Cloud CPE Solution Release Notes

Release 2.1.1
9 March 2017
Revision 1

These Release Notes accompany Release 2.1.1 of the Juniper Networks® Cloud CPE Solution. They contain installation information, and describe new and changed features, limitations, and known and resolved issues in the software.

Contents

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 provide network services for branch offices for their customers or by Enterprise IT departments in a campus and branch environment. In this documentation, 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 this documentation.

- 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 this documentation.

- 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:

- Network Service Orchestrator, together with Network Service Controller, provides ETSI-compliant management of the life cycle of network service instances.
- Network Service Controller provides the VIM.
- The CPE device provides the NFV infrastructure (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.
- Network Service Designer, which enables 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	Up to 5 sites, 2 VNFs per site	Up to 10 VNFs
Production	Up to 1000 sites, 2 VNFs per site	Up to 500 VNFs, 20 VNFs per Contrail compute node

Installation Instructions

To install Release 2.1.1 of the Cloud CPE solution, follow the instructions in the http://www.juniper.net/techpubs/en_US/nfv2.1/information-products/pathway-pages/deployment-guide.html or 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-D102 for the Cloud CPE Solution 2.1.1. This image is included with the Contrail Service Orchestration 2.1.1 software.

When you set up a distributed deployment with a NFX250 platform, you must upload this image with Administration Portal. When you configure activation data for NFX250 devices in Administration Portal, you must specify this image as the boot image.

New and Changed Features

This section describes the new features and enhancements to existing features in Release 2.1.1 of the Juniper Networks Cloud CPE Solution.

- **Support for additional parameters in fault messages**—Real time alerts generated by Contrail Service Orchestration now contain comprehensive information such as the type of alert, severity, customer name, site, and timestamp.
- **Support for three deployment models**—You can use one Contrail Service Orchestration installation to manage the following deployments:
  - A centralized deployment only
  - A distributed deployment only
  - A centralized and a distributed deployment.

    In this case you cannot share POPs or network services between the centralized and distributed deployment. You must create separate POPs and network services for the centralized deployment and for the distributed deployment. You can use the same tenant with one POP in a distributed deployment and another POP in a centralized deployment.
- **Support for Contrail Service Orchestration high availability**—You can now install Contrail Service Orchestration with high availability for infrastructure services and microservices in a production environment. If an infrastructure service or microservice fails, current operations for that service do not recover; however, any new operations proceed as normal.
- **Support for use of SRX Series Services Gateway as a CPE device at a customer site**—You can now use the following platforms as CPE devices for a distributed deployment:
  - SRX300 Series Services Gateway
  - SRX320 Series Services Gateway
  - SRX340 Series Services Gateway
  - SRX345 Series Services Gateway

  You add each SRX Series Services Gateway as a device to your Contrail Service Orchestration deployment and configure the tenant, site, and service in Administration Portal or the API.

  Customers at sites that use SRX Series Services Gateways configure and activate the devices through Customer Portal.
- **Support for use of vSRX on an x86 server as a CPE device**—You can now deliver vSRX network services using vSRX on an x86 server as a CPE device. The device can be located at a customer site or in the service provider cloud. In both cases, you configure

the site in Contrail Service Orchestration as an on-premise site. Your customers must configure and activate vSRX CPE devices as they would SRX Series Services Gateways.

- **Support for advanced policy-based routing and associated monitoring**—You can now configure advanced policy-based routing (APBR) on the Internet links for a CPE device to classify outgoing traffic based on routing applications. APBR allows you to define flexible traffic-handling capabilities that offer granular control for forwarding packets based on application attributes. All CPE devices—NFX250 devices, SRX Series Services Gateways and vSRX instances—support this functionality.

  You can also use IP monitoring on the WAN links to track the performance of APBR.

- **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.

- **Support for configuration of third-party devices**—You can now specify custom parameters and corresponding values in Contrail Service Orchestration for a third-party device such as a provider edge (PE) router in a distributed deployment or an SDN gateway in a centralized deployment. You can use the custom properties for various purposes, such as logging and accounting. You specify the custom properties for a tenant or site through Administration Portal or the API. When Network Service Orchestrator activates a network service for the tenant or site, the customer properties are configured on the device.

- **Dedicated OpenStack Keystone for Contrail Service Orchestration in a centralized deployment**—You can now configure a dedicated OpenStack Keystone for Contrail Service Orchestration in a centralized deployment. Previously, you used the Contrail OpenStack Keystone to authenticate Contrail Service Orchestration operations in a centralized deployment. This feature provides enhanced security for the service provider network because customers and Cloud CPE infrastructure components use separate OpenStack Keystone tokens.

  When you use this feature, you configure each VIM to include service profiles that specify settings to access to the infrastructure components. You also associate the service profile and VIM with each customer.

- **Management of licenses for physical and virtual devices**—You can now use Contrail Service Orchestration to install and track licenses on physical and virtual devices that it manages. You can upload a license to Contrail Service Orchestration with Administration Portal or API calls. You can then use API calls to install the license on a device and to verify that the licenses are successfully installed. In addition, we provide a license installation tool to automate the process for using API calls to upload and install licenses to one device, a specific range of devices, or multiple devices. You can also use the tool to retrieve a license for a site or device.

- **Updates to Administration Portal**—Administration Portal offers several feature updates:

- Support for configuration of custom parameters and corresponding values on a third-party PE router that connects to CPE devices at customer sites.

  You configure these settings as custom properties for a tenant site.

- Device profiles for SRX Series Services Gateways and vSRX implementations used as CPE devices.
- Support for configuration of authorization and authentication of tenant administrators through a dedicated OpenStack Keystone deployment.
- Support for uploading of VNF license files to Contrail Service Orchestration.

- **Updates to Customer Portal**—Customer Portal offers several feature updates:
  - Enhancements to the startup wizard to simplify activation of sites that host CPE devices.
  - Enhancements to improve the management of CPE devices and their associated network services.
  - Support for use of SRX Series Services Gateways and vSRX as CPE devices.
    - Support for application based routing and associated monitoring for vSRX VNFs on CPE devices
    - Configuration of service polices for SRX Series Services Gateways.

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:

- 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	1U rack-mounted server

Software Tested for COTS Servers

Table 3 on page 7 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 Contrail Cloud Platform nodes and servers	Each of the following operating systems has been tested: • Ubuntu 14.04 LTS • Ubuntu 14.04.1 LTS • Ubuntu 14.04.2 LTS
Operating system for Contrail Analytics host in a distributed deployment	Ubuntu 14.04.2 LTS
Operating system for Contrail Service Orchestration servers and their VMs	Ubuntu 14.04.5 LTS for all other servers and VMs
Hypervisor on Contrail Service Orchestration servers	• Centralized deployment: Contrail Release 3.0.2 with OpenStack (Liberty or Kilo), 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 Analytics	Contrail Release 3.0.2 with OpenStack (Liberty or Kilo)

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.
- The software described in Table 5 on page 8.

  You must use these specific versions of the software for the Cloud CPE solution 2.1.1.

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 (GE) XFP optics	1

Table 4: Network Devices Tested for the Contrail Cloud Platform *(continued)*

Function	Device	Model	Quantity
Management switch	Juniper Networks EX Series Ethernet Switch	EX3300-48T switch with: • 48 10/100/1000 GE interfaces • 4 built-in 10 GE 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 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 Release 3.0.2 with OpenStack (Liberty or Kilo), 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 Analytics	Contrail Release 3.0.2 with OpenStack (Liberty or Kilo)
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 2.1.1

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 9.

  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 router with MS-MPC line card	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-S1 device • NFX250-S2 device • SRX300 Services Gateway • SRX320 Services Gateway • SRX340 Services Gateway • SRX345 Services Gateway • vSRX 15.1X49D61	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 Liberty or Kilo
Network Functions Virtualization (NFV)	Contrail Service Orchestration Release 2.1.1
Contrail Analytics	Contrail Release 3.0.2 with OpenStack (Liberty or Kilo)
NFX Software	Junos OS Release 15.1X53-D102
Routing and Security for NFX250 device	vSRX KVM Appliance MD5 SHA1 15.1X49-D61
Operating system for vSRX used as a CPE device on an x86 server	vSRX KVM Appliance MD5 SHA1 15.1X49-D61
Operating system for SRX Series Services Gateway used as a CPE device	15.1X49-D60
Operating system for MX Series router used as PE router	16.1R3.00
Operating system for SRX Series Services Gateway used as an SDN WAN gateway	15.1X49D65

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 10 shows the required hardware specifications for node servers and servers in a demo environment.

Table 8: Demo Environment

Function	Option 1	Option 2	Option 3
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	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	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	One GE or 10 GE interface
Contrail Service Orchestration Servers (includes Contrail Analytics in a VM)			
Number of nodes or servers	6	3	1
vCPUs	4	8	24
RAM	16 GB	32 GB	96 GB
Contrail Cloud Platform for a Centralized Deployment			
Number of nodes or servers	1	1	1
vCPUs	16	16	16
RAM	64 GB	64 GB	64 GB

Table 9 on page 11 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 GE or 10 GE 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 server • 3 regional server
vCPUs	48
RAM	256 GB
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 Contrail 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 12 shows complete details about the VMs required for a test environment.

Table 10: Details of 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 13 on page 16.
csp-central-infravm	Third-party applications used as infrastructure services	• 4 CPU • 16 GB RAM • 200 GB hard disk storage	See Table 13 on page 16.
csp-central-msvm	All microservices, including GUI applications, plus the following components: • HAProxy Configuration • ETCD • Kubemaster • Kubeminion • SIM client	• 4 vCPUs • 16 GB RAM (Minimum requirement) • 200 GB hard disk storage	See Table 13 on page 16.
csp-regional-infravm	Third-party applications used as infrastructure services	• 4 vCPUs • 16 GB RAM • 200 GB hard disk storage	See Table 13 on page 16.
csp-regional-msvm	All microservices, including GUI applications, plus the following components: • HAProxy Configuration • ETCD • Kubemaster • Kubeminion • SIM client	• 4 vCPUs • 16 GB RAM • 200 GB hard disk storage	See Table 13 on page 16.
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 13 on page 16.

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

Name of VM	Components That Installer Places in VM	Resources Required	Ports to Open
csp-contrail-analytics-vm	For a distributed deployment, you install Contrail on this VM to make use of Contrail Analytics. For a centralized deployment, you can use the Contrail OpenStack in the Contrail Cloud Platform.	• 4 vCPUs • 16 GB RAM • 200 GB hard disk storage	See Table 13 on page 16.

Table 11 on page 13 shows complete details about VMs and microservice collections required for a production environment without infrastructure services HA. The microservices are installed directly on the server.

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

Name of VM or Microservice Collection	VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-installer-vm	VM	—	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 13 on page 16.
csp-central-infravm	VM	Third -party applications used as infrastructure services	• 8 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 13 on page 16.
csp-central-ms	Microservice collection	All microservices, including GUI applications, plus the following components: • HAProxy Configuration • ETCD • Kubemaster • Kubeminion • SIM client	• 48 CPUs • 256 GB RAM	See Table 13 on page 16.
csp-regional-infravm	VM	Third -party applications used as infrastructure services	• 8 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 13 on page 16.

Table 11: Details of VMs and Microservice Collections for a Production Environment Without HA *(continued)*

Name of VM or Microservice Collection	VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-regional-ms	Microservice collection	All microservices, including GUI applications, plus the following components: • HAProxy Configuration • ETCD • Kubemaster • Kubeminion • SIM client	• 48 CPUs • 256 GB RAM	See Table 13 on page 16.
csp-space-vm	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 13 on page 16.
csp-contrail-analytics-vm	VM	For a distributed deployment, you install Contrail OpenStack on this VM. For a centralized deployment, you can use Contrail OpenStack in the Contrail Cloud Platform for Contrail Analytics functionality.	• 8 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 13 on page 16.

Table 12: Details of VMs and Microservice Collections for a Production Environment with HA

Name of VM or Microservice Collection	VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-installer-vm	VM	—	• 4 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 13 on page 16.
csp-central-infravm1	VM	Third-party applications used as infrastructure services	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 13 on page 16.

Table 12: Details of VMs and Microservice Collections for a Production Environment with HA *(continued)*

Name of VM or Microservice Collection	VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-central-infravm2	VM	Third-party applications used as infrastructure services	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 13 on page 16.
csp-central-infravm3	VM	Third-party applications used as infrastructure services	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 13 on page 16.
csp-central-lbvm	VM	Load-balancing applications	• 6 vCPUs • 48 GB RAM • 300 GB hard disk storage	See Table 13 on page 16.
csp-central-ms	Microservice collection	All microservices, including GUI applications, plus the following components: • HAProxy Configuration • ETCD • Kubemaster • Kubeminion • SIM client	• 48 CPUs • 256 GB RAM	See Table 13 on page 16.
csp-regional-infravm1	VM	Third-party applications used as infrastructure services	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 13 on page 16.
csp-regional-infravm2	VM	Third-party applications used as infrastructure services	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 13 on page 16.
csp-regional-infravm3	VM	Third-party applications used as infrastructure services	• 6 vCPUs • 48 GB RAM • 500 GB hard disk storage	See Table 13 on page 16.

Table 12: Details of VMs and Microservice Collections for a Production Environment with HA *(continued)*

Name of VM or Microservice Collection	VM or Microservice Collection	Components That Installer Places in VM	Resources Required	Ports to Open
csp-regional-ms	Microservice collection	All microservices, including GUI applications, plus the following components: • HAProxy Configuration • ETCD • Kubemaster • Kubeminion • SIM client	• 48 CPUs • 256 GB RAM	See Table 13 on page 16.
csp-regional-lbvm	VM	Load-balancing applications	• 6 vCPUs • 48 GB RAM • 300 GB hard disk storage	See Table 13 on page 16.
csp-space-vm	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 13 on page 16.
csp-contrail-analytics-vm	VM	For a distributed deployment, the administrators install Contrail Service Orchestration (contrail_analytics) on this VM. For a centralized deployment, you can use the Contrail OpenStack in the Contrail Cloud Platform.	• 8 vCPUs • 32 GB RAM • 300 GB hard disk storage	See Table 13 on page 16.

Table 13 on page 16 shows the ports that you must open on all VMs in the Cloud CPE solution.

Table 13: Ports to Open on VMs in the Cloud CPE Solution

53	2379	4194	5665	6379	8082	9042	10255
80 through 83	2380	5000	5671	6543	8083	9090	15100
443	2888	5044	5672	7804	8085	9093	15672
1414	3306	5432	6000	8006	8086	9160	30000 through 32767
1947	3888	5543	6001	8016	8090	9200	35357

Table 13: Ports to Open on VMs in the Cloud CPE Solution *(continued)*

2181	4001	5601	6002	8080	8091	10248	—

Accessing GUIs

Table 14 on page 17 shows the URLs and login credentials for the GUIs for a non-redundant Contrail Service Orchestration installation.

Table 14: Access Details for the GUIs

GUI	URL	Login Credentials
Administration Portal	http://*central-IP-Address*:81/admin-portal-ui/index.html where: *central-IP-Address*—IP address of the server or VM that hosts the microservices for the central POP For example: *http://192.0.2.1:81/admin-portal-ui/index.html*	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/self-care-portal-ui/index.html where: *central-IP-Address*—IP address of the server or VM that hosts the microservices for the central POP For example: *http://192.0.2.1:82/self-care-portal-ui/index.html*	Specify the credentials when you create the Customer either In Administration Portal or with API calls.
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.
Network Service Director	http://*central-IP-Address*:83/nsd-ui/index.html where: *central-IP-Address*—IP address of the server or VM that hosts the microservices for the central POP For example: *http://192.0.2.1:83/nsd-ui/index.html*	Specify the OpenStack Keystone username and password The default username is **cspadmin** and the default password is **passw0rd**.

Table 14: Access Details for the GUIs *(continued)*

GUI	URL	Login Credentials
Service and Infrastructure Monitor	http://*central-IP-Address*:1947/icingaweb2 where: *central-IP-Address*—IP address of the server or 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 15 on page 18.

Table 15: 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 • Demonstration version of Deep Packet Inspection (DPI) • Firewall • Unified Threat Management (UTM)	• Centralized deployment • Distributed deployment supports firewall and UTM	EMS microservice
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	EMS microservice
Silver Peak VX	WAN optimization	Distributed deployment, NFX250 platform only	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 what 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 DHCP subscribers.
  - Junos OS software for the SRX Series 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 for the Cloud CPE Solution Release 2.1.1.

- 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 may drop traffic. **[CXU-1242]**

- If you do not use NAT in your network, you must set the rp_filter variable in JDM to 0 on all interfaces for an NFX Series device. This action enables source routing while preventing source filtering. **[CXU-1311]**
- Some data that you import in Administration Portal might not be visible in the GUI.

  [CXU-1580]
- 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]
- You cannot delete licenses from devices that Contrail Service Orchestration manages.

  [CXU-3632]

Known Issues

This section lists known issues for the Cloud CPE Solution Release 2.1.1.

- When you deploy a microservice directly on a server, you might not be able to ping infrastructure service IP addresses from inside Kubernetes pods.

  Workaround: Execute the following commands to resolve the issue:

  1. Clear the post-routing rules in **iptables**:

     ```
     root@host:~/# for i in $( iptables -t nat --line-numbers -L | grep ^[0-9] | awk '{ print $1 }'
     | tac ); do iptables -t nat -D POSTROUTING $i; done
     ```
  2. Restart the flanneld service.

     ```
     root@host:~/# service flanneld restart
     ```

  [CD-729]
- 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]
- If a VNF fails, there might be a short delay before the recovery process begins.

Workaround: Monitor the recovery process to ensure that the VNF restarts after a short while.

[CXU-2836]

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

  [CXU-2846]

- The network service recovery process might fail because Contrail Service Orchestration cannot retrieve the configuration settings for the VNF.

  Workaround: Terminate the VNF process and restart the VNF from the command line.

  [CXU-2860]

- Connectivity between the regional microservices server and a CPE device might fail with a timeout error.

  Workaround: None

  [CXU-2995]

- Installation of more than 300 licenses might fail with a timeout error.

  Workaround: Repeat the installation.

  [CXU-3663]

- After you activate an SRX Series Services Gateway in Customer Portal and then deactivate it, the GUI might still show the status of the device as **Activating** on the Monitor page.

  Workaround: Refresh the Monitor page in Customer Portal.

  [CXU-3750]

- 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 in Customer Portal.

  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]**

- Logs for CPE devices in Customer Portal do not specify whether or not the deployment of a VNF is successful.

Workaround: None

[CXU-3802]

- 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]

- If you create multiple rules for APBR and then delete them, Customer Portal still displays the first rule that you configured.

  Workaround: Click **OK** to close the page, then reopen it. The first rule that you created is no longer visible.

  [CXU-3831]

- You can only create a single on-premise site for a tenant in Administration Portal if the WAN-0 and WAN-1 ports on the CPE device are ge-0/0/0 and ge-0/0/1 for an SRX Series Services Gateway or vSRX implementation, or ge-0/0/10 and ge-0/0/11 for an NFX250 device.

  Workaround: For an SRX Series Services Gateway or vSRX implementation acting as a CPE device, use the **Import Tenant** option to import the tenant and site data or use the API to set up the site. There is no workaround for an NFX250 CPE device.

  [CXU-3838]

- When you configure an on-premise site for an SD-WAN topology, you must provide an IP prefix and default gateway for the device, although Contrail Service Orchestration does not use the values.

  Workaround: Enter any valid values in the fields if you want to use Administration Portal to configure the sites. Otherwise, either use the **Import Tenant** option to import the tenant and site data or use the API to set up the site.

  [CXU-3839], [CXU-4560]

- You can only create a single on-premise site for a tenant in Administration Portal if the WAN-0 and WAN-1 ports on the CPE device are ge-0/0/0 and ge-0/0/1 for an SRX Series Services Gateway or vSRX implementation, or ge-0/0/10 and ge-0/0/11 for an NFX250 device.

  Workaround: Use the **Import Tenant** option or the API to edit the configuration for the correct interfaces and to create the sites.

  [CXU-3840]

- 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.

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

  [CXU-3854]

- When you log into Kibana for the first time, you might see an error.

  Workaround: Click *Settings* to refresh the page.

  [CXU-3875]

- When you deactivate an NFX250 device by deleting the CPE device from the list of active devices, the operation might fail.

  Workaround: None

  [CXU-3880]

- You cannot monitor an SD-WAN network service on a CPE device through Customer Portal.

  Workaround: Use the Service and Infrastructure Monitor page to monitor the service.

  [CXU-3881]

- 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: Edit the customer settings in the JSON file. **[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 when you select http-get for the probe type when you configure IP monitoring for a CPE device. Otherwise, the configuration fails.

  [CXU-4571]

- if you use the device template NFX_deployment_option_4 on the NFX250 device, the customer cannot deploy the Silver Peak VX VNF through Customer Portal on that NFX250 device.

Workaround: Use API calls to deploy the Silver Peak VX VNF on a device.

[CXU-4585]

Resolved Issues

This section lists resolved issues for the Cloud CPE solution Release 2.1.1.

- If you create objects such as EMS, VIMs, or sites with the APIs, then you cannot edit them in Administration Portal. If you need to modify an object, you must use RESTful API calls to modify them. If you create these type of objects in Administration Portal, you can edit them with Administration Portal.

  [CXU-1756]

- You cannot delete a VIM or an EMS independently of a POP in Administration Portal. When you delete a POP, the VIM and EMS associated with it are also deleted.

  [CXU-2477]

- Administration Portal does not include logs about configuring PNEs.

  [CXU-2559]

- In Customer Portal, the percentage (%) indicator that shows progress of a service activation might not display the correct value.

  Workaround: None

  [CXU-2763]

- The default action for a firewall policy rule on the NFX250 device is *Deny*.

  [CXU-2799]

- You cannot reorder firewall rules for a network service in Customer Portal. Firewall rules are applied in the order that they appear.

  Workaround: Delete the firewall rules and reconfigure them in the order that Contrail Service Orchestration should apply them.

  [CXU-2800]

- A firewall service is always included in a service chain for a distributed deployment. You cannot remove the firewall service from an NFX250 device in Customer Portal.

  [CXU-2802]

- Occasionally, a Cisco CSR-1000V VNF might restart multiple times after it fails.

  Workaround: Delete the recovery process and restart the VNF from the command line.

  [CXU-2840]

- You cannot delete part of a PNE configuration for a centralized deployment.

  Workaround: Delete the PNE and add it again with the required settings.

  [CXU-2847]

- The recovery process for a VNF might fail with the error **Configuration with CMS job ID 'None', status 'None' failed**.

  Workaround: Terminate the VNF process and restart the VNF from the command line.

  [CXU-2852]

- You might not be able to configure VLANs on a CPE device in Customer Portal.

  Workaround: Use the default username and password (**cspadmin** and **passw0rd**) instead of the username and password that you configured for the customer.

  [CXU-3523]

- If you do not specify optional settings about a license that you want to upload in Administration Portal, the upload fails.

  Workaround: Specify optional settings for a license that you want to upload through Administration Portal.

  [CXU-3706]

- You cannot use the Silver Peak VX VNF.

  Workaround: None

  [CXU-3803]

- When you use an SRX Series Services Gateway as a CPE device for a tenant that already has sites that use NFX250 CPE devices, authentication of the SRX Series Services Gateway through SSH might fail.

  Workaround: Do not use a combination of NFX250 devices and SRX Series Services Gateways as CPE devices at different sites for the same tenant.

  [CXU-3834]

- When you configure a VNF in Network Service Designer, values that you add for a field that accepts multiple values do not appear in the GUI.

  Workaround: After you specify a value in the field, use the drop-down menu for the field to again select each value that you want to use.

  [CXU-3874]

- A VNF that provides vSRX functionality with the Junos Space EMS is not available in Network Service Designer.

  Workaround: Use the VNF that provides vSRX functionality with the EMS microservice for a centralized deployment.

  [CXU-3878]

- Configuration of an MX Series Router as an SDN gateway with the Juniper-MX-MIS device template fails.

  Workaround: Use the Juniper-MX device template.

  [CXU-3879]

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.

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

9 March 2017—Revision 1, Cloud CPE Solution Release 2.1.1