Cloud CPE Solution Release Notes

Release 3.0.1
27 July 2017
Revision 1

These Release Notes accompany Release 3.0.1 of the Juniper Networks® Cloud CPE Solution. They contain installation information, and they describe new and changed features, limitations, and known and resolved issues in the software.

Contents

Introduction 2
New and Changed Features 3
Node Servers and Servers Tested in the Cloud CPE Solution 5
Software Tested for COTS Servers 6
Network Devices and Software Tested for the Contrail Cloud Platform (Centralized Deployment) 6
Network Devices and Software Tested for Use with CPE Devices (Distributed Deployment) 8
Minimum Hardware Requirements for the Cloud CPE Solution 9
Software and VM Requirements 11
Accessing GUIs 21
VNFs Supported 22
Licensing 23
Known Behavior 24
Known Issues 26
Resolved Issues 30
Installation Instructions 32
Software Installation Requirements for the NFX250 Device 32
Requesting Technical Support 32
Self-Help Online Tools and Resources 33
Opening a Case with JTAC 33
Revision History 33

Copyright © 2017, Juniper Networks, Inc.

Introduction

The Juniper Networks Cloud Customer Premises Equipment (CPE) 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. Based on the European Telecommunications Standards Institute (ETSI) standards for Network Functions Virtualization (NFV) management and orchestration (MANO), the Cloud CPE solution offers end-to-end provisioning of Layer 4 through Layer 7 network services through an open, cloud-based architecture. The solution supports both Juniper Networks and third-party virtualized network functions (VNFs) that network providers use to create the network services.

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.

The Cloud CPE solution 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:

Copyright © 2017, Juniper Networks, Inc.

- 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 components connect to Network Service Orchestrator through its RESTful API:

- 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 the Cloud CPE solution, 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 the Cloud CPE solution in a demonstration (demo) or production environment. Table 1 on page 3 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 Sites and VNFs Supported for a Distributed Solution	Number of VNFs Supported for a Centralized Deployment
Demo non-HA Configuration	25 sites, 2 VNFs per site	Up to 10 VNFs
Production non-HA Configuration	Up to 200 sites, 2 VNFs per site	Up to 500 VNFs, 20 VNFs per Contrail compute node
Trial HA Configuration	Up to 200 sites, 2 VNFs per site	Up to 100 VNFs, 20 VNFs per Contrail compute node
Production HA Configuration	Up to 2000 sites, 2 VNFs per site	Up to 500 VNFs, 20 VNFs per Contrail compute node

New and Changed Features

- **Support for customizing applications and SLA policies for on-premise sites**—You can now use Customer Portal to customize applications and service-level agreement (SLA) policies for on-premise sites.

Copyright © 2017, Juniper Networks, Inc.

  - To view the applications on a SD-WAN links in the network, select **Monitor** > **Overview** to view the geographical map that displays points of presence (PoPs), sites, and connections. Click an SD-WAN link on the map to view details about the applications on the link.
  - To view summary statistics for the applications on an SD-WAN link, select **Tenants** > **Tenant Name** > **Tenant Applications**.
  - To view more detailed statistics about the applications on an SD-WAN link, select **Tenants** > **Tenant Name** > **Site Name** .

- **Monitoring applications on an SD-WAN link**—You can now use Administration Portal to monitor information about applications on SD-WAN links and on-premise sites in an SD-WAN configuration.
  - To view the applications on a SD-WAN links in the network, select **Monitor** > **Overview** to view the geographical map that displays PoPs, sites, and connections. Click an SD-WAN link on the map to view details about the applications on the link.
  - To view summary statistics for the applications on an SD-WAN link, select **Tenants** > **Tenant Name** > **Tenant Applications**.
  - To view more detailed statistics about the applications on an SD-WAN link, select **Tenants** > **Tenant Name** > **Site Name**.
- **Support for Riverbed Steelhead VNF on NFX250 devices**—You can now use the Riverbed Steelhead application as a VNF for WAN optimization on an NFX250 device.
- **New port number for Administration Portal**—The port number for Administration Portal has changed to 443 from 81. When you access Administration Portal, you use the URL http*://central-IP-Address*, where *central-IP-Address* is the IP address of the VM that hosts the microservices for the central POP. For example: *http://192.0.2.1*.
- **Support for 2000 NFX250 devices for a Contrail Service Orchestration installation**—Each Contrail Service Orchestration installation can support up to 2000 NFX250 devices, with one NFX250 device at a site.
- **Support for microservices high availability for distributed deployments**—Microservices high availability (HA) is now supported for distributed deployments. In Cloud CPE Soluton releasese before 3.0, microservices high availability is supported only for centralized deployments.
- **Enhanced onboarding of VNFs and design capabilities for network services**—The Designer Tools suite now includes three components for creating network services based on Juniper Networks and third-party VNFs:
  - Configuration Designer, which you use to create configuration templates that determine how VNFs are implemented in a deployment.
  - Resource Designer, which you use to create VNF packages that specify the network functions, function chains, performance, and a configuration template.
  - Network Service Designer, which you use to create network services packages based on VNF packages. This component was available in previous releases.

Copyright © 2017, Juniper Networks, Inc.

- **Addition of license cost as a performance goal in Network Service Designer**—You can now specify the cost of a VNF license as a performance goal when you create a network service with the Designer Tools.
- **Support for enabling VNF recovery**—You can now specify whether to enable automatic recovery for VNFs in a network service instance in a centralized deployment. You can enable this feature through Administration Portal or the API. In previous releases, automatic recovery was permanently enabled for all VNFs. Disabling automatic recovery for a VNF allows you to quickly investigate a network problem or a problem with the VNF itself. Enabling automatic recovery increases resiliency and automaticity of the implementation.
- **Support for NFX250-LS1 Model**—You can now deliver network services on an NFX250-LS1 Network Services Platform in addition to the NFX250-S1 and NFx250-S2 models supported previously.
- **Streamlined activation process for CPE devices**—You can now activate NFX250 and SRX CPE devices in Customer Portal. NFX250 devices require a code for activation; however, SRX Series devices do not.

  Previously, you activated NFX250 devices by entering the activation code through the NFX console and SRX Series devices by copying the configuration from Customer Portal and pasting it into the SRX Series console.
- **Support for port-forwarding on NFX250 devices**—Port-forwarding is now enabled for all NFX250 device templates. Port-forwarding enables Contrail Service Orchestration to manage an NFX250 device through a single IP address
  - The NFX_deployment_option_4 and NFX_Basic_SDWAN_CPE templates offer device-initiated connections (outbound SSH) with port-forwarding capability.
  - The NFX_deployment_option_1 template offers port-forwarding with the connection initiated by Contrail Service Orchestration.
  - The NFX_Internet_Managed _CPE template uses IP connectivity without IPsec.
- **Support for configuring device templates in Administration Portal**—You can now create additional device templates and modify existing device templates from the Administration Portal. Previously, you could use only the device templates installed with Contrail Service Orchestration and you could not modify them. Log in to Administration Portal and click **Resources > Device Templates** to access the following options:
  - Clone—Clone an existing device template with your preferred configuration and customize it as needed.
  - Edit—Modify the routing configuration and LAN configuration for an existing device template.
  - Import—Import a new device template in JSON format from your local machine.

Node Servers and Servers Tested in the Cloud CPE Solution

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

Copyright © 2017, Juniper Networks, Inc.

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

Table 2 on page 6 lists the node servers and servers that have been tested for these functions in the Cloud CPE solution. You should use these specific node servers or servers for the Cloud CPE solution.

Table 2: COTS Node Servers and Servers Tested in the Cloud CPE Solution

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	1 U rack-mounted server

Software Tested for COTS Servers

Table 3 on page 6 shows the software that has been tested for the Cloud CPE solution. You must use these specific versions of the software when you implement the Cloud CPE solution.

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
Operating system for VMs on Contrail Service Orchestration servers	Ubuntu 14.04.5 LTS
Hypervisor on Contrail Service Orchestration servers	• Centralized deployment: Contrail Cloud Platform Release 3.0.2, 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 3.0.2 with Heat v2 APIs
Contrail Analytics	Contrail Release 4.0

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 7.

Copyright © 2017, Juniper Networks, Inc.

- The software described in Table 5 on page 7.

  You must use these specific versions of the software for the Cloud CPE Solution release 3.0.1.

Table 4: Network Devices Tested for the Contrail Cloud Platform

Function	Device	Model	Quantity
SDN gateway router	Juniper Networks MX Series 3D Universal Edge Router	MX80-48T router with two 10-Gigabit Ethernet interfaces containing XFP transceivers	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	QFX5100-48S-AFI switch with: • 48 10-Gigabit Ethernet interfaces containing SFP+ transceivers • 6 QSFP+ transceiver interfaces	1

Table 5: Software Tested in the Cloud CPE Centralized Deployment

Function	Software and Version
Operating system for MX Series router	Junos OS Release 14.2R3
Operating system for EX Series switch	Junos OS Release 12.3R10
Operating system for QFX Series switch	Junos OS Release 13.2X51-D38
Hypervisor on Contrail Service Orchestration servers	Contrail Cloud Platform Release 3.0.2 or VMware ESXi Version 5.5.0
Element management system software	EMS microservice Junos Space Network Management Platform Release 15.1R1 (for VNFs that require this product)
Software-defined networking (SDN) for a centralized deployment	Contrail Cloud Platform Release 3.0.2
Contrail Analytics	Contrail Release 4.0
Virtualized infrastructure manager (VIM) and virtual machine (VM) orchestration	OpenStack Liberty or Kilo
Authentication and Authorization	OpenStack Liberty or Kilo
Network Functions Virtualization (NFV)	Contrail Service Orchestration Release 3.0.1

Copyright © 2017, Juniper Networks, Inc.

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 8.
- The software described in Table 7 on page 8.

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

Table 6: Network Devices Tested for the Distributed Deployment

Function	Device	Model	Quantity
PE router and IPsec concentrator	Juniper Networks MX Series 3D Universal Edge Router	• MX960, MX480, or MX240 router with MS-MPC line card • MX80 or MX104 router with MX-MIC line card • Other MX Series routers with an MS-MPC or MX-MIC are supported	1 per POP
SDN gateway for SD-WAN Edge	Juniper Networks SRX Series Services Gateway	SRX4200 Services Gateway	1 per POP
CPE device	• 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 • vSRX 15.1X49-D100	1 per customer site

Table 7: Software Tested in the Distributed Deployment

Function	Software and Version
Hypervisor on Contrail Service Orchestration 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)	Contrail Service Orchestration Release 3.0.1
Contrail Analytics	Contrail Release 4.0
NFX Software	Junos OS Release 15.1X53-D47
Routing and Security for NFX250 device	vSRX KVM Appliance MD5 SHA1 15.1X49-D100
Operating system for vSRX used as a CPE device on an x86 server	vSRX KVM Appliance MD5 SHA1 15.1X49-D100

Copyright © 2017, Juniper Networks, Inc.

Table 7: Software Tested in the Distributed Deployment *(continued)*

Function	Software and Version
Operating system for SRX Series Services Gateway used as a CPE device	Junos OS Release 15.1X49-D100
Operating system for MX Series router used as PE router	Junos OS Release 16.1R3.00
Operating system for SRX Series Services Gateway used as an SDN WAN gateway	Junos OS Release 15.1X49-D100

Minimum Hardware Requirements for the Cloud CPE Solution

Table 2 on page 6 lists the makes and models of node servers and servers that you can use in the Cloud CPE solution. When you obtain node servers and servers for the Cloud CPE Solution, 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 9 shows the required hardware specifications for node servers and servers in a demo environment and in a trial high avalability (HA) environment.

Table 8: Demo Environment or Trial High Availability Environment

Function	Demo Environment	Trial 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 GE interface	One GE or 10 GE interface
Contrail Service Orchestration Servers (includes Contrail Analytics in a VM)		
Number of nodes or servers	1	3
vCPUs	48	48

Copyright © 2017, Juniper Networks, Inc.

Table 8: Demo Environment or Trial High Availability Environment *(continued)*

Function	Demo Environment	Trial HA Environment
RAM	128 GB	128 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	16	48
RAM	64 GB	256 GB

Table 9 on page 10 shows the required hardware specifications for node servers and servers in a production environment.

Table 9: Production Environment

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 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
Number of nodes or servers for an HA environment	6 • 3 central servers • 3 regional servers
vCPUs	48
RAM	256 GB

Copyright © 2017, Juniper Networks, Inc.

Table 9: Production Environment *(continued)*

Server Function	Values
Contrail Analytics Server for a Distributed Deployment	
Number of nodes or servers	1
vCPUs	48
RAM	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 VM Requirements

You must use the software versions that were tested in the Cloud CPE solution. This section shows the VMs required for each type of environment.

Table 10 on page 11 shows complete details about the VMs required for a demo environment. High availabilty is not included with the demo environment.

Table 10: Details for VMs for a 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 19.
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 19.
csp-central-msvm	All microservices, including GUI applications	• 4 vCPUs • 32 GB RAM • 200 GB hard disk storage	See Table 14 on page 19.
csp-regional-infravm	Third-party applications used as infrastructure services	• 4 vCPUs • 32 GB RAM • 200 GB hard disk storage	See Table 14 on page 19.

Copyright © 2017, Juniper Networks, Inc.

Table 10: Details for VMs for a Demo Environment *(continued)*

Name of VM	Components That Installer Places in VM	Resources Required	Ports to Open
csp-regional-msvm	All microservices, including GUI applications	• 4 vCPUs • 32 GB RAM • 200 GB hard disk storage	See Table 14 on page 19.
csp-regional-fmpmlb	Load balancer for device to Fault Management Performance Management (FMPM) microservice connectivity	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-space-vm	Junos Space Virtual Appliance and database—required only if you deploy virtualized network functions (VNFs) that use this EMS	• 4 vCPUs • 32 GB RAM • 200 GB hard disk storage	See Table 14 on page 19.
csp-contrail-analytics-vm	Contrail Analytics for a distributed deployment For a centralized deployment, you specify use of Contrail Analytics in the Contrail Cloud Platform.	• 4 vCPUs • 32 GB RAM • 200 GB hard disk storage	See Table 14 on page 19.

Table 11 on page 12 shows complete details about the VMs for a trial high availability environment.

Table 11: VMs for a Trial Environment

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 19.
csp-central-infravm1	Third-party applications used as infrastructure services	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-central-infravm2	Third-party applications used as infrastructure services	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-central-infravm3	Third-party applications used as infrastructure services	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-central-lbvm1	Load-balancing applications	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.

Copyright © 2017, Juniper Networks, Inc.

Table 11: VMs for a Trial Environment *(continued)*

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-central-lbvm2	Load-balancing applications	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-central-lbvm3	Load-balancing applications	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-central-msvm1	All microservices, including GUI applications	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-central-msvm2	All microservices, including GUI applications	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-regional-infravm1	Third-party applications used as infrastructure services	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-regional-infravm2	Third-party applications used as infrastructure services	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-regional-infravm3	Third-party applications used as infrastructure services	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-regional-msvm1	All microservices, including GUI applications	• 6 CPUs • 48 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-regional-msvm2	All microservices, including GUI applications	• 6 CPUs • 48 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-regional-lbvm1	Load-balancing applications	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-regional-lbvm2	Load-balancing applications	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.

Copyright © 2017, Juniper Networks, Inc.

Table 11: VMs for a Trial 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 19.
csp-space-vm	Junos Space Virtual Appliance and database—required only if you deploy VNFs that use this EMS	• 6 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-contrail-analytics-vm1	Contrail Analytics for a distributed deployment For a centralized deployment, you specify use of Contrail Analytics in the Contrail Cloud Platform.	• 6 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-contrail-analytics-vm2	Contrail Analytics for a distributed deployment For a centralized deployment, you specify use of Contrail Analytics in the Contrail Cloud Platform.	• 6 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-contrail-analytics-vm3	Contrail Analytics for a distributed deployment For a centralized deployment, you specify use of Contrail Analytics in the Contrail Cloud Platform.	• 6 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-regional-fmpmlb1	Load balancer for device to FMPM microservice connectivity	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-regional-fmpmlb2	Load balancer for device to FMPM microservice connectivity	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-regional-fmpmlb3	Load balancer for device to FMPM microservice connectivity	• 4 vCPUs • 16 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.

Table 12 on page 15 shows complete details about VMs and microservice collections required for a production environment without high availability.

Copyright © 2017, Juniper Networks, Inc.

Table 12: VMs for a Production Environment Without High Availability

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 19.
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 19.
csp-central-msvm	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
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 19.
csp-regional-msvm	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-regional-fmpmlb	Load balancer for device to Fault Management Performance Management (FMPM) microservice connectivity	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
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 19.
csp-contrail-analytics-vm	Contrail Analytics for a distributed deployment For a centralized deployment, you specify use of Contrail Analytics in the Contrail Cloud Platform.	• 8 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-central-elkvm	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-regional-elkvm	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.

Copyright © 2017, Juniper Networks, Inc.

Table 13 on page 16 shows complete details about VMs and microservice collections required for a production environment with high availability.

Table 13: VMs for a Production Environment with High Availability

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 19.
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 19.
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 19.
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 19.
csp-central-lbvm1	Load-balancing applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-central-lbvm2	Load-balancing applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-central-lbvm3	Load-balancing applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-central-msvm1	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-central-msvm2	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-central-msvm3	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
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 19.

Copyright © 2017, Juniper Networks, Inc.

Table 13: VMs for a Production Environment with High Availability *(continued)*

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
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 19.
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 19.
csp-regional-msvm1	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-regional-msvm2	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-regional-msvm3	All microservices, including GUI applications	• 16 vCPUs • 64 GB RAM • 500 GB hard disk storage	See Table 14 on page 19.
csp-regional-lbvm1	Load-balancing applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-regional-lbvm2	Load-balancing applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-regional-lbvm3	Load-balancing applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
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 19.
csp-contrail-analytics-vm1	Contrail Analytics for a distributed deployment For a centralized deployment, you specify use of Contrail Analytics in the Contrail Cloud Platform.	• 8 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.

Copyright © 2017, Juniper Networks, Inc.

Table 13: VMs for a Production Environment with High Availability *(continued)*

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-contrail-analytics-vm2	Contrail Analytics for a distributed deployment For a centralized deployment, you specify use of Contrail Analytics in the Contrail Cloud Platform.	• 8 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-contrail-analytics-vm3	Contrail Analytics for a distributed deployment For a centralized deployment, you specify use of Contrail Analytics in the Contrail Cloud Platform.	• 8 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-central-elkvm1	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-central-elkvm2	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-central-elkvm3	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-regional-elkvm1	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-regional-elkvm2	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-regional-elkvm3	Logging applications	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-regional-fmpmlb1	Load balancer for device to FMPM microservice connectivity	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.
csp-regional-fmpmlb2	Load balancer for device to FMPM microservice connectivity	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.

Copyright © 2017, Juniper Networks, Inc.

Table 13: VMs for a Production Environment with High Availability *(continued)*

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-regional-fmpmlb3	Load balancer for device to FMPM microservice connectivity	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 14 on page 19.

Table 14 on page 19 shows the ports that must be open on all VMs in the Cloud CPE Solution to enable the following types of CSO communications:

- External—CSO user interface (UI) and CPE connectivity
- Internal—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 VMs in the Cloud CPE Solution

Port Number	CSO Communication Type	Port Function
22	External and internal	SSH
80	internal	HAProxy
82	External	Customer Portal
83	External	Network Service Designer
443	External and internal	HTTPS, including Administration Portal
1414	internal	Cassandra Java Virtual Machine (JVM)
1936	External	HAProxy status page
1947	External	Icinga service
2181	internal	ZooKeeper client
2379	internal	etcd client communication
2380	internal	etcd peer
2888	internal	ZooKeeper follower
3000	External	Grafana
3306	internal	MySQL
3888	internal	ZooKeeper leader

Copyright © 2017, Juniper Networks, Inc.

Table 14: Ports to Open on VMs in the Cloud CPE Solution *(continued)*

Port Number	CSO Communication Type	Port Function
4001	internal	SkyDNS etcd discover
4505, 4506	internal	Salt communications
5000	External	Keystone public
5044	internal	Beats
5543	internal	Logstash UDP
5601	External	Kibana UI
5665	internal	Icinga API
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)
7804	External	Device connectivity
8006	internal	Network Service Orchestrator
8016	internal	Notification engine
8080	internal	cAdvisor
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
9042	internal	Cassandra native transport

Copyright © 2017, Juniper Networks, Inc.

Table 14: Ports to Open on VMs in the Cloud CPE Solution *(continued)*

Port Number	CSO Communication Type	Port Function
9090	internal	Swift Proxy Server
9160	internal	Cassandra
9200	internal	Elasticsearch
10248	internal	kubelet healthz
15100	internal	Logstash TCP
15672	internal	RabbitMQ management
30000-32767	internal	Kubernetes service node range
30900	External	Prometheus
35357	internal	Keystone private

Accessing GUIs

Table 15 on page 21 shows the URLs and login credentials for the GUIs for a Contrail Service Orchestration installation.

Table 15: Access Details for the GUIs

GUI	URL	Login Credentials
Administration Portal	http://*central-IP-Address*: where: *central-IP-Address*—IP address of the VM that hosts the microservices for the central POP For example: *http://192.0.2.1*	Specify the OpenStack Keystone username and password. The default username is **cspadmin** and the default password is **passw0rd**.
Customer Portal	http://*central-IP-Address*:82 where: *central-IP-Address*—IP address of the VM that hosts the microservices for the central POP For example: *http://192.0.2.1:82*	Specify the credentials when you create the Customer either In Administration Portal or with API calls.

Copyright © 2017, Juniper Networks, Inc.

Table 15: Access Details for the GUIs *(continued)*

GUI	URL	Login Credentials
Kibana	http://*infra-vm-IP-Address*:5601 where: *infra-vm-IP-Address*—IP address of the VM that hosts the infrastructure services for a central or regional POP For example: *http://192.0.2.2:5601*	Login credentials are not needed.
Designer Tools—Log in to Network Service Designer and click the menu in the top left of the page to access the other designer tools.	http://*central-IP-Address*:83 where: *central-IP-Address*—IP address of the VM that hosts the microservices for the central POP For example: *http://192.0.2.1:83*	Specify the OpenStack Keystone username and password. The default username is **cspadmin** and the default password is **passw0rd**.
Service and Infrastructure Monitor	http://*central-IP-Address*:1947/icingaweb2 where: *central-IP-Address*—IP address of the VM that hosts the microservices for the central POP For example: *http://192.0.2.1:1947/icingaweb2*	The default username is **icinga** and the default password is **csoJuniper**.

VNFs Supported

The Cloud CPE solution supports the Juniper Networks and third-party VNFs listed in Table 16 on page 22.

Table 16: VNFs Supported by the Cloud CPE Solution

VNF Name	Network Functions Supported	Deployment Model Support	Element Management System Support
Juniper Networks vSRX	• Network Address Translation (NAT) • Demonstration version of Deep Packet Inspection (DPI) • Firewall • Unified Threat Management (UTM)	• Centralized deployment • Distributed deployment supports NAT, firewall, and UTM	EMS microservice

Copyright © 2017, Juniper Networks, Inc.

Table 16: VNFs Supported by the Cloud CPE Solution *(continued)*

VNF Name	Network Functions Supported	Deployment Model Support	Element Management System Support
LxCIPtable (a free, third party VNF based on Linux IP tables)	• NAT • Firewall	Centralized deployment	EMS microservice
Cisco Cloud Services Router 1000V Series (CSR-1000V)	Firewall	Centralized deployment	Junos Space Network Management Platform
Riverbed Steelhead	WAN optimization	Distributed deployment, NFX250 platform only, not available if you use the NFX_Basic_SDWAN_CPE device template	EMS microservice
Silver Peak VX	WAN optimization	Distributed deployment, NFX250 platform only, not available if you use the NFX_Basic_SDWAN_CPE device template	EMS microservice

Licensing

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

The Cloud CPE solution 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.

Copyright © 2017, Juniper Networks, Inc.

  - 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 DHCP 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.

Known Behavior

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks Cloud CPE Solution Release 3.0.1.

- For a centralized deployment, use the following command to check that the JSM Heat resource is available in Contrail OpenStack on the Contrail Controller..

  1. Log in to the Contrail Controller node as root.

  ```
  root@hostHeat resource-type-list | grep JSM
  ```

  If the file is missing,

  1. Copy the **jsm.py** file to the directory **/etc/heat/heat.conf** on the Contrail Controller node.

  2. Restart the heat engine.

- When you use Customer Portal to activate a network service on a network link, you must configure the following settings for each VNF in the network service:
  - Hostname
  - NTP server
  - DNS name server
- We recommend that you use the current version of the Google Chrome Web browser to access Contrail Service Orchestration GUIs.
- When a tenant object is created through Administration Portal or the API, 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, the Junos Space Virtual Appliance might fail to discover a VNF or Contrail OpenStack might drop traffic.

  [CXU-1242]

Copyright © 2017, Juniper Networks, Inc.

- Contrail Service Orchestration does not offer a single 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.

  [CXU-3630]

- You can use Administration Portal to upload licenses to Contrail Service Orchestration; however, you cannot use 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.

  [CXU-3631]

- 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 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 encrypted value for the root password in the ENC_ROOT_PASSWORD field.
  5. Click **Save**.

  [CXU-5990]

- You can use the logs on an NFX250 device to review the status of the device's activation through Customer Portal.

  [CXU-6188]

- When you have more than five sites configured in Customer Portal, you cannot access the configuration links for all the sites in the topology on the Monitor page.

  Workaround: Select the site in the left navigation pane to configure it.

  [CXU-6590]

- When you activate a CPE device in Customer Portal, there is no indicator for the status of the activation.

  Workaround: None

  [CXU-6705]

- You might see **quotaclient error compute** messages in the **nso-pyramid-api.log** Network Service orchestration log.

Copyright © 2017, Juniper Networks, Inc.

Workaround: Ignore the messages.

[CXU-7003]

Known Issues

This section lists known issues for the Juniper Networks Cloud CPE Solution Release 3.0.1.

- Administration Portal might take a short while to update data fields after you delete objects.

  [CXU-1806]

- Some notifications about the success or failure of create and delete operations in Administration Portal are difficult to understand.

  Workaround: Monitor the create, update, or delete status of the object in the object table.

  [CXU-2364]

- You cannot add a firewall rule for the UTM function in a network service that uses the vSRX VNF.

  [CXU-2846]

- Deactivating an SRX Series Services Gateway acting as a CPE device might not remove all configuration settings from the device.

  Workaround: Manually delete the configuration settings from the SRX Series Services Gateway.

  [CXU-3754]

- You cannot deploy two network services simultaneously on a CPE device.

  Workaround: Deploy only one network service on a CPE device.

  [CXU-3756]

- The device profile srx-deployment-option-1 assigns OAM traffic to the fxp0 interface, which is not available on the SRX Series Services Gateway.

  Workaround: Edit the stage 1 configuration for the CPE device in Customer Portal to use an interface other than fxp0 for OAM traffic. **[CXU-3779]**

- The traffic rate value does not change when you monitor a service on an SRX Series Services Gateway in Customer Portal.

  Workaround: None

  [CXU-3822]

- The NFX250 device does not receive communications to block unicast reverse path forwarding (uRPF) because two interfaces on the NFX250 device communicate separately with one interface on the regional microservices server.

Copyright © 2017, Juniper Networks, Inc.

Workaround: Disable the uRPF check in JDM on all interfaces for each NFX Series device.

[CXU-3854]

- You must use a different router for a PE in a distributed deployment and an SDN gateway in a centralized deployment. You cannot use the same router for both of these functions.

  Workaround: None

  [CXU-4173]

- You must configure the VLAN settings for an NFX250 device before you configure the Silver Peak VX VNF in Customer Portal.

  [CXU-4402]

- An end user cannot change the password for Customer Portal if the current password is not available.

  Workaround: Delete and re-create the customer with Administration Portal or the API.

  [CXU-4537]

- You cannot edit the settings for a customer in Administration Portal.

  Workaround: Use Administration Portal to import a JSON file that contains the correct data for the customer. **[CXU-4538]**

- You can only view one network service at a time on a CPE device in Customer Portal.

  [CXU-4551]

- When you configure the MX Series router as an IPsec concentrator in a distributed deployment, you must specify the Internet Gateway of the IPsec concentrator in the default routing instance. Otherwise, the IPsec tunnel is not established.

  [CXU-4566]

- You must specify a target URL if you select http-get for the probe type when you configure IP monitoring for a CPE device in Customer Portal, Network Service Designer, or the APIs. Otherwise, the configuration fails.

  [CXU-4571]

- Deployment of the NFX Series device behind NAT is not supported.

  Workaround: None

  [CXU-5296]

- After you install CSO, the username and password that CSO uses to access Contrail Analytics might not match the corresponding username and password in Contrail Analytics.

  Workaround: Complete the following actions:

  1. Log in to the CSO central infrastructure VM as root.

Copyright © 2017, Juniper Networks, Inc.

2. View the username that CSO uses to access Contrail Analytics.

   ```
   root@host:~/# etcdctl get /csp/infra/contrailanalytics/queryuser
   <username>
   ```

   <username> is the actual value that the query returns.

3. View the password that CSO uses to access Contrail Analytics.

   ```
   root@host:~/# etcdctl get /csp/infra/contrailanalytics/querypassword
   <password>
   ```

   <password> is the actual value that the query returns.

   If the username and password match the values configured in Contrail Analytics, you do not need to take further action. The default username configured in Contrail Analytics is admin and the default password is contrail123.

If the username and password do not match the values in Contrail Analytics, update them on the central infrastructure VM as follows:

1. Log in to the CSO central infrastructure VM as root.

2. Update the username and password with the values configured in Contrail Analytics.

   ```
   root@host:~/# etcdctl set /csp/infra/contrailanalytics/queryuser
   <contrail-analytics-username>
   root@host:~/# etcdctl set /csp/infra/contrailanalytics/querypassword
   <contrail-analytics-password>
   ```

[CXU-5873]

- The configuration for a CPE device might not be removed when you deactivate the device in Administration Portal.

  Workaround: To deactivate the CPE device, first delete the configuration from the CPE device with Customer Portal, and then deactivate the device with Administration Portal. **[CXU-6059]**

- You cannot edit or delete login credentials that you configure for a tenant when you create the tenant in Administration Portal.

  Workaround: Delete the tenant and re-create it. **[CXU-6217]**

- You cannot edit the Deployment Type (vCPE-Only or uCPE-Only) in a request that you create with Network Service Designer.

  Workaround: Create a new request. **[CXU-6474]**

- After you have assigned a device template to a CPE device in Administration Portal, you might not be able to change the device template.

  Workaround: Use Administration Portal to delete the on-premise site for the CPE device and then re-create the site. **[CXU-6648]**

Copyright © 2017, Juniper Networks, Inc.

- Using Heat v2 API on Contrail 3.0.2, we support only 120 Contrail Service Orchestration instances for a centralized deployment. Use of more Contrail Service Orchestration instances for a centralized deployment results in high latency and timeout issues due to Contrail bug https://bugs.launchpad.net/juniperopenstack/+bug/1676983.

  Workaround: Use fewer than 120 Contrail Service Orchestration instances for a centralized deployment with Heat v2 API or use Heat v1 APi for larger numbers of Contrail Service Orchestration instances.

  [CXU-6697]

- After you complete an operation in Customer Portal, the GUI might not update to show the latest status.

  Workaround: Refresh the Web page in Customer Portal.

  [CXU-6701]

- Device templates do not contain an option for configuring the root password of a CPE device.

  Workaround: Configure the root password on the CPE device.

  [CXU-9510]

- TCP ports other than port 22 are blocked by the security group that is created when a network service in a centralized deployment is activated.

  Workaround: Configure the security group manually to open the required ports.

  [CXU-9841]

- You might not be able to access a third-party VNF through SSH if you have more than one NFX Series device in the same Layer 2 network.

  Workaround: Use only one NFX Series device in a Layer 2 network.

  [CXU-10139]

- Information might be missing from the log files associated with importing tenants.

  Workaround: None

  [CXU-11078]

- The location of a site or POP on the geographical map on the Monitor page in Administration Portal might not be correct, even though the street address is correct.

  Workaround: None

  [CXU-11115]

- When you design a VNF package with Resource Designer, always select the Direct-OAM-Reachability option for the VNF capability field on the Basic VNF Information page. Selecting this option enables correct operation of service chaining for the VNF.

  Workaround: None

  [CXU-11284]

Copyright © 2017, Juniper Networks, Inc.

- When you install the Cloud CPE solution with for a high availability deployment, the RabbitMQ cluster might not contain all three infrastructure services machines.

  Workaround:

  After you install the Cloud CPE solution and load the microservices data:

  1. Log in to the RabbitMQ dashboard for the central microservices with the following credentials:
     - URL—*central-microservices-vip*:15672, where *central-microservices-vip* is the virtual IP address for the HA proxy for the central microservices machine.
     - username—cspmq
     - password—password that you specified for the infrastructure services VM
  2. Check the RabbitMQ overview to see whether all three infrastructure services machines are available in the cluster.
  3. For each infrastructure services machine that does not appear in the cluster, log in to the machine as root and execute the following commands:

     ```
     root@host:~/# service rabbitmq-server stop
     root@host:~/# rm -rf /var/lib/rabbitmq/mnesia/
     root@host:~/# service rabbitmq-server start
     ```

  4. Check the RabbitMQ overview for the central microservices to see whether all three infrastructure services machines are available in the cluster.
  5. Repeat Steps 1 through 4 for the regional microservices VM, using the virtual IP address of the HA proxy for the regional microservices.

  [CXU-11310]

- The microservices might not recover immediately after a load balancer VM or an infrastructure services VM failover in a high availability deployment.

  Workaround: Wait for 20 minutes before using CSO GUIs or APIs after a load balancer VM experiences a failover, and wait for 5 minutes before using CSO GUIs or APIs after an infrastructure services VM experiences a failover.

  [CXU-11314]

Resolved Issues

This section lists fixed issues for the Juniper Networks Cloud CPE Solution Release 3.0.1.

- Remote activation of an NFX250 device might fail because a VNF can not be activated.

  Workaround: Use Administration portal to delete the device and then re-configure its activation data. **[CXU-6576]**

- Remote activation of an NFX Series CPE device configured for SD-WAN might fail.

Copyright © 2017, Juniper Networks, Inc.

Workaround: Repeat the activation for the CPE device.

[CXU-9746]

- The design tools might not be available when you install Contrail Service Orchestration.

  Workaround: Log in to the **centralmsvm** VM as rootand restart the restart the **csp-design-tools** pod.

  [CXU-9799]

- If you import a JSON file that contains details of multiple CPE devices into Administration Portal, some devices might not be detected.

  Workaround: Reimport the JSON file.

  [CXU-9820]

- Device templates do not contain an option that provides the IP address and port details that customers need to log into a VNF on an NFX Series device.

  Workaround: Log in to the NFX Series device through the console and get the IP address of the gateway router's internet ports.

  [CXU-9880]

- You cannot use the **Activate Device** option in Customer Portal to activate a vSRX CPE device.

  Workaround: Copy the stage-1 configuration for the device from the Monitor page in Customer Portal to the console screen of the vSRX instance and commit the configuration.

  [CXU-9985]

- The utility on the Monitor page in Customer Portal for dragging and dropping a network service might not work.

  Workaround: Clear your browser cache and repeat the drag and drop operation.

  [CXU-10042]

- The Activate Device status for an on-premise site on the Monitor page in Customer Portal might persist after you activate the CPE device.

  Workaround: After you activate a device, log out of Customer Portal and log in again. Customer Portal displays the correct status for the device activation.

  [CXU-10043]

- The **provision_vm** tool that you can use to provision virtual machines during the installtion of Contrail Service Orchestration requires Internet access.

  Workaround: Provision the VMs manually if you do not use Internet access for the installation.

  [CXU-10093]

- Application data on an SD-WAN link for an SRX Series CPE device might not be visible.

  Workaround: None

Copyright © 2017, Juniper Networks, Inc.

[CXU-10308]

Installation Instructions

Two CSO installers are available:

- A plug-and play-installer for a demo environment

  This installer offers a snapshot version of CSO that you can install in a few minutes by copying the installer TAR file to the CSO server, expanding the TAR file, and running the installer. The settings for the deployment, such as the VM resources, are preconfigured and you cannot modify them.

- A full-version installer

  You must use this installer for a production or trial environment and you can use it for a demo environment if you want to be able to customize the installation settings. To install this version, follow the instructions in the **Read Me** file that is included with the software installation package.

Software Installation Requirements for the NFX250 Device

The NFX250 device requires the Junos OS Release 15.1X53-D47for the Cloud CPE Solution 3.0.1.

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.

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 JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Copyright © 2017, Juniper Networks, Inc.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

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

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

Revision History

27 July 2017—Revision 1, Cloud CPE Solution Release 3.0.1

Copyright © 2017, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.