, see Configuring Virtual Port Group.

Supported Platforms Contrail 5.1

Table 1 on page 11 lists the orchestrator releases and the corresponding operating systems and kernel versions supported by Contrail Release 5.1.

Table 1: Supported Platforms

Contrail Release	Orchestrator Release	Deployment Tool	Operating System, Kernel, and Key Components Version
Contrail Release 5.1	Kubernetes 1.12	Ansible	• CentOS 7.6—Linux Kernel Version 3.10.0-957 Docker version: 18.06.0-ce
	OpenShift 3.11	Ansible	• RHEL7.6—Linux Kernel Version 3.10.0-957.12.1
	OpenStack Rocky	Ansible	• CentOS 7.6—Linux Kernel Version 3.10.0-957 Ansible version: 2.5.2 Docker version: 18.03.1-ce
		Ansible	• Ubuntu-16.04.5 - Linux Kernel Version 4.15.0-45-generic
		Ansible	• Ubuntu-18.04.2 - Linux Kernel Version 4.15.0-46-generic
	OpenStack Queens	Ansible	• CentOS 7.6—Linux Kernel Version 3.10.0-957 Ansible version: 2.5.2 Docker version: 18.03.1-ce
		Juju Charms	• Ubuntu 18.04.2—Linux Kernel Version 4.15.0-48-generic MaaS Version: 2.4.2
	OpenStack Ocata	Ansible	• CentOS 7.6—Linux Kernel Version 3.10.0-957 Ansible version: 2.5.2 Docker version: 18.06.0-ce
		Helm	• Ubuntu 16.04.3—Linux Kernel Version 4.4.0-112-generic Docker version: 17.03.2-ce Helm version: 2.7.2 Kubernetes version: 1.9.3
	Red Hat OpenStack Platform 13	RHOSP 13 director	• RHEL7.6—Linux Kernel Version 3.10.0-957.12.1
	VMware vCenter 6.7	Ansible	• ESX version 6.5 CentOS VM version running vRouter: CentOS 7.5—Linux Kernel Version 3.10.0-862.9.1
	None	Ansible	Windows 2016
	Mesos	Ansible	CentOS 7.6—Linux Kernel Version 3.10.0-957

Table 2 on page 12 lists the AppFormix release to use with Contrail Release 5.1.

Table 2: AppFormix Release

Contrail Release	AppFormix Release
Contrail Release 5.1	2.9.10

Known Behavior

This section lists known limitations with this release.

- CEM-5441 On a freshly provisioned Contrail + Appformix cluster, to enable the live data streaming the web sockets between Contrail UI and Appformix server need to be established. In R5.1 this need to be triggered once by login to the Appformix UI.
- CEM-5402 Though the APIs allow 4 byte ASN, the backend code only support 2 byte ASN. Do not use 4 byte ASN in API integrations.
- CEM-5400 Configuring both tagged and un-tagged vlan in Contrail Fabric VPG is not supported.
- CEM-5334 The multi cloud gateway on the cloud will allow traffic from only a vRouter or Controller nodes to reach to the On-Prem cluster. So in case of deployment where the On-Prem open stack cluster need to be extended to the K8s cluster on the cloud, the k8s master must be defined in one of the vRouters on the cloud.
- CEM-5287 Multicloud Provision may fail in add_tunnel routes, if the initial subcluster extension is rerun .If the initial subcluster extension fails user need to delete the subcluster and extend it again.
- CEM-5284 Cloud Compute/vrouter nodes will not be listed in the cluster-nodes/compute node page, all nodes/computes will be listed in the servers page
- CEM-5283 For all-in-one cluster, where vrouter and openstack roles exist on the same node, "enable_haproxy" must not be enabled (set to 'yes') in the ansible yaml file. This is because of multicast traffic restrictions when vrouter is running.
- CEM-5141/CEM-4503 For deleting compute nodes, the UI workflow will not work. Instead, update the instances.yaml with “ENABLE_DESTROY: True” and “roles:” (leave it empty) and run the following playbooks.

```
ansible-playbook  -i inventory/ -e orchestrator=openstack --tags nova
playbooks/install_openstack.yml
ansible-playbook  -i inventory/ -e orchestrator=openstack
playbooks/install_contrail.yml
```

For example:

```
global_configuration:
    ENABLE_DESTROY: True
...
...
instances:
...
```

```
...
  srvr5:
    provider: bms
    ip: 19x.xxx.x.55
    roles:
...
...
```

- CEM-5290 While adding AWS cloud to an already existing public cloud with Azure, the AWS credentials need to be manually added in Contrail-Command container. Perform the following steps to add AWS credentials manually.

  1. Log in to the contrail_command container.

     ```
     docker exec -it contrail_command bash
     export CONTRAIL_CONFIG=/etc/contrail/contrail.yml
     ```

  2. Get the public cloud UUID.

     ```
     contrailcli list cloud
     ```

  3. Use the following command to get the cloud_user_refs for the <*public_cloud_uuid*> public cloud UUID.

     ```
     contrailcli show cloud <public_cloud_uuid> | grep -A 4 cloud_user_refs
     cloud_user_refs:

         uuid: <cloud_user_ref>
         to:
         sol4-public-cloud-user-<cloud_user_ref>
         href: ""
     ```

  4. Replace the UUID in the **cloud_user.yaml** with the <*cloud_user_ref*> UUID of your cluster.

     ```
     cat <<EOF > cloud_user.yaml
     resources:

         data:
         uuid: “<cloud_user_ref>”
         aws_credential:
         access_key: XXXXXXX
         secret_key: YYYYYYYYYYYY
         kind: cloud_user
         operation: UPDATE
         EOF
     ```

  5. Use the following command to sync the **cloud_user.yaml** file.

     ```
     contrailcli sync cloud_user.yaml
     ```

  6. Verify that the credentials are updated.

     ```
     contrailcli show cloud_user <cloud_user_ref>
     ```


NOTE: The instance name or the hostname must be in lowercase so that it is consistent across all components.

- CEM-5282 When Azure cloud is extended to On-Prem cluster running on RHEL hosts, contrail-status shows vRouters running on Azure as initializing, though the services are up. This is due to the Red Hat issue https://access.redhat.com/solutions/2766251.
- CEM-5043 VNI update on a LR doesnt update the RouteTable. Workaround is to delete the LogicalRouter and create a new LogicalRouter with the new VNI.
- CEM-5042 Adding new subnet on an already provisioned VPC is not supported. If all the subnets are added during initial bringup of VPC, nodes can be added incrementally to the subnets anytime.
- CEM-5041 Provisioning of Region or VPC objects only on the cloud without any nodes is not supported. Add atleast one node while provisioning Region/VPC.
- CEM-5024 Current multi cloud provisioning does not enable the On-prem TOR to exchange public cloud subnets with the On-Prem controllers. The user need to add static routes on the controllers to all the public cloud subnets.
- CEM-4943 After deleting and reprovisioning public cloud infra, though the nodes get deleted from the cloud, the API server and Kubernetes will have stale entries for the deleted objects. To clean up the stale entries, run the following housekeeping scripts:

  1. Log in to the command container.
  2. Navigate to the **contrail-multi-cloud** folder.

     ```
     cd /usr/share/contrail/contrail-multi-cloud/
     ```

  3. Run the following script.

     ```
     TF_STATE=/root/contrail-multi-cloud/terraform.tfstate
     INVENTORY=inventories/inventory.yml
     TOPOLOGY=/root/contrail-multi-cloud/topology.yml ./housekeeper.sh
     ```

     NOTE: If you run the script after provisioning, ensure that TF_STATE is the backup file. For example:

     ```
     TF_STATE=/root/contrail-multi-cloud/terraform.tfstate.backup
     INVENTORY=inventories/inventory.yml
     TOPOLOGY=/root/contrail-multi-cloud/topology.yml ./housekeeper.sh
     ```

- CEM-4941 The multicloud gateway on the public cloud cannot be shared across different subnets. Each subnet must have its own gateway.
- CEM-4865 Provisioning of Contrail Controllers on public cloud is not supported. Controllers need to be provisioned On-prem.

- CEM-4862 The cloud security objects associated with the underlay fabric in cloud cannot be configured with port range or CIDR.
- CEM-4381 Contrail Fabric device manager tasks can fail if one or more Contrail API servers is down. Contrail-status on the Contrail config nodes can be used to determine if this situation occur.
- CEM-4370 After creating a PNF Service Instance, the fields like PNF eBGP ASN*, RP IP Address, PNF Left BGP Peer ASN*, Left Service VLAN*, PNF Right BGP Peer ASN* ,Right Service VLAN* cannot be modified. If there is a need to modify these values, delete and re-create the Service Instance with intended values.
- CEM-4190 IPtables rules are not updated on MC-GW nodes. As a workaround, you must configure IPtables on the on-premise MC-GW nodes with INPUT and FORWARD and default ACCEPT policy.
- CEM-3959 BMS movement across TORs is not supported. To move BMS across TORs the whole VPG need to be moved. That means if there are more than one BMS associated to one VPG, and one of the BMS need to be moved, the whole VPG need to be deleted and re-configured as per the new association.
- CEM-3324 Users cannot provision Contrail Cluster entirely in Public cloud. Contrail Cluster need to be On-Prem and vRouters can be extended to public cloud.
- JCB-204796 In a Helm-based provisioned cluster, VM launch fails if MariaDB replication is set to >1.
- JCB-202874 After deleting a vRouter chart with DPDK, the NICS do not rebind to the host in Helm.
- JCB-190956 While creating ironic-provision, service address in the subnet must be pointing to openstack ironic node ip/kolla internal vip.
- JCB-187320 On a DPDK compute **vif list –rate** core-dumps with traffic.
- JCB-187287 High Availability provisioning of Kubernetes master is not supported.
- JCB-186493 When a snapshot of an active VM fails, shutdown the VM before generating the snapshot.
- JCB-184837 After provisioning Contrail by using a Helm-based provisioned cluster, restart nova-compute container.
- JCB-184776 When the vRouter receives the head fragment of an ICMPv6 packet, the head fragment is immediately enqueued to the assembler. The flow is created as hold flow and then trapped to the agent. If fragments corresponding to this head fragment are already in the assembler or if new fragments arrive immediately after the head fragment, the assembler releases them to flow module. Fragments get enqueued in the hold queue if agent does not write flow action by the time the assembler releases fragments to the flow module. A maximum of three fragments are enqueued in the hold queue at a time. The remaining fragments are dropped from the assembler to the flow module.

  As a workaround, the head fragment is enqueued to assembler only after flow action is written by agent. If the flow is already present in non-hold state, it is immediately enqueued to assembler.

- JCB-177787 In DPDK vRouter use cases such as SNAT and LBaaS that require netns, jumbo MTU cannot be set. Maximum MTU allowed: <=1500.
- JCB-177541 When you receive an error message during Kolla provisioning, rerunning the code will not work. In order for the provisioning to work, restart provisioning from scratch.
- JCB-171466 Metadata SSL works only in HA deployment mode.
- JCB-163773 A false alarm for config service is generated when **config** and **configdb** services are installed on different nodes. Ignore the false alarm.
- JCB-162927 SR-IOV with DPDK co-existence deployment is not supported using contrail-helm-deployer.

Deprecated Items

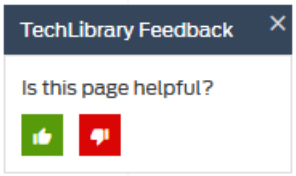
The following feature has been deprecated in Contrail Release 5.1.

- Contrail Global Controller

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 system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide 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 https://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: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- 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 https://support.juniper.net/support/requesting-support/.

Revision History

April 2019—Revision 1, Contrail 5.1

