

Contrail Service Orchestration

Contrail Service Orchestration (CSO) Installation and Upgrade Guide

Published
2021-06-04

Release
5.1.2

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 (CSO) Installation and Upgrade Guide
5.1.2

Copyright © 2021 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 Requirements for Contrail Service Orchestration | 15

Server Requirements for Contrail Service Orchestration | 15

Network Devices and Software Tested in 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

Storage Requirements | 23

Port Requirements for CSO VMs | 24

3

Install Contrail Service Orchestration by using CLI

Remove a Previous CSO Deployment | 28

Provision VMs on Contrail Service Orchestration Servers | 29

Before You Begin | 30

Create a Bridge Interface for KVM Hypervisors | 30

Download the Installer for KVM Hypervisor | 32

Download the Installer for ESXi Hypervisor | 34

Verify Connectivity of the VMs | 36

Install Contrail Service Orchestration | 36

Deploy CSO | 36

Perform a Health Check of Infrastructure Components | 48

4

Post Installation Tasks

Retrieve Passwords for Infrastructure Components | 53

Apply Security Patches | 54

Functions of Microservices | 55

View Information About Microservices | 55

5

Upgrade Contrail Service Orchestration

Upgrade Contrail Service Orchestration from Release 4.1.2 to Release 5.1.2 | 59

Impact of the CSO Upgrade | 59

Back up Contrail Service Orchestration 4.1.2 Databases | 61

Upgrade Contrail Service Orchestration | 62

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

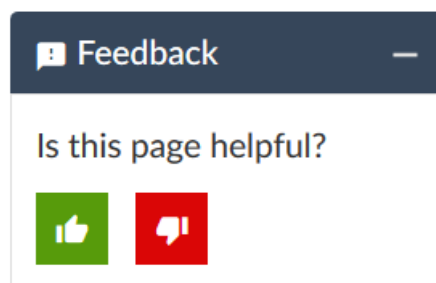
Table 2: Text and Syntax Conventions (*continued*)

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 software-defined wide area network (SD-WAN), software-defined local area network (SD-LAN), and SRX series next-generation firewall management solutions offer automated branch connectivity while improving network service delivery and agility. Contrail Service Orchestration (CSO) is a multitenant 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 and their customers. CSO multitenancy provides security and tenant isolation that prevents the objects and users belonging to one tenant or operating company (OpCo) from seeing or interacting with the objects and users belonging to another tenant or operating company.

CSO can be deployed in one of two ways:

- As a downloadable, **on-premise platform** in which you (or your company) function as the Service Provider administrator (cspadmin user). In an on-premise deployment, the cspadmin user has complete read-write management access and responsibility for the CSO microservices 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 guarantee the authenticity of official Juniper Networks software.
- As a **software as a service (SaaS) platform**, hosted in a public cloud, to which tenants and operating companies (OpCos) subscribe. In a SaaS deployment, Juniper Networks manages the necessary micro-services infrastructure, the secure orchestration and management (OAM) infrastructure, and the underlay networks that are required to enable access to CSO and its solutions.

CSO offers the following solutions:

- Contrail SD-WAN solution—The Contrail SD-WAN solution offers a flexible and automated way to route traffic through the cloud by using overlay networks.
- Contrail Managed LAN (SD-LAN) solution—The managed LAN solution enables CSO to manage and monitor remote LAN devices such as certain EX Series LAN switches, Mist WiFi access points, and certain SRX Series next-generation firewall devices.
- Hybrid WAN (Distributed CPE) deployment model—In a hybrid WAN deployment, customers access network services from a customer premises equipment (CPE) device which is located at the customer's site.

CSO uses conceptual and logical elements as building blocks to complete deployments in the GUI. Portals in CSO help to separate the administrators from the customers. CSO has an Administration Portal and a Customer Portal available.

- Administration Portal—GUI to manage resources, customers, and availability of network services. This portal uses the RESTful APIs of other CSO components.

- Customer Portal—GUI to manage sites, CPE devices, and network services for organizations.

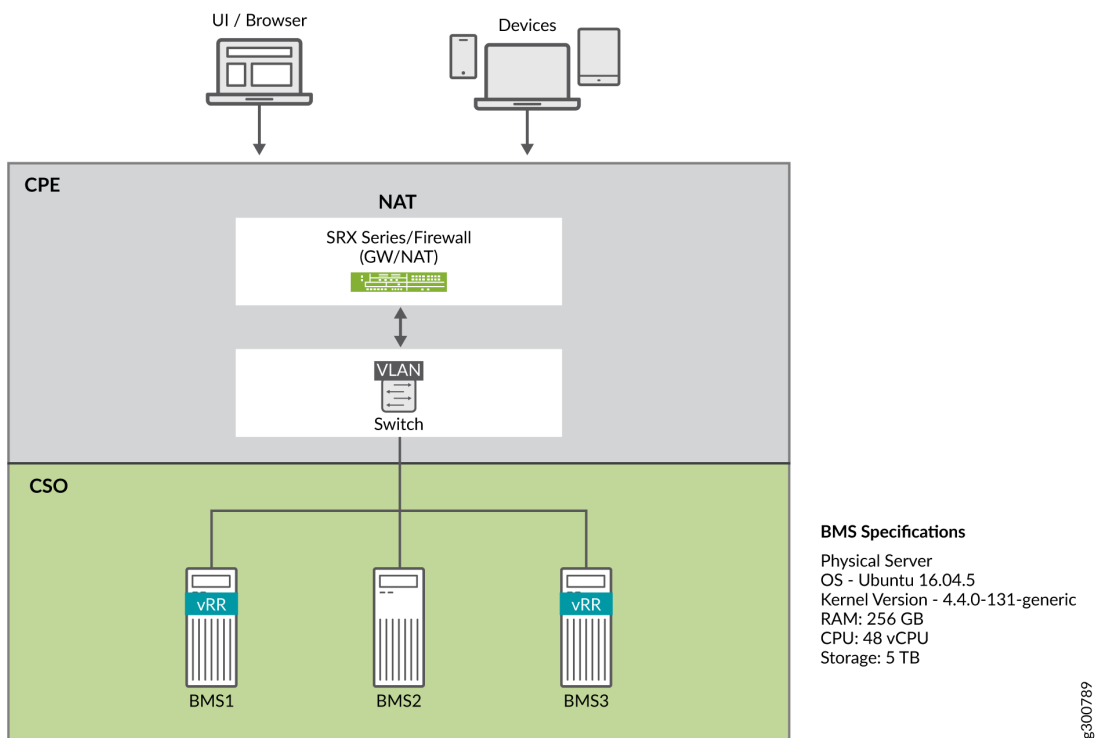
These two portals offer role-based access control (RBAC) for administrators and operators.

This guide provides information about installing the CSO Release 5.1.2 as an on-premise solution. Additionally, the guide covers information about upgrading CSO Release 4.1.2 to CSO Release 5.1.2.

NOTE: The upgrade procedure for CSO Release 5.1.1 to CSO Release 5.1.2 is not supported.

Figure 1 on page 12 shows CSO deployed on-premise.

Figure 1: On-Premises CSO Deployment



For detailed information about configuring CSO, see the [Contrail Service Orchestration \(CSO\) Deployment Guide](#).

RELATED DOCUMENTATION

Contrail Service Orchestration (CSO) Deployment Guide

Contrail Service Orchestration (CSO) Solutions Overview

Contrail Service Orchestration Administration Portal User Guide

Contrail Service Orchestration Customer Portal User Guide

2

CHAPTER

Hardware and Software Requirements

Hardware and Software Requirements for Contrail Service Orchestration | 15

Minimum Requirements for Servers and VMs | 19

Hardware and Software Requirements for Contrail Service Orchestration

IN THIS SECTION

- [Server Requirements for Contrail Service Orchestration | 15](#)
- [Network Devices and Software Tested in Hybrid WAN \(Distributed CPE\) and SD-WAN Deployments | 16](#)

Contrail Service Orchestration (CSO) 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 cloud customer premises equipment (CPE) and software-defined wide area network (SD-WAN) solutions.

Server Requirements for Contrail Service Orchestration

You must use COTS servers for the following functions:

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

NOTE: CSO Release 5.1.0 supports only KVM hypervisors. CSO Release 5.1.1 and later support KVM and ESXi 6.7 hypervisors.

[Table 3 on page 15](#) lists the server requirements.

Table 3: Server Requirements

Number of Servers	vCPUs per Server	Memory per Server	Disk Size per Server
3	48	256 GB RAM	5 TB

For ESXi hypervisors, each virtual machine (VM) must be created with a single partition.

For KVM hypervisors, OS and Data partitions are automated.

Table 4 on page 16 lists the software that has been tested for the 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 COTS Servers

Description	Version
Operating system for all COTS servers	Ubuntu 16.04.5 LTS NOTE: You must 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	Ubuntu 16.04.5 LTS <ul style="list-style-type: none"> • You must install Ubuntu 16.04.5 LTS on the VMs that you configure manually. . • The provisioning tool installs Ubuntu 16.04.5 LTS on all the VMs that it configures.
Hypervisor on CSO 5.1.2 servers	KVM hypervisor 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 4.1.4.0-65

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

Table 5 on page 17 shows the network devices that have been tested for the hybrid WAN (distributed CPE) and the SD-WAN deployments.

Table 5: Network Devices Tested for Hybrid WAN Distributed Deployment and SD-WAN Deployments

Function	Device	Model
Provider Edge (PE) router and IPsec concentrator (hybrid WAN deployment only)	MX Series 3D Universal Edge Router	<ul style="list-style-type: none"> • MX960, MX480, or MX240 router withan MS-MPC • MX80 or MX104 router with an MS-MIC • Other MX Series routers with an MS-MPC or MS-MIC <p>See MPCs Supported by MX Series Routers and MICs Supported by MX Series Routers for information about MX Series routers that support MS-MPCs and MS-MICs.</p>
Provider hub device (SD-WAN deployment only)	Juniper Networks SRX Series Services Gateways 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 deployment)	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 hybrid WAN and SD-WAN deployments.

Table 6: Software Tested for Hybrid WAN and SD-WAN Deployments

Function	Software and Version
Hypervisor on CSO 5.1.2	KVM hypervisor 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
Operating system for NFX150 device	Junos OS Release 18.2X85-D12
Operating system for NFX250 device	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 an SRX Series Services Gateway used as a CPE device or spoke device	Junos OS Release 15.1X49-D172
Operating system for an MX Series router used as a PE router	Junos OS Release 16.1R3.00
Operating system for an MX Series router used as a hub device in an SD-WAN implementation	Junos OS Release 16.1R5.7
Operating system for an SRX Series Services Gateway used as a hub device in an SD-WAN implementation	Junos OS Release 15.1X49-D172

RELATED DOCUMENTATION

Minimum Requirements for Servers and VMs | 19

Minimum Requirements for Servers and VMs

IN THIS SECTION

- [Minimum Hardware Requirements for Servers | 19](#)
- [Minimum Requirements for VMs on CSO Servers | 20](#)
- [Storage Requirements | 23](#)
- [Port Requirements for CSO VMs | 24](#)

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.

NOTE: CSO Release 5.1.0 supports only KVM hypervisors. CSO Release 5.1.1 and later support KVM and ESXi 6.7 hypervisors.

[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>

Table 7: Specification for servers (continued)

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

Minimum Requirements for VMs on CSO Servers

See [Table 9 on page 21](#) for detailed information on the number of VMs needed and minimum requirements for CSO VMs .

For ESXi deployment, do not deploy more than 1 infrastructure or microservice instance on a single server.

For information about the ports that must be open on VMs for all deployments, see [Table 10 on page 24](#).

[Table 9 on page 21](#) shows details about the VMs for a CSO 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.

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 CSO Deployment

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required
startupserver1	Startup server VM	<ul style="list-style-type: none"> • 4 vCPUs • 16 GB RAM • 400 GB hard disk storage
infra1	Third-party applications used as infrastructure services	<ul style="list-style-type: none"> • 10 vCPUs • 64 GB RAM • 500 GB hard disk storage
infra2	Third-party applications used as infrastructure services	<ul style="list-style-type: none"> • 10 vCPUs • 64 GB RAM • 500 GB hard disk storage
infra3	Third-party applications used as infrastructure services	<ul style="list-style-type: none"> • 10 vCPUs • 64 GB RAM • 500 GB hard disk storage
microservices1	All microservices, including GUI applications	<ul style="list-style-type: none"> • 10 CPUs • 64 GB RAM • 250 GB hard disk storage
microservices2	All microservices, including GUI applications	<ul style="list-style-type: none"> • 10 vCPUs • 64 GB RAM • 250 GB hard disk storage
microservices3	All microservices, including GUI applications	<ul style="list-style-type: none"> • 10 vCPUs • 64 GB RAM • 250 GB hard disk storage
monitoring1	Monitoring applications	<ul style="list-style-type: none"> • 4 vCPUs • 24 GB RAM • 250 GB hard disk storage

Table 9: Details of VMs for CSO Deployment (*continued*)

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required
monitoring2	Monitoring applications	<ul style="list-style-type: none"> • 4 vCPUs • 24 GB RAM • 250 GB hard disk storage
monitoring3	Monitoring applications	<ul style="list-style-type: none"> • 4 vCPUs • 24 GB RAM • 250 GB hard disk storage
contrailanalytics1	Contrail Analytics for a distributed deployment.	<ul style="list-style-type: none"> • 16 vCPUs for ESXi deployment 12 vCPUs for KVM deployment • 48 GB RAM • 500 GB hard disk storage
contrailanalytics2	Contrail Analytics for a distributed deployment.	<ul style="list-style-type: none"> • 16 vCPUs for ESXi deployment 12 vCPUs for KVM deployment • 48 GB RAM • 500 GB hard disk storage
contrailanalytics3	Contrail Analytics for a distributed deployment.	<ul style="list-style-type: none"> • 16 vCPUs for ESXi deployment 12 vCPUs for KVM deployment • 48 GB RAM • 500 GB hard disk storage
proxy1	Proxy VM	<ul style="list-style-type: none"> • 2 vCPUs • 8 GB RAM • 100 GB hard disk storage
proxy2	Proxy VM	<ul style="list-style-type: none"> • 2 vCPUs • 8 GB RAM • 100 GB hard disk storage
k8master1	Kubernetes master node	<ul style="list-style-type: none"> • 2 vCPUs • 4 GB RAM • 100 GB hard disk storage
k8master2	Kubernetes master node	<ul style="list-style-type: none"> • 2 vCPUs • 4 GB RAM • 100 GB hard disk storage

Table 9: Details of VMs for CSO Deployment (*continued*)

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required
k8master3	Kubernetes master node	<ul style="list-style-type: none"> • 2 vCPUs • 4 GB RAM • 100 GB hard disk storage
vrr1	Virtual route reflector (VRR) VM	<ul style="list-style-type: none"> • 4 vCPUs • 32 GB RAM
vrr2	Virtual route reflector (VRR) VM	<ul style="list-style-type: none"> • 4 vCPUs • 32 GB RAM
sblb1	Proxy VM—Southbound	<ul style="list-style-type: none"> • 2 vCPUs • 8 GB RAM • 400 GB hard disk storage
sblb2	Proxy VM—Southbound	<ul style="list-style-type: none"> • 2 vCPUs • 8GB RAM • 400 GB hard disk storage

Storage Requirements

For KVM hypervisor, OS and Data partitions are automated

For the ESXi hypervisor, each VM must be created with a single partition. All the *microservices* VMs must be created with an additional separate disk for *Swift* storage.

To create additional hard disk for each for *microservices* VM in the ESXi hypervisor:

1. Open the vSphere Web Client.
2. Right-click a virtual machine in the inventory and select **Edit Settings**.
3. On the **Virtual Hardware** tab, click **New Standard Hard Disk**.
4. Select **New Hard Disk** from the New device drop-down menu at the bottom of the wizard.
5. Specify the size of the hard disk.

NOTE: You must allocate at least 100 GBs.

6. Expand New hard disk and select **Thin Provision**. Mention appropriate location for storage.
7. Click **Save**.

A new disk `/dev/sdb` will be attached to the VMs.

Port Requirements for CSO VMs

Table 10 on page 24 and Table 11 on page 25 show the ports that must be open on all CSO VMs and OAM Hubs 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 10: 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
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
SBLB_IP:2216	TCP/gRPC	External	Telemetry data from device

Table 10: Ports to Open on CSO VMs (*continued*)

Port Number	Protocol	CSO Communication Type	Port Function
SBLB_IP:6514	TCP	External	Device secure syslog over TLS

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
NAT_IP:8529	TCP	External	ArangoDB

Table 11: Ports to Open on OAM Hub

OAMHUB_IP:500	ISAKMP	External	OAMHUB IPSEC connection
OAMHUB_IP:4500	IPSec	External	OAMHUB IPSEC connection
OAMHUB_IP:50	Encapsulated Security Protocol (ESP)	External	OAMHUB IPSEC connection
OAMHUB_IP:51	Authentication Header (AH)	External	OAMHUB IPSEC connection

RELATED DOCUMENTATION

3

CHAPTER

Install Contrail Service Orchestration by using CLI

[Remove a Previous CSO Deployment | 28](#)

[Provision VMs on Contrail Service Orchestration Servers | 29](#)

[Install Contrail Service Orchestration | 36](#)

[Perform a Health Check of Infrastructure Components | 48](#)

Remove a Previous CSO Deployment

You can remove a previous deployment and install a new version of CSO.

If you do not have previous deployment, proceed with [“Provision VMs on Contrail Service Orchestration Servers” on page 29](#).

To remove a previous CSO deployment:

1. Remove the VMs on the physical server.
 - a. Log in to the CSO server as a root user.
 - b. View the list of VMs.

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

Output:

```
Id   Name      State
2    <vm-name> running
```

- c. Remove each VM and its contents.

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

- d. Delete the Ubuntu source directories and the Ubuntu VM.

```
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.

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

3. Clear the Ubuntu cache.

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

RELATED DOCUMENTATION

[Provision VMs on Contrail Service Orchestration Servers | 29](#)

Provision VMs on Contrail Service Orchestration Servers

IN THIS SECTION

- [Before You Begin | 30](#)
- [Create a Bridge Interface for KVM Hypervisors | 30](#)
- [Download the Installer for KVM Hypervisor | 32](#)
- [Download the Installer for ESXi Hypervisor | 34](#)
- [Verify Connectivity of the VMs | 36](#)

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

NOTE: If you use a 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 bridge interface enables the VMs to communicate with the network.

Assumptions/Prerequisites:

- Network devices (routers) must be configured with the required configurations.
- All the physical servers where KVM VMs are provisioned must have Ubuntu 16.04.5 LTS installed.
- All the VMs where CSO components are deployed must have Ubuntu 16.04.5 LTS OS installed.
- Ensure that the VMs and associated resources meet the requirements as given at [“Minimum Requirements for Servers and VMs” on page 19](#).
- You must have a DNS server with high availability for the on-premise Kubernetes cluster.

- Verify the DNS server configuration on the servers.
- All the VMs must have SSH enabled.
- All the VMs must be on the same subnet.
- All the VMs can reach one another.
- All the operations and installations must be run as root user.
- Verify that all the VMs have the correct Fully Qualified Domain Name (FQDN).

Before You Begin

Before you begin, you must:

- Configure the physical servers.
- Ensure that the VMs meet the server requirements listed in [“Minimum Requirements for Servers and VMs” on page 19](#).

Each type of the CSO VM must be distributed across different servers in different racks to avoid server or top-of-rack switch failure. We recommend that you use three servers.

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

NOTE: CSO Release 5.1.0 only supports KVM hypervisors. CSO Release 5.1.1 and later support KVM hypervisors and ESXi version 6.7 hypervisors.

Create a Bridge Interface for KVM Hypervisors

If you use a 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. The bridge interface enables the VMs to communicate with the network.

To create a bridge interface:

1. Log in as root user 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: You must perform this step on all the servers. 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.x.2
    netmask 255.255.255.0
    network 192.168.x.0
    broadcast 192.168.x.255
    gateway 192.168.x.1
    bridge_ports eno2
    dns-nameservers 8.8.8.8
    dns-search example.net
```

5. Navigate to the directory where the CSO .tar file has been downloaded on each of the servers and run the following scripts:

```
root@host:~/Contrail_Service_Orchestration_5.1.2/ci_cd# ls -ltr setup_bms.sh
-rwxr-xr-x 1 root root 716 Oct 10 01:57 setup_bms.sh
root@host:~/Contrail_Service_Orchestration_5.1.2/ci_cd# ./setup_bms.sh
```

```
br0      Link encap:Ethernet  HWaddr 0c:c4:7a:98:94:75
         inet addr:192.168.x.2  Bcast:192.168.x.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)

```

You must run these scripts on all the servers.

Download the Installer for KVM Hypervisor

To download the installer for KVM hypervisors and then provision the VMs:

1. Log in as root user to the CSO server.
2. Download the appropriate installer package from the [CSO Downloads](#) page.

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

3. Expand the installer package.

```
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.

4. Run the **deploy.sh** command. Use the interactive script to create configuration files for the environment specific topology.

```
root@host:~/Contrail_Service_Orchestration_5.1.2./ deploy.sh
```

```

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

*****
Server Details
*****
Please select hypervisor (kvm/esxi) [kvm]:
Provide range of private IP addresses to be used for creating VMs

```



```

[192.168.x.0/24]: --> CSO VM subnet
Please provide Gateway IP for VMs [192.168.x.1]: --> Assuming 1st IP of the
private subnet/network
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.x.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.x.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.x.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 [<dns ips will be taken from
severs resolv.conf>]:
Provide password for VRR VMs:
Confirm Password:
Provide password for Contrail VMs:
Confirm Password:
Number of VRR instances : 2 --> Will be 2 for HA and 1 for Non HA
Redundancy group for VRR0 : 0
Provide routable IP for VRR1 []:10.x.x.3 --> Routable IP of Device to VRR
communication
Redundancy group for VRR1 : 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]:
Please provide commonname for CSO certificate (FQDN) []:jcs.example.net -->
Domain use to create a self-signed certificate
CSO certificate validity (in days): [365]:
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
Is this 4.1 to 5.1 migration (applies only for blue-green deployment) (y/n) [n]:

```

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

Download the Installer for ESXi Hypervisor

To download the installer for ESXi hypervisors and then provision the VMs:

1. Download the appropriate installer package from the [CSO Downloads](#) page on any of the servers.
Use the Contrail Service Orchestration installer package if you have purchased Network Service Orchestrator and Network Service Controller licenses for a distributed deployment.
2. Expand the installer package.

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

The expanded package contains *ESXi-5.1.2.tgz* under **/Artifacts** folder.

Extract *ESXi-5.1.2.tgz* package.

The *ESXi-5.1.2.tgz* package contains the **ubuntu-16.04-server-cloudimg-amd64.ova** file and the **junos-vrr-x86-64-15.1F6-S7.2.ova** file.

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

The default username is *root*.

4. Provision the VRR VMs using the **junos-vrr-x86-64-15.1F6-S7.2.ova** file.

Enable NETCONF for the VRR VMs.

After you provision the VMs:

1. Assign an IP address to the logical interface(*ens192*) associated with the VM.

For example:

```
auto ens192
iface ens192 inet static
address 192.168.10.47 Juniper Business Use Only

netmask 255.255.255.0
network 192.168.10.0
broadcast 192.168.10.255
gateway 192.168.10.1
dns-nameservers x.x.x.x
dns-search example.net
```

2. Configure a valid hostname for the VMs. and update the **/etc/hostname** file.

NOTE: The hostnames must start and end with an alphanumeric character. The hostnames can contain only the following special characters—hyphen (-) and period (.). The hostnames cannot contain uppercase letters.

3. Update the **/etc/hosts** file.

For example: 127.0.1.1 <hostname>.example.net <hostname>

4. Reboot the VMs.

Verify Connectivity of the VMs

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



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

RELATED DOCUMENTATION

[Apply NAT Rules](#)

Install Contrail Service Orchestration

IN THIS SECTION

- [Deploy CSO | 36](#)

Deploy CSO

After you have provisioned the VMs, to deploy CSO:

1. Copy the installer package file from the central CSO server to the *startupserver1* VM.

```
scp csoc<version>.tar.gz root@<startupserver1 IP>:/root/
```
2. Log in to the *startupserver1* VM as root user.

Run the **get_vm_details.sh** script to find the IP address of the *startupserver1* VM. Use SSH to access the VM.

3. Expand the installer package.

```
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.

4. • For KVM hypervisors:

Run the **deploy.sh** script.

```
1. Deploy CSO
2. Replace VM
0. Exit
#Your choice: [1 --> CSO Infra Deployment; 2 --> Replace existing VM, currently
  supports only KVM k8-master node replacement]
```

• For ESXi hypervisor:

Run the **deploy.sh** script. Use the interactive script to create configuration files for the environment specific topology.

```
1. Deploy CSO
2. Replace VM
0. Exit
#Your choice: [1 --> CSO Infra Deployment; 2 --> Replace existing VM, currently
  supports only KVM k8-master node replacement]
```

```
root@host:~/Contrail_Service_Orchestration_5.1.2./ 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).
Specify additional disk for Swift storage: /dev/sdb --> Give /dev/sdb 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
startupserver1: 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. Deploy microservices.

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

6. Apply NAT rules. To review the details of the ports, see [Table 10 on page 24](#).

- a. Run `./get_vm_details.sh` script to find the IP addresses of each component.

```

root@startupserver1:~/Contrail_Service_Orchestration_6.0.0#
./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_confd_sblb : 192.168.10.49
mariadb : 192.168.10.17
nginx_nsd : 192.168.10.18
```

- b. 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).
- Apply the following 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 monitoring1 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_sblb 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 startupserver1 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_confd
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_confd_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-6514 match
destination-address-name public
set security nat static rule-set cso rule syslog-6514 match destination-port
6514
set security nat static rule-set cso rule syslog-6514 then static-nat
prefix-name haproxy_confd_sblb
set security nat static rule-set cso rule syslog-6514 then static-nat
prefix-name mapped-port 6514
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 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
monitoring1

```

```

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 monitoring1
set security nat static rule-set cso rule grafana-3000 then static-nat
prefix-name mapped-port 3000

```

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

```

set system host-name example.net
set system root-authentication encrypted-password
"$5$.eexxxTzK$KpQKybUds3P89Y9N5ol2FubLREaliyh9see.hCBJo5"
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 monitoring1 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_sblb 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 startupserver1 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 syslog-6514 match
destination-address-name public
set security nat static rule-set cso rule syslog-6514 match destination-port
6514
set security nat static rule-set cso rule syslog-6514 then static-nat
prefix-name haproxy_conf_d_sblb
set security nat static rule-set cso rule syslog-6514 then static-nat
prefix-name mapped-port 6514
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_confd
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_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 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 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
  monitoring1
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 monitoring1
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 13-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

```

7. Load the data.

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

You can run the `./get_vm_details.sh` script to find the IP address of each component.

It is recommended to take snapshots of the VMs for ESXi deployment.

RELATED DOCUMENTATION

[Provision VMs on Contrail Service Orchestration Servers | 29](#)

Backup and Restore of Contrail Service Orchestration (CSO) Databases

Perform a Health Check of Infrastructure Components

After you install or upgrade CSO, you can run the `components_health.sh` script to check health 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 Stack
- Icinga
- RabbitMQ
- Etcd
- Rsyslog
- Kubernetes
- ZooKeeper
- Contrail Analytics

To check the status of infrastructure components:

1. Log in to the startupserver1 VM as root user.
2. Navigate to the CSO directory in the startupserver1 VM.

For example:

```
root@host:~/# cd Contrail_Service_Orchestration_5.1.2
root@host:~/Contrail_Service_Orchestration_5.1.2#
```

3. Check the health status of individual infrastructure components or of all the components in the environment.

- To check the health status of an individual infrastructure component:

```
root@startupserver1:/opt/Contrail_Service_Orchestration_5.1.2#
./components_health.sh --component=<component_name>
```

For Example:

```
root@startupserver1:/opt/Contrail_Service_Orchestration_5.1.2#
./components_health.sh --component=elasticsearch
```

- To check the health status of all the components in the environment:

```
root@startupserver1:/opt/Contrail_Service_Orchestration_5.1.2#
./components_health.sh
```

After a couple of minutes, the status of each infrastructure component 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',
INFO      'Arangodb', 'Keystone', 'Elasticsearch', 'Elk_Elasticsearch', 'Icinga',
INFO      'Rabbitmq', 'Etcd', 'Rsyslog', 'Kubernetes', 'Elk_Logstash', 'Elk_Kibana',
INFO      'Zookeeper', 'Contrail_Analytics']
INFO      ***** HEALTH CHECK COMPLETED IN CENTRAL
ENVIRONMENT *****

```

RELATED DOCUMENTATION

[Retrieve Passwords for Infrastructure Components](#) | 53

4

CHAPTER

Post Installation Tasks

Retrieve Passwords for Infrastructure Components | 53

Apply Security Patches | 54

Functions of Microservices | 55

Retrieve 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** user password for the administration portal are displayed on the console after you finish answering the questions in the Setup Assistance.

You can access the administration portal by navigating to NAT IP address using a Web browser. The default username is **cspadmin**. The default password is shown after running `./deploy.sh` script while provisioning the VMs as mentioned in [“Provision VMs on Contrail Service Orchestration Servers” on page 29](#).

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

To retrieve passwords for all infrastructure component, perform the following steps:

1. Log in to the *startupserver1* VM as root user.
2. Navigate to the CSO directory in the *startupserver1* VM.

For example:

```
root@host:~/# cd Contrail_Service_Orchestration_5.1.2
root@host:~/Contrail_Service_Orchestration_5.1.2#
```

3. Run the following command to retrieve the dynamic passwords that were generated during installation.

```
root@startupserver1:/opt/Contrail_Service_Orchestration_5.1.2# ./python.sh
deploy_manager/utils/decrypt_password.py
```



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

To reset the **cspadmin** user password from the CSO Installer webpage:

1. Click **Forget Password?** on the login page of the CSO Installer webpage.

A verification code is sent to the registered e-mail ID.

2. Type the verification code in the password field on the CSO Installer webpage, and then follow the instructions to reset the password.

RELATED DOCUMENTATION

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

Apply Security Patches

You can apply in-service security patches to CSO microservices without rebooting the VMs.

Applying in-service security patches is only applicable to microservices and is not supported for infrastructure components such as Cassandra, RabbitMQ, and OS kernel. This process does not impact sites or CSO workflows.

You can always revert to the previous version of the microservice if the patching was not successful.

To apply security patches:

1. Download the TAR file that contains the hotfix.

The **patch.sh** script is bundled in the TAR file.

2. Run the **patch.sh** script on the *startupserver1* VM to apply the security patches.

The script performs in-service patching of CSO microservices.

RELATED DOCUMENTATION

Functions of Microservices

View Information About Microservices

When you log in to Kibana,the Discover page 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 the logs and to 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 55](#) provides the basic functions of each microservice. The list is limited to some of the public 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.
Configuration template service	Provides configuration template management features for the CSO solution. The features include maintenance of a database of configuration templates, template syntax validation (for example—Jinga2, Python, YANG RPC), template execution with input parameters using YANG RPC, and input/output validation (if the corresponding schema is provided).
cslm	Maintains the data model of the EMS device for device management functions. The data model contains information such as device objects, abstract configuration, device inventory object, configuration template object, device profile object, and device image object.

Table 12: Functions of Microservices (*continued*)

Microservice	Description
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.
design-tools-central	Provides an interface to network function virtualization design tools to create configuration templates, VNF definitions, and network service definitions.
Dataview service (central)	Serves the northbound applications such as portals or operations support systems (OSS), read-only data with paging, sorting and, rich queries.
Element management service (central)	Maintains the data model of the EMS device for device management functions. This data model contains device object, abstract configuration, device inventory object, configuration template object, device profile object, and device image object.
Fault and Performance Monitoring (FMPM) Collector Services	Describes the APIs used by the 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.
Intent-based policy management	Provides policy management and SLA profile object management services to enable software-defined WAN (SD-WAN) functions.
Inventory management service (central)	Provides generic inventory management functions.
Job service	<ul style="list-style-type: none"> • Provides job management functionality. • Supports the creation of synchronous and asynchronous jobs, track status, rack start and completion time.
Policy and SLA management service	Enables software-defined WAN (SD-WAN) functions.

Table 12: Functions of Microservices (*continued*)

Microservice	Description
Routing manager service	Provides APIs to manage routing operations such as creating VPN, interfacing to route reflector, enabling 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.
Template service	Provides configuration template management features for the CSO solution. The features include maintenance of a database of configuration templates, template syntax validation (for example—Jinja2, Python, YANG RPC), template execution with input parameters using YANG RPC, and input/output validation (if the corresponding schema is provided).
Tenant, site and service manager service	Provides APIs for tenant, site, and service management.
Topology service	Provides APIs for modeling topologies and working with network elements such as devices, hubs, spokes, policy enforcement points, and other objects.
VIM	Provides common APIs to create virtual networks, and virtual links, instantiate VNFs, and instantiate service chains for various virtual network infrastructures.

RELATED DOCUMENTATION

| *Contrail Service Orchestration Monitoring and Troubleshooting Guide*

5

CHAPTER

Upgrade Contrail Service Orchestration

Upgrade Contrail Service Orchestration from Release 4.1.2 to Release 5.1.2 | 59

Upgrade Contrail Service Orchestration from Release 4.1.2 to Release 5.1.2

SUMMARY

Follow this procedure to upgrade from CSO Release 4.1.2 to CSO Release 5.1.2.

The upgrade procedure only supports upgrading CSO Release 4.1.2 *medium* deployment to CSO Release 5.1.2 *HA* deployment.

You will require 3 new servers to install CSO 5.1.2 HA solution. For details, refer to [“Hardware and Software Requirements for Contrail Service Orchestration” on page 15](#).

IN THIS SECTION

- [Impact of the CSO Upgrade | 59](#)
- [Back up Contrail Service Orchestration 4.1.2 Databases | 61](#)
- [Upgrade Contrail Service Orchestration | 62](#)

Impact of the CSO Upgrade

Table [Table 13 on page 59](#) describes the impact of the CSO upgrade from Release 4.1.2 to 5.1.2.

Table 13: Impact of the CSO upgrade from Release 4.1.2 to 5.1.2.

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 4.1.2 to 5.1.2. (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 4.1.2 to 5.1.2

Scenario	Tenant Public Pool	LANs with Public IPs	Site NAT Pool on WAN	PE Multi-homing	Shared Bearer WAN Links
CSO 4.1.2 tenants and sites on-boarded with CSO 4.1.2	Not supported	Not supported	Not supported	Not supported	Not supported
CSO 4.1.2 tenants for sites on-boarded post upgrade to CSO 5.1.2	Not supported	Not supported	Supported	Supported	Supported
New tenants created post upgrade to CSO 5.1.2	Supported	Supported	Supported	Supported	Supported

Back up Contrail Service Orchestration 4.1.2 Databases

1. Download the CSO Release 5.1.2 tar file from the [CSO Downloads](#) page to the CSO 4.1.2 *installervm*.
2. Extract the **upgrade512_FRS.tgz** file from the tar file 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. Synchronize the data between nodes.

```
cso_backupnrestore -b nodetool_repair
```

5. Backup CSO Release 4.1.2. data using **cso_backupnrestore** command.

```
cso_backupnrestore -b backup -s backup412
```

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

- Cassandra
- Elasticsearch
- ArangoDB
- MariaDB
- Etcd
- Zookeeper
- Icinga
- Swift
- CAN
- HAProxy certificates
- CSO 4.1.2 installation configs

Upgrade Contrail Service Orchestration

Before you begin

You must shutdown *centrallbvm1*, *centrallbvm2*, *centrallbvm3*, *sblb1*, *sblb2*, *VRR1*, and *VRR2* VMs in CSO 4.1.2 before starting with CSO 5.1.2 upgrade. This is required to replicate these IPs in CSO 5.1.2 setup.

You will re-use the 4 public IPs from CSO 4.1.2 for CSO 5.1.2 deployment.

The 4 public IPs are—

- CSO 4.1.2 Central VIP (HAPROXY)
- SBLB VIP
- VRR1
- VRR2

The devices in CSO 5.1.2. will use the same SBLB certificate used in CSO 4.1.2.

NOTE: See [“Minimum Requirements for Servers and VMs” on page 19](#) for details on the VMs and associated resources required for CSO 5.1.2 servers.

Make sure you have the required NAT rules in place.

Sample SRX config

```
set version 15.1X49-D170.4
set groups 511Enable interfaces ge-0/0/0 unit 0 family inet address 10.x.30.234/19
set groups 511Enable interfaces ge-0/0/0 unit 0 family inet address 10.x.30.239/19
set groups 511Enable interfaces ge-0/0/2 unit 0 family inet address 10.x.30.237/19
set groups 511Enable interfaces ge-0/0/2 unit 0 family inet address 10.x.30.247/19
set groups 511Enable routing-options static route 156.4.0.0/16 next-hop 10.x.21.195
set groups 511Enable routing-options static route 156.19.0.0/16 next-hop 10.x.21.195
set groups vamsi-msb routing-options static route 100.124.0.2/32 next-hop 10.x.7.189
set apply-groups vamsi-msb
set apply-groups 511Enable
set system host-name <example.net>
set system root-authentication encrypted-password
"$5$KltWtn8m$Wtp8JeQnWaMANUyDfwiz4a8FRZW"
set system login class user1_class permissions view
set system login class user1_class permissions view-configuration
set system login class user1_class allow-commands ssh
set system login user user1 uid 2007
```

```

set system login user user1 class user1_class
set system login user user1 authentication encrypted-password <password>
set system services ssh
set system syslog user * any emergency
set system syslog file messages any any
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set system license autoupdate url https://ael.juniper.net/junos/key_retrieval
set security address-book global address haproxy 192.168.10.48/32
set security address-book global address vrr-2 192.168.10.30/32
set security address-book global address vrr-1 192.168.10.29/32
set security address-book global address sblb 192.168.10.49/32
set security address-book global address monitoring1 192.168.10.31/32
set security address-book global address startupserver1 192.168.10.47/32
set security address-book global address nginx 192.168.10.16/32
set security address-book global address public 10.x.30.234/32
set security address-book global address sblbpublic 10.x.30.239/32
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 telemetry-444 match
destination-address-name public
set security nat static rule-set cso rule telemetry-444 match destination-port 444
set security nat static rule-set cso rule telemetry-444 then static-nat prefix-name
haproxy
set security nat static rule-set cso rule telemetry-444 then static-nat prefix-name
mapped-port 444
set security nat static rule-set cso rule rsyslog-514 match destination-address-name
sblbpublic
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
  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
  sblbpublic
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
  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
  192.168.10.18/32
set security nat static rule-set cso rule designtools-83 then static-nat prefix
  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
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
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
  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
192.168.10.5/32
set security nat static rule-set cso rule CRL-8060 then static-nat prefix
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
192.168.10.33/32
set security nat static rule-set cso rule es-9210 then static-nat prefix mapped-port
9210
set security nat static rule-set cso rule arango match destination-address
10.x.30.239/32
set security nat static rule-set cso rule arango match destination-port 8529
set security nat static rule-set cso rule arango then static-nat prefix
192.168.10.22/32
set security nat static rule-set cso rule arango then static-nat prefix mapped-port
8529
set security nat static rule-set cso rule verr-179-5 match destination-address
10.x.30.237/32
set security nat static rule-set cso rule verr-179-5 then static-nat prefix
192.168.10.29/32
set security nat static rule-set cso rule verr-179-6 match destination-address
10.x.30.247/32
set security nat static rule-set cso rule verr-179-6 then static-nat prefix
192.168.10.30/32
set security policies from-zone trust to-zone trust policy default-permit match
source-address any
set security policies from-zone trust to-zone trust policy default-permit match
destination-address any
set security policies from-zone trust to-zone trust policy default-permit match
application any
set security policies from-zone trust to-zone trust policy default-permit then
permit
set security policies from-zone trust to-zone untrust policy default-permit match
source-address any

```

```

set security policies from-zone trust to-zone untrust policy default-permit match
  destination-address any
set security policies from-zone trust to-zone untrust policy default-permit match
  application any
set security policies from-zone trust to-zone untrust policy default-permit 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 permit-all
set security zones security-zone trust tcp-rst
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 ge-0/0/1.0
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-0/0/0.0
set security zones security-zone untrust interfaces ge-0/0/2.0
set interfaces ge-0/0/0 description "UI & SBLB internet facing"
set interfaces ge-0/0/0 unit 0 family inet address 10.x.20.202/19
set interfaces ge-0/0/1 description "CSO facing"
set interfaces ge-0/0/1 unit 0 family inet address 192.168.10.1/24
set interfaces ge-0/0/2 description "VRRs Public IPs"
set interfaces ge-0/0/2 unit 0 family inet
set routing-options static route 1.1.1.0/24 next-hop 192.168.10.2
set routing-options static route 0.0.0.0/0 next-hop 10.x.31.254
set routing-options static route 151.10.0.0/16 next-hop 10.x.7.189
set routing-options static route 151.70.10.0/24 next-hop 10.x.2.246
set routing-options static route 156.15.0.0/16 next-hop 10.x.21.195
set routing-options static route 51.1.0.0/16 next-hop 10.x.21.195
set applications application netconf protocol tcp

```

```

set applications application netconf destination-port 7804
set applications application netconf description "Netconf over ssh"
set applications application syslog-tcp protocol tcp
set applications application syslog-tcp destination-port 514
set applications application syslog-tcp description "Syslog 514 over TCP"
set applications application control-plane-logs protocol tcp
set applications application control-plane-logs destination-port 3514
set applications application control-plane-logs description "Contol plane logs
over TCP"
set applications application NFX-GRPC-Custom-Port protocol tcp
set applications application NFX-GRPC-Custom-Port destination-port 2216
set applications application NFX-GRPC-Custom-Port description "GRPC 2216 Port for
NFX 250 devices"
set applications application CRL protocol tcp
set applications application CRL destination-port 8060
set applications application CRL description "Custom CRL Port to download"

```

Upgrading CSO 4.1.2 to CSO 5.1.2

1. You will re-use the 4 public IPs from CSO 4.1.2 for CSO 5.1.2 deployment.
2. Copy the backup directory of CSO 4.1.2 to CSO 5.1.2.
3. Provision the VMs in the new servers of CSO 5.1.2. For details, refer to [“Provision VMs on Contrail Service Orchestration Servers” on page 29](#).
4. During the provisioning, select yes for upgrade.
5. Provide the CSO 4.1.2 **settings.yaml** complete backup path to be restored.
For example—**/root/backup412/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 *startupserver1* VM.
./get_vm_details.sh
7. Copy the backup directory of CSO 4.1.2 to CSO 5.1.2 *startupserver1* VM.
8. Run **cso_backupnrestore** script from CSO 5.1.2 *startupserver1* VM.
cso_backupnrestore -b backup -s <backupname>

For example—**cso_backupnrestore -b backup -s backup512**

The command will create a folder by the name of *backupname* under **/backup** directory on the *startupserver1* VM.

9. Run the following command on CSO 5.1.2 *startupserver1* 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/backup412/backups/jan9upgrade51data/2020-01-09T10:51:37
Enter the 4.1 configs backup path: /root/backup412/backups/config_backups
Please Enter 4.1 Central VIP IP: 10.213.30.238
Enter the 5.1 backup path: /backups/backup512/2020-01-09T18:47:08/
```

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/backup512/2020-01-09T18:47:08/#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'
```

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

If the restore procedure fails for any of the above components, you must retry to restore only those components.

12. Synchronize the data between nodes.

```
cso_backupnrestore -b nodetool_repair
```

13. Copy the certificate from CSO 4.1.2 backup folder to SBLB HA Proxy.

```
salt-cp -G "roles:haproxy_conf_sblb"
```

```
/root/backups/config_backups/haproxycerts/minions/minions/csp-regional-sblb1.TNL2OQ.
regional/files/etc/pki/tls/certs/ssl_cert.pem /etc/pki/tls/certs
```

```
salt-cp -G "roles:haproxy_conf_sblb"
```

```
/root/backups/config_backups/haproxycerts/minions/minions/csp-regional-sblb1.TNL2OQ.
regional/files/etc/pki/tls/certs/ssl_cert.crt /etc/pki/tls/certs
```

Restart the SBLB HA Proxy.

```
salt -C "G@roles:haproxy_conf_d_sblb" cmd.run "service haproxy restart"
```

14. Copy the certificate from CSO 4.1.2 backup folder to Central HA Proxy.

```
salt-cp -G "roles:haproxy_conf_d"
/root/backups/config_backups/haproxycerts/minions/minions/csp-central-lbvm1.HBLGHQ.
central/files/etc/pki/tls/certs/ssl_cert.pem /etc/pki/tls/certs
```

```
salt-cp -G "roles:haproxy_conf_d"
/root/backups/config_backups/haproxycerts/minions/minions/csp-central-lbvm1.HBLGHQ.
central/files/etc/pki/tls/certs/ssl_cert.crt /etc/pki/tls/certs
```

Restart the Central HA Proxy.

```
salt -C "G@roles:haproxy_conf_d" cmd.run "service haproxy restart"
```

15. Run the following commands on installer VM to update the Nginx certificates.

```
kubectrl get secret -n central | grep cso-ingress-tls
```

```
cso-ingress-tls kubernetes.io/tls                2          17d
```

```
kubectrl delete secret cso-ingress-tls -n central
kubectrl create secret tls cso-ingress-tls --key
/root/backups/config_backups/haproxycerts/minions/minions/csp-central-lbvm1.5R8JKN.
central/files/etc/pki/tls/certs/ssl_cert.key
--cert /root/backups/config_backups/haproxycerts/minions/minions/csp-central-lbvm1.5R8JKN.
central/files/etc/pki/tls/certs/ssl_cert.crt -n central
```

16. Upgrade to CSO 5.1.2 by running **upgrade.sh** script..

17. Restore the SD-WAN and security reports.

```
cso_backupnrestore -b restore -s backuppath -t '*' -c 'swift_report' -r 'yes'
```

18. Restart all the *fmpm-provider-core* pods by deleting them.

```
root@startupserver1:~# kubectrl get pods -n central|grep fmpm-provider-core
```

```
csp.csp-fmpm-provider-core-647ff6598d-4qxxd      1/1      Running    0
2d18h
```

csp.csp-fmpm-provider-core-647ff6598d-94wdx 2d18h	1/1	Running	0
csp.csp-fmpm-provider-core-647ff6598d-dt6vj 2d18h	1/1	Running	0
csp.csp-fmpm-provider-core-647ff6598d-hbnw2 2d18h	1/1	Running	0
csp.csp-fmpm-provider-core-647ff6598d-mx8fn 2d18h	1/1	Running	0
csp.csp-fmpm-provider-core-647ff6598d-zd2zt 2d18h	1/1	Running	0

```
root@startupserver1:~# kubectl delete pod csp.csp-fmpm-provider-core-647ff6598d-4qxxd
csp.csp-fmpm-provider-core-647ff6598d-94wdx csp.csp-fmpm-provider-core-647ff6598d-dt6vj
csp.csp-fmpm-provider-core-647ff6598d-hbnw2 csp.csp-fmpm-provider-core-647ff6598d-mx8fn
csp.csp-fmpm-provider-core-647ff6598d-zd2zt -n central
```

19. Restore Contrail Analytics Node (CAN) database.

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

Copy *analyticsdb* backup from CSO 4.1.2 backup folder to the respective CAN node in CSO 5.1.2.

The *analyticsdb* backup files are located at

```
/root/backups/backup411/2020-05-21T00:43:50/central/can/can<x>
```

```
ssh root@<new-can-ip-[123]>
```

```
docker cp 0000/mc-* analyticsdb:/root
```

```
docker exec -it analyticsdb bash
```

```
mv /root/mc-*
```

```
/var/lib/cassandra/data/ContrailAnalyticsCql/statstablebystrtagv3-c5e9b4c056f711ea8a948909f467ce30
```

```
#The path may be different based on uuid #The path may be different based on uuids
```

```
cd
```

```
/var/lib/cassandra/data/ContrailAnalyticsCql/statstablebystrtagv3-c5e9b4c056f711ea8a948909f467ce30
```

```
chown -R cassandra:cassandra *
```

```
nodetool refresh -- ContrailAnalyticsCql statstablebystrtagv3
```

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

RELATED DOCUMENTATION

Backup and Restore of Contrail Service Orchestration (CSO) Databases