

Contrail Service Orchestration

Contrail Service Orchestration Installation and Upgrade Guide

Published
2020-07-09

Release
5.1

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, 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.

Contrail Service Orchestration Contrail Service Orchestration Installation and Upgrade Guide
5.1

Copyright © 2020 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation | v

Documentation and Release Notes | v

Documentation Conventions | v

Documentation Feedback | viii

Requesting Technical Support | viii

Self-Help Online Tools and Resources | ix

Creating a Service Request with JTAC | ix

1

Introduction

Contrail Service Orchestration Overview | 11

2

Hardware and Software Requirements

Hardware and Software for Contrail Service Orchestration | 15

Servers Requirements for Contrail Service Orchestration | 15

Network Devices and Software Tested in the Hybrid WAN (Distributed CPE) and SD-WAN Deployments | 16

Minimum Requirements for Servers and VMs | 19

Minimum Hardware Requirements for Servers | 19

Minimum Requirements for VMs on CSO servers | 20

3

Installing Contrail Service Orchestration with CLI

Removing a Previous Deployment | 27

Provisioning VMs on Contrail Service Orchestration Servers | 28

Before You Begin | 29

Creating a Bridge Interface for KVM | 30

Downloading the Installer for KVM Hypervisor | 31

Downloading the Installer for ESXi Hypervisor | 34

Verifying Connectivity of the VMs | 35

Installing Contrail Service Orchestration | 36

Copying the Installer Package to the startupserver_1 VM | 36

Performing a Health Check of Infrastructure Components | 38

Performing a Health Check of Infrastructure Components | 39

4

Post Installation Tasks

Generating and Encrypting Passwords for Infrastructure Components | 44

Applying NAT Rules | 45

Applying Security Patches | 56

Viewing Information About Microservices | 56

| 59

5

Upgrading Contrail Service Orchestration

Upgrading Contrail Service Orchestration from Release 4.1.1 to Release 5.1.1 | 61

Impact of the CSO Upgrade | 61

Backing up Contrail Service Orchestration 4.1.1 Databases | 63

Upgrading Contrail Service Orchestration | 64

Upgrading Contrail Service Orchestration from Release 5.1.0 to Release 5.1.1 | 66

Upgrading Contrail Service Orchestration | 66

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | v
- Documentation Conventions | v
- Documentation Feedback | viii
- Requesting Technical Support | viii

Use this guide to install and upgrade the Contrail Service Orchestration on-premise solution.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Documentation Conventions

[Table 1 on page vi](#) defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page vi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

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

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

1

CHAPTER

Introduction

Conrail Service Orchestration Overview | 11

Contrail Service Orchestration Overview

Juniper Networks Contrail SD-WAN, SD-LAN, and NGFW management solutions offer automated branch connectivity while improving network service delivery and agility. CSO is a multi-tenant platform that manages physical and virtual network devices, creates and manages Juniper Networks and third-party virtualized network functions (VNFs), and uses those elements to deploy network solutions for both enterprises and service providers (SPs) and their customers. CSO multi-tenancy provides security and tenant isolation that keeps the objects and users belonging to one tenant or operating company (OpCo) from seeing or interacting with those of another tenant or OpCo.

The CSO can be deployed in one of two ways:

- As a downloadable, on-premise platform in which you (or your company) become the SP administrator (cspadmin user). In an on-premise deployment, the cspadmin user has complete read-write management access and responsibility for the CSO micro-services platforms, orchestration and management infrastructure, and all underlay networks needed to allow access to CSO and its solutions. All CSO releases are delivered in signed packages that contain digital signatures to ensure official Juniper Networks software.
- As a software as a service (SaaS) platform, hosted in a public cloud, to which tenants and OpCos subscribe. In an SaaS deployment, Juniper Networks manages the necessary micro-services infrastructure, the secure orchestration and management (OAM) infrastructure, and underlay networks needed to allow access to CSO and its solutions.

This guide provides information about installing the Contrail Service Orchestration (CSO) Release 5.1 on-premise solution.

CSO offers following solutions:

- Contrail SD-WAN Solution—The Contrail SD-WAN solution offers a flexible and automated way to route traffic through the cloud using overlay networks.
- Contrail Managed LAN Solution (SD-LAN)—The Managed LAN solution allows CSO to manage and monitor remote LAN devices like certain EX Series LAN switches, Mist WiFi access points, and certain SRX Series next generation firewall (NGFW) devices.
- Hybrid WAN (Distributed CPE) Deployment Model—In a Hybrid WAN deployment, customers access network services from a CPE device, located at the customer's site.

This guide provides information about installing the Contrail Service Orchestration (CSO) Release 5.1 on-premise solution.

The following CSO components connect to Network Service Orchestrator through its RESTful API:

- Administration Portal—GUI to manage resources, customers, and availability of network services. It uses the RESTful APIs of other Contrail Service Orchestration components.

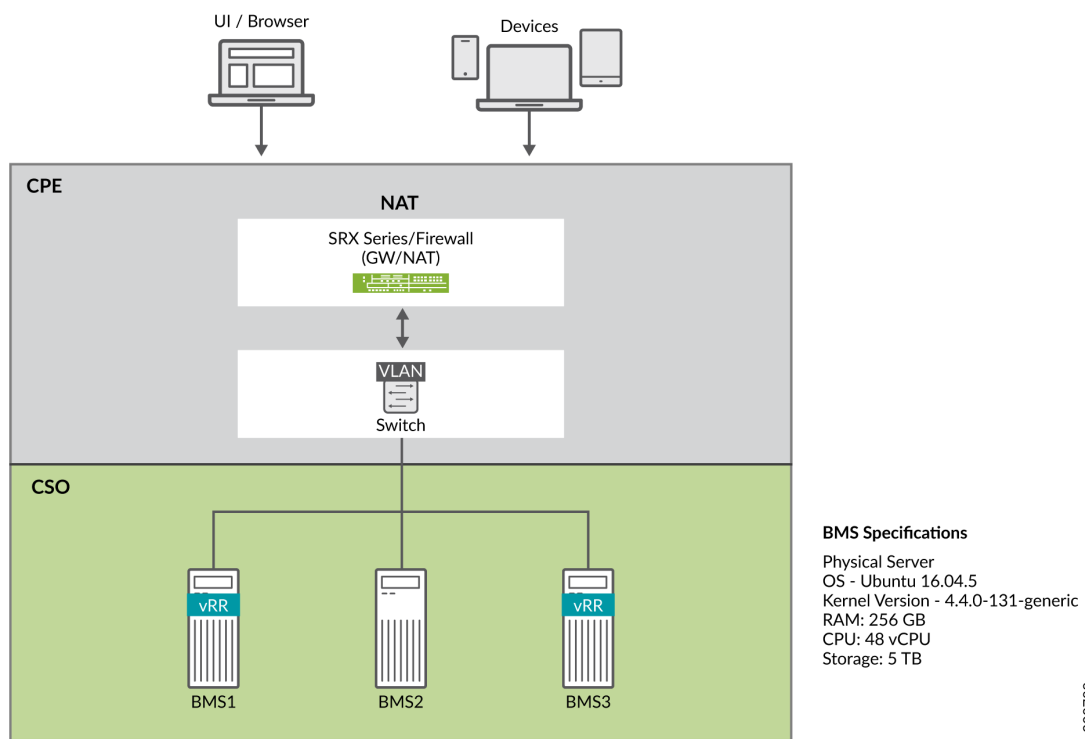
- Customer Portal—GUI to manage sites, customer premises equipment (CPE) devices, and network services for organizations.

The portals offer role-based access control (RBAC) for administrators and operators.

NOTE: CSO Release 5.1.0 only supports KVM hypervisor whereas CSO 5.1.1 supports KVM as well ESXi 6.7 hypervisors.

NOTE: The upgrade procedure for CSO Release 4.1.x to 5.1.0 is not supported.

Figure 1: HA Deployment Topology



For detailed information on configuring Contrail Service Orchestration, see *Contrail Service Orchestration (CSO) Deployment Guide*.

RELATED DOCUMENTATION

Contrail Service Orchestration (CSO) Deployment Guide

Contrail Service Orchestration (CSO) Solutions Overview

2

CHAPTER

Hardware and Software Requirements

Hardware and Software for Contrail Service Orchestration | 15

Minimum Requirements for Servers and VMs | 19

Hardware and Software for Contrail Service Orchestration

IN THIS SECTION

- Servers Requirements for Contrail Service Orchestration | 15
- Network Devices and Software Tested in the Hybrid WAN (Distributed CPE) and SD-WAN Deployments | 16

Contrail Service Orchestration requires commercial off-the-shelf (COTS) servers, specific network devices, and specific software versions. The following sections list the hardware and software that are required and have been tested for the hybrid WAN and SD-WAN solutions.

Servers Requirements for Contrail Service Orchestration

Use COTS servers for the following functions:

- Contrail Service Orchestration (CSO) servers.
- Contrail Analytics servers.

Table 3 on page 15 lists the server requirements

Table 3: Server Requirements

Deployment Type	Number of Servers	vCPUs per Server	Memory per Server	Disk Size per Server
Standalone (PoC) Deployment	1	48	256 GB RAM	2 TB
HA Deployment	3	48	256 GB RAM	5 TB

For the ESXi hypervisor, each VM must be created with a single partition.

For KVM hypervisor, OS and Data partitions are automated

Table 4 on page 16 shows the software that has been tested for COTS servers used in the hybrid WAN solution. You must use these specific versions of the software when you implement the hybrid WAN and SD-WAN solutions.

Table 4: Software Tested for the COTS Servers

Description	Version
Operating system for all COTS servers	Ubuntu 16.04.5 LTS NOTE: Ensure that you perform a fresh install of Ubuntu 16.04.5 LTS on the CSO servers in your deployment because upgrading from a previous version to Ubuntu 16.04.5 LTS might cause issues with the installation.
Operating system for VMs on CSO servers	<ul style="list-style-type: none"> • Ubuntu 16.04.5 LTS for VMs that you configure manually and not with the provisioning tool. • The provisioning tool installs Ubuntu 16.04.5 LTS in all VMs.
Hypervisor on CSO 5.1 0 servers	KVM provided by the Ubuntu operating system on the server NOTE: A mix of different hypervisors across machines is not supported.
Hypervisor on CSO 5.1 1 and above servers	KVM provided by the Ubuntu operating system on the server or VMware ESXi Version 6.7. NOTE: A mix of different hypervisors across machines is not supported.
Additional software for CSO servers	Secure File Transfer Protocol (SFTP)
Contrail Analytics	Contrail Release 4.1.3.0-185

Network Devices and Software Tested in the Hybrid WAN (Distributed CPE) and SD-WAN Deployments

Table 5 on page 17 shows the network devices that have been tested for the distributed deployment and the SD-WAN implementation.

Table 5: Network Devices Tested for the Distributed Deployment and SD-WAN Implementation

Function	Device	Model
PE router and IPsec concentrator (Hybrid WAN distributed deployment only)	Juniper Networks MX Series 3D Universal Edge Router	<ul style="list-style-type: none"> • MX960, MX480, or MX240 router with a Multiservices MPC line card • MX80 or MX104 router with Multiservices MIC line card • Other MX Series routers with a Multiservices MPC or Multiservices MIC line card <p>See MPCs Supported by MX Series Routers and MICs Supported by MX Series Routers for information about MX Series routers that support Multiservices MPC and MIC line cards.</p>
Provider hub device (SD-WAN implementation only)	Juniper Networks SRX Series Services Gateway vSRX on an x86 server	<ul style="list-style-type: none"> • SRX1500 Services Gateway • SRX4100 Services Gateway • SRX4200 Services Gateway • vSRX
CPE device (Hybrid WAN deployment) or spoke device (SD-WAN implementation)	NFX Series Network Services Platforms SRX Series Services Gateways vSRX on an x86 server	<ul style="list-style-type: none"> • NFX250-LS1 device • NFX250-S1 device • NFX250-S2 device • NFX150-S1 • NFX150-S1E • NFX150-C-S1 • NFX150-C-S1-AE/AA • NFX150-C-S1E-AE/AA • SRX300 Services Gateway • SRX320 Services Gateway • SRX340 Services Gateway • SRX345 Services Gateway • SRX1500 Services Gateway • SRX4200 Services Gateway • SRX4100 Services Gateway • SRX550M Services Gateway • vSRX

Table 6 on page 18 shows the software tested for the distributed deployment. You must use these specific versions of the software when you implement a distributed deployment and SD-WAN solution.

Table 6: Software Tested in the Distributed Deployment and SD-WAN Solution

Function	Software and Version
Hypervisor on CSO 5.1.0 servers	KVM provided by the Ubuntu operating system on the server
Hypervisor on CSO 5.1.1 and above servers	KVM provided by the Ubuntu operating system on the server or VMware ESXi Version 6.7.
Authentication and Authorization	OpenStack Mitaka
Network Functions Virtualization (NFV)	CSO Release 5.1.0
Contrail Analytics	Contrail Release 4.1.3.0-185
NFX150 Software	Junos OS Release 18.2X85-D12
NFX250 Software	Junos OS Release 15.1X53-D497
Routing and Security for NFX250 device	vSRX KVM Appliance 15.1X49-D172
Operating system for vSRX used as a CPE device on an x86 server	vSRX KVM Appliance 15.1X49-D172
Operating system for SRX Series Services Gateway used as a CPE device or spoke device	Junos OS Release 15.1X49-D172
Operating system for MX Series router used as PE router	Junos OS Release 16.1R3.00
Operating system for MX Series router used as a hub device for an SD-WAN implementation	Junos OS Release 16.1R5.7
Operating system for SRX Series Services Gateway used as a hub device for an SD-WAN implementation	Junos OS Release 15.1X49-D172

RELATED DOCUMENTATION

Minimum Requirements for Servers and VMs

IN THIS SECTION

- [Minimum Hardware Requirements for Servers | 19](#)
- [Minimum Requirements for VMs on CSO servers | 20](#)

Minimum Hardware Requirements for Servers

For information about the makes and models of servers that you can use in the hybrid WAN solution, see [Table 4 on page 16](#). When you obtain servers for the hybrid WAN and SD-WAN 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.

[Table 7 on page 19](#) shows the specification for the servers for the hybrid WAN or SD-WAN solution.

Table 7: Specification for servers

Item	Requirement
Storage	<p>Storage drive can be one of the following types:</p> <ul style="list-style-type: none">• Serial Advanced Technology Attachment (SATA)• Serial Attached SCSI (SAS)• Solid-state drive (SSD) <p>NOTE: Solid-state drive (SSD) is preferred storage for better performance.</p>
CPU	One 64-bit dual processor, type Intel Sandybridge, such as Intel Xeon E5-2670v3 @ 2.4 Ghz or higher specification
Network interface	One 1-Gigabit Ethernet or 10-Gigabit Ethernet interface

The number of servers that you require depends on your deployment.

[Table 8 on page 20](#) shows the required hardware specifications for servers in the supported deployments. The server specifications are slightly higher than the sum of the virtual machine (VM) specifications listed in “[Minimum Requirements for VMs on CSO servers](#)” on page 20, because some additional resources are required for the system software.

Table 8: Server Requirements

Function	Standalone Deployment	HA Deployment
<i>Contrail Service Orchestration (CSO) Servers</i>		
Number of nodes or servers	1	3
vCPUs per node or server	48	48
RAM per node or server	256 GB	256 GB

Minimum Requirements for VMs on CSO servers

The number of VMs needed and minimum requirements for CSO VMs depend on the deployment environment and whether or not you use high availability (HA):

- For a standalone deployment, see [Table 9 on page 21](#).
- For an HA deployment, see [Table 10 on page 22](#).

For information about the ports that must be open on VMs for all deployments, see [Table 11 on page 24](#).

[Table 9 on page 21](#) shows details about the VMs for a standalone deployment. You need 6 Virtual Machines (VMs) including Virtual Route Reflector (VRR) and 1 public IP address for deploying all the required services.

NOTE: For ESXi deployment, all the VMs must have 500 GB of hard disk storage. For KVM deployment VM storage requirements, refer to [Table 9 on page 21](#).

Table 9: Details of VMs for a Standalone Deployment

Name of VM	Components That Installer Places in VM	Resources Required
startupserver_1	Installer VM	<ul style="list-style-type: none"> • 4 vCPUs • 16 GB RAM • 550 GB hard disk storage
k8-infra_1	Third-party applications used as infrastructure services	<ul style="list-style-type: none"> • 10 CPU • 64 GB RAM • 500 GB hard disk storage
k8-microservices_1	All microservices, including GUI applications	<ul style="list-style-type: none"> • 8 CPU • 64 GB RAM • 250 GB hard disk storage
csp-vrr-vm1	Virtual route reflector (VRR)	<ul style="list-style-type: none"> • 4 vCPUs • 8 GB RAM
monitoring_1	Monitoring VM	<ul style="list-style-type: none"> • 6 vCPUs • 16 GB RAM • 100 GB hard disk storage
contrail_analytics_1	Contrail Analytics server	<ul style="list-style-type: none"> • 12 vCPUs • 48 GB RAM • 500 GB hard disk storage

[Table 10 on page 22](#) shows details about the VMs for a HA deployment.

You need 22 Virtual Machines (VMs) including Virtual Route Reflector (VRR) for deploying all the required services. Additionally you require 3 routable IP addresses, 1 IP address for NAT server and 2 IP addresses for VRR for the HA deployment.

NOTE: For ESXi deployment, all the VMs must have 500 GB of hard disk storage. For KVM deployment VM storage requirements, refer to [Table 10 on page 22](#).

Table 10: Details of VMs for a HA Deployment

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required
startupserver_1	Startup server VM	<ul style="list-style-type: none"> • 4 vCPUs • 16 GB RAM • 400 GB hard disk storage
k8-infra_1	Third-party applications used as infrastructure services	<ul style="list-style-type: none"> • 10 vCPUs • 64 GB RAM • 500 GB hard disk storage
k8-infra_2	Third-party applications used as infrastructure services	<ul style="list-style-type: none"> • 10 vCPUs • 64 GB RAM • 500 GB hard disk storage
k8-infra_3	Third-party applications used as infrastructure services	<ul style="list-style-type: none"> • 10 vCPUs • 64 GB RAM • 500 GB hard disk storage
k8-microservices_1	All microservices, including GUI applications	<ul style="list-style-type: none"> • 10 CPUs • 64 GB RAM • 250 GB hard disk storage
k8-microservices_2	All microservices, including GUI applications	<ul style="list-style-type: none"> • 10 vCPUs • 64 GB RAM • 250 GB hard disk storage
k8-microservices_3	All microservices, including GUI applications	<ul style="list-style-type: none"> • 10 vCPUs • 64 GB RAM • 250 GB hard disk storage
monitoring_1	Monitoring applications	<ul style="list-style-type: none"> • 4 vCPUs • 24 GB RAM • 250 GB hard disk storage
monitoring_2	Monitoring applications	<ul style="list-style-type: none"> • 4 vCPUs • 24 GB RAM • 250 GB hard disk storage
monitoring_3	Monitoring applications	<ul style="list-style-type: none"> • 4 vCPUs • 24 GB RAM • 250 GB hard disk storage

Table 10: Details of VMs for a HA Deployment (*continued*)

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required
contrail_analytics_1	Contrail Analytics for a distributed deployment.	<ul style="list-style-type: none"> • 12 vCPUs • 48 GB RAM • 500 GB hard disk storage
contrail_analytics_2	Contrail Analytics for a distributed deployment.	<ul style="list-style-type: none"> • 12 vCPUs • 48 GB RAM • 500 GB hard disk storage
contrail_analytics_3	Contrail Analytics for a distributed deployment.	<ul style="list-style-type: none"> • 12 vCPUs • 48 GB RAM • 500 GB hard disk storage
proxy_1	Proxy VM	<ul style="list-style-type: none"> • 2 vCPUs • 8 GB RAM • 100 GB hard disk storage
proxy_2	Proxy VM	<ul style="list-style-type: none"> • 2 vCPUs • 8 GB RAM • 100 GB hard disk storage
k8-master1	Kubernetes master node	<ul style="list-style-type: none"> • 2 vCPUs • 4 GB RAM • 100 GB hard disk storage
k8-master2	Kubernetes master node	<ul style="list-style-type: none"> • 2 vCPUs • 4 GB RAM • 100 GB hard disk storage
k8-master3	Kubernetes master node	<ul style="list-style-type: none"> • 2 vCPUs • 4 GB RAM • 100 GB hard disk storage
csp-vrr-vm1	Virtual route reflector (VRR) VM	<ul style="list-style-type: none"> • 4 vCPUs • 32 GB RAM
csp-vrr-vm2	Virtual route reflector (VRR) VM	<ul style="list-style-type: none"> • 4 vCPUs • 32 GB RAM

Table 10: Details of VMs for a HA Deployment (*continued*)

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required
proxy_sblb1	Proxy VM—Southbound	<ul style="list-style-type: none"> • 2 vCPUs • 8 GB RAM • 400 GB hard disk storage
proxy_sblb2	Proxy VM—Southbound	<ul style="list-style-type: none"> • 2 vCPUs • 8GB RAM • 400 GB hard disk storage

Table 11 on page 24 shows the ports that must be open on all CSO VMs to enable the following types of CSO communications:

- External—CSO UI and CPE connectivity
- Internal—Between CSO components

The **deploy.sh** script opens these ports on each VM.

Table 11: Ports to Open on CSO VMs

Port Number	Protocol	CSO Communication Type	Port Function
NAT_IP:443	HTTPs	External	UI Access
NAT_IP:83	TCP	External	Network Service Designer UI
NAT_IP:8060	HTTP	External	Certification Revocation List
NAT_IP:500	ISAKMP	External	OAMHUB IPSEC connection
NAT_IP:4500	IPSec	External	OAMHUB IPSEC connection
VRR_publicIP:22	SSH	External and internal	Secure logins
VRR_publicIP:179	BGP	External	BGP for VRR
NAT_IP:7804	TCP/Netconf	External	Device connectivity
SBLB_IP:514	TCP/Syslog	External	Device syslog receiving port
SBLB_IP:3514	TCP/Syslog	External	Device security log receiving port

Table 11: Ports to Open on CSO VMs (*continued*)

Port Number	Protocol	CSO Communication Type	Port Function
SBLB_IP:2216	TCP/gRPC	External	Telemetry data from device

NOTE: The following ports are only used for troubleshooting. You can either enable or disable it with the same or different NAT.

NAT_IP:5601	TCP	External	Kibana UI—CSO log visualizer to trouble shoot
NAT_IP:9210	TCP	External	Elasticsearch
NAT_IP: 15672	TCP	External	RabbitMQ management tool
NAT_IP:5000	TCP	External	Keystone public
NAT_IP:3000	TCP	External	Grafana
NAT_IP:8081		External	Contrail Analytics
NAT_IP:8082		External	Contrail Analytics
NAT_IP:90	TCP	External	Apache to salt master

RELATED DOCUMENTATION

[Hardware and Software for Contrail Service Orchestration | 15](#)

[Provisioning VMs on Contrail Service Orchestration Servers | 28](#)

3

CHAPTER

Installing Contrail Service Orchestration with CLI

Removing a Previous Deployment | **27**

Provisioning VMs on Contrail Service Orchestration Servers | **28**

Installing Contrail Service Orchestration | **36**

Performing a Health Check of Infrastructure Components | **38**

Removing a Previous Deployment

You should remove a previous deployment and perform a new installation.

NOTE: The upgrade procedure for CSO Release 4.1.x to 5.1.0 is not supported.

If you do not have previous deployment, proceed with [“Provisioning VMs on Contrail Service Orchestration Servers” on page 28](#)

To remove a previous installation:

1. Remove VMs on the physical server.

- a. Log in to the CSO server as root.

- b. View the list of VMs.

For example:

```
root@host:~/# virsh list --all
```

Output:

Id	Name	State
2	<vm-name>	running

- c. Remove each VM and its contents.

For example:

```
root@host:~/# virsh destroy <vm-name>
root@host:~/# virsh undefine <vm-name>
```

Where, <vm-name> is the name of VM you want to delete.

- d. Delete the Ubuntu source directories and VM.

For example:

```
root@host:~/# rm -rf /root/disks
root@host:~/# rm -rf /root/disks_can
root@host:~/# cd /root/ubuntu_vm
```

```
root@host:~/# rm -rf <vm-name>
```

2. Delete the old Salt minion keys.

For example:

```
root@host:~/# salt-key -D
```

3. Clear Ubuntu cache.

```
root@host:~/# clear ubuntu cache $ sync && echo 1 | sudo tee /proc/sys/vm/drop_caches
```

RELATED DOCUMENTATION

[Provisioning VMs on Contrail Service Orchestration Servers](#) | 28

Provisioning VMs on Contrail Service Orchestration Servers

IN THIS SECTION

- [Before You Begin](#) | 29
- [Creating a Bridge Interface for KVM](#) | 30
- [Downloading the Installer for KVM Hypervisor](#) | 31
- [Downloading the Installer for ESXi Hypervisor](#) | 34
- [Verifying Connectivity of the VMs](#) | 35

Virtual Machines (VMs) on the Contrail Service Orchestration (CSO) servers host the infrastructure services and some components.

NOTE: If you use the KVM hypervisor while installing a Distributed CPE (Hybrid WAN) or an SD-WAN solution, you must create a bridge interface on the physical server. The bridge interface should map the primary network interface (Ethernet management interface) on each CSO server to a virtual interface before you create VMs. This action enables the VMs to communicate with the network.

Assumptions/Prerequisites:

- Network machines (routers) are configured with required configurations.
- All the physical servers where KVM VMs are provisioned should have Ubuntu 16.04.5 LTS.
- All the VMs where CSP components are deployed should have Ubuntu 16.04.5 LTS OS.
- See [“Minimum Requirements for Servers and VMs” on page 19](#) for details of the VMs and associated resources required for each deployment.
- Verify the DNS server configuration on the servers.
- All the machines have SSH enabled.
- All the VMs are on the same subnet.
- All the machines are reachable between each other.
- All the operations and installations are to be run as *root* user.
- Verify all the machines have the correct FQDN.
- For CSO release 5.1.0 installation, verify you have internet access.

Before You Begin

NOTE: CSO Release 5.1.0 supports only the KVM hypervisor, whereas CSO Release 5.1.1 supports KVM as well ESXi version 6.7 hypervisors.

Before you begin you must:

- Configure the physical servers.
- The VMs must match the server requirement as given in [“Minimum Requirements for Servers and VMs” on page 19](#).

CSO VMs of each type must be distributed across different servers in different racks to avoid server or TOR switch failure. It is recommended to use 3 servers.

- Install Ubuntu 16.04.5 LTS as the operating system for the physical servers.

Creating a Bridge Interface for KVM

If you use the KVM hypervisor, you must create a bridge interface on the physical server that maps the primary network interface (Ethernet management interface) on each CSO server to a virtual interface before you create the VMs. This action enables the VMs to communicate with the network.

To create the bridge interface:

1. Log in as *root* on the CSO server.
2. View the network interfaces configured on the server to obtain the name of the primary interface on the server.

```
root@host:~/# ifconfig
```

3. Set up the KVM host.

```
* apt-get update
* apt-get install libvirt-bin
```

4. Modify the **/etc/network/interfaces** file to map the primary network interface to the virtual interface *br0*.

NOTE: Note: You must perform this step on all the servers in the HA deployment. Address of *eno2* must be changed.

For example, use the following configuration to map the primary interface *eno2* to the virtual interface *br0*:

```
auto eno2
iface eno2 inet manual
    up ifconfig eno2 0.0.0.0 up

auto br0
```

```

iface br0 inet static
    address 192.168.10.2
    netmask 255.255.255.0
    network 192.168.x.0
    broadcast 192.168.10.255
    gateway 192.168.10.1
    bridge_ports eno2
    dns-nameservers 8.8.8.8
    dns-search example.net

```

5. Navigate to the untar CSO location on one of the servers and run the following commands:

```

root@ccra-68:~/Contrail_Service_Orchestration_5.1.0/ci_cd# ls -ltr
setup_bms.sh
-rwxr-xr-x 1 root root 716 Oct 10 01:57 setup_bms.sh
root@ccra-68:~/Contrail_Service_Orchestration_5.1.0/ci_cd# ./setup_bms.sh

```

```

br0      Link encap:Ethernet  HWaddr 0c:c4:7a:98:94:75
         inet addr:192.168.10.2  Bcast:192.168.10.255  Mask:255.255.255.0
         inet6 addr: fe80::ec4:7aff:fe98:9475/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:437072 errors:0 dropped:0 overruns:0 frame:0
         TX packets:211101 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:72297668 (72.2 MB)  TX bytes:46647766 (46.6 MB)

```

Run the script on all the servers.

Downloading the Installer for KVM Hypervisor

To provision the VMs:

1. Log in as *root* to the CSO server.

When you log in as *root* on the CSO server, you are placed in the home directory, **/root**.

2. Download the appropriate installer package from the [CSO Downloads](#) page.

Use the Contrail Service Orchestration installer if you have purchased licenses for both Network Service Orchestrator and Network Service Controller licenses for a distributed deployment.

- Expand the installer package, which has a name specific to its contents and the release. For example, if the name of the installer package is `cso<version>.tar.gz`:

```
root@host:~/# tar -xvzf cso<version>.tar.gz
```

The expanded package is a directory that has the same name as the installer package and contains the installation files.

- Run the **deploy.sh** command and use an interactive script to create configuration files for the environment topology.

```
root@host:~/Contrail_Service_Orchestration_5.1.0./ deploy.sh
```

```
*****
Generic Questions
*****
Do you need a Standalone/HA deployment (1/2) [2]:2

*****
Server Details
*****
Please select hypervisor (kvm/esxi) [kvm]:
Please provide Gateway IP for VMs []:192.168.10.1 --> Assuming 1st IP of the
private subnet/network
Provide range of private IP addresses to be used for creating VMs []:
192.168.10.0/24 --> CSO VM subnet
Provide VIP (for admin portal and SBLB usage) for VMs []:10.x.x.2 --> Routable
IP of CSO UI Access
*****

Provide the management IPs cidr of server 1 [192.168.10.2/32]: Assuming 2nd IP
of the private subnet/network
Provide the password for root user of server 1:
Confirm Password:
Provide the management interface of server 1 [eno1]:
Provide the lan interface of server 1 [eno2]:

Provide the management IPs cidr of server 2 [192.168.10.3/32]: Assuming 3rd IP
of the private subnet/network
Provide the password for root user of server 2:
Confirm Password:
Provide the management interface of server 2 [eno1]:
Provide the lan interface of server 2 [eno2]:
```



```

Provide the management IPs cidr of server 3 [192.168.10.4/32]: Assuming 4th IP
  of the private subnet/network
Provide the password for root user of server 3:
Confirm Password:
Provide the management interface of server 3 [eno1]:
Provide the lan interface of server 3 [eno2]:

Please provide the CSO reachable subnet for device communication []:10.x.x.0/24
--> Device/CSO reachable subnet
Provide domain name for VMs [example.net]:
Provide comma separated list of dns nameservers []:
Provide password for VRR VMs:
Confirm Password:
Provide password for Contrail VMs:
Confirm Password:
Number of VRR instances []:2
Please provide redundancy group for vrr1 (0/1) []:0
Provide routable IP for VRR1 []:10.x.x.3 --> Routable IP of Device to vRR
communication
Please provide redundancy group for vrr1 (0/1) []:1
Provide routable IP for VRR1 []:10.x.x.4 --> Routable IP of Device to vRR
communication

*****
Authentication and Other Questions
*****
Create new ssh-key for VM authentication? (y/n) []:y --> (y) will generate a
ssh-key and store at $HOME/.ssh/id_rsa
----
Create new ssh-key for VM authentication? (y/n) [n]:n --> (n) provide ssh key
to access the CSOVMs
Provide absolute path for public ssh-key file []: /secrets/sshkeys/id_rsa.pub
----
Provide Email Address for cspadmin user []:
The Autonomous System Number for BGP [64512]:
----
Do you have a signed certificate for CSO? (y/n) [n]:y
Please provide the certificate path: /root/csp-application-deployment/certs
----
Do you have a signed certificate for CSO? (y/n) [n]:n
Please provide commonname for CSO certificate (FQDN): jcs.example.net --> Domain
use to create a self-signed certificate

----

```

```

DNS name of CSO Customer Portal []:jcs.example.net --> Domain of
signed/self-signed certificate
DNS name of CSO Admin Portal (can be same as Customer Portal) []:jcs.example.net
--> Domain of signed/self-signed certificate

Timezone for the servers in topology [America/Los_Angeles]:
List of ntp servers (comma separated) []:ntp.example.net
CSO certificate validity (in days) [365]:
Specify data directory to be used for infra components [/mnt/data]:
Is this is 4.1 to 5.1 migration (applies only for blue-green deployment) (y/n)
[n]:

```

For KVM hypervisor, in case of standalone deployment, run the **setup_NAT_rule.sh** script on the BMS. For details, refer to [“Applying NAT Rules” on page 45](#).

Downloading the Installer for ESXi Hypervisor

To provision the VMs:

1. Log in to one of the CSO BMS servers as root.
2. Download the appropriate installer package from the [CSO Downloads](#) page.
Use the Contrail Service Orchestration installer if you have purchased licenses for both Network Service Orchestrator and Network Service Controller licenses for a distributed deployment.

3. Expand the installer package, which has a name specific to its contents and the release. For example, if the name of the installer package is **cso<version>.tar.gz**:

```
root@host:~/# tar -xvzf cso<version>.tar.gz
```

The expanded package is a directory that has the same name as the installer package and contains the installation files.

The package contains **ubuntu-16.04-server-cloudimg-amd64.ova** and **junos-vrr-x86-64-15.1F6-S7.2.ova** files.

4. Provision the VMs using **ubuntu-16.04-server-cloudimg-amd64.ova** file except VRR.
The VMs must match the server requirement as given in [“Minimum Requirements for Servers and VMs” on page 19](#).

NOTE: You must set the *default-password* parameter at the time of OVA upload while spawning the ubuntu VM. Once the VM is up, you can login with the password configured.

The default username is *ubuntu*.

5. Provision the VRRs using **junos-vrr-x86-64-15.1F6-S7.2.ova** file.

After your provision the VMs:

- Assign an IP address to logical interface, *ens192* associated with the VM.
- Configure VMs with a valid hostname and update the **/etc/hosts** file.

NOTE: The hostnames must start and end with an alphanumeric character. The hostnames can contain only these special characters—hyphen (-) or period (.).

- Enable *netconf* for VRRs.
- Configure SSH to allow root access to all the VMs.
- Reboot the VMs.

Verifying Connectivity of the VMs

From each VM, verify that you can ping the IP addresses and hostnames of all the other servers, nodes, and VMs in the CSO.



CAUTION: If the VMs cannot communicate with all the other hosts in the deployment, the installation will fail.

RELATED DOCUMENTATION

Installing and Configuring Contrail Service Orchestration

[Applying NAT Rules](#) | 45

Installing Contrail Service Orchestration

IN THIS SECTION

- [Copying the Installer Package to the startupserver_1 VM | 36](#)

Copying the Installer Package to the startupserver_1 VM

After you have provisioned the VMs, perform the following steps:

1. Copy the installer package file from the central CSO server to the *startupserver_1* VM.

```
scp cso<version>.tar.gz root@<startupserver_1 IP>:/root/
```

2. Log in to the *startupserver_1* VM as root.

Run **get_vm_details.sh** script to find the IP address of the *startupserver_1* VM. Use SSH to access the VM.

3. Expand the installer package.

For example, if the name of the installer package is **cso<version>.tar.gz**:

```
root@host:~/# tar -xvzf cso<version>.tar.gz
```

The contents of the installer package are placed in a directory with the same name as the installer package. In this example, the name of the directory is **cso<version>**.

4. ● For KVM hypervisor:

Run the **deploy.sh** command.

- For ESXi hypervisor:

Run **deploy.sh** script and use an interactive script to create configuration files for the environment topology.

```
root@host:~/Contrail_Service_Orchestration_5.1.1./ deploy.sh
```

```
Do you need a Standalone/HA deployment (1/2) [2]
Please select hypervisor (kvm/esxi) [esxi] ---> Please select esxi for
```

```

this option.
    Enter the number of cluster groups [3]: ---> Please give the number of
ESXi hosts as value
    Do all your VMs have same password for root [y]:
    Enter the password common for all the VMs:
    Confirm Password:
    Provide the list/comma separated VM IPs for cluster group 1 ---> Please
provide the ips for all VMs spawned in host1(excluding VRR).

    Sample inputs:
    List of IPs: 192.168.10.5-192.168.10.10
    Comma separated IPs: 192.168.10.5,192.168.10.8,192.168.10.12
    List of IPs and Comma separated IPs: 192.168.10.5-192.168.10.10,192.168.10.12

    Provide the list/comma separated VM IPs for cluster group 2 ---> Please
provide the ips for all VMs spawned in host2(excluding VRR).
    Provide the list/comma separated VM IPs for cluster group 3 ---> Please
provide the ips for all VMs spawned in host3(excluding VRR).
    Is CSO behind NAT (y/n) [y] --> Give y for this option.
    Provide routable IP for VRR1 ---> This should be the VRR reachable IP
configured in vSRX
    Provide private IP for VRR1 ---> This should be the VRR VM ip
    Provide list/comma separated list of 10 IPs to be used for load balancers
---> Please provide the free ips to be used. You can assign free ips which
are not used by the CSO VMs.

    Summary of IP Addressss used for VMs:
    k8-infra1: 192.168.10.2
    monitoring1: 192.168.10.4
    k8-microservices1: 192.168.10.3
    contrail_analytics1: 192.168.10.6
    startupserver_1: 192.168.10.5
    Do you want to proceed(y/n) []: ---> Please give 'y' for this option if
all the ips assignments are correct.

```

5. Run the following command to deploy microservices.

```
./python.sh micro_services/deploy_micro_services.py
```

6. Run the following command to load the data.

```
./python.sh micro_services/load_services_data.py
```

You can run **./get_vm_details.sh** script to find the IP addresses for each component.

RELATED DOCUMENTATION

[Provisioning VMs on Contrail Service Orchestration Servers | 28](#)

Installing and Configuring Contrail Service Orchestration

Performing a Health Check of Infrastructure Components

IN THIS SECTION

- [Performing a Health Check of Infrastructure Components | 39](#)

Performing a Health Check of Infrastructure Components

After you install or upgrade CSO, you can run the **components_health.sh** script to perform a health check of all infrastructure components. This script detects whether any infrastructure component has failed and displays the health status of the following infrastructure components:

- SaltStack
- Cassandra
- MariaDB
- Swift
- Redis
- ArangoDb
- Keystone
- Elasticsearch
- Elk Elasticsearch
- Icinga
- RabbitMQ
- Etcd
- Rsyslog
- Kubernetes
- ELK Logstash
- ELK Kibana
- ZooKeeper
- Contrail Analytics

To check the status of infrastructure components:

1. Log in to the `startupserver_1` VM as root.
2. Navigate to the CSO directory in the `startupserver_1` VM.

For example:

```
root@host:~/# cd Contrail_Service_Orchestration_5.1.1
root@host:~/Contrail_Service_Orchestration_5.1.1#
```

3. Run the **components_health.sh** script.

To check the status of one of infrastructure components, run the following command:

```
root@startupserver_1:/opt/Contrail_Service_Orchestration_5.1.1#
./components_health.sh --component=<component_name>
```

For Example:

```
root@startupserver_1:/opt/Contrail_Service_Orchestration_5.1.1#
./components_health.sh --component=elasticsearch
```

To check the health component of the environments, run the following command:

```
root@startupserver_1:/opt/Contrail_Service_Orchestration_5.1.1#
./components_health.sh
```

After a couple of minutes, the status of each infrastructure component for central and regional environments is displayed.

For example:

```
INFO      Updating the mine and syncing the grains
INFO      *****
INFO      HEALTH CHECK FOR INFRASTRUCTURE COMPONENTS STARTED IN CENTRAL ENVIRONMENT
INFO      *****

INFO      Health Check for Infrastructure Component Saltstack Started
INFO      The Infrastructure Component Saltstack is Healthy

INFO      Health Check for Infrastructure Component Cassandra Started
INFO      The Infrastructure Component Cassandra is Healthy

INFO      Health Check for Infrastructure Component Mariadb Started
INFO      The Infrastructure Component Mariadb is Healthy

INFO      Health Check for Infrastructure Component Swift Started
INFO      The Infrastructure Component Swift is Healthy

INFO      Health Check for Infrastructure Component Redis Started
INFO      The Infrastructure Component Redis is Healthy

INFO      Health Check for Infrastructure Component Arangodb Started
INFO      The Infrastructure Component Arangodb is Healthy

INFO      Health Check for Infrastructure Component Keystone Started
INFO      The Infrastructure Component Keystone is Healthy
```



```

INFO      Health Check for Infrastructure Component Elasticsearch Started
INFO      The Infrastructure Component Elasticsearch is Healthy

INFO      Health Check for Infrastructure Component Elk_Elasticsearch Started
INFO      The Infrastructure Component Elk_Elasticsearch is Healthy

INFO      Health Check for Infrastructure Component Icinga Started
INFO      The Infrastructure Component Icinga is Healthy

INFO      Health Check for Infrastructure Component Rabbitmq Started
INFO      The Infrastructure Component Rabbitmq is Healthy

INFO      Health Check for Infrastructure Component Etcd Started
INFO      The Infrastructure Component Etcd is Healthy

INFO      Health Check for Infrastructure Component Rsyslog Started
INFO      The Infrastructure Component Rsyslog is Healthy

INFO      Health Check for Infrastructure Component Kubernetes Started
INFO      The Infrastructure Component Kubernetes is Healthy

INFO      Health Check for Infrastructure Component Elk_Logstash Started
INFO      The Infrastructure Component Elk_Logstash is Healthy

INFO      Health Check for Infrastructure Component Elk_Kibana Started
INFO      The Infrastructure Component Elk_Kibana is Healthy

INFO      Health Check for Infrastructure Component Zookeeper Started
INFO      The Infrastructure Component Zookeeper is Healthy

INFO      Health Check for Infrastructure Component Contrail_Analytics Started
INFO      The Infrastructure Component Contrail_Analytics is Healthy

INFO      Overall result:
INFO      The following Infrastructure Components are Healthy:
INFO      ['Saltstack', 'Cassandra', 'Mariadb', 'Swift', 'Redis',
'Arangodb', 'Keystone', 'Elasticsearch', 'Elk_Elasticsearch', 'Icinga',
'Rabbitmq', 'Etcd', 'Rsyslog', 'Kubernetes', 'Elk_Logstash', 'Elk_Kibana',
'Zookeeper', 'Contrail_Analytics']
INFO      ***** HEALTH CHECK COMPLETED IN CENTRAL ENVIRONMENT
*****

```

RELATED DOCUMENTATION

| [Generating and Encrypting Passwords for Infrastructure Components](#) | 44

4

CHAPTER

Post Installation Tasks

Generating and Encrypting Passwords for Infrastructure Components | 44

Applying NAT Rules | 45

Applying Security Patches | 56

Viewing Information About Microservices | 56

Generating and Encrypting Passwords for Infrastructure Components

CSO uses an algorithm to automatically generate a dynamic password for the following infrastructure components:

- Cassandra
- Keystone
- MariaDB
- RabbitMQ
- Icinga
- Prometheus
- ArangoDB
- Elasticsearch
- ZooKeeper

The automatically generated passwords for each infrastructure component and the **cspadmin** password for Administration Portal are displayed on the console after you complete answering the Setup Assistance questions.

You can access the Administration portal by navigating to NAT IP address via internet browser. The initial user name is **cspadmin** and the initial password is shown after running **./deploy.sh** script under topic [4](#).

NOTE: You must note the automatically generated password that is displayed on the console as they are not saved in the system.

To enhance the password security, the length and pattern for each password is different and the password is encrypted. The passwords in the log file are masked.

Run the following script to retrieve passwords for all infrastructure components:

```
CSO> ./python.sh deploy_manager/utils/decrypt_password.py
```



CAUTION: You can't retrieve the **cspadmin user** password. It can only be reset from the CSO Installer webpage or CLI.

Follow the steps to reset the **cspadmin user** password from the CSO Installer webpage:

1. Click **Forget Password?** on the login page of the CSO Installer webpage.
2. Receive a verification code to the registered e-mail ID.
3. Type the received verification code as the password on the CSO Installer webpage.
4. Follow the steps to reset the password.

RELATED DOCUMENTATION

[Installing Contrail Service Orchestration](#) | 36

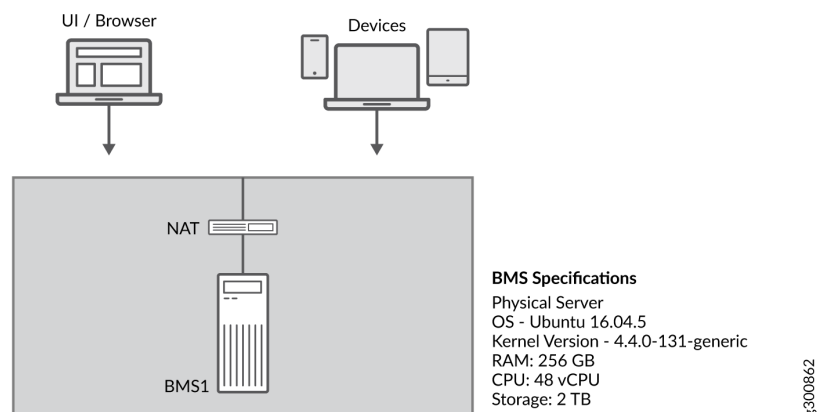
Applying NAT Rules

After installing CSO, you must apply NAT rules.

For standalone deployment—

This is applicable only if you have the standard standalone topology.

Figure 2: Standard Standalone Deployment



1. Log in to the BMS as **root**.
2. Run the following command from the CSO home directory:

```
cd ci_cd# ./setup_NAT_rule.sh
```

NOTE: Once the BMS gets rebooted, re-run the script in the [step 2](#) to repopulate the iptables.

For HA deployment—

NOTE: `setup_NAT_rule.sh` script is not supported for the HA deployment.

To review the details on the ports, see [Table 11 on page 24](#).

Run `./get_vm_details.sh` script to find the IP addresses for each component.

```
root@startupserver_1:~/Contrail_Service_Orchestration_5.1.1#
./get_vm_details.sh
```

```
Load Balancer IP:
    nginx : 192.168.10.16
    keystone : 192.168.10.20
    haproxy_conf : 192.168.10.48
    etcd : 192.168.10.19
    haproxy_conf_sb : 192.168.10.49
    mariadb : 192.168.10.17
    nginx_nsd : 192.168.10.18
```

Configure next-hop at the gateway for VRR public IP addresses (for example—10.x.x.3 and 10.x.x.4) to point to the SRX IP address (for example—10.x.x.2).

- Here is the NAT configuration for any public facing device:

```
## Public address space
set security address-book global address public 10.x.x.2/32
set security address-book global address vrr-1-public 10.x.x.3/32
set security address-book global address vrr-2-public 10.x.x.4/32

### Private CSO address space (192.168.10.0/24)
set security address-book global address monitoring_1 192.168.10.31/32
set security address-book global address keystone 192.168.10.20/32
set security address-book global address nginx 192.168.10.16/32
set security address-book global address nginx_nsd 192.168.10.18/32
set security address-book global address haproxy_conf 192.168.10.46/32
set security address-book global address haproxy_conf_sb 192.168.10.47/32
set security address-book global address vrr-1 192.168.10.29/32
set security address-book global address vrr-2 192.168.10.30/32
set security address-book global address startupserver_1 192.168.10.45/32

set security nat source rule-set inetAccess from zone trust
```

```

set security nat source rule-set inetAccess to zone untrust
set security nat source rule-set inetAccess rule inet match source-address
192.168.10.0/24
set security nat source rule-set inetAccess rule inet match destination-address
0.0.0.0/0
set security nat source rule-set inetAccess rule inet match application any
set security nat source rule-set inetAccess rule inet then source-nat interface

set security nat static rule-set cso from zone untrust
set security nat static rule-set cso rule adminportal-443 match
destination-address-name public
set security nat static rule-set cso rule adminportal-443 match destination-port
443
set security nat static rule-set cso rule adminportal-443 then static-nat
prefix-name nginx
set security nat static rule-set cso rule adminportal-443 then static-nat
prefix-name mapped-port 443
set security nat static rule-set cso rule designtools-83 match
destination-address-name public
set security nat static rule-set cso rule designtools-83 match destination-port
83
set security nat static rule-set cso rule designtools-83 then static-nat
prefix-name nginx_nsd
set security nat static rule-set cso rule designtools-83 then static-nat
prefix-name mapped-port 443
set security nat static rule-set cso rule outbound-ssh-7804 match
destination-address-name public
set security nat static rule-set cso rule outbound-ssh-7804 match destination-port
7804
set security nat static rule-set cso rule outbound-ssh-7804 then static-nat
prefix-name haproxy_conf
set security nat static rule-set cso rule outbound-ssh-7804 then static-nat
prefix-name mapped-port 7804
set security nat static rule-set cso rule rsyslog-514 match
destination-address-name public
set security nat static rule-set cso rule rsyslog-514 match destination-port 514
set security nat static rule-set cso rule rsyslog-514 then static-nat prefix-name
haproxy_conf_sblb
set security nat static rule-set cso rule rsyslog-514 then static-nat prefix-name
mapped-port 514
set security nat static rule-set cso rule syslog-3514 match
destination-address-name public
set security nat static rule-set cso rule syslog-3514 match destination-port 3514
set security nat static rule-set cso rule syslog-3514 then static-nat prefix-name

```



```

haproxy_confd_sblb
set security nat static rule-set cso rule syslog-3514 then static-nat prefix-name
mapped-port 3514
set security nat static rule-set cso rule syslog-2216 match
destination-address-name public
set security nat static rule-set cso rule syslog-2216 match destination-port 2216
set security nat static rule-set cso rule syslog-2216 then static-nat prefix-name
haproxy_confd_sblb
set security nat static rule-set cso rule syslog-2216 then static-nat prefix-name
mapped-port 2216
set security nat static rule-set cso rule CRL-8060 match destination-address-name
public
set security nat static rule-set cso rule CRL-8060 match destination-port 8060
set security nat static rule-set cso rule CRL-8060 then static-nat prefix-name
haproxy_confd
set security nat static rule-set cso rule CRL-8060 then static-nat prefix-name
mapped-port 8060

set security nat static rule-set cso rule vrr-1 match destination-address-name
vrr-1-public
set security nat static rule-set cso rule vrr-1 then static-nat prefix-name vrr-1
set security nat static rule-set cso rule vrr-2 match destination-address-name
vrr-2-public
set security nat static rule-set cso rule vrr-2 then static-nat prefix-name vrr-2

set security nat static rule-set cso rule kibana-5601 match
destination-address-name public
set security nat static rule-set cso rule kibana-5601 match destination-port 5601
set security nat static rule-set cso rule kibana-5601 then static-nat prefix-name
haproxy_confd
set security nat static rule-set cso rule kibana-5601 then static-nat prefix-name
mapped-port 5601
set security nat static rule-set cso rule rabbitmq-15672 match
destination-address-name public
set security nat static rule-set cso rule rabbitmq-15672 match destination-port
15672
set security nat static rule-set cso rule rabbitmq-15672 then static-nat
prefix-name ngnix
set security nat static rule-set cso rule rabbitmq-15672 then static-nat
prefix-name mapped-port 15672
set security nat static rule-set cso rule es-9210 match destination-address-name
public
set security nat static rule-set cso rule es-9210 match destination-port 9210
set security nat static rule-set cso rule es-9210 then static-nat prefix-name

```

```

monitoring_1
set security nat static rule-set cso rule es-9210 then static-nat prefix-name
mapped-port 9210
set security nat static rule-set cso rule keystone-port-5000 match
destination-address-name public
set security nat static rule-set cso rule keystone-port-5000 match destination-port
5000
set security nat static rule-set cso rule keystone-port-5000 then static-nat
prefix-name keystone
set security nat static rule-set cso rule keystone-port-5000 then static-nat
prefix-name mapped-port 5000
set security nat static rule-set cso rule can-8081 match destination-address-name
public
set security nat static rule-set cso rule can-8081 match destination-port 8081
set security nat static rule-set cso rule can-8081 then static-nat prefix-name
haproxy_confd_sblb
set security nat static rule-set cso rule can-8081 then static-nat prefix-name
mapped-port 8081
set security nat static rule-set cso rule can-8082 match destination-address-name
public
set security nat static rule-set cso rule can-8082 match destination-port 8082
set security nat static rule-set cso rule can-8082 then static-nat prefix-name
haproxy_confd_sblb
set security nat static rule-set cso rule can-8082 then static-nat prefix-name
mapped-port 8082
set security nat static rule-set cso rule grafana-3000 match
destination-address-name public
set security nat static rule-set cso rule grafana-3000 match destination-port
3000
set security nat static rule-set cso rule grafana-3000 then static-nat prefix-name
monitoring_1
set security nat static rule-set cso rule grafana-3000 then static-nat prefix-name
mapped-port 3000

```

- The following configuration is only applicable if you have SRX as your firewall. Apply similar rules if you have any other third party firewall.

```

set system host-name example.net
set system root-authentication encrypted-password
"$5$.eexxxTzK$KpQKybUds3P89Y9N5ol2FubLREaliyh9see.hCBo5"
set system services ssh root-login allow
set system services netconf ssh
set system services dhcp-local-server group jdhcp-group interface fxp0.0
set system services dhcp-local-server group jdhcp-group interface irb.0
set system services web-management https system-generated-certificate
set system name-server 8.8.8.8
set system name-server 8.8.4.4
set system syslog archive size 100k
set system syslog archive files 3
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set system max-configurations-on-flash 5
set system max-configuration-rollbacks 5
set security address-book global address public 10.x.x.2/32
set security address-book global address vrr-1-public 10.x.x.3/32
set security address-book global address vrr-2-public 10.x.x.4/32
set security address-book global address monitoring_1 192.168.10.31/32
set security address-book global address keystone 192.168.10.20/32
set security address-book global address nginx 192.168.10.16/32
set security address-book global address nginx_nsd 192.168.10.18/32
set security address-book global address haproxy_confd 192.168.10.46/32
set security address-book global address haproxy_confd_sb1b 192.168.10.47/32
set security address-book global address vrr-1 192.168.10.29/32
set security address-book global address vrr-2 192.168.10.30/32
set security address-book global address startupserver_1 192.168.10.45/32
set security screen ids-option untrust-screen icmp ping-death
set security screen ids-option untrust-screen ip source-route-option
set security screen ids-option untrust-screen ip tear-drop
set security screen ids-option untrust-screen tcp syn-flood alarm-threshold 1024
set security screen ids-option untrust-screen tcp syn-flood attack-threshold 200
set security screen ids-option untrust-screen tcp syn-flood source-threshold 1024
set security screen ids-option untrust-screen tcp syn-flood destination-threshold
2048
set security screen ids-option untrust-screen tcp syn-flood timeout 20
set security screen ids-option untrust-screen tcp land
set security nat source rule-set inetAccess from zone trust

```

```

set security nat source rule-set inetAccess to zone untrust
set security nat source rule-set inetAccess rule inet match source-address
192.168.10.0/24
set security nat source rule-set inetAccess rule inet match destination-address
0.0.0.0/0
set security nat source rule-set inetAccess rule inet match application any
set security nat source rule-set inetAccess rule inet then source-nat interface
set security nat static rule-set cso from zone untrust
set security nat static rule-set cso rule adminportal-443 match
destination-address-name public
set security nat static rule-set cso rule adminportal-443 match destination-port
443
set security nat static rule-set cso rule adminportal-443 then static-nat
prefix-name nginx
set security nat static rule-set cso rule adminportal-443 then static-nat
prefix-name mapped-port 443
set security nat static rule-set cso rule rsyslog-514 match
destination-address-name public
set security nat static rule-set cso rule rsyslog-514 match destination-port 514
set security nat static rule-set cso rule rsyslog-514 then static-nat prefix-name
haproxy_conf_d_sblb
set security nat static rule-set cso rule rsyslog-514 then static-nat prefix-name
mapped-port 514
set security nat static rule-set cso rule syslog-3514 match
destination-address-name public
set security nat static rule-set cso rule syslog-3514 match destination-port 3514
set security nat static rule-set cso rule syslog-3514 then static-nat prefix-name
haproxy_conf_d_sblb
set security nat static rule-set cso rule syslog-3514 then static-nat prefix-name
mapped-port 3514
set security nat static rule-set cso rule designtools-83 match
destination-address-name public
set security nat static rule-set cso rule designtools-83 match destination-port
83
set security nat static rule-set cso rule designtools-83 then static-nat
prefix-name nginx_nsd
set security nat static rule-set cso rule designtools-83 then static-nat
prefix-name mapped-port 443
set security nat static rule-set cso rule outbound-ssh-7804 match
destination-address-name public
set security nat static rule-set cso rule outbound-ssh-7804 match destination-port
7804
set security nat static rule-set cso rule outbound-ssh-7804 then static-nat
prefix-name haproxy_conf_d

```

```

set security nat static rule-set cso rule outbound-ssh-7804 then static-nat
prefix-name mapped-port 7804
set security nat static rule-set cso rule kibana-5601 match
destination-address-name public
set security nat static rule-set cso rule kibana-5601 match destination-port 5601
set security nat static rule-set cso rule kibana-5601 then static-nat prefix-name
haproxy_confid
set security nat static rule-set cso rule kibana-5601 then static-nat prefix-name
mapped-port 5601
set security nat static rule-set cso rule syslog-2216 match
destination-address-name public
set security nat static rule-set cso rule syslog-2216 match destination-port 2216
set security nat static rule-set cso rule syslog-2216 then static-nat prefix-name
haproxy_confid_sblb
set security nat static rule-set cso rule syslog-2216 then static-nat prefix-name
mapped-port 2216
set security nat static rule-set cso rule CRL-8060 match destination-address-name
public
set security nat static rule-set cso rule CRL-8060 match destination-port 8060
set security nat static rule-set cso rule CRL-8060 then static-nat prefix-name
haproxy_confid
set security nat static rule-set cso rule CRL-8060 then static-nat prefix-name
mapped-port 8060
set security nat static rule-set cso rule rabbitmq-15672 match
destination-address-name public
set security nat static rule-set cso rule rabbitmq-15672 match destination-port
15672
set security nat static rule-set cso rule rabbitmq-15672 then static-nat
prefix-name nginx
set security nat static rule-set cso rule rabbitmq-15672 then static-nat
prefix-name mapped-port 15672
set security nat static rule-set cso rule es-9210 match destination-address-name
public
set security nat static rule-set cso rule es-9210 match destination-port 9210
set security nat static rule-set cso rule es-9210 then static-nat prefix-name
monitoring_1
set security nat static rule-set cso rule es-9210 then static-nat prefix-name
mapped-port 9210
set security nat static rule-set cso rule keystone-port-5000 match
destination-address-name public
set security nat static rule-set cso rule keystone-port-5000 match destination-port
5000
set security nat static rule-set cso rule keystone-port-5000 then static-nat
prefix-name keystone

```

```

set security nat static rule-set cso rule keystone-port-5000 then static-nat
prefix-name mapped-port 5000
set security nat static rule-set cso rule can-8081 match destination-address-name
public
set security nat static rule-set cso rule can-8081 match destination-port 8081
set security nat static rule-set cso rule can-8081 then static-nat prefix-name
haproxy_confd_sblb
set security nat static rule-set cso rule can-8081 then static-nat prefix-name
mapped-port 8081
set security nat static rule-set cso rule can-8082 match destination-address-name
public
set security nat static rule-set cso rule can-8082 match destination-port 8082
set security nat static rule-set cso rule can-8082 then static-nat prefix-name
haproxy_confd_sblb
set security nat static rule-set cso rule can-8082 then static-nat prefix-name
mapped-port 8082
set security nat static rule-set cso rule grafana-3000 match
destination-address-name public
set security nat static rule-set cso rule grafana-3000 match destination-port
3000
set security nat static rule-set cso rule grafana-3000 then static-nat prefix-name
monitoring_1
set security nat static rule-set cso rule grafana-3000 then static-nat prefix-name
mapped-port 3000

set security nat static rule-set cso rule vrr-1 match destination-address-name
vrr-1-public
set security nat static rule-set cso rule vrr-1 then static-nat prefix-name vrr-1
set security nat static rule-set cso rule vrr-2 match destination-address-name
vrr-2-public
set security nat static rule-set cso rule vrr-2 then static-nat prefix-name vrr-2

set security policies from-zone trust to-zone trust policy trust-to-trust match
source-address any
set security policies from-zone trust to-zone trust policy trust-to-trust match
destination-address any
set security policies from-zone trust to-zone trust policy trust-to-trust match
application any
set security policies from-zone trust to-zone trust policy trust-to-trust then
permit
set security policies from-zone trust to-zone untrust policy trust-to-untrust
match source-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust
match destination-address any

```

```

set security policies from-zone trust to-zone untrust policy trust-to-untrust
match application any
set security policies from-zone trust to-zone untrust policy trust-to-untrust
then permit
set security policies from-zone untrust to-zone untrust policy default-permit
match source-address any
set security policies from-zone untrust to-zone untrust policy default-permit
match destination-address any
set security policies from-zone untrust to-zone untrust policy default-permit
match application any
set security policies from-zone untrust to-zone untrust policy default-permit
then permit
set security policies from-zone untrust to-zone trust policy default-permit match
source-address any
set security policies from-zone untrust to-zone trust policy default-permit match
destination-address any
set security policies from-zone untrust to-zone trust policy default-permit match
application any
set security policies from-zone untrust to-zone trust policy default-permit then
permit
set security policies default-policy deny-all
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces irb.0
set security zones security-zone untrust screen untrust-screen
set security zones security-zone untrust host-inbound-traffic system-services
all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/2.0
set interfaces ge-0/0/1 description "Public Facing"
set interfaces ge-0/0/1 unit 0 proxy-arp restricted
set interfaces ge-0/0/1 unit 0 family inet address 10.x.x.2/24
set interfaces ge-0/0/5 description Host-1
set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/6 description Host-2
set interfaces ge-0/0/6 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/7 description Host-3
set interfaces ge-0/0/7 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces irb unit 0 family inet address 192.168.10.1/24
set vlans vlan-trust vlan-id 3
set vlans vlan-trust l3-interface irb.0
set protocols l2-learning global-mode switching
set protocols lldp interface all

```

```
set protocols rstp interface all
set routing-options static route 0.0.0.0/0 next-hop 10.x.x.254
```

RELATED DOCUMENTATION

| [Installing Contrail Service Orchestration](#) | 36

Applying Security Patches

You can apply in-service patches to CSO microservices without having to reboot the VMs.

This feature is applicable only to microservices and is not supported for infrastructure components like Cassandra, RabbitMQ, kernel etc. The process does not impact sites or CSO workflows.

You can always revert the applied patch in case of unsuccessful execution.

You can follow the following steps to apply security patches:

- Download the tar file that contains the hotfix.
- Run patch script - **patch.sh** to apply security patches.

The script is bundled in the tar file which needs to be executed on the startupserver_1 VM.

The script performs in-service patching of CSO microservices.

RELATED DOCUMENTATION

| *Contrail Service Orchestration Monitoring and Troubleshooting Guide*

| [Viewing Information About Microservices](#) | 56

Viewing Information About Microservices

When you log into Kibana, you see the Discover page, which displays a chart of the number of logs for a specific time period and a list of events for the deployment. You can filter this data to view subsets of logs

and add fields to the table to find the specific information that you need. You can also change the time period for which you view events.

[Table 12 on page 57](#) provides basic functions of each microservice. The list is limited to some of the external facing microservices.

Table 12: Functions of Microservices

Microservice	Description
Activation Service (Central)	Provides network activation functions to enable zero touch provisioning of devices.
ams	Monitors and autonomously collects data without system or human intervention.
cslm	Maintains EMS device data model for device management functions. The data model contains information like device objects, abstract configuration, device inventory object, configuration template object, device profile object, device image object etc.
Configuration Template Service	Provides configuration template management features for the CSO solution. The features include maintaining a database of config templates, template syntanx validation (e.g jinja2, python, yang rpc), template execution with input parameters using Yang RPC, and input/output validation (provided corresponding schema is given).
Device Management Service (Central)	<ul style="list-style-type: none"> • Manages the lifecycle of device objects. Each device object provides an abstraction for one or more physical or virtual network devices. • Provides APIs for device management.
Dataview Service (Central)	Serves the northbound applications such as portals or OSS systems, read-only data with paging, sorting and rich queries.
design-tools-central	Provides interface to Network Function Virtualization Design Tools to create config templates, VNF definitions and network service definitions.

Table 12: Functions of Microservices (continued)

Microservice	Description
Element Management Service (Central)	Maintains EMS device data model for device management functions. This data model contains device objects, abstract config, device inventory object, config template object, device profile object, device image object etc.
Fault and Performance Monitoring (FMPM) Collector Services	Describes APIs used by fault monitoring and performance monitoring system for collecting service check results from telemetry agents.
IAM Service	Provides identity and access management features.
IAM Service (No Authentication)	Provides identity and access management features during password recovery procedures.
Image Management Service (Central)	Provides image management functions.
Inventory Management Service (Central)	Provides generic inventory management functions.
Job Service	<ul style="list-style-type: none"> • Provides job management functionality. • Supports creation of synchronous and asynchronous jobs, track status, rack start and completion time.
Intent based Policy Management	Provides Policy and SLA profile object management service to enable software-defined WAN (SD-WAN) functions.
Policy and SLA management Service	Enables software-defined WAN (SDWAN) function.
Routing Manager Service	Provides APIs to manage routing operations such as to create VPN, interface to route-reflector, enable routing on CPE locations.
Schema Service	<ul style="list-style-type: none"> • Provides highly available, persistent data store for various schemas used by CSP applications. • Provides APIs to create, read, update, and delete schemas.
Shared Object Service	Varies based on type of schema.
Signature Manager Service	Manages application signatures

Table 12: Functions of Microservices (*continued*)

Microservice	Description
Template Service	<p>Provides config template of CSO management feature.</p> <p>This feature maintains database of config templates, template syntax validation (e.g - jinja2, python, yang rpc), template execution with input parameters using Yang RPC, and input/output validation ((provided corresponding schema is given).</p>
Topology Service	Provides API for modeling topologies and working with network elements like devices, hubs, spokes, policy enforcement points and other objects.
Tenant, Site and Service Manager Service	Provides APIs for tenant, site and service management.
VIM	Provides common APIs to create virtual networks, virtual links, instantiate VNFs, instantiate service chains for various virtual network infrastructures.

RELATED DOCUMENTATION

| *Contrail Service Orchestration Monitoring and Troubleshooting Guide*

5

CHAPTER

Upgrading Contrail Service Orchestration

Upgrading Contrail Service Orchestration from Release 4.1.1 to Release 5.1.1 | **61**

Upgrading Contrail Service Orchestration from Release 5.1.0 to Release 5.1.1 | **66**

Upgrading Contrail Service Orchestration from Release 4.1.1 to Release 5.1.1

SUMMARY

Follow this procedure to upgrade from CSO Release 4.1.1 to CSO Release 5.1.1.

The upgrade procedure only supports upgrading CSO Release 4.1.1 *medium* deployment to CSO Release 5.1.1 *HA* deployment.

You will require 3 new servers to install CSO 5.1.1 HA solution. For details, refer to [“Hardware and Software for Contrail Service Orchestration” on page 15](#).

IN THIS SECTION

- [Impact of the CSO Upgrade | 61](#)
- [Backing up Contrail Service Orchestration 4.1.1 Databases | 63](#)
- [Upgrading Contrail Service Orchestration | 64](#)

Impact of the CSO Upgrade

Table [Table 13 on page 61](#) describes the impact of the CSO upgrade from Release 4.1.1 to 5.1.1.

Table 13: Impact of the CSO upgrade from Release 4.1.1 to 5.1.1.

Site-to-site tunnels support before the site upgrade				Site-to-site tunnels support after the site upgrade			
Old Site WAN IP	New Site WAN IP	Site-to-site Tunnels Support	Comments	Old Site WAN IP	New Site WAN IP	Site-to-site Tunnels Support	Comments
Public	Public	Yes	Old sites can establish site-to-site tunnels with the new sites with public IPs.	Public	Public	Yes	Old sites can establish site-to-site tunnels with the new sites with public IPs.

Table 13: Impact of the CSO upgrade from Release 4.1.1 to 5.1.1. (continued)

Site-to-site tunnels support before the site upgrade				Site-to-site tunnels support after the site upgrade			
Old Site WAN IP	New Site WAN IP	Site-to-site Tunnels Support	Comments	Old Site WAN IP	New Site WAN IP	Site-to-site Tunnels Support	Comments
Public	Private IP (asymmetric NAT)	No	You need to create interfaces on the older sites for destination NAT to connect to the sites with private IP addresses.	Public	Private IP (asymmetric NAT)	Yes	Site-to-site tunnels are established after the site upgrade.
Public	Private IP (symmetric NAT)	No	Symmetric NAT interfaces are not supported.	Public	Private IP (symmetric NAT)	No	Symmetric NAT interfaces are not supported.

Table 14: Impact on sites and tenants post CSO upgrade from Release 4.1.1 to 5.1.1

Scenario	Tenant Public Pool	LANs with Public IPs	Site NAT Pool on WAN	PE Multi-homing	Shared Bearer WAN Links
CSO 4.1.1 tenants and sites on-boarded with CSO 4.1.1	Not supported	Not supported	Not supported	Not supported	Not supported
CSO 4.1.1 tenants for sites on-boarded post upgrade to CSO 5.1.1	Not supported	Not supported	Supported	Supported	Supported
New tenants created post upgrade to CSO 5.1.1	Supported	Supported	Supported	Supported	Supported

Backing up Contrail Service Orchestration 4.1.1 Databases

1. Download the CSO Release 5.1.1 tar file from the [CSO Downloads](#) page to the *installervm*.
2. Extract the 4.1.1 patch tar to `/deployments/central/file_root/` and save it as *upgrade51* and run the below salt command.

```
salt '*' state.apply upgrade51 saltenv=central
python /usr/local/bin/setup_cso51_migration.py
```

```
[0] Install patch
[1] Exit
```

Select 0 to install the patch script.

3. Install *nfs-client*.

```
salt '*' state.apply upgrade51.install_nfs_client saltenv=central > nfs_client_status
```

4. Backup CSO Release 4.1.1. data using `cso_backupnrestore` command.

```
cso_backupnrestore -b backup -s 411backup
```

The `cso_backupnrestore` script included backing up of the following components—

- Cassandra
- Elasticsearch
- ArangoDB
- MariaDB
- Etcd
- Zookeeper
- Icinga
- Swift
- HAProxy certificates
- CSO 4.1.1 installation configs

Upgrading Contrail Service Orchestration

Before you begin

You must shutdown *centrallbvm1*, *centrallbvm2*, *centrallbvm3*, *sblb1*, *sblb2*, *VRR1*, and *VRR2* VMs in CSO 4.1.1 before starting with CSO 5.1.1 upgrade. This is required to replicate these IPs in CSO 5.1.1 setup.

You will re-use the 4 public IPs from CSO 4.1.1 for CSO 5.1.1 deployment.

The 4 public IPs are—

- CSO 4.1.1 Central VIP (HAPROXY)
- SBLB VIP
- VRR1
- VRR2

The devices in CSO 5.1.1. will use the same SBLB certificate used in CSO 4.1.1.

NOTE: See [“Minimum Requirements for Servers and VMs” on page 19](#) for details on the VMs and associated resources required for CSO 5.1.1 servers.

Make sure you have the required NAT rules in place. For details, refer to [“Applying NAT Rules” on page 45](#)

Upgrading CSO 4.1.1 to CSO 5.1.1

1. You will re-use the 4 public IPs from CSO 4.1.1 for CSO 5.1.1 deployment.
2. Copy the backup directory of CSO 4.1.1 to CSO 5.1.1.
3. Provision the VMs in the new servers of CSO 5.1.1. For details, refer to [“Provisioning VMs on Contrail Service Orchestration Servers” on page 28](#).
4. During the provisioning, select yes for upgrade.

5. Provide the CSO 4.1.1 **settings.yaml** complete backup path to be restored.

For example—`/root/backup411/config_backups/.config/settings.yaml`

Make sure CSO 5.1 and CSO 4.1 infra password are same.

6. Run `./get_vm_details.sh` to identify the IP address of the *startupserver_1* VM.

`./get_vm_details.sh`

7. Copy the backup directory of CSO 4.1.1 to CSO 5.1.1 *startupserver_1* VM.

8. Run **cso_backupnrestore** script from CSO 5.1.1 *startupserver_1* VM.

```
cso_backupnrestore -b backup -s <backupname>
```

For example—**cso_backupnrestore -b backup -s 511backup**

The command will create a folder by the name of *backupname* under **/backup** directory on the *startupserver_1* VM.

9. Run the following command on CSO 5.1.1 *startupserver_1* VM.

```
salt '*' state.apply upgrademigration41 saltenv=central
```

10. Run the **pre_restore_task** script.

```
python /usr/local/bin/pre_restore_task.py
```

```
Enter the 4.1 backup path:
/root/411backup/backup411/backups/jan9upgrade51data/2020-01-09T10:51:37
Enter the 4.1 configs backup path:
/root/411backup/backup411/backups/config_backups
Please Enter 4.1 Central VIP IP: 10.213.30.238
Enter the 5.1 backup path: /backups/511backup/2020-01-09T18:47:08/
```

11. Restore the data by using **cso_backupnrestore** script.

Note the 5.1 *backup path* from step 10.

backuppath is 5.1 backup path from above for

```
ex./backups/511backup/2020-01-09T18:47:08/#cso_backupnrestore -b restore -s backuppath -t '*'  
-c 'mariadb'
```

```
#cso_backupnrestore -b restore -s backuppath -t '*' -c 'zookeeper'
```

```
#cso_backupnrestore -b restore -s backuppath -t '*' -c 'elasticsearch'
```

```
#cso_backupnrestore -b restore -s backuppath -t '*' -c 'arangodb'
```

```
#cso_backupnrestore -b restore -s backuppath -t '*' -c 'icinga'
```

```
#cso_backupnrestore -b restore -s backuppath -t '*' -c 'cassandra'
```

```
#cso_backupnrestore -b restore -s backuppath -t '*' -c 'swift'
```

12. Upgrade to CSO 5.1.1 by running **upgrade.sh** script.

For details, refer to [“Upgrading Contrail Service Orchestration from Release 5.1.0 to Release 5.1.1” on page 66](#).

13. Restore Contrail Analytics Node (CAN).

```
./python.sh upgrade/migration_scripts/common/can_migration.py
```

After a successful upgrade, CSO is functional and you can log in to the Administrator Portal and the Customer Portal.

Upgrading Contrail Service Orchestration from Release 5.1.0 to Release 5.1.1

SUMMARY

Follow this procedure to upgrade from CSO Release 5.1.0 to CSO Release 5.1.1.

Take snapshot of your current configuration and VMs from your hypervisor management utility before you proceed with the upgrade process.

You can roll back to the previous CSO release if the upgrade is unsuccessful, provided you have taken snapshots of the VMs.

IN THIS SECTION

- [Upgrading Contrail Service Orchestration | 66](#)

Upgrading Contrail Service Orchestration

NOTE: You must have at least 40 GB in the `/root` directory to run the upgrade script.

You must not delete previously installed CSO 5.1.0 folder from the *startupserver* VM.

Follow this procedure to upgrade from CSO Release 5.1.0 to CSO Release 5.1.1.

1. Download the CSO Release 5.1.1 installer package from the [CSO Downloads](#) page to the *startupserver_1* VM.
2. Log in to the *startupserver_1* VM as root.
3. On the *startupserver_1* VM, extract the installer package.

For example, if the name of the installer package is **Contrail_Service_Orchestration_5.1.1.tar.gz**,

```
root@host:~/# tar -xvzf Contrail_Service_Orchestration_5.1.1.tar.gz
```

The contents of the installer package are extracted in a directory with the same name as the installer package.

4. Navigate to the CSO Release 5.1.1 directory in the *startupserver_1* VM.

```
root@host:~/# cd Contrail_Service_Orchestration_5.1.1
```

```
root@host:~/Contrail_Service_Orchestration_5.1.1#
```

5. You can view the list of files in the *Contrail_Service_Orchestration_5.1.1*.

```
root@host:~/Contrail_Service_Orchestration_5.1.1# ls
```

The *Contrail_Service_Orchestration_5.1.1.tar.gz* file includes the **upgrade.sh** script.

6. Run the **upgrade.sh** script.



WARNING: Before you upgrade ensure that all ongoing jobs in Administration Portal and Customer Portal are stopped; otherwise, the upgrade process will fail. During the upgrade, you experience a downtime as CSO goes into maintenance mode.

```
root@host:~/Contrail_Service_Orchestration_5.1.1# ./upgrade.sh
```

```
INFO      =====
INFO      Overall Upgrade Summary
INFO      =====
INFO      config_update : success
INFO      CSO Health-Check Before Upgrade : success
INFO      cso_backup_before_upgrade : NA
INFO      infra_upgrade : success
INFO      Central Microservices Upgrade : success
INFO      Regional Microservices upgrade : success
INFO      Load Microservices Data : success
INFO      CSO Health-Check after Upgrade : success
INFO      =====
INFO      CSO is successfully upgraded to Release
```

```
Contrail_Service_Orchestration_5.1.1
INFO      =====
```

Depending on your deployment, it may take up to 60 minutes to complete this task.

You can view the **upgrade.log** file which is available at **root/Contrail_Service_Orchestration_5.1.1/logs** folder.

If an error occurs, you must fix the error and re-run the **upgrade.sh** script. When you re-run the **upgrade.sh** script, the script continues to execute from the previously failed step.

If it fails after 2 attempts, contact Juniper Networks support for further assistance.

You can run **./python.sh deploy_manager/utils/decrypt_password.py** command to decrypt the passwords for each infrastructure component.

After a successful upgrade, CSO is functional and you can log in to the Administrator Portal and the Customer Portal.