

Contrail Service Orchestration Release Notes

Release 4.0.2
11 January 2019
Revision 5

These Release Notes accompany Release 4.0.2 of Juniper Networks® Contrail Service Orchestration (CSO). These Release Notes contain installation and upgrade information, and describe new and changed features, limitations, and known and resolved issues in the software.

Contents

| | |
|--|----|
| Introduction | 3 |
| Installation and Upgrade | 4 |
| Software Downloads | 5 |
| Installation Instructions | 6 |
| Software Installation Requirements for NFX Series Network Services | |
| Platform | 6 |
| Upgrade Instructions | 7 |
| Installation and Upgrade Limitations | 7 |
| Post-Installation Instructions | 8 |
| New and Changed Features in Contrail Service Orchestration Release 4.0.2 | 8 |
| Servers, Software, and Network Devices Tested | 8 |
| Hardware, Software, and Virtual Machine Requirements for CSO | 9 |
| VNFs Supported | 9 |
| Licensing | 9 |
| Accessing the CSO GUIs | 10 |
| Known Behavior | 10 |
| AWS Spoke | 11 |
| Policy Deployment | 11 |
| SD-WAN | 12 |
| Security Management | 12 |
| Site and Tenant Workflow | 12 |
| Topology | 13 |
| User Interface | 14 |
| General | 14 |

| | |
|--|----|
| Known Issues | 16 |
| AWS Spoke | 17 |
| CSO HA | 17 |
| SD-WAN | 24 |
| Security Management | 25 |
| Site and Tenant Workflow | 26 |
| General | 29 |
| Resolved Issues | 38 |
| Documentation Updates | 41 |
| Documentation Feedback | 41 |
| Requesting Technical Support | 41 |
| Self-Help Online Tools and Resources | 42 |
| Creating a Service Request with JTAC | 42 |
| Revision History | 42 |

Introduction

Juniper Networks Contrail Service Orchestration (CSO) transforms traditional branch networks, offering opportunities for high flexibility of the network, rapid introduction of new services, automation of network administration, and cost savings. The solution supports both Juniper Networks and third-party virtualized network functions (VNFs) that network providers use to create network services.

CSO Release 4.0.2 is a secure software-defined WAN (SD-WAN) solution that builds on the capabilities of CSO Release 4.0.0 and the Cloud CPE solution. The following are the highlights of the features available in Release 4.0.2:

- Secure OAM redundancy
- IPsec tunnel encryption
- PKI certificates
- PPPoE over ADSL or VDSL links

CSO can be implemented by service providers to offer network services to their customers or by Enterprise IT departments in a campus and branch environment. In these release notes, service providers and Enterprise IT departments are called *service providers*, and the consumers of their services are called *customers*.

The solution offers the following deployment models:

- Cloud CPE distributed deployment Model (*distributed deployment*)

In the distributed deployment, customers access network services on a CPE device, located at a customer's site. These sites are called *on-premise sites* in these release notes.

Sites can be configured as one of the following types:

- Hybrid WAN
- SD-WAN

In a distributed deployment:

- Network Service Orchestrator, together with Network Service Controller, provides ETSI-compliant management of the life cycle of network service instances.
 - Network Service Controller provides the VIM.
 - The CPE device provides the NFV infrastructure.
- Cloud CPE centralized deployment Model (*centralized deployment*)

In a centralized deployment, customers access network services in a service provider's cloud. Sites that access network services in this way are called *cloud sites* in these release notes.

In this deployment, CSO uses the following components for the NFV environment:

- Network Service Orchestrator provides ETSI-compliant management of the life cycle of network service instances.
- Contrail Cloud Platform provides the underlying software-defined networking (SDN), NFV infrastructure (NFVI), and the virtualized infrastructure manager (VIM).

CSO can be deployed in three deployment types—small, medium, or large.

[Table 1 on page 4](#) shows the number of sites and VNFs supported for each environment.

Table 1: Number of Sites and VNFs Supported

| Deployment Type | Number of VNFs Supported for a Centralized Deployment | Number of Sites and VNFs Supported for a Distributed Deployment | Number of Sites Supported for an SD-WAN Deployment | |
|-----------------|---|---|--|-----------------|
| | | | Hub and Spoke Sites | Full Mesh Sites |
| Small | 10 VNFs | Up to 450, 2 VNFs per site | Up to 450 | Up to 100 |
| Medium | 100 VNFs, 20 VNFs per Contrail compute node | Up to 3500, 2 VNFs per site | Up to 3500 | Up to 200 |
| Large | 500 VNFs, 20 VNFs per Contrail compute node | Up to 5000, 2 VNFs per site | Up to 5000 | Up to 200 |

Installation and Upgrade

From CSO Release 4.0.0 onward, you can install CSO using a new GUI-based installer as well as through the existing CLI installer.



NOTE:

- When you install or upgrade CSO by using the CLI, ensure that you save the passwords for each infrastructure component when they are displayed on the console because these passwords are encrypted and are not displayed again.

In addition, during the installation, ensure that you save the Administration Portal password that is displayed on the console. For the upgrade, you must log in using the password configured for the previously installed version of CSO.

- If you are using the GUI installer, after the installation is successful, click the [View all IP addresses and passwords](#) link to view all the IP addresses used by CSO and the passwords for various CSO components.

Ensure that you save the passwords for each CSO component (the *cspadmin* password, used for the Administration Portal login, is the most important) because these passwords are not displayed again.

- [Software Downloads](#)
- [Installation Instructions](#)

- [Software Installation Requirements for NFX Series Network Services Platform](#)
- [Upgrade Instructions](#)
- [Installation and Upgrade Limitations](#)
- [Post-Installation Instructions](#)

Software Downloads

[Table 2 on page 5](#) displays the supported versions and download links for CSO Release 4.0.2 and associated software components. We recommend that you use the CSO Downloader to download and install CSO.

Table 2: CSO and Associated Software Components

| Product | Supported Version | Download Link |
|---|-------------------------------|--|
| CSO Downloader (available for Windows, MacOS, and Linux Desktop versions) | 4.0.2 | https://www.juniper.net/support/downloads/?p=cso |
| Contrail Service Orchestration | 4.0.2 | https://www.juniper.net/support/downloads/?p=cso |
| Juniper Identity Management Service (JIMS) | 1.1.1R1 | Pre-bundled with CSO and also available here: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/75619.html |
| Contrail Analytics | 4.1.1.0-130 | Pre-bundled with CSO |
| Contrail Cloud Platform | 3.2.5 | https://webdownload.juniper.net/swdl/dl/secure/site/1/record/69888.html |
| NFX150 CPE device | Junos OS Release 18.2X85D10 | <ul style="list-style-type: none"> • Install Package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83605.html • Install Media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83606.html |
| NFX250 CPE device | Junos OS Release 15.1X53-D492 | <ul style="list-style-type: none"> • Install Package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83615.html • Install Media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83617.html |

Table 2: CSO and Associated Software Components (continued)

| Product | Supported Version | Download Link |
|------------------------|-------------------------------|---|
| SRX Series CPE device | Junos OS Release 15.1X49-D145 | <ul style="list-style-type: none"> SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory Services Gateway (SRX550M): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83527.html SRX1500: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83529.html SRX1500 (USB): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83531.html SRX1500 (PXE): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83532.html SRX4100, SRX4200: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83528.html SRX4100, SRX4200 (USB): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83530.html SRX4100, SRX4200 (PXE): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83533.html |
| vSRX | Junos OS Release 15.1X49-D145 | <ul style="list-style-type: none"> vSRX (Compressed tar file (TGZ) for upgrade): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83534.html vSRX (KVM appliance): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83537.html vSRX (Hyper-V image): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83538.html vSRX (VMware appliance with SCSI virtual disk (.ova)): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83536.html vSRX (VMware appliance with IDE virtual disk (.ova)): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/83535.html |
| MX Series (hub device) | Junos OS Release 16.1R5 | https://www.juniper.net/support/downloads/ |

Installation Instructions

A full-version installer is available for CSO Release 4.0.2, which can be used for small, medium, and large deployments. For more information, follow the instructions in the [Installation and Upgrade Guide](#) or the README file that is included with the software installation package.



NOTE: The physical servers on which you install CSO must have Internet access to download the libvirt packages. After the packages are downloaded, you do not need Internet access for the rest of the CSO installation.

Software Installation Requirements for NFX Series Network Services Platform

When you set up a distributed deployment with an NFX150 or an NFX250 device, you must use Administration Portal or the CSO API to:

1. Upload the software image to CSO.

2. Specify this image as the boot image when you configure activation data.

For more information, see https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/nfx-series/product/.

Upgrade Instructions



NOTE: You can upgrade to CSO Release 4.0.2 from CSO Release 3.3.1 or Release 4.0.1.

If your installed version of CSO is not Release 4.0.1 or 3.3.1 then you must perform a fresh installation of CSO Release 4.0.2.

If your installed version is CSO Release 3.3.1 or Release 4.0.1, you can use a script (`upgrade.sh`) to directly upgrade to CSO Release 4.0.2. If the upgrade is unsuccessful, you can roll back to CSO Release 3.3.1 or Release 4.0.1 respectively.



NOTE: Before you run the `upgrade.sh` script for upgrading a medium deployment running Release 4.0.1 to Release 4.0.2, complete the following steps:

1. `tar -xvzf Contrail_Service_Orchestration_4.0.2.tar.gz`
2. `cd Contrail_Service_Orchestration_4.0.2/`
3. `sed -i "79 s/^/#/" scripts/setup_assist_upgrade.py`

For more information, see *Upgrading Contrail Service Orchestration Overview* in the [Installation and Upgrade Guide](#).

Installation and Upgrade Limitations

- For SD-WAN deployments, CPE devices behind NAT are supported only for Internet links.
- If the Kubernetes minion node in the central or regional microservices virtual machine (VM) goes down, the pods on the minion node are moved to another Kubernetes minion node. When you bring the minion node back up, the pods do not automatically rebalance across the nodes.
- The VM on which the virtual route reflector (VRR) is installed supports only one management interface.

Post-Installation Instructions

- After you successfully install CSO, you must configure SMTP settings—After you log in for the first time to the CSO GUI, you must configure the SMTP settings for your deployment on the SMTP Settings page (**Administration > SMTP**).
- Accessing GUIs—We recommend that you use Google Chrome version 60 or later to access the CSO GUIs. For more information, see *Accessing the Contrail Services Orchestration GUIs* in the Deployment Guide.

New and Changed Features in Contrail Service Orchestration Release 4.0.2

This section describes the new features or enhancements to existing features in Contrail Service Orchestration (CSO) Release 4.0.2. For new and changed features in CSO Release 4.0.0, see the CSO 4.0.0 Release Notes at

https://www.juniper.net/documentation/en_US/cso4.0/information-products/pathway-pages/4.0/index.html.

- **CHAP authentication support for PPPoE**—From Release 4.0.2 onward, Contrail Service Orchestration enables you to choose CHAP authentication for PPPoE. You can now choose either PAP or CHAP as the authentication protocol for PPPoE when you configure a site. PPPoE is available only on ADSL and VDSL links and in previous releases supported only PAP authentication.
- **ZTP of NFX250 over ADSL and VDSL links**—From Release 4.0.2 onward, Contrail Service Orchestration supports ZTP of NFX250 devices with static and DHCP-based addressing over ADSL and VDSL links. The staging script (`dsl-pre-staging.tgz`) performs the configuration based on input YAML and configures JDM, JCP, and GWR for provisioning ADSL and VDSL links. After this, ZTP can be done over the link.



NOTE: In CSO Release 4.0.2, ZTP is not supported with PPPoE over ADSL and VDSL links.

- **MX Series routers as cloud hub**—From Release 4.0.2, Contrail Service Orchestration supports MX Series routers as cloud hub devices.
- **Ability to specify the supported platform while uploading a device image**—From Release 4.0.2, Contrail Service Orchestration enables you to specify the supported device when you upload a device image. This field is not mandatory. However, information provided in this field is useful in identifying the right image while upgrading physical SRX family devices during the Site Upgrade workflow.

Servers, Software, and Network Devices Tested

From CSO Release 4.0.0 onward, the information in this section is moved to the *Hardware and Software Required for Contrail Service Orchestration* topic in the *Contrail Service Orchestration Installation and Upgrade Guide*.

Hardware, Software, and Virtual Machine Requirements for CSO

From CSO Release 4.0.0 onward, the information in this section is moved to the *Minimum Requirements for Servers and VMs* topic in the *Contrail Service Orchestration Installation and Upgrade Guide*.

VNFs Supported

CSO supports the Juniper Networks and third-party VNFs listed in [Table 3 on page 9](#).

Table 3: VNFs Supported by Contrail Service Orchestration

| VNF Name | Version | Network Functions Supported | Deployment Model Support | Element Management System Support |
|---|---------------------------------|---|--|--|
| Juniper Networks vSRX | vSRX KVM Appliance 15.1X49-D145 | <ul style="list-style-type: none"> Network Address Translation (NAT) Demonstration version of Deep Packet Inspection (DPI) Firewall Unified threat management (UTM) | <ul style="list-style-type: none"> Centralized deployment Hybrid WAN and SD-WAN deployments supports NAT, firewall, and UTM. | Element Management System (EMS) microservice, which is included with CSO |
| LxCIPtable (a free, third party VNF based on Linux IP tables) | 14.04 | <ul style="list-style-type: none"> NAT Firewall | Centralized deployment | EMS microservice |
| Cisco Cloud Services Router 1000V Series (CSR-1000V) | 3.15.0 | Firewall | Centralized deployment | Junos Space Network Management Platform |
| Riverbed SteelHead | 9.2.0 | WAN optimization | Hybrid WAN deployment—NFX250 and NFX150 platforms. | EMS microservice |
| Fortinet | 5.6.3 | Firewall | Hybrid WAN and SD-WAN deployments—NFX250 and NFX150 platforms. | EMS microservice |
| Single-legged Ubuntu | 16.04 | Firewall | Hybrid WAN and SD-WAN deployments—NFX250 and NFX150 platforms. | EMS microservice |

Licensing

You must have licenses to download and use the Juniper Networks CSO. When you order licenses, you receive the information that you need to download and use CSO. If you did not order the licenses, contact your account team or Juniper Networks Customer Care for assistance.

The CSO licensing model depends on whether you use a centralized or distributed deployment:

- For a centralized deployment, you need licenses for Network Service Orchestrator and for Contrail Cloud Platform. You can either purchase both types of licenses in one Cloud CPE MANO package or you can purchase each type of license individually.

You also need licenses for:

- Junos OS software for the MX Series router, EX Series switch, and QFX Series switch in the Contrail Cloud Platform.
 - VNFs that you deploy.
 - (Optional) Licenses for Junos Space Network Management Platform, if you deploy VNFs that require this EMS.
- For a distributed deployment, Juniper Networks has introduced bundled licenses in addition to the a la carte (existing) licenses. The SD-WAN bundle license, which includes hardware and software licenses, can be purchased as subscription or perpetual licenses.

An SD-WAN bundle includes licenses for hardware (SRX Series and NFX Series), Junos OS, SD-WAN features, and CSO for orchestration and management.

The licenses for Junos OS software and hardware for the MX Series router is not included as part of the SD-WAN bundle and must be purchased separately.

Accessing the CSO GUIs



NOTE: We recommend that you use Google Chrome Version 60 or later to access the CSO GUIs.

From CSO Release 4.0.0 onward, the information in this section is moved to *Accessing the Contrail Services Orchestration GUIs* topic in the *CSO Deployment Guide*.

Known Behavior

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks CSO Release 4.0.2.

- [AWS Spoke](#)
- [Policy Deployment](#)
- [SD-WAN](#)
- [Security Management](#)
- [Site and Tenant Workflow](#)
- [Topology](#)
- [User Interface](#)
- [General](#)

AWS Spoke

- When an AWS spoke site is being provisioned and the vSRX instance is coming up, all traffic from the LAN and WAN subnets (configured during site creation) is stopped for 16–30 minutes. After the device is activated and if intent-based policies are configured, the traffic flows as configured.
- The cloud formation template includes a new route table to forward traffic to the vSRX device. If you have configured manual routing between your subnets and VMs, then the new route table replaces the manual routing with only one route forwarding the traffic to the vSRX device.
- The current supported Junos OS release for the AWS spoke is Junos OS Release 15.1X49.D145. When a new qualified image is posted in AWS marketplace, the procedure to update the Amazon Machine Image (AMI) ID is as follows:
 1. Log in Administration Portal.
 2. Select **Resources > Device Templates**.
The Device Template page appears.
 3. Select **vSRX_AWS_SDWAN_Endpoint_option_1**.
 4. Select **Edit Device Template > Template Settings**.
The Template Settings page appears.
 5. Modify the image ID to the AMI ID for your region.
 6. Click **Save**.
 7. Proceed with the workflow for the cloud formation template in AWS.
- When you create a cloud spoke site, the default link fields and backup link fields are not applicable.

Policy Deployment

- An SD-WAN policy deployment is successful even if there is no matching WAN link meeting the SLA. This is expected behavior and is done so that when a WAN link matching the SLA becomes available, traffic is routed through that link.
- The policy intents defined for a firewall or an SD-WAN policy must not have conflicts with other policy intents in that policy because such conflicts lead to inconsistent behavior. For example:
 - You cannot define an SD-WAN policy with one policy intent for application X and SLA profile S-1 and another policy intent for application X and SLA profile S-2.

- You cannot define two firewall policy intents with the same source and destination endpoints but one with action Allow and another with action Deny.

SD-WAN

- On the WAN tab of the *Site-Name* page, the link metrics graph displays aggregated data. Therefore, in cases where the aggregation interval overlaps between source and destination link data, the link metrics graph displays incorrect data.
- If the SD-WAN mode is **Real-Time Optimized** and a path switch is triggered because a link goes down, sometimes the link switch event displayed in the CSO GUI does not contain the SLA violation metric details.
- On the SD-WAN Events page, when you mouse over the **Reason** field of link switch events, sometimes **Above Target** is displayed instead of the absolute SLA metric value for very large values (for example, for an SLA metric value that is 100 times the target value).
- When an SD-WAN policy is deployed and a high rate of traffic flows through the CPE device, this might lead to network congestion and introduce delays or cause traffic. However, even though an SLA violation is reported, the traffic does not switch to a different link.
- In device redundancy mode, when you reboot a node, the device fails to generate a few system logs. Because a few system logs are not generated, the link switch event in CSO displays the source interface same as the destination interface.
- Sometimes duplicate link switch events are displayed on the Link Switch Events page.

Security Management

- Intrusion prevention system (IPS) is not supported. Therefore, in the IPS report, the attack name from the IPS signatures is displayed as UNKNOWN.
- SSL Proxy is not supported on SRX300 and SRX320 series devices.

Site and Tenant Workflow

- In the Configure Site workflow, use IP addresses instead of hostnames for the NTP server configuration.
- CSO uses hostname-based certificates for device activation. The regional microservices VM hostname must be resolvable from the CPE device.
- CSO uses RSA key based authentication when establishing an SSH connection to a managed CPE device. The authentication process requires that the device has a configured root password, and you can use Administration Portal to specify the root password in the device template.

To specify a root password for the device:

1. Log in to Administration Portal.
2. Select **Resources > Device Templates**.

3. Select the device template and click **Edit**.
 4. Specify the plain text root password in the **ENC_ROOT_PASSWORD** field.
 5. Click **Save**.
- When you try to deploy a LAN segment on an SRX Series spoke device, the CSO GUI allows you to select more than one port for a LAN segment. However, for SRX Series devices, only one port for a LAN segment can be deployed; multiple ports in a LAN segment can be deployed only on NFX Series devices.
 - Tenant Administrator users cannot delete sites.
 - On a site with an NFX Series device, if you deploy a LAN segment without the VLAN ID specified, CSO uses an internal VLAN ID meant for internal operations and this VLAN ID is displayed in the UI. There is no impact on the functionality.
 - CSO does not push the default class-of-service configuration on the hub device. You must configure this configuration manually to ensure that the hub configuration is synchronized with the spoke configuration.
 - On a cloud hub shared by multiple tenants, by default, CSO does not add a default route and no security policies are configured for the traffic to reach the Internet. You must add the default route and the required security policies for the site traffic to reach the Internet through the cloud hub.
 - If you do not use the redirect service from Juniper Networks (redirect.juniper.net), after you upgrade an NFX Series device to Junos OS Release 15.1X53-D473 or later, the device is unable to connect to the regional server because the phone home server certificate (**phd-ca.crt**) is reverted to the factory default.

Workaround: Manually copy the regional certificate to the NFX Series device.

- If an NFX250 CPE device is pre-staged to use CSO as the phone-home server, bypassing the redirect service from Juniper Networks, you must add the following configuration to prevent the CSO certificate from being overwritten during a reboot:

```
set system phone-home ca-certification-file /root/phcd-ca.crt
```

Topology

- DHCP configuration on WAN links on a SD-WAN hub is not supported.
- Automatic hub-meshing is not supported. Hub-meshing must be performed manually in order for traffic to flow between the hubs.
- On-premise hubs are not supported.

User Interface

- When you use Mozilla Firefox to access the CSO GUIs, a few pages do not work as expected. We recommend that you use Google Chrome version 60 or later to access the CSO GUIs.

General

- Ensure that you enable port number 443, which is required for phone home services and device activation. Previously, port number 444 was supported for phone home services and device activation.
- The following are the limitations of doing image upgrade from the Image Landing page:
 - JDM images cannot be upgraded parallelly. The upgraded have to be done in a sequence because the connection to CSO gets reestablished when the primary JDM reboots and that affects the upgrade operation of the other JDM.
 - GWR cluster nodes should not be upgraded (neither parallelly nor sequentially) from the Image Landing page because the cluster nodes should always run the same version.

We recommend that you use the Site Upgrade workflow which handles the image upgrade of both JDM and GWR cluster appropriately

- When you edit a tenant, changing the deployment plan from Hybrid WAN to SD-WAN or vice versa is not supported, although the field is displayed as editable.
- For a centralized deployment, use the following procedure to check that the JSM Heat resource is available in Contrail OpenStack on the Contrail Controller node.



NOTE: This procedure must be performed on all the Contrail Controller nodes in your CSO installation.

1. Log in to the Contrail Controller node as root.
2. To check whether the JSM Heat resource is available, execute the **heat resource-type-list | grep JSM** command.

If the search returns the text **OS::JSM::Get Flavor**, the file is available in Contrail OpenStack.

3. If the file is missing, do the following:

- a. Use Secure Copy Protocol (SCP) to copy the `jsm_contrail_3.py` file to the following directory:
 - For Heat V1 APIs, the `/usr/lib/python2.7/dist-packages/contrail_heat/resources` directory on the Contrail Controller node.
 - For Heat V2 APIs, the `/usr/lib/python2.7/dist-packages/vnc_api/gen/heat/resources` directory on the Contrail Controller node.



NOTE: The `jsm_contrail_3.py` file is located in the `/root/Contrail_Service_Orchestration_4.0.2/scripts` directory on the VM or server on which you installed CSO.

- b. Rename the file to `jsm.py` in the Heat resource directory to which you copied the file.
 - c. Restart the Heat services by executing the `service heat-api restart && service heat-api-cfn restart && service heat-engine restart` command.
 - d. After the services restart successfully, verify that the JSM Heat resource is available as explained in Step 2. If it is not available, repeat Step 3.
- In vCPE deployments, when a tenant object is created through Administration Portal or the API for a centralized deployment, Contrail OpenStack adds a default security group for the new tenant. This default security group denies inbound traffic and you must manually update the security group in Contrail OpenStack to allow ingress traffic from different networks. Otherwise, Contrail OpenStack might drop traffic.
 - In vCPE deployments, CSO does not provide a remote procedure call (RPC) to get the device identifier for a specific site. You can use multiple API calls or the license installation tool to obtain the device identifier for a specific site.
 - On an NFX Series device:
 - To activate a virtualized network function (VNF), perform the following steps:
 1. Add the VNF to the device.
 2. Initiate the activation workflow and ensure that the job is 100% completed.
 - To retry the activation of a VNF that failed, perform the following steps:
 1. Deactivate the VNF.
 2. Remove the VNF.

3. Add the VNF to the device.
 4. Initiate the activation workflow and ensure that the job is 100% completed.
- The Ubuntu VNF interface toward the LAN segment of the vSRX gateway router is not automatically provisioned by CSO. You must manually provision the interface as follows:
 - On a LAN segment that does not use a VLAN, execute the **ifconfig ens5 ip-prefix** command, where **ip-prefix** is the IP prefix of the LAN subnet.
 - On a LAN segment that uses a VLAN, execute the following commands:

```
vconfig add ens5 vlan-id
ifconfig ens5.vlan-id ip-prefix
```

where **vlan-id** is the VLAN ID of the LAN and **ip-prefix** is the IP prefix of the LAN subnet.

- Class-of-service (CoS) configuration on Layer 2 interfaces (ge-0/0/*) is not supported on NFX150 CPE devices.
- Image upgrade of a vSRX gateway router on NFX Series devices from the Image Landing page is not supported.

Workaround: Upgrade the image by using the Site Upgrade workflow from the Site Landing Page.

- In CSO Release 4.0.1, the collection of service metrics is disabled by default for SRX Series and NFX150 devices, so the **get_service_metrics** API does not return any data.

To enable the collection of service metrics:

1. On the infrastructure VM or, if regions are present, the regional infrastructure VM, log in as root and execute the **etcdctl set /telemetry-agent/metric_collection ENABLE** command.
2. To restart the telemetry agent microservice:
 - If no regions are present, log in to the microservices VM as root and execute the **kubectrl delete pods csp.csp-telemetry-agent -n regional** command.
 - If regions are present, log in to the regional microservices VM as root and execute the **kubectrl delete pods csp.csp-telemetry-agent** command.

The collection of service metrics data is enabled, and you can use the **get_service_metrics** API to obtain the data.

Known Issues

This section lists known issues in Juniper Networks CSO Release 4.0.2.

- [AWS Spoke](#)
- [CSO HA](#)

- [SD-WAN](#)
- [Security Management](#)
- [Site and Tenant Workflow](#)
- [General](#)

AWS Spoke

- The AWS device activation process takes up to 30 minutes. If the process does not complete in 30 minutes, a timeout might occur and you must retry the process. You do not need to download the cloud formation template again.

To retry the process:

1. Log in to Customer Portal.
2. Access the Activate Device page, enter the activation code, and click **Next**.
3. After the **CREATE_COMPLETE** message is displayed on the AWS server, click **Next** on the Activate Device page to proceed with device activation.

Bug Tracking Number: CXU-19102.

CSO HA

- In an HA setup, users are not able to log into CSO for about five minutes after one of the central servers hosting the HAproxy VRRP master has been brought down.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-28255

- In an HA setup, users are not able to log into CSO when the Contrail server that hosts the MariaDB master has been brought down. This is because the MariaDB cluster is unhealthy when the server that hosts the MariaDB master is down. CSO recovers when the MariaDB master is back online.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-27178

- After a power failure, CAN installed on a physical server does not come up online correctly.

Workaround:

Follow these steps to restore CAN installed on a physical server:

1. Log in to the CAN server and **scp** the **/root/can_bkp** folder to installer VM.
2. Reimage the server.
3. Navigate to the **Contrail_Service_Orchestration_4.0.2** folder.

4. Execute **DEPLOYMENT_ENV=central ./deploy_infra_services.sh** on installer VM until it starts deploying NTP.
5. Execute **salt '*'contrail*' network.hw_addr eth0**.
csp-contrailanalytics-3.4D5UTX.central: 52:54:00:2c:a6:4d
csp-contrailanalytics-1.4D5UTX.central: 52:54:00:2b:4f:da
csp-contrailanalytics-2.4D5UTX.central: 52:54:00:ea:ee:67
6. Open **deployments/central/roles.conf**. Search for can1, can2 and can3. Make sure that the MAC addresses listed in (4) matches the field **hardware_address** for each of can1, can2 and can3.
7. Open **deployment/central/topology.conf**, and edit servers under **[TARGETS] servers = csp-contrailanalytics-1, csp-contrailanalytics-2, csp-contrailanalytics-3**.
8. Execute **DEPLOYMENT_ENV=central ./deploy_infra_services.sh**.
9. Check health of CAN by executing **./components_health.sh**.
10. To restore the data back, copy the backed up **can_bkp** folder from installer VM to the respective CAN servers under **root/**.
11. Execute the following steps on all three CAN servers:
 - a. **root@sspt-ubuntu5-vm7:~# docker exec controller service cassandra stop**
 - b. **root@sspt-ubuntu5-vm7:~# docker exec analyticsdb service cassandra stop**
 - c. **root@sspt-ubuntu5-vm7:~# docker exec -it controller bash**
 - d. **root@sspt-ubuntu5-vm7(controller):/var/lib/cassandra# rm -rf ***
 - e. **root@sspt-ubuntu5-vm7(controller): exit**
 - f. **root@sspt-ubuntu5-vm7:~# docker exec -it analyticsdb bash**
 - g. **root@sspt-ubuntu5-vm7(analyticsdb):/var/lib/cassandra# rm -rf ***
 - h. **root@sspt-ubuntu5-vm7(analyticsdb): exit**
 - i. **root@sspt-ubuntu5-vm7:~# cd can_bkp/analyticsdb_old/**

- j. `root@sspt-ubuntu5-vm7:~/can_bkp/analyticsdb_old/cassandra# docker cp commitlog/ analyticsdb:/var/lib/cassandra`
- k. `root@sspt-ubuntu5-vm7:~/can_bkp/analyticsdb_old/cassandra# docker cp data/ analyticsdb:/var/lib/cassandra`
- l. `root@sspt-ubuntu5-vm7:~/can_bkp/analyticsdb_old/cassandra# docker cp saved_caches/ analyticsdb:/var/lib/cassandra`
- m. `root@sspt-ubuntu5-vm7:~# cd can_bkp/controller_old/`
- n. `root@sspt-ubuntu5-vm7:~/can_bkp/controller_old/cassandra# docker cp commitlog/ controller:/var/lib/cassandra`
- o. `root@sspt-ubuntu5-vm7:~/can_bkp/controller_old/cassandra# docker cp data/ controller:/var/lib/cassandra`
- p. `root@sspt-ubuntu5-vm7:~/can_bkp/controller_old/cassandra# docker cp saved_caches/ controller:/var/lib/cassandra`
- q. `root@sspt-ubuntu5-vm7:~# docker exec controller chown -R cassandra:cassandra /var/lib/cassandra/`
- r. `root@sspt-ubuntu5-vm7:~# docker exec analyticsdb chown -R cassandra:cassandra /var/lib/cassandra/`
- s. `root@sspt-ubuntu5-vm7:~# docker exec analyticsdb service cassandra start`
- t. `root@sspt-ubuntu5-vm7:~# docker exec controller service cassandra start`

12. Check health of CAN by executing `./components_health.sh`.

- As part of VRR recovery process in case of power failure, a tenant named recovery is created for restoring the VRR configuration. However, if the configuration that needs to be recovered is huge, the recovery tenant creation times out and fails even though the configuration is successfully restored to VRR in due course.

Workaround: There is no workaround required as the configuration is usually restored to VRR even if the recovery tenant creation has timed out.

Bug Tracking Number: CXU-27197

- In a CSO HA environment, two RabbitMQ nodes are clustered together, but the third RabbitMQ node does not join the cluster. This might occur just after the initial installation, if a virtual machine reboots, or if a virtual machine is powered off and then powered on.

Workaround: Do the following:

1. Log in to the installer VM.
2. Navigate to the current deployment directory for CSO—for example, `/root/Contrail_Service_Orchestration_4.0.2/`.
3. Execute the `./recovery.sh` command.
4. Specify the option to recover RabbitMQ and press Enter.
5. In the RabbitMQ dashboards for the central and regional microservices VMs, confirm that all the available infrastructure nodes are present in the cluster.

Bug Tracking Number: CXU-12107

- When a high availability (HA) setup comes back up after a power outage, MariaDB instances do not come back up on the VMs.

Workaround:

Perform the following steps to recover the MariaDB instances:

1. Log in to the installer VM.
2. Navigate to the current deployment directory for CSO; for example, `/root/Contrail_Service_Orchestration_4.0.2/`.
3. Execute the `sed -i "s@/var/lib/mysql/grastate.dat@/mnt/data/mysql/grastate.dat@g" recovery/components/recover_mariadb.py` command
4. Execute the `./recovery.sh` command.
5. Specify the option to recover MariaDB and press Enter.

Bug Tracking Number: CXU-20260

- In some cases, when power fails, the ArangoDB cluster does not form.

Workaround:

1. Log in to the centralinfravm3 VM.
2. Execute the following commands:


```
service arangodb3.cluster stop
cd /var/lib/arangodb3 && mv setup.json setup.json.old
```

3. Log in to the centralinfravm2 VM.

4. Execute the following commands:

```
service arangodb3.cluster stop  
cd /var/lib/arangodb3 && mv setup.json setup.json.old
```

5. Log in to the centralinfravm1 VM.

6. Execute the following commands:

```
service arangodb3.cluster stop  
cd /var/lib/arangodb3 && mv setup.json setup.json.old
```

7. On the centralinfravm1 VM, execute the **service arangodb3.cluster start** command and wait for 20 seconds for the command to finish executing.

8. On the centralinfravm2 VM, execute the **service arangodb3.cluster start** command and wait for 20 seconds for the command to finish executing.

9. On the centralinfravm3 VM, execute the **service arangodb3.cluster start** command and wait for 20 seconds for the command to finish executing.

Bug Tracking Number: CXU-20346

- In a HA setup, if you shut down all the CSO servers, after the servers are restarted successfully, MariaDB and ArangoDB fail to form their respective clusters.

Workaround:

1. Perform a clean reboot of the central infrastructure VMs.
2. After the VMs have rebooted successfully, check the cluster health on the HAproxy page (<http://central-ip-address:1936>, where *central-IP-address* is the IP address of the VM that hosts the microservices for the central POP).
3. If the MariaDB and ArangoDB clusters are still down, you can recover the clusters by performing the following procedures:
 - To recover the MariaDB cluster, perform the following steps:
 - a. On the centralinfravm1 VM, execute the **service mysql stop** command.
 - b. On the centralinfravm2 VM, execute the **service mysql stop** command.
 - c. On the centralinfravm3 VM, execute the **service mysql stop** command.
 - d. On all three central infrastructure VMs, verify that the service has stopped executing the **service mysql status** command.

- e. On the centralinfravm1 VM, start the service by executing the **service mysql start** command.
- f. On the centralinfravm2 VM, start the service by executing the **service mysql start** command.
- g. On the centralinfravm3 VM, start the service by executing the **service mysql start** command.
- h. On all three central infrastructure VMs, verify that the service has started executing the **service mysql status** command.
- To recover the ArangoDB cluster, perform the following steps:
 - a. On the centralinfravm1 VM, execute the **service arangodb3.cluster stop** command.
 - b. On the centralinfravm2 VM, execute the **service arangodb3.cluster stop** command.
 - c. On the centralinfravm3 VM, execute the **service arangodb3.cluster stop** command.
 - d. On all three central infrastructure VMs, verify that the service has stopped executing the **ps -aef|grep arangodb** command.
 - e. On the centralinfravm1 VM, start the service by executing the **service arangodb3.cluster start** command.
 - f. On the centralinfravm2 VM, start the service by executing the **service arangodb3.cluster start** command.
 - g. On the centralinfravm3 VM, start the service by executing the **service arangodb3.cluster start** command.
 - h. On all three central infrastructure VMs, verify that the service has started executing the **ps -aef|grep arangodb** command.

Bug Tracking Number: CXU-21819.

- In a HA setup, if you onboard devices and deploy policies on the devices and if one of the policy deployments is in progress when a microservices or infrastructure node goes down, the deployment job is stuck in the **In Progress** state for about 90 minutes (the default timeout value), and you cannot perform deploy operations for the tenant for about 90 minutes.

Workaround: Wait for the job to fail and then redeploy the policy.

Bug Tracking Number: CXU-21922

- If an infrastructure node goes down in a HA setup in which all nodes were previously up, and you create a firewall policy and try to deploy the policy, the deployment job is stuck in the in-progress state and a Redis timeout error is displayed in the job log.

Workaround:

1. Wait for approximately 90 minutes for the job to fail.
2. Bring up the infrastructure node that was down.
3. Redeploy the firewall policy.

Bug Tracking Number: CXU-24559

- While you are upgrading CSO (Production Environment with HA) from Release 3.3.1 to Release 4.0.2, the upgrade fails after a snapshot is taken because the regional Kubernetes node is in the Not Ready status.

Workaround: Restart the Docker service.

1. On the regional K8 master node, run the following commands:
 - **service docker stop**
 - **rm -rf /var/lib/docker/***
 - **service docker start**
2. Run the **./upgrade.sh** script.

Bug Tracking Number: CXU-25625

- You cannot access the Administration Portal login page if the flannel network subnet is changed.

Workaround:

1. Log in to central microservices VMs.
2. In all central microservices VMs, run the following commands in parallel:

service flanneld stop

service docker stop

service flanneld start

sleep 10

service docker start

After executing these commands, wait for 10 minutes.

3. On any one of the central microservices VM, run the following command to delete all pods:

kubectrl delete pods --all --force --grace-period=0 -n central

Bug Tracking Number: CXU-23736

SD-WAN

- Link affinity does not work when there are multiple links with the same cost. There may be frequent switch between equal cost links and that might cause network flapping.

Workaround: Ensure that the cost values are different for each of the links.

Bug Tracking Number: CXU-27969

- On the Site SLA Performance page, applications with different SLA scores are plotted at the same coordinate on the x-axis.

Workaround: None.

Bug Tracking Number: CXU-19768

- When all local breakout links are down, site to Internet traffic fails even though there is an active overlay to the hub.

Workaround: None.

Bug Tracking Number: CXU-19807

- If the Internet breakout WAN link of the cloud hub is not used for provisioning the overlay tunnel by at least one spoke site in a tenant, then traffic from sites to the Internet is dropped.

Workaround: Ensure that you configure a firewall policy to allow traffic from security zone trust-*tenant-name* to zone untrust-*wan-link*, where *tenant-name* is the name of the tenant and *wan-link* is the name of the Internet breakout WAN link.

- Bug Tracking Number: CXU-21291
- On the SD-WAN Events page, for link switch events, if you mouse over the **Reason** field, the values displayed for the SLA metrics are the ones that are recorded when the system logs are sent from the device and not the values for which the SLA violation was detected.

Workaround: None.

Bug Tracking Number: CXU-21461

- In a hub-and-spoke topology with multitenancy enabled, when a spoke site is configured with two MPLS and two Internet links with MPLS selected as the default, traffic from the hub to the spoke site takes the same path instead of taking the path (link) on which the traffic was received by the hub (incoming WAN link). However, there is no traffic loss.

Workaround: Remove the static route with the next hop and replace it with a static route with the qualified next hop.

Bug Tracking Number: CXU-23197

- If a WAN link on a CPE device goes down, the WAN tab of the *Site-Name* page (in Administration Portal) displays the corresponding link metrics as **N/A**.

Workaround: None.

Bug Tracking Number: CXU-23996

- If a tenant has a real-time-optimized site, link switch events (on the Monitor page) might display the same WAN link for both source and destination tunnels.

Workaround: None.

Bug Tracking Number: CXU-24154

- If you delete a cloud hub that is created in Release 3.3.1, CSO does not delete the stage-2 configuration.

Workaround: You must manually delete the stage-2 configuration from the device.

Bug Tracking Number: CXU-25764

Security Management

- When a certificate renewal is triggered from the VPN Authentication page under the Certificate tab, the certificate table becomes empty after renewing the certificate.

Workaround: Refresh the Certificate page to display the required certificate details.

Bug Tracking Number: CXU-25561

- On the Active Database page in Customer Portal, the wrong installed device count is displayed. The count displayed is for all tenants and not for a specific tenant.

Workaround: None.

Bug Tracking Number: CXU-20531

- If a cloud hub is used by two tenants, one with public key infrastructure (PKI) authentication enabled and other with preshared key (PSK) authentication enabled, the commit configuration operation fails. This is because only one IKE gateway can point to one policy and if you define a policy with a certificate then the preshared key does not work.

Workaround: Ensure that the tenants sharing a cloud hub use the same type of authentication (either PKI or PSK) as the cloud hub device.

Bug Tracking Number: CXU-23107

- If UTM Web-filtering categories are installed manually (by using the **request system security utm web-filtering category install** command from the CLI) on an NFX150 device, the intent-based firewall policy deployment from CSO fails.

Workaround: Uninstall the UTM Web-filtering category that you installed manually by executing the **request security utm web-filtering category uninstall** command on the NFX150 device and then deploy the firewall policy.

Bug Tracking Number: CXU-23927

- On the Identity Management page, if you click **Download JIMS**, the Juniper Identity Management Service (JIMS) software is downloaded in HTML format.

Workaround: Download the JIMS software from the [Download Software](#) page.

Bug Tracking Number: CXU-24278

- If SSL proxy is configured on a dual CPE device and if the traffic path is changed from one node to another node, the following issue occurs:
 - For cacheable applications, if there is no cache entry the first session might fail to establish.
 - For non-cacheable applications, the traffic flow is impacted.

Workaround: None.

Bug Tracking Number: CXU-25526

- The UTM policy configuration is not deployed on an SD-WAN site with the SRX device model SRX345-DUAL-AC.

Workaround:

1. Add the SRX345-DUAL-AC device model to the schema file.



NOTE: In the schema-svc docker, the schema file is available at `/opt/csp-schema-data/*configuration.json`.

2. Restart the pod.

Bug Tracking Number: CXU-25706

Site and Tenant Workflow

- Porting of cloud hub sites to tenants fails if the cloud hub site names exceed 15 characters.

Workaround: Ensure that cloud hub site names do not exceed 15 characters even though you can have cloud hub site names of up to 256 characters in the global instance.

Bug Tracking Number: CXU-28078

- ZTP for NFX150 may fail before creating the vlink. Though ZTP goes through successfully on retry, service chain activation may fail.

Workaround: Delete and add the site so that ZTP goes through successfully in one attempt.

Bug Tracking Number: CXU-27967

- During site activation, activation of NFX250 dual CPE connected to MX series cloud hub device may fail with the following error message: **No existing device_initiated device connection.**

Workaround: Retry the failed ZTP job from the administration portal.

Bug Tracking Number: CXU-27902

- After a site upgrade, status of policies that are associated with the site appears as pending deployment even though they are already deployed.

Workaround: Trigger a policy deployment job to deploy the policies. CSO does not deploy the policies unless there are updates to the policy, but the status of policies are appropriately updated after you run a deployment job.

Bug Tracking Number: CXU-27528

- SLA profiles created by a tenant are not deleted when the tenant is deleted.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-27054

- If you create a new tenant with the name of a tenant that was deleted, certain inconsistencies such as policy deployment failure are noticed.

Workaround: When you create a tenant, ensure that you do not use the same name as that of a deleted tenant.

Bug Tracking Number: CXU-26886

- Site upgrade for hub sites that were created using custom device profile or cloned device profile is incomplete.

Workaround:

- After the upgrade, go to tssm core docker by entering the following command: **docker exec -it *docker name* bash**
- In the docker run the following command: **root@csp:/# cd /opt/meta_data/**
- From **/opt/meta_data**, run **cp SRX_Advanced_SDWAN_HUB_option_1_upgrade.yaml custom_device_profile_upgrade.yaml**

Bug Tracking Number: CXU-26532

- The tenant delete operation fails when CSO is installed with an external Keystone.

Workaround: You must manually delete the tenant from the Contrail OpenStack user interface.

Bug Tracking Number: CXU-9070

- If you try to activate a branch SRX Series device with the factory-default configuration, the stage-1 configuration commit might fail when there are active DHCP server bindings on the device. This is because of the default DHCP server settings present in factory-default configuration.

Workaround: When you are pre-staging the CPE device for activation, remove the DHCP server-related configuration from the device by executing the following commands on the Junos OS CLI:

```
set system services dhcp-local-server group jdhcp-group interface fxp0.0
set system services dhcp-local-server group jdhcp-group interface irb.0
```

Bug Tracking Number: CXU-13446

- In some cases, if automatic license installation is enabled in the device profile, after ZTP is complete, the license might not be installed on the CPE device even though license key is configured successfully.

Workaround: Reinstall the license on the CPE device by using the Licenses page on the Administration Portal.

Bug Tracking Number: PR1350302.

- For a tenant, LAN segments with overlapping IP prefixes across sites are not supported.

Workaround: Create LAN segments with unique IP prefixes across sites for the tenant.

Bug Tracking Number: CXU-20494

- When the primary and backup interfaces of the CPE device uses the same WAN interface of the hub, the backup underlay might be used for Internet or site-to-site traffic even though the primary links are available.

Workaround: Ensure that you connect the WAN links of each CPE device to unique WAN links of the hub.

Bug Tracking Number: CXU-20564

- After you configure a site, you cannot modify the configuration either before or after activation.

Workaround: None.

Bug Tracking Number: CXU-21165

- On the Configure Site page, the values that you specify for the time zone and the IP address of the NTP server are not being pushed to the device.

Workaround: Configure the NTP server IP address and the time zone on the device, manually:

1. Log in to the device.
2. In the configuration mode, run the following commands:
 - **set system ntp server *IP address***
 - **set system time-zone *time zone***
3. Commit the changes

Bug Tracking Number: CXU-23971

- On an NFX250 device, if you disable (detach) a failed service successfully and then try to delete the site, the site is not deleted.

Workaround: None.

Bug Tracking Number: CXU-24355

- When you try to activate a site with an SRX Series device, ZTP might fail with an error during the installation of the default trusted certificates.

Workaround: Retry the failed job after some time.

Bug Tracking Number: CXU-24487

- If you try to activate a site with an MPLS link by using DHCP, the default route pointing to the MPLS gateway is added to the hub device, which results in Internet traffic from the hub taking the MPLS link.

Workaround: None.

Bug Tracking Number: CXU-24666

- If you trigger the tenant creation workflow, the tenant might be displayed in the CSO GUI even before the job is completed. If you then try to trigger workflows for that tenant, the subsequent jobs fail because the tenant creation job is not completed.

Workaround: Wait for the tenant creation job to complete successfully before triggering any workflows for the tenant.

Bug Tracking Number: CXU-24783

- The Configure Site operation for a cloud spoke site fails.

Workaround: None.

Bug Tracking Number: CXU-24795

- The Configure Site operation fails if you import a cloud hub with a name that is different from that of other tenants.

Workaround: While you are importing a cloud hub, specify the same name that is used while onboarding a cloud hub for a global service provider.

Bug Tracking Number: CXU-25740

- You cannot configure a site with dual CPE devices if WAN links are used exclusively for local breakout traffic.

Workaround: While you are creating a site and enabling the link for local breakout, instead of selecting the **Use only for breakout traffic** option, select **Use for breakout & WAN** traffic. Also, while you are configuring a site ensure that the WAN link is connected to a hub.

Bug Tracking Number: CXU-25776

General

- If a link or connectivity to CSO flaps during a site upgrade or image upgrade, the upgrade job remains stuck in the in progress state.

Workaround: Use Rest APIs to mark the job as failed and the site status as provisioned, and then retry the upgrade job.

Bug Tracking Number: CXU-27726

- In an HA setup, the Synchronize_Device_Inventory job that was triggered as part of load_service remains incomplete in an unknown state. However, this does not impact any of the workflows.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-28004

- When users rebuild a small deployment with the UI installer and using custom-generated certificates, the underlay tunnels for the NFX250 device remain down if there is a mismatch between the default host name and the custom-generated host name.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-27976

- If you upload images with the same filename for two different device families, the file gets overwritten.

Workaround: Rename the files before uploading to CSO.

Bug Tracking Number: CXU-27713

- If multiple sites are using the same MX series cloud hub, IPSec overlay tunnels for some of the WAN links may fail to come up and show the following error: **Negotiation failed with error code NO_PROPOSAL_CHOSEN received from peer (5 times)**.

Workaround: Clear the IPSec session from the connected MX series cloud hub by executing the **clear services ipsec-vpn ipsec security-associations** command.

Bug Tracking Number: CXU-27638

- For spokes connected to MX hub, OAM tunnels are displayed in the data overlay section of the Monitor > Overview page and the Sites > WAN pages of the administration portal. This does not have any functional impact.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-27449

- After a cloud hub device is rebooted, the device connectivity to CSO is lost. This problem occurs in CSO Release 4.0.2 that has been upgraded from CSO Release 3.3.1 and has the stage-2 configuration applied.

Workaround: Disable and enable **lo0** on the device.

To disable and enable the **lo0** interface, log in to the cloud hub device and run the following commands from the configuration mode:

1. **set interface lo0 disable**
2. **commit**
3. **delete interface lo0 disable**
4. **commit and quit**

Bug Tracking Number: CXU-27420

- ZTP for SRX devices fails. This problem occurs if the SRX device was connected to clients on the LAN side before ZTP and has bindings that are not cleared during ZTP.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-27376

- ZTP of NFX-250 over PPPoE fails and incomplete configuration is pushed to the device.

Workaround: Use links other than PPPoE for ZTP of NFX-250.

Bug tracking number: CXU-27357

- On NFX models NFX150-C-S1, NFX150-C-S1-AE, and NFX150-C-S1-AA, VNFs that require more than 4 GB of memory (for example, Riverbed, Fortinet) fail to launch.

Workaround: For Ubuntu VNF, you can reduce the memory requirement from CSO to enable launching the VNF.

Bug Tracking Number: CXU-27180

- In high-availability setups where the login page and logo have been updated, the old login image gets displayed occasionally when the page is refreshed.

Workaround: Restart the **csp.admin-portal-ui** Docker images.

Bug Tracking Number: CXU-27037

- SRX cluster devices are not listed in the device selection window for pushing licenses to devices.

Workaround: For SRX cluster devices, manually install the license from the device CLI.

Bug tracking number: CXU-26654

- Reverting CSO from 4.0.2 to 3.3.1 fails when CAN is unhealthy.

Workaround:

Run the following commands:

```
root@canvm:~# docker exec -it analyticsdb bash
```

```
root@canvm(analyticsdb):/# service cassandra status
```

If Cassandra is not running, go to `/var/log/cassandra/debug.log` and look for error messages similar to: `DEBUG [main] 2018-09-27 01:01:34,857 CommitLogReader.java:223 - Replaying /var/lib/cassandra/commitlog/CommitLog-6-1537967618037.log (CL version 6, messaging version 10, compression null) ERROR [main] 2018-09-27 01:01:35,660 CommitLogReader.java:214 Exiting due to error while processing commit log during initialization.`

Delete the commit logs that are causing the error:

```
root@canvm(analyticsdb):/# rm
```

```
/var/lib/cassandra/commitlog/CommitLog-6-1537967618037.log
```

Run the following command to restart Cassandra: `root@canvm(analyticsdb):/# service cassandra restart`

Log in to controller container, using the `docker exec -it controller bash` command, and follow the preceding steps to check whether Cassandra is running in controller container and to delete the logs if necessary.

On high availability setups, repeat this on all nodes.

Run `./components_health.sh` on the installer VM to ensure CAN is healthy.

Bug Tracking Number: CXU-26456

- In an SD-WAN, traffic from LAN to WAN stops after a single-legged Ubuntu VNF has been brought up. This problem occurs because of port cross connect between the left interface of VNF and GWR interface (on NFX250) or Flowd tap interface (for NFX150).

Workaround: Remove port cross connect configuration. You can do it either on the device or by using Stage 2 template.

Bug Tracking Number: CXU-26282

- GRE tunnel fails to come up online when a new site is added. This problem occurs because the new site uses the PPPoE IP that was originally-assigned to the tunnel even though the tunnel IP has since changed because of renegotiation by PPPoE.

Workaround: Use the fixed IPs (through CHAP/PAP authentication or CPE Mac address) for clients when you use PPPoE.

Bug Tracking Number: CXU-26606

- On an Ubuntu VNF spawned on an NFX250 device, the ping command to a website address (fully qualified domain name) does not work.

Workaround:

1. In Resource Designer, clone the existing ubuntu-fw-NFX250 template for the NFX250 device.
2. Edit the template and ensure that offloads are disabled for the Left Interface.
3. Click Next and complete the edit operation.

Bug tracking number: CXU-24985

- GWR may fail to come up after an NFX device image has been upgraded.

Workaround:

Follow these steps to manually restart the VNF from JDM:

1. Find the GWR VNF name using the `virsh list` command.
2. Start the GWR VNF using the `virsh start GWR-VNF-Name` command.

Bug Tracking Number: CXU-24823

- If you create VNF instances in the Contrail cloud by using Heat Version 2.0 APIs, a timeout error occurs after 120 instances are created.

Workaround: Contact Juniper Networks Technical Support.

Bug Tracking Number: CXU-15033

- The provisioning of CPE devices fails if all VRRs within a redundancy group are unavailable.

Workaround: Recover the VRR that is down and retry the provisioning job.

Bug Tracking Number: CXU-19063

- After the upgrade, the health check on the standalone Contrail Analytics Node (CAN) fails.

Workaround:

1. Log in to the CAN VM.
2. Execute the **docker exec analyticsdb service contrail-database-nodemgr restart** command.
3. Execute the **docker exec analyticsdb service cassandra restart** command.

Bug Tracking Number: CXU-20470

- The load services data operation or health check of the infrastructure components might fail if the data in the Salt server cache is lost because of an error.

Workaround: If you encounter a Salt server-related error, do the following:

1. Log in to the installer VM.
2. Execute the **salt '*' deployutils.get_role_ips 'cassandra'** command to confirm whether one or more Salt minions have lost the cache.
 - If the output returns the IP address for all the Salt minions, this means that the Salt server cache is fine; proceed to step 7.
 - If the IP address for some minions is not present in the output, this means that the Salt server has lost its cache for those minions and must be rebuilt as explained from step 3.
3. Navigate to the current deployment directory for CSO; for example, **/root/Contrail_Service_Orchestration_4.0.2/**.
4. Redeploy the central infrastructure services (up to the NTP step):
 - a. Execute the **DEPLOYMENT_ENV=central ./deploy_infra_services.sh** command.
 - b. Press Ctrl+c when you see the following message on the console:

```
2018-04-10 17:17:03 INFO utils.core Deploying roles set(['ntp']) to servers
['csp-central-msvm', 'csp-contrailanalytics-1', 'csp-central-k8mastervm',
'csp-central-infravm']
```

5. Redeploy the regional infrastructure services (up to the NTP step):
 - a. Execute the **DEPLOYMENT_ENV=regional ./deploy_infra_services.sh** command.
 - b. Press Ctrl+c when you see a message similar to the one for the central infrastructure services.
6. Execute the **salt '*' deployutils.get_role_ips 'cassandra'** command and confirm that the output displays the IP addresses of all the Salt minions.
7. Re-run the load services data operation or the health component check that had previously failed.

Bug Tracking Number: CXU-20815

- For an MX Series cloud hub device, if you have configured the Internet link type as OAM_and_DATA, the reverse traffic fails to reach the spoke device if you do not configure additional parameters by using the Junos OS CLI on the MX Series device.

Workaround:

1. Log in to the MX Series device and access the Junos OS CLI.
2. Find the **next-hop-service outside-service-interface** multiservices interface as follows:
 - a. Execute the **show configuration | display set | grep outside-service-interface** command.
 - b. In the output of the command, look for the multiservices (ms-) interface corresponding to the service set that CSO created on the device.

The name of the service set is in the format **ssettenant-name_DefaultVPN-tenant-name**, where *tenant-name* is the name of the tenant.

The following is an example of the command and output:

```
show configuration | display set | grep outside-service-interface
set groups mx-hub-Acme-Acme_DefaultVPN-vpn-routing-config services
service-set ssetAcme_DefaultVPN-Acme next-hop-service
outside-service-interface ms-1/0/0.4008
```

In this example, the tenant name is Acme and the multiservices interface used is ms-1/0/0.4008.

3. After you determine the correct interface, add the following configuration on the device: **set routing-instances WAN_0 interface *ms-interface***
where *ms-interface* is the name of the multiservices interface obtained in the preceding step.
4. Commit the configuration.

Bug Tracking Number: CXU-21818

- In Resource Designer, if you add a VNF that does not require a password and trigger the Add VNF Manager workflow, you are asked to enter a password even though the VNF does not require it.

Workaround: Even for VNFs that do not require a password, enter a dummy password in Resource Designer when you are creating a VNF package.

Bug Tracking Number: CXU-21845.

- In a full mesh topology, the simultaneous deletion of LAN segments on all sites is not supported.

Workaround: Delete LAN segments on one site at a time.

Bug Tracking Number: CXU-21936

- When you install the CSO Downloader app on MacOS, you might receive an error message indicating that the application cannot be opened because it is from an unidentified developer.

Workaround: Access the MacOS **Security & Privacy** settings and allow the CSO Downloader app to be opened and continue with the installation.

Bug Tracking Number: CXU-22661

- If you run the script to revert an upgraded CSO Release 4.0.0 setup to CSO Release 3.3.1, the revert operation fails because of an ArangoDB cluster error.

Workaround: Use the same workaround as CXU-20346.

Bug Tracking Number: CXU-23338

- On a CSO setup with secure OAM configured, if you bring up the FortiGate VNF and then apply the license on the VNF, the VNF reboots. However, after rebooting, sometimes the VNF does not come back up.

Workaround: To ensure that the VNF comes back up, deactivate the VNF and then reactivate it by performing the following steps:

1. Log in to the JDM CLI of the NFX Series device and access configuration mode.
2. Deactivate the VNF by executing the **deactivate virtual-network-functions Fortinet-oob-2-Firewall** command.

3. Commit the changes by executing the **commit** command.
4. Rollback the changes by executing the **rollback 1** command
5. Commit the changes by executing the **commit** command.
6. Exit the configuration mode by executing the **quit** command.
7. Execute the **show virtual-network-functions** command and confirm that the status is **Running alive**, which means that the VNF is up.

Bug Tracking Number: CXU-23371.

- If one or more VRRs are down, jobs might take a long time to complete, or, in some cases, fail.

Workaround: Ensure that all VRRs are up before trying the Add Tenant or Add Site workflows.

Bug Tracking Number: CXU-23710

- The image upgrade of the vSRX gateway router on NFX Series devices by using the CSO GUI is not supported.

Workaround: Upgrade the image by using the CLI of the NFX Series device.

Bug Tracking Number: CXU-23804.

- On an NFX Series device with a Ubuntu VNF instantiated, if you use SSH to do log in to the VNF by using the loopback IP address (configured for secure OAM) with port 49154, the connection does not work.

Workaround:

1. Use SSH to log in to the vSRX gateway router by using the loopback IP address.
2. Use SSH to log in to the OAM IP address of the Ubuntu VNF with username **root** and password **passwOrd**.
3. In the Ubuntu VNF, add a route to the IP address of the machine from where you want to log in by using SSH.

You can now use SSH to log in from the configured machine by using the loopback IP address with port 49154.

Bug Tracking Number: CXU-23953

- If you are using the GUI installer to install CSO, sometimes the installation page freezes (percentage completion on the VMs does not change) during the installation because of a Rest API timeout.

Workaround: Reload the CSO installation page in the browser, which will update the status of the installation.

Bug Tracking Number: CXU-24471

- When you reboot a device from the Tenant Devices or Devices pages, the reboot job fails because the connectivity is lost during the reboot.

Workaround: Check the operational status of the device on the Tenant Devices or Devices page. During the reboot phase, the operational status of the device is **Down**. After the device is successfully rebooted and connectivity is restored, the operational status of the device changes to **Up**. You can now trigger operations on the device by using the CSO GUI.

Bug Tracking Number: CXU-24512

- If you are using the GUI installer to install CSO, sometimes the UI freezes during the installation and no installation progress is seen. However, the installation continues in the backend.

Workaround: Perform the following tasks:

1. Reload the installation UI page in the browser.
If the UI page loads successfully, no further action is needed. If the UI page does not load, proceed to step 2.
2. Log in to the installer VM as root.
3. Kill the existing processes triggered by the GUI installer by executing the **kill \$(sudo lsof -t -i:8080)** command.
4. Navigate to the **/root/cso_dl/Contrail_Service_Orchestration_4.0.2/** directory.
5. Restart the Flask server by executing the **bash run_ui.sh** command.
6. After you see the **==== INFO Installer App initialized =====** message on the console, reload the installation UI page in the browser.

Bug Tracking Number: CXU-24552

- For an NFX250 device, the Ubuntu VNF service chain configuration is incorrect if you set **SINGLE_SSH_TO_NFX** to False and then instantiate a service.

Workaround: None.

Bug Tracking Number: CXU-25018

- In CSO Release 4.0.1, while you are converting a hub that is created in Release 3.3.1 to a secure OAM hub by using the stage-2 template, the job fails even though the device configuration is updated.

Workaround: Roll back the stage-2 configuration, save the stage-2 configuration, and redeploy.

Bug Tracking Number: CXU-25531

- The upgrade from CSO Release 3.3.1 to Release 4.0.1 fails, because the pods do not get deleted.

Workaround: Delete the pods and rerun the **upgrade.sh** script.

1. Log in to the microservice VM.
2. Execute the **kubectrl delete deployments,svc,pods,ds,events --all --grace-period=0 --force** command.
3. After the command is successfully executed, rerun the **upgrade.sh** script.

Bug Tracking Number: CXU-25737

- On the Audit Logs page, Username and Role columns do not display the actual name and the role of the user, respectively. Instead, the name of the user is displayed as Admin and role of the user is displayed as _member_.admin.

Workaround: None.

Bug Tracking Number: CXU-25189

- An error occurs while EEPROM contents for copper ports are being read.

Workaround: None.

Bug Tracking Number: PR1372217

- For a device that is provisioned for an OpCo tenant, the software image upgrade fails if you try to upgrade the software image from the Device Images page.

Workaround: None

Bug Tracking Number: CXU-25663

- Because of insufficient buffer size, vSRX performs queue scheduling incorrectly and drop packets.

Workaround: Set the buffer size to 3000 microseconds by executing the **set class-of-service schedulers scheduler-name buffer-size temporal 3000** command.

Bug Tracking Number: PR1361720.

Resolved Issues

The following issues are resolved in Juniper Networks CSO Release 4.0.2.

- In a CSO HA environment, ZTP for a tenant added after a virtual route reflector (VRR) recovery remains inconclusive.

Bug Tracking Number: CXU-27340.

- In device redundancy mode, while creating a NAT pool, the Routing Instance field is not displayed.

Bug Tracking Number: CXU-25880

- On a Dual CPE device, the deployment of the AllSite_AUTONAT_Policy policy fails.

Bug Tracking Number: CXU-25855

- The ZTP of an NFX250 device fails.

Bug Tracking Number: CXU-25822.

- For some sites, the Configure Site operation fails and the following error message is displayed:

Policy is out of sync between RE and PFE fpc0. Please resync before commit.

Bug Tracking Number: CXU-25808.

- While upgrading CSO from Release 3.3.1 to Release 4.0.1, if link-interface or link-name mappings in Redis are lost, the link utilization graph is not displayed.

Bug Tracking Number: CXU-25728.

- After you upgrade CSO to Release 4.0.1, you cannot delete tenants that are created in CSO Release 3.3.1.

Bug Tracking Number: CXU-25716.

- In CSO Release 4.0.1, the site upgrade fails for sites with vSRX as a CPE device.

Bug Tracking Number: CXU-25713.

- The operation to delete tenants fails and the following error is displayed:

PMTask Fail {"status_code": "409", "error_tag": "Refs Exist", "error_message": "Operation can not be completed since the resource is still being referred to. ", "error_app_message": "Delete when resource still referred":
[u'/topology-service/termination-point/edea81b3-fc95-4d19-beea-e56ecfce3fb3',
u'/topology-service/termination-point/1ba769cc-00d6-4ad3-914e-913cb4d707eb',
u'/topology-service/termination-point/a74ff397-6993-437f-ba67-4ef0d57620bc',
u'/topology-service/termination-point/b9a5dd21-3025-4cce-b8a9-7df6d32cf51f',
u'/topology-service/termination-point/89c9f27d-4f68-4972-9c10-7ab68805d146',
u'/topology-service/termination-point/6afba242-6905-4d3e-8295-4b7b5e791fdd',
u'/topology-service/termination-point/e627802b-ec97-4343-8f5c-4c53415d3353']",
"error_diag": "This error occurs when a resource is attempted for modification or deletion when there are child resources still referring to it. ", "error_code": "40006"}

Bug Tracking Number: CXU-25686.

- On an MX Series device, after you apply the stage-2 configuration, the BGP route is hidden.

Bug Tracking Number: CXU-25665.

- When you delete an SD-WAN policy, the custom application group associated with the SD-WAN is not deleted.

Workaround: Log in to the device, and delete the custom application group.

Bug Tracking Number: CXU-25657.

- On a gateway router, the application identification license and the application signature that are installed are lost.

Bug Tracking Number: CXU-25641.

- The activation of an NFX250 as an SD-WAN CPE device with an ADSL or VDSL WAN link fails if you set the global parameter USE_SINGLE_SSH of the device template to False.

Bug Tracking Number: CXU-25573.

- After you upgrade CSO from Release 3.3.1 to Release 4.0.1, the widgets are not displayed in the Dashboard.

Bug Tracking Number: CXU-25405.

- While you are editing a role, when you clear an object, the implied capabilities that are listed under the object are cleared.

Bug Tracking Number: CXU-25386.

- For an Application Quality of Experience (AppQoE) tenant, an SLA profile with only the Throughput parameter is not supported.

Bug Tracking Number: CXU-25378.

- The tenant name cannot be the same across different operating companies.

Bug Tracking Number: CXU-25225.

- The POP location on the geographical map is incorrect if you do not validate the address while you are creating a POP.

Bug Tracking Number: CXU-25060.

- On the Monitor Overview Page page, a green check mark appears even though the operational state of a device that is going through the RMA process is Down, Expected, or RMA.

Bug Tracking Number: CXU-24933.

- The site upgrade for a dual CPE site fails because CSO does not support image upgrade.

Bug Tracking Number: CXU-24823.

- When you generate reports for operating companies and their tenants, the customized logo is not displayed.

Bug Tracking Number: CXU-24729.

- If all the infrastructure VMs are not up, reports cannot be generated.

Bug Tracking Number: CXU-24560.

- The class-of-service scheduler configuration does not take effect on the CPE device.

Bug Tracking Number: CXU-20708

- After you upgrade a site with an NFX250 device, the monitoring page does not display any data. This is because the telemetry agent is uninstalled during the site upgrade.

Bug Tracking Number: CXU-19455.

- CSO might not come up after a power failure.

Bug Tracking Number: CXU-16530

Documentation Updates

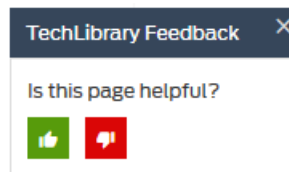
This section lists the errata and changes in the CSO documentation:

- Starting CSO release 4.0.2, the Contrail Service Orchestration (CSO) HTTP API Reference and Developer Guide is available only in html format. The guide is available at https://www.juniper.net/documentation/en_US/cso4.0/information-products/pathway-pages/API_Guide/index.html.
- From CSO Release 4.0.0, the following new guides are available:
 - *CSO Installation and Upgrade Guide*
 - *CSO Monitoring and Troubleshooting Guide*
- The installation and upgrade information, which was previously a part of the *CSO Deployment Guide*, is moved to the *CSO Installation and Upgrade Guide*.

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

11 January 2019—Revision 5, CSO Release 4.0.2

06 November 2018—Revision 4, CSO Release 4.0.2

30 October 2018—Revision 3, CSO Release 4.0.2

26 October 2018—Revision 2, CSO Release 4.0.2

24 October 2018—Revision 1, CSO Release 4.0.2

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be 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.