Contrail Service Orchestration Release Notes

Release 3.2.1
24 October 2018
Revision 6

These Release Notes accompany Release 3.2.1 of the Juniper Networks® Contrail Service Orchestration. They contain installation information, and they describe new and changed features, limitations, and known and resolved issues in the software.

Contents

Introduction

The Juniper Networks Contrail Service Orchestration (CSO) solution 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 the network services.

Contrail Service Orchestration (CSO) Release 3.2.1 is a secure software-defined WAN (SD-WAN) solution that builds on the capabilities of CSO Release 3.2. The following are the highlights of the features available in Release 3.2:

- SD-WAN
  - Centralized application, service-level agreement (SLA), and performance management
  - Intent-based advanced policy-based routing (APBR)
  - Traffic visualization and monitoring at a per-application level across branch sites
- Security management
  - Intent-based firewall policies
  - Network Address Translation (NAT) policy management
  - UTM policy management
  - Threats map
  - Application visibility and signature management
  - Security reports

The solution 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 Centralized Deployment Model (*centralized deployment*)

  In the 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.

- 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.

- A combined centralized and distributed deployment

In this combined deployment, the network contains both cloud sites and on-premise sites. One customer can have both types of sites; however, you cannot use the same network service package for cloud sites and on-premise sites. If you require the same network service for cloud sites and on-premise sites, you must create two identical network service packages with different names.

CSO uses the following components for the NFV environment:

- When end users access network services in the cloud:
  - Network Service Orchestrator provides ETSI-compliant management of the life cycle of network service instances.

    This application includes RESTful APIs that you can use to create and manage network service catalogs.
  - Contrail Cloud Platform provides the underlying software-defined networking (SDN), NFV infrastructure (NFVI), and the virtualized infrastructure manager (VIM).
- When end users access network services on a local CPE device:
  - 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 NFVI.

The following Contrail Service Orchestration (CSO) components connect to Network Service Orchestrator through its RESTful API:

NOTE: **From CSO Release 3.1.1 onward, the Administration and Customer Portals are unified into a single portal with role-based access control (RBAC) enforcement.**

- Administration Portal, which you use to set up and manage your virtual network and customers through a graphical user interface (GUI).
- Customer Portal, which is an application that you can provide to customers to enable them to manage sites and services for their organizations through a GUI.
- The Designer Tools, which enable design, creation, management, and configuration of network services through a GUI. Network services are stored in the network service catalog.
- Service and Infrastructure Monitor, which works with Icinga, an open source enterprise monitoring system to provide real-time data about Contrail Service Orchestration, such as the status of virtualized network functions (VNFs), virtual machines (VMs), and physical servers; information about physical servers' resources; components of a network service (VNFs and VMs hosting a VNF); counters and other information for VNFs.

You can deploy Contrail Service Orchestration in a demonstration (demo) or production environment. Table 1 on page 5 shows the number of sites and VNFs supported for each environment.

Table 1: Number of Sites and VNFs Supported

Contrail Service Orchestration Environment Type	Number of VNFs Supported for a Centralized Deployment	Number of Sites and VNFs Supported for a Distributed Solution	Number of Sites Supported for an SD-WAN Deployment
Demo environment without HA	10 VNFs	25 sites, 2 VNFs per site	25
Demo environment with HA	100 VNFs, 20 VNFs per Contrail compute node	200 sites, 2 VNFs per site	200, up to 50 full mesh sites
Production environment without HA	500 VNFs, 20 VNFs per Contrail compute node	200 sites, 2 VNFs per site	200, up to 50 full mesh sites
Production environment with HA	500 VNFs, 20 VNFs per Contrail compute node	2200 sites, 2 VNFs per site	3000

Installation

Installation Instructions

A full-version installer is available for Release 3.2.1. You must use this installer for a production environment. You can also use it to install a demo environment if you want to customize the installation settings.

After copying the installer tar file to the CSO server and expanding the file, you provision the VMs, and run a script to create a file of settings for the installation. You then run the installer, which takes approximately an hour to install CSO. Finally, you start the CSO infrastructure services and microservices.

NOTE: From CSO Release 3.1.1 onward, you do not need Internet access from the CSO server to install CSO.

For more information, follow the instructions in the Deployment Guide or the README file that is included with the software installation package.

Configuring Name Servers on CPE Devices

To configure the name server on a CPE device, you must use the custom properties to provide the name server details when you are adding a tenant.

Software Installation Requirements for NFX250 Network Services Platform

The NFX250 requires the Junos OS Release 15.1X53-D47 for CSO Release 3.2.1.

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

1. Upload the image to Contrail Service Orchestration.
2. Specify this image as the boot image when you configure activation data.

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

Software Downloads for SRX Series Devices

The Contrail Service Orchestration (CSO) software package does not contain the images for the SRX1500, SRX4100, and SRX4200 devices. You can download these images by using the following links:

- SRX1500: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/73612.html
- SRX1500 USB: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/73615.html
- SRX1500 Preboot Execution Environment (PXE): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/73616.html
- SRX4100 and SRX4200: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/73611.html
- SRX4100 and SRX4200 USB: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/73614.html
- SRX4100 and SRX4200 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/73617.html

New and Changed Features in Contrail Service Orchestration Release 3.2.1

No new features are introduced in CSO Release 3.2.1. For new and changed features in CSO Release 3.2, see the *Contrail Service Orchestration 3.2 Release Notes* available at https://www.juniper.net/documentation/en_US/nfv3.2/information-products/pathway-pages/3.2/index.html .

Servers, Software, and Network Devices Tested

- Node Servers and Servers Tested in the Contrail Service Orchestration
- Software Tested for COTS Servers

- Network Devices and Software Tested for the Contrail Cloud Platform (Centralized Deployment)
- Network Devices and Software Tested for Use with CPE Devices (Distributed Deployment)

Node Servers and Servers Tested in the Contrail Service Orchestration

CSO uses commercial off-the-shelf (COTS) node servers or servers for both the centralized and distributed deployments for the following functions:

- Contrail Service Orchestration central and regional servers
- Contrail Analytics servers
- Contrail Cloud Platform in the centralized deployment

Table 2 on page 7 lists the node servers and servers that have been tested for these functions in Contrail Service Orchestration. You should use these specific node servers or servers for Contrail Service Orchestration.

Table 2: COTS Node Servers and Servers Tested in Contrail Service Orchestration

Option	Vendor	Model	Type
1	QuantaPlex	T41S-2U 4-Node server	Multinode server accepting 4 nodes
2	Supermicro	SuperServer Model SYS-2028TPHC1TR-OTO-4	Multinode server accepting 4 nodes
3	Dell	PowerEdge R420 rack server	1U rack-mounted server

Software Tested for COTS Servers

Table 3 on page 7 shows the software that has been tested for Contrail Service Orchestration. You must use these specific versions of the software when you implement Contrail Service Orchestration.

Table 3: Software Tested for the COTS Nodes and Servers

Description	Version
Operating system for all COTS nodes and servers	Ubuntu 14.04.5 LTS NOTE: Ensure that you perform a fresh installation of Ubuntu 14.04.5 LTS on the CSO servers in your deployment because upgrading from a previous version to Ubuntu 14.04.5 LTS might cause issues with the CSO installation.
Operating system for VMs on Contrail Service Orchestration servers	• Ubuntu 14.04.5 LTS for VMs that you configure manually and not with the provisioning tool • The provisioning tool installs Ubuntu 14.04.5 LTS in all VMs.

Table 3: Software Tested for the COTS Nodes and Servers (continued)

Description	Version
Hypervisor on Contrail Service Orchestration servers	• Centralized deployment: Contrail Cloud Platform Release 3.2.5 , or VMware ESXi Version 5.5.0 • Distributed deployment: KVM provided by the Ubuntu operating system on the server or VMware ESXi Version 5.5.0
Additional software for Contrail Service Orchestration servers	Secure File Transfer Protocol (SFTP)
Software defined networking (SDN) for a centralized deployment	Contrail Cloud Platform Release 3.2.5 with Heat v2 APIs
Contrail Analytics	Contrail Release 4.0.2

Network Devices and Software Tested for the Contrail Cloud Platform (Centralized Deployment)

The Contrail Cloud Platform has been tested with:

- The network devices described in Table 4 on page 8.
- The software described in Table 5 on page 8.

You must use these specific versions of the software for CSO Release 3.2.1.

Table 4: Network Devices Tested for the Centralized Deployment

Function	Device	Model	Quantity
SDN gateway router	Juniper Networks MX Series 3D Universal Edge Router	MX80-48T router with two 10-Gigabit Ethernet XFP optics	1
Management switch	Juniper Networks EX Series Ethernet Switch	EX3300-48T switch with: • 48 10/100/1000-Gigabit Ethernet interfaces • 4 built-in 10-Gigabit Ethernet SFP transceiver interfaces	1
Data switch	Juniper Networks QFX Series Switch	QFX 5100-48S-AFI switch with: • 48 SFP+ transceiver interfaces • 6 QSFP+ transceiver interfaces	1

Table 5: Software Tested in the Centralized Deployment

Function	Software and Version
Operating system for MX Series router	Junos OS Release 14.2R3
Operating system for QFX Series switch	Junos OS Release 13.2X51-D38

Table 5: Software Tested in the Centralized Deployment (continued)

Function	Software and Version
Hypervisor on CSO servers	KVM provided by the Ubuntu operating system on the server or VMware ESXi Version 5.5.0
Element management system software	EMS microservice Junos Space Network Management Platform Release 15.1R1 (See *VNFs Supported by Contrail Service Orchestration* for VNFs that require this product)
Software defined networking (SDN), including Contrail Analytics, for a centralized deployment	Contrail Release 3.2.5 with OpenStack Mitaka
Virtualized infrastructure manager (VIM) and virtual machine (VM) orchestration	OpenStack Mitaka
Authentication and Authorization	OpenStack Mitaka
Network Functions Virtualization (NFV)	CSO Release 3.2.1

Network Devices and Software Tested for Use with CPE Devices (Distributed Deployment)

The distributed deployment has been tested with:

- The network devices described in Table 6 on page 9.
- The software described in Table 7 on page 10.

  You must use these specific versions of the software when you implement the distributed deployment.

Table 6: Network Devices Tested for the Distributed Deployment and SD-WAN Implementation

Function	Device	Model	Quantity
PE router and IPsec concentrator (Hybrid WAN distributed deployment only)	Juniper Networks MX Series 3D Universal Edge Router	• MX960, MX480, or MX240 router with Multiservices MPC line card • MX80 or MX104 router with Multiservices MIC line card • Other MX Series routers with an Multiservices MPC or Multiservices MIC line card See MPCs Supported by MX Series Routers and MICs Supported by MX Series Routers for information about MXSeries routers that support Multiservices MPC and MIC line cards.	—

Table 6: Network Devices Tested for the Distributed Deployment and SD-WAN Implementation (continued)

Function	Device	Model	Quantity
Cloud hub device (SD-WAN implementation only)	Juniper Networks MX Series 3D Universal Edge Router Juniper Networks SRX Series Services Gateway	• MX Series router with Multiservices MIC line card. See MPCs Supported by MX Series Routers and MICs Supported by MX Series Routers for information about MXSeries routers that support Multiservices MPC and MIC line cards. • SRX1500Services Gateway • SRX4100 Services Gateway • SRX4200 Services Gateway	—
On-premise hub device (SD-WAN implementation only)	Juniper Networks SRX Series Services Gateway	• SRX1500 Services Gateway • SRX4100 Services Gateway • SRX4200 Services Gateway	—
(Hybrid WAN deployment) or spoke device (SD-WAN implementation)	• NFX250 Series Network Services Platform • SRX Series Services Gateway • vSRX on an x86 server	• NFX250-LS1 device • NFX250-S1 device • NFX250-S2 device • SRX300 Services Gateway • SRX320 Services Gateway • SRX340 Services Gateway • SRX345 Services Gateway • SRX550 High Memory Services Gateway (SRX550M) • vSRX	1 per customer site

Table 7: Software Tested in the Distributed Deployment and SD-WAN Solution

Function	Software and Version
Hypervisor on CSO servers	KVM provided by the Ubuntu operating system on the server or VMware ESXi Version 5.5.0
Authentication and Authorization	OpenStack Mitaka
Network Functions Virtualization (NFV)	CSO Release 3.2.1
Contrail Analytics	Contrail Release 4.0.2.35
NFX Software	Junos OS Release 15.1X53-D47
Routing and Security for NFX250 device	vSRX KVM Appliance 15.1X49-D125
Operating system for vSRX used as a CPE device on an x86 server	vSRX KVM Appliance 15.1X49-D125
Operating system for SRX Series Services Gateway used as a CPE device or spoke device	Junos OS Release 15.1X49-D125
Operating system for MX Series router used as PE router	Junos OS Release 16.1R3.00

Table 7: Software Tested in the Distributed Deployment and SD-WAN Solution (continued)

Function	Software and Version
Operating system for MX Series Router used as a hub device for an SD-WAN implementation	Junos OS Release 16.1R5.00
Operating system for SRX Series Services Gateway used as a hub device for an SD-WAN implementation	Junos OS Release 15.1X49-D125

Hardware, Software, and Virtual Machine Requirements for the Contrail Service Orchestration

Minimum Hardware Requirements for the Contrail Service Orchestration

Table 2 on page 7 lists the makes and models of node servers and servers that you can use in Contrail Service Orchestration. When you obtain node servers and servers for CSO, we recommend that you:

- Select hardware that was manufactured within the last year.
- Ensure that you have active support contracts for servers so that you can upgrade to the latest firmware and BIOS versions.

The number of node servers and servers that you require depends on whether you are installing a demo or a production environment.

Table 8 on page 11 shows the required hardware specifications for node servers and servers in a demo environment.

Table 8: Demo Environment or Demo HA Environment

Function	Demo Environment	Demo HA Environment
Node or Server Specification		
Storage	Greater than 1 TB of one of the following types: • Serial Advanced Technology Attachment (SATA) • Serial Attached SCSI (SAS) • Solid-state drive (SSD)	Greater than 1 TB of one of the following types: • SATA • SAS • SSD
CPU	One 64-bit dual processor, type Intel Sandybridge, such as Intel Xeon E5-2670v3 @ 2.5 GHz or higher specification	One 64-bit dual processor, type Intel Sandybridge, such as Intel Xeon E5-2670v3 @ 2.5 GHz or higher specification
Network interface	One Gigabit Ethernet (GE) or 10 Gigabit Ethernet interface	One Gigabit Ethernet or 10 Gigabit Ethernet interface

Table 8: Demo Environment or Demo HA Environment (continued)

Function	Demo Environment	Demo HA Environment
Contrail Service Orchestration Servers (includes Contrail Analytics in a VM)		
Number of nodes or servers	1	3
vCPUs per node or server	48	48
RAM per node or server	256 GB	256 GB
Contrail Cloud Platform for a Centralized Deployment		
Number of nodes or servers	1	4–8 • 3 nodes for Contrail controller, and analytics • 1–4 Contrail compute nodes
vCPUs per node or server	48	48
RAM per node or server	256 GB	256 GB

Table 9 on page 12 shows the required hardware specifications for node servers and servers in a production environment.

Table 9: Production Environment (HA and non-HA)

Server Function	Values
Node or Server Specification	
Storage	Greater than 1 TB of one of the following types: • SATA • SAS • SSD
CPU	One 64-bit dual processor, type Intel Sandybridge, such as Intel Xeon E5-2670v3 @ 2.5 GHz or higher specification
Network interface	One Gigabit Ethernet (GE) or 10 Gigabit Ethernet interface
Contrail Service Orchestration Servers	
Number of nodes or servers for a non-HA environment	2 • 1 central server • 1 regional server

Table 9: Production Environment (HA and non-HA) (continued)

Server Function	Values
Number of nodes or servers for an HA environment	6 • 3 central server • 3 regional server
vCPUs per node or server	48
RAM per node or server	256 GB
Contrail Analytics Server for a Distributed Deployment	
Number of nodes or servers	1
vCPUs per node or server	48
RAM per node or server	256 GB
Contrail Cloud Platform for a Centralized Deployment	
Number of nodes or servers	4–28 • 3 nodes for Contrail controller, and analytics • 1–25 Contrail compute nodes
vCPUs per node or server	48
RAM per node or server	256 GB

Software and Virtual Machine Requirements

You must use the software versions that were tested in Contrail Service Orchestration. This section shows the VMs required for each type of environment.

Table 10 on page 13 shows complete details about the VMs required for a demo environment. HA is not included with the demo environment.

Table 10: Details of VMs for a Non-HA Demo Environment

Name of VM	Components That Installer Places in VM	Resources Required	Ports to Open
csp-installer-vm	—	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-central-infravm	Third-party applications used as infrastructure services	• 4 CPU • 32 GB RAM • 200 GB hard disk storage	See Table 14 on page 21.

Table 10: Details of VMs for a Non-HA Demo Environment (continued)

Name of VM	Components That Installer Places in VM	Resources Required	Ports to Open
csp-central-msvm	All microservices, including GUI applications	• 4 vCPUs • 32 GB RAM • 200 GB hard disk storage	See Table 14 on page 21.
csp-regional-infravm	Third-party applications used as infrastructure services	• 4 vCPUs • 24 GB RAM • 200 GB hard disk storage	See Table 14 on page 21.
csp-regional-msvm	All microservices, including GUI applications	• 4 vCPUs • 24 GB RAM • 200 GB hard disk storage	See Table 14 on page 21.
csp-regional-sblb	Load balancer for device to Fault Management Performance Management (FMPM) microservice connectivity	• 4 vCPUs • 8 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-space-vm	Junos Space Virtual Appliance and database—required only if you deploy virtualized network functions (VNFs) that use this EMS	• 4 vCPUs • 16 GB RAM • 200 GB hard disk storage	See Table 14 on page 21.
csp-contrailanalytics-1	Contrail Analytics for a distributed deployment For a centralized or combined deployment, you use Contrail Analytics in the Contrail Cloud Platform.	• 8 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-vrr-vm	Virtual route reflector (VRR)	• 4 vCPUs • 8 GB RAM • 200 GB hard disk storage	See Table 14 on page 21.
csp-central-k8mastervm	Central K8 Master VM	• 4 vCPUs • 8 GB RAM • 200 GB hard disk storage	-
csp-regional-k8mastervm	Regional K8 Master VM	• 4 vCPUs • 8 GB RAM • 200 GB hard disk storage	-

NOTE: For non-HA demo configurations, we recommend one server with 48 vCPUs and 256 GB RAM. Non-HA demo configurations have been validated with a server with 24 vCPUs and 256GB RAM , but performance issues may occur over longer periods of time.

Table 11 on page 15 shows complete details about VMs and microservice collections required for a production environment without HA.

Table 11: Details of VMs for a Production Environment Without HA

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-installer-vm	—	• 4 vCPUs • 64 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-central-infravm	Third -party applications used as infrastructure services	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-central-msvm	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-infravm	Third -party applications used as infrastructure services	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-msvm	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-sblb	Load balancer for device to microservice connectivity	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-space-vm	Junos Space Virtual Appliance and database—required only if you deploy VNFs that use this EMS	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-central-elkvm	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-regional-elkvm	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-vrr-vm	VRR	• 4 vCPUs • 8 GB RAM • 200 GB hard disk storage	See Table 14 on page 21.
csp-central-k8mastervm	Central K8 Master VM	• 4 vCPUs • 8 GB RAM • 200 GB hard disk storage	-

Table 11: Details of VMs for a Production Environment Without HA (continued)

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-regional-k8mastervm	Regional K8 Master VM	• 4 vCPUs • 8 GB RAM • 200 GB hard disk storage	-
csp-contrailanalytics-1	Contrail Analytics for a distributed deployment For a centralized or combined deployment, you use Contrail Analytics in the Contrail Cloud Platform.	• 48 vCPUs • 256 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.

Table 12 on page 16 shows complete details about the VMs for a demo HA environment.

Table 12: Details of VMs for a demo HA Environment

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-installer-vm	—	• 4 vCPUs • 48 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-central-infravm1	Third-party applications used as infrastructure services	• 4 vCPUs • 32 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-central-infravm2	Third-party applications used as infrastructure services	• 4 vCPUs • 32 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-central-infravm3	Third-party applications used as infrastructure services	• 4 vCPUs • 32 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-central-lbvm1	Load-balancing applications	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-central-lbvm2	Load-balancing applications	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-central-lbvm3	Load-balancing applications	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.

Table 12: Details of VMs for a demo HA Environment (continued)

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-central-msvm1	All microservices, including GUI applications	• 8 CPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-central-msvm2	All microservices, including GUI applications	• 8 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-central-msvm3	All microservices, including GUI applications	• 8 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-infravm1	Third-party applications used as infrastructure services	• 4 vCPUs • 32 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-infravm2	Third-party applications used as infrastructure services	• 4 vCPUs • 32 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-infravm3	Third-party applications used as infrastructure services	• 4 vCPUs • 32 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-msvm1	All microservices, including GUI applications	• 8 CPUs • 32 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-msvm2	All microservices, including GUI applications	• 8 CPUs • 32 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-msvm3	All microservices, including GUI applications	• 8 CPUs • 32 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-lbvm1	Load-balancing applications	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-regional-lbvm2	Load-balancing applications	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.

Table 12: Details of VMs for a demo HA Environment (continued)

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-regional-lbvm3	Load-balancing applications	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-space-vm	Junos Space Virtual Appliance and database—required only if you deploy VNFs that use this EMS	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-contrailanalytics-1	Contrail Analytics for a distributed deployment For a centralized or combined deployment, you use Contrail Analytics in the Contrail Cloud Platform.	• 16 vCPUs • 48 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-regional-sblb1	Load balancer for device to FMPM microservice connectivity	• 4 vCPUs • 24 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-regional-sblb2	Load balancer for device to FMPM microservice connectivity	• 4 vCPUs • 24 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-vrr-vm	Virtual route reflector (VRR)	• 4 vCPUs • 8 GB RAM • 200 GB hard disk storage	See Table 14 on page 21.

Table 13 on page 18 shows complete details about VMs and microservice collections required for a production environment with HA.

Table 13: Details of VMs for a Production Environment with HA

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-installer-vm	—	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-central-infravm1	Third-party applications used as infrastructure services	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.

Table 13: Details of VMs for a Production Environment with HA (continued)

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-central-infravm2	Third-party applications used as infrastructure services	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-central-infravm3	Third-party applications used as infrastructure services	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-central-lbvm1	Load-balancing applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-central-lbvm2	Load-balancing applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-central-lbvm3	Load-balancing applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-central-msvm1	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-central-msvm2	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-central-msvm3	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-infravm1	Third-party applications used as infrastructure services	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-infravm2	Third-party applications used as infrastructure services	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-infravm3	Third-party applications used as infrastructure services	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.

Table 13: Details of VMs for a Production Environment with HA (continued)

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-regional-msvm1	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-msvm2	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-msvm3	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 21.
csp-regional-lbvm1	Load-balancing applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-regional-lbvm2	Load-balancing applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-regional-lbvm3	Load-balancing applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-space-vm	Junos Space Virtual Appliance and database—required only if you deploy VNFs that use this EMS	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-central-elkvm1	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-central-elkvm2	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-central-elkvm3	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-regional-elkvm1	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.

Table 13: Details of VMs for a Production Environment with HA (continued)

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-regional-elkvm2	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-regional-elkvm3	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-regional-sblb1	Load balancer for device to FMPM microservice connectivity	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-regional-sblb2	Load balancer for device to FMPM microservice connectivity	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-regional-sblb3	Load balancer for device to FMPM microservice connectivity	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.
csp-vrr-vm	Virtual route reflector (VRR)	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 21.

Table 14 on page 21 shows the ports that must be open on all VMs in CSO to enable the following types of CSO communications:

- External—CSO user interface (UI) and CPE connectivity
- Internal—Connectivity between CSO components

The provisioning tool opens these ports on each VM; however, if you provision the VMs manually, you must manually open the ports on each VM.

Table 14: Ports to Open on CSO VMs

Port Number	CSO Communication Type	Port Function
22	External and internal	SSH
80	Internal	HAProxy
83	External	Network Service Designer
179	External	BGP for VRR

Table 14: Ports to Open on CSO VMs (continued)

Port Number	CSO Communication Type	Port Function
443	External and internal	HTTPS, including Administration Portal and Customer Portal
514	Internal	Syslog receiving port
1414	Internal	Cassandra Java Virtual Machine (JVM)
1936	External	HAProxy status page
1947	External	Icinga service
2181	Internal	ZooKeeper client
2216	External	CSO telemetry converter
2379	Internal	etcd client communication
2380	Internal	etcd peer
2888	Internal	ZooKeeper follower
3000	External	Grafana
3306	Internal	MySQL
3514	External	Contrail Analytics Syslog receiving port
3888	Internal	ZooKeeper leader
4001	Internal	SkyDNS etcd discover
4443	Internal	HAProxy
4505, 4506	Internal	Salt communications
5000, 5001	Internal	Keystone public
5044	Internal	Beats
5543	Internal	Logstash UDP
5601	External	Kibana UI
5665	Internal	Icinga API
5666	Internal	icinga nrpe

Table 14: Ports to Open on CSO VMs (continued)

Port Number	CSO Communication Type	Port Function
5671	Internal	RabbitMQ SSL listener
5672	Internal	RabbitMQ client
6000	Internal	Swift Object Server
6001	Internal	Swift Container Server
6002	Internal	Swift Account Server
6379	Internal	Redis
6543	Internal	Virtualized Network Function manager (VNFM)
7000	Internal	Kubernetes API server
7804	External	Device connectivity
8006	Internal	Network Service Orchestrator
8016	Internal	Notification engine
8080	Internal	cAdvisor
8081	Internal	Contrail Analytics
8082	Internal	Device Management Service (DMS) central
8083	Internal	Activation Service (AS) central
8085	Internal	DMS Schema
8086	Internal	Contrail Analytics
8090, 8091	Internal	Generic container
8528	Internal	Arango Cluster
8529	Internal	Arango DB
8530	Internal	Arango Cluster
8531	Internal	Arango Cluster
9042	Internal	Cassandra native transport
9090	Internal	Swift Proxy Server

Table 14: Ports to Open on CSO VMs (continued)

Port Number	CSO Communication Type	Port Function
9091	Internal	xmltec-xmlmail tcp
9101	External and internal	HA proxy exporter
9102	Internal	jetdirect
9160	Internal	Cassandra
9200	Internal	Elasticsearch
10000	Internal	Docker repository from CSP installer
10248	Internal	kubelet healthz
10255	Internal	kubelet
15100	Internal	Logstash TCP
15672	Internal	RabbitMQ management
30000-32767	Internal	Kubernetes service node range
30900	External	Prometheus
30901	Internal	Kubernetes
35357	Internal	Keystone private

VNFs Supported

CSO supports the Juniper Networks and third-party VNFs listed in Table 15 on page 24.

Table 15: VNFs Supported by CSO

VNF Name	Version	Network Functions Supported	Deployment Model Support	Element Management System Support
Juniper Networks vSRX	vSRX KVM Appliance 15.1X49-D125	• Network Address Translation (NAT) • Demonstration version of Deep Packet Inspection (DPI) • Firewall	• Centralized deployment • Distributed deployment supports NAT, and firewall	Element Management System (EMS) microservice, which is included with Contrail Service Orchestration (CSO)
LxCIPtable (a free, third party VNF based on Linux IP tables	14.04	• NAT • Firewall	Centralized deployment	EMS microservice

Table 15: VNFs Supported by CSO (continued)

VNF Name	Version	Network Functions Supported	Deployment Model Support	Element Management System Support
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	Distributed deployment, NFX250 platform only	EMS microservice
Silver Peak VX	VXOA 8.0.5.0_61631	WAN optimization	Distributed deployment, NFX250 platform only	EMS microservice

Licensing

You must have licenses to download and use 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, you need licenses for Network Service Orchestrator and for Network Service Controller.

  You also need licenses for the following items, depending on which you use in your deployment.

  - The vSRX application that provides the security gateway for the NFX250 device or the vSRX implementation used as a CPE device.
  - VNFs that you deploy.
  - Junos OS software for the MX Series router, including licenses for subscribers.
  - Junos OS software for the SRX Services Gateways.

- For a combined centralized and distributed deployment, you need licenses for components for both types of deployment.

Accessing GUIs

NOTE: We recommend that you use Google Chrome Version 60 or later to access the Contrail Service Orchestration (CSO) GUIs.

Table 16 on page 26 shows the URLs and login credentials for the GUIs for a non-redundant CSO installation.

Table 16: Access Details for the GUIs

GUI	URL	Login Credentials
Administration Portal	https://*central-IP-Address* where: *central-IP-Address*—IP address of the VM that hosts the microservices for the central POP For example: *https://192.0.2.1*	Specify the OpenStack Keystone username and password. The default username is **cspadmin** and the default password is **passw0rd**.
Customer Portal	Same as the URL used to access the Administration Portal	Specify the credentials when you create the Customer either In Administration Portal or with API calls.
Designer Tools—Log into Network Service Designer and click the menu in the top left of the page to access the other designer tools.	https://*central-IP-Address*:83 where: *central-IP-Address*—IP address of the VM that hosts the microservices for the central POP For example: *https://192.0.2.1:83*	Specify the OpenStack Keystone username and password. The default username is **cspadmin** and the default password is **passw0rd**.

Table 16: Access Details for the GUIs (continued)

GUI	URL	Login Credentials
Kibana This tool provides a visual representation of log files. You can use it to monitor: • Network services in a central or regional POP • Microservices in the deployment	http://*infra-vm-IP-Address* | *ha-proxy-IP-Address*:5601 where: *infra-vm-IP-Address*—IP address of the VM that hosts the infrastructure services for a central or regional POP. Use this option to monitor network services. *ha-proxy-IP-Address*—IP address of high availability (HA) proxy. Use this option to monitor the microservices. • For a non-HA deployment, use the IP address of the VM that hosts the microservices for the central POP. • For an HA deployment, use the virtual IP address that you provide for the HA proxy when you install CSO. For example: *http://192.0.2.2:5601*	Login credentials are not needed.
Grafana and Prometheus These tools provide monitoring and troubleshooting for the infrastructure services in Contrail Service Orchestration. You use Prometheus to create queries for the infrastructure services and Grafana to view the results of the queries in a visual format.	• Prometheus—*ha-proxy-IP-Address*:30900 • Grafana—*ha-proxy-IP-Address*:3000 where: *ha-proxy-IP-Address*—IP address of HA proxy • For a non-HA deployment, use the IP address of the VM that hosts the microservices for the central POP. • For an HA deployment, use the virtual IP address that you provide for the HA proxy when you install CSO. For example: *http://192.0.2.2:30900*	Login credentials are not needed.

Changes in Behavior

This section lists changes in behavior of the CSO features.

- From CSO Release 3.2 onward, editing a LAN segment assigned to a site is no longer supported.

Known Behavior

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks CSO Release 3.2.1.

Application Visiblity

- Application Visibility data is displayed only when there is at least one SD-WAN policy configured on the SD-WAN CPE.

Installation

- Deployments where CSO is behind NAT require spokes and hubs to be able to reach the VRR without NAT.
- For SD-WAN deployments, CPE behind NAT is not supported.
- If the Kubernetes minion node in the central or regional microservices VM goes down, the pods on the minion node are moved to the Kubernetes master node. When you bring the minion node back up, the pods do not automatically rebalance across the nodes.
- In CSO Release 3.2.1, the virtual machine (VM) on which the virtual route reflector (VRR) is installed supports only one management interface.
- Before upgrading vSRX by using CSO, execute the **request system storage cleanup** command on the vSRX from the Junos OS CLI.

Policy Deployment

- The deployment of fiirewall policies with UTM profiles fails on sites (devices) on which UTM licenses are not present. Ensure that you install the required licenses before deploying firewall policies that are associated with UTM profiles.

  In addition, when you add new sites or departments, firewall policies that are automatically deployed to the sites might fail if licenses are not installed. In such cases, install the licenses on the applicable sites and re-deploy the failed policy.
- After ZTP of SD-WAN CPE, you must install APBR licenses and app signatures prior to deploying SD-WAN policies through the administrator portal GUI .
- 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.
- If you are creating an SLA profile and want to specify the advanced configuration, then you must specify the maximum upstream rate, maximum upstream burst size, maximum downstream rate, and maximum downstream burst size.
- Dynamic SLA is not supported for full mesh topology; only static policies are supported.

Security Management

- In CSO Release 3.2.1, intrusion prevention system (IPS) is not supported. Therefore, in the IPS report, the attack name from the IPS signatures is displayed as UNKNOWN.
- In CSO Release 3.2.1, SSL Proxy is not supported on SRX300 and SRX320 series devices.

- When you create an antivirus profile, the engine types Kaspersky and Juniper Express are not supported.
- Firewall rules are pushed to the device depending on the order in which the firewall policy intents are resolved.

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 CPE.
- You can use the Administration Portal to upload licenses to Contrail Service Orchestration; however, you cannot use the Administration Portal to install licenses on physical or virtual devices that Contrail Service Orchestration manages. You must use the APIs or the license installation tool to install licenses on devices.
- Contrail Service Orchestration 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 the Administration Portal to specify the root password in the device template.

  To specify a root password for the device:

  1. Log in to the Administration Portal.
  2. Select **Resources>Device Templates**.
  3. Select the device template and click **Edit**.
  4. Specify the encrypted value for the root password in the **ENC_ROOT_PASSWORD** field.
  5. Click **Save**.

- In CSO Release 3.2.1, 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 Seriesdevices.
- 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.

- Site names across tenants must be unique—that is, you cannot use the same site name across tenants.
- In rare cases, site routes are not advertised to the hub, which results in the sites not being reachable.

  Workaround: Delete the LAN segments for the sites that are not reachable and add the LAN segments again.

Topology

- Changing the DHCP IP address on the OAM interface is not supported.
- Hybrid-WAN and SD-WAN deployments using the same MX Series device as a hub is not supported.
- When using MX as a SD-WAN hub, NAT configuration must be done on MX Series routers using Stage-2 configuration templates.
- DHCP configuration on WAN links on a SD-WAN hub is not supported.
- CSO Release 3.2.1 does not support automatic hub-meshing. Hub-meshing must be performed manually in order for traffic to flow between the hubs.
- IP addresses of the first two WAN interfaces of a site that is part of a full mesh topology deployment cannot be changed once it is provisioned.

User Interface

- When you use Mozilla Firefox to access the Contrail Service Orchestration (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.
- The preferred link for the underlay is not displayed in the GUI.

General

- In CSO Release 3.2.1, 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_3.2.1/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.

Known Issues

This section lists the known issues for the Juniper Networks CSO Release 3.2.1.

CSO HA

- In a three-node setup, two nodes are clustered together, but the third node is not part of the cluster. In addition, in some cases, the RabbitMQ nodes are also not part of the cluster. This is a rare scenario, which can 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 RabbitMQ dashboard for the central microservices VM (http://*central-microservices-vip*:15672) and the regional microservices VM (http://*regional-microservices-vip*:15672).

  2. Check the RabbitMQ overview in the dashboards to see if all the available infrastructure nodes are present in the cluster.

  3. If an infrastructure node is not present in the cluster, do the following:

     a. Log in to the VM of that infrastructure node.

     b. Open a shell prompt and execute the following commands sequentially:

        rabbitmqctl stop_app

        service rabbitmq-server stop

        rabbitmqctl stop_app command

        rm -rf /var/lib/rabbitmq/mnesia/

        service rabbitmq-server start

        rabbitmqctl start_app

  4. In the RabbitMQ dashboards for the central and regional microservices VMs, confirm that all the available infrastructure nodes are present in the cluster.

  [CXU-12107]

- Data in the Maria database instances of a cluster mode can go out of sync when a central Infrastructure fails.

  Workaround: You must manually synchronize the Maria database instances. Contact Juniper Networks Technical Support for instructions. [CXU-13128]

- In an HA deployment, when one of the central infrastructure hosts goes down, the SD-WAN workflow fails.

  Workaround: Contact Juniper Networks Technical Support. [CXU-16273]

- CSO may not come up after a power failure.

  Workaround: Contact Juniper Networks Technical Support. [CXU-16530]

- Data in Maria DB instances in cluster mode may go out of sync upon central infrastructure failures.

Workaround: You must manually synchronize the Maria DB instances. Contact Juniper Networks Technical Support for instructions. [CXU-13128’

- In HA deployment, when one of the central infrastructure host is down, SD-WAN workflows fail.

  Workaround: Contact Juniper Networks Technical Support. [CXU-16273]

- Sometimes CSO may not come up after power failure.

  Workaround: Contact Juniper Networks Technical Support. [CXU-16530]

Installation

- In a HA setup, the time configured for the CAN VMs might not be synchronized with the time configured for the other VMs in the setup. This can cause issues in the throughput graphs.

  Workaround:

  1. Log in to can-vm1 as root.
  2. Modify the */etc/ntp.conf* file to point to the desired NTP server.
  3. Restart the NTP process.

  After the NTP process restarts successfully, can-vm2 and can-vm3 automatically re-synchronize their times with can-vm1.

  [CXU-15681]

Policy Deployment

- Automatic Policy deployments on new Site addition (for example, auto NAT, firewall, SD-WAN) can sometimes fail due to trusted certificate installations on the device happening in parallel.

  Workaround: To redeploy the failed job, open the **Configuration > Deployments > History** window, select the failed job and click **Re-Deploy**. [CXU-16652]

- If you create a firewall policy and deploy it to the device, and subsequently create one or more firewall policy intents without re-deploying the policy, the firewall policy is automatically deployed to the device when there's a change in the topology, such as the addition of a new site, department, or LAN segment.

  Workaround: Create firewall policy intents when you intend to deploy them to the device and re-deploy the policy. [CXU-15794]

Site and Tenant Workflow

- ZTP for SRX Series devices will not work with a redirect server because a BOOTSTRAP complete message is not received when ZTP is initiated through a redirect server.

  Workaround: Use a CSO regional server instead of a redirect server for CPE activation. [CXU-14099]

- ZTP fails on SRX 3xx Series device CPE because DHCP bindings already exist on CPE.

  Workaround: Manually clear the DHCP bindings on the CPE and restart ZTP. [CXU-13446]

- 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. [CXU-9070]

- When both the OAM and data interfaces are untagged, ZTP fails when using a NFX Series platform as CPE.

  Workaround: Use tagged interfaces for both OAM and data. [CXU-15084]

- The tenant creation job might fail if connectivity from CSO to VRR is lost during job execution.

  Workaround: If the tenant creation job fails and the tenant is created in CSO, delete the tenant and retrigger the tenant creation. [CXU-16884]

Topology

- When configuring the SRX spoke in the multihoming topology with a cloud hub and enterprise hub, the administration portal displays a **Primary Hub and Secondary Hub must belong to a same Device Family** error message.

  Workaround: Click **OK** to dismiss this error. You can ignore this error message. [CXU-16662]

- When an MX Series device is used as a hub, site-to-site traffic in the reverse direction in the hub-and-spoke topology might not take the desired path from the hub to the originating spoke. However, there is no traffic loss.

  Workaround: None. [CXU-15970]

- On link failover, in some cases, the traffic between the hub and spoke takes an incorrect physical path because the existing session flow is not updated with the new generic routing encapsulation (GRE) interface information. However, there is no traffic loss.

  Workaround: None. [PR 1341274]

- In case of GRE over IPsec, the GRE tunnel's OAM status might be displayed as **Up** even when tunnel source interface is **Down** because of which alarms might not be triggered. However, there is no impact on the traffic flow.

  Workaround: None. [PR 1341283]

User Interface

- Sorting by **Administrator** in the tenant page displays an error message.

  Workaround: This is an invalid error message. Click **OK** to continue. [CXU-16642]

- If sites are removed without first undeploying the associated policies, the removal of SLA profiles fails.

  Workaround: Delete and deploy all the associated SD-WAN policies before removing sites. [CXU-13179]

General

- If you create a report definition that is scheduled to run at a later date and time, the report is not generated.

  Workaround: Modify the report definition to run the report immediately and then generate the report. [CXU-11677]

- 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. [CXU-15033]

- When you perform the microservices VM failure tests and the Kubernetes nodes go to the **not ready** state, some Docker pods might not come up in the **running** state.

  Workaround: Contact Juniper Networks Technical Support. [CXU-16541]

- The reboot of the central infrastructure VM is not supported.

  Workaround: If the VM reboots, contact Juniper Networks Technical Support. [CXU-17242]

Resolved Issues

The following issues are resolved in Juniper Networks CSO Release 3.2.1.

- Whenever a new site is added and auto-NAT is enabled, a NAT policy job is triggered for all existing sites as well as for the new site. There is no impact to functionality; however, you will see additional jobs listed in the system.
- Site-to-site traffic in the reverse direction in the hub-and-spoke topology mightnot take the desired path from the hub to the originating spoke. [CXU-16070]
- The WAN link status does not change in the Site Management page of the Administration Portal when there are Link Up and LInk Down alarms. [CXU-16636]

Documentation Updates

This section lists the errata and changes in the CSO Release 3.2.1 documentation:

- **Configuring devices from the POPs landing page**—From CSO Release 3.1 onward, you can configure devices from the POPs page as follows:

1. Select **Resources > POPs > *Pop-Name***.

   The *Pop-Name* page appears.

2. Click the **Routers** tab.

3. Select the device that you want to configure and click the **Configure Device** button.

   The Stage 2 Config page appears. This page is dynamically rendered based on stage-2 configuration specified in the device profile.

4. Enter the configuration data on the page.

5. Click **Save** to save the configuration.

   A confirmation message is displayed and the deployment status changes to **pending deployment**.

6. Click **Deploy** to save and deploy the configuration.

   A confirmation message is displayed indicating that the job is created and subsequently that the job was successful. You can click **Deploy History** to view the job logs.

7. Click **Cancel** to go back to the *Pop-Name* page.

- **Monitoring screen events**—From CSO Release 3.2 onward, you can view and monitor screen events from the Screen Events page. To access this page, select **Monitor > Security Events > Screen** in Customer Portal.

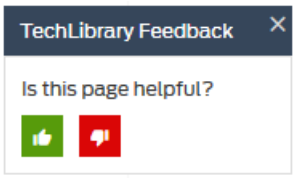
  You can use the Screen Events page to view information about screen events based on screen options:

  - The information displayed about screen events includes information about ICMP screening, IP screening, TCP screening, and UDP screening.
  - You can use the time-range slider to focus on the period in which you are most interested. After you select the time range, all of the data presented in your view is refreshed automatically. You can also use the **Custom** button to set a custom time range.
  - There are two ways to view your data—summary view and detailed view. To view summary data, click the **Summary View** tab; to view detailed data, click the **Detail View** tab.

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/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at https://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://www.juniper.net/support/requesting-support.html.

Revision History

24 October 2018—Revision 6

24 May 2018—Revision 5

2 March 2018—Revision 4

26 February 2018—Revision 3

23 February 2018—Revision 2

20 February 2018—Revision 1, Contrail Service Orchestration Release 3.2.1