JUNIPER NETWORKS | Engineering Simplicity

Contrail Service Orchestration

Contrail Service Orchestration (CSO) Installation and Upgrade Guide

Published
2022-12-21

RELEASE
6.3.0

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

Contrail Service Orchestration Contrail Service Orchestration (CSO) Installation and Upgrade Guide
6.3.0

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 This Guide

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

CHAPTER 1

Introduction

Contrail Service Orchestration Overview

Juniper Networks Contrail software-defined wide area network (SD-WAN), 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. 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.
- Next Generation Firewall (NGFW) solution—The NGFW solution provides remote network security through the use of SRX Series NGFW devices as CPE at the branch 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.

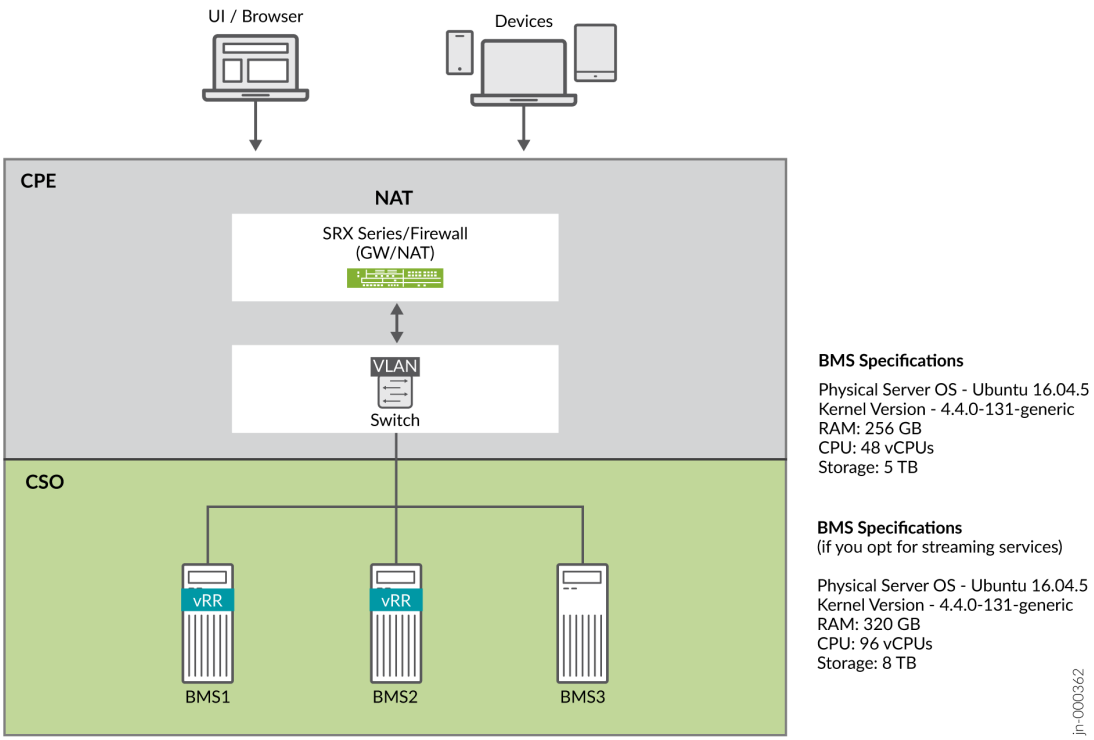
- Administration Portal—GUI to manage resources, customers, and availability of network services. This portal uses the RESTful APIs of other CSO components.
- Customer Portal—GUI to manage sites, CPE devices, and network services for organizations.

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

This guide provides information about installing the CSO Release 6.3.0 as an on-premise solution. Additionally, the guide covers information about upgrading CSO Release 6.1.0 to CSO Release 6.3.0.

Figure 1 on page 3 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

- Deployment Guide
- 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

IN THIS SECTION

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

Table 1 on page 5 lists the server requirements. Starting in Release 6.3.0, CSO supports syslog streaming services, which enable users to access the device syslog notifications. You can opt for streaming services by enabling the streaming option during the install or upgrade procedure. The syslogs are streamed in real-time and can be retrieved through REST API calls.

Table 1: Server Requirements

Specifications	Without Streaming Services	With Streaming Services
Number of Servers	3	3
vCPUs per Server	48 (56 for ESXi)	96

Table 1: Server Requirements *(Continued)*

Specifications	Without Streaming Services	With Streaming Services
Memory per Server	256 GB RAM	320 GB RAM
Disk Size per Server	5 TB	8 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 2 on page 6 lists the software that has been tested for the COTS servers used in the SD-WAN solution. You must use these specific versions of the software when you implement the SD-WAN solutions.

Table 2: 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, except Contrail Analytics VMs, on CSO servers	Ubuntu 16.04.5 LTS
Operating system for Contrail Analytics VMs on CSO servers	CentOS version 7.7.1908
Hypervisor on CSO 6.3.0 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)

Table 2: Software Tested for COTS Servers *(Continued)*

Description	Version
Contrail Analytics	Contrail Networking Release 21.4.61

Network Devices and Software Tested in SD-WAN Deployments

Table 3 on page 7 shows the network devices that have been tested for SD-WAN deployments.

Table 3: Network Devices Tested for SD-WAN Deployments

Function	Device	Model
Provider hub device (SD-WAN deployment only)	SRX Series Services Gateways vSRX 3.0 on an x86 server	• SRX1500 Services Gateway • SRX4100 Services Gateway • SRX4200 Services Gateway • SRX4600 Services Gateway • vSRX 3.0

Table 3: Network Devices Tested for SD-WAN Deployments *(Continued)*

Function	Device	Model
CPE device or branch site device (SD-WAN deployment)	NFX Series Network Services Platforms SRX Series Services Gateways vSRX 3.0 on an x86 server	• 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 • SRX380 Services Gateway • SRX550M Services Gateway • SRX1500 Services Gateway • SRX4100 Services Gateway • SRX4200 Services Gateway • SRX4600 Services Gateway • vSRX 3.0

Table 3: Network Devices Tested for SD-WAN Deployments *(Continued)*

Function	Device	Model
Enterprise hub	SRX Series Services Gateways	• SRX1500 Services Gateway • SRX4100 Services Gateway • SRX4200 Services Gateway • SRX4600 Services Gateway • SRX380 Services Gateway • vSRX 3.0

Table 4 on page 9 shows the software tested for the distributed deployment. You must use these specific versions of the software when you implement a SD-WAN deployment.

Table 4: Software Tested for SD-WAN Deployments

Function	Software and Version
Hypervisor on CSO 6.3.0	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 6.3.0
Contrail Analytics	Contrail Networking Release 21.4.61
Operating system for NFX150 devices	Junos OS Release 20.4R3-S4
Operating system for NFX250 devices	Junos OS Release 18.4R3-S5
Routing and security for NFX250 devices	vSRX KVM Appliance 20.4R3-S4

Table 4: Software Tested for SD-WAN Deployments *(Continued)*

Function	Software and Version
Operating system for vSRX 3.0 used as a CPE device on an x86 server	vSRX KVM Appliance 20.4R3-S4
Operating system for an SRX Series Services Gateway used as a CPE device or branch site device	Junos OS Release 20.4R3-S4
Operating system for an SRX Series Services Gateway used as a hub device in an SD-WAN implementation	Junos OS Release 20.4R3-S4

RELATED DOCUMENTATION

Minimum Requirements for Servers and VMs | 10

Minimum Requirements for Servers and VMs

IN THIS SECTION

Minimum Hardware Requirements for Servers

For information about the makes and models of servers that you can use, see "Hardware and Software Requirements for Contrail Service Orchestration" on page 5. When you obtain servers for SD-WAN solution, we recommend that you:

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

Table 5 on page 11 shows the specification for the servers for SD-WAN solution.

Table 5: Specification for servers

Item	Requirement
Storage	Storage drive can be one of the following types: • Serial Advanced Technology Attachment (SATA) • Serial Attached SCSI (SAS) • Solid-state drive (SSD) **NOTE**: Solid-state drive (SSD) is preferred storage for better performance.
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 6 on page 11 shows the required hardware specifications for servers. 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 12, because some additional resources are required for the system software.

Table 6: Server Requirements

Server Specifications	**Without Streaming Services**	**With Streaming Services**
	Resources Required	Resources Required
Number of nodes or servers	3	3

Table 6: Server Requirements *(Continued)*

Server Specifications	Without Streaming Services	With Streaming Services
	Resources Required	Resources Required
vCPUs per node or server	48 (56 for ESXi)	96
RAM per node or server	256 GB	320 GB

Minimum Requirements for VMs on CSO Servers

See Table 7 on page 12 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 8 on page 18.

Table 7 on page 12 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. If you opt for streaming services, then you need 25 VMs. Additionally you require 3 routable IP addresses, 1 IP address for NAT server and 2 IP addresses for VRR.

Table 7: Details of VMs for CSO Deployment

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required
startupserver1	Startup server VM	• 4 vCPUs • 16 GB RAM • 1.5 TB hard disk storage

Table 7: Details of VMs for CSO Deployment *(Continued)*

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required
infra1	Third-party applications used as infrastructure services	• 10 vCPUs • 64 GB RAM • 500 GB hard disk storage
infra2	Third-party applications used as infrastructure services	• 10 vCPUs • 64 GB RAM • 500 GB hard disk storage
infra3	Third-party applications used as infrastructure services	• 10 vCPUs • 64 GB RAM • 500 GB hard disk storage
microservices1	All microservices, including GUI applications	• 20 vCPUs • 64 GB RAM • 500 GB hard disk storage
microservices2	All microservices, including GUI applications	• 20 vCPUs • 64 GB RAM • 500 GB hard disk storage
microservices3	All microservices, including GUI applications	• 20 vCPUs • 64 GB RAM • 500 GB hard disk storage

Table 7: Details of VMs for CSO Deployment *(Continued)*

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required
monitoring1	Monitoring applications	• 4 vCPUs • 24 GB RAM • 500 GB hard disk storage
monitoring2	Monitoring applications	• 4 vCPUs • 24 GB RAM • 500 GB hard disk storage
monitoring3	Monitoring applications	• 4 vCPUs • 24 GB RAM • 500 GB hard disk storage
contrailanalytics1	Contrail Analytics for a distributed deployment.	• 1. 16 vCPUs for ESXi deployment 2. 12 vCPUs for KVM deployment • 48 GB RAM • 500 GB hard disk storage
contrailanalytics2	Contrail Analytics for a distributed deployment.	• 1. 16 vCPUs for ESXi deployment 2. 12 vCPUs for KVM deployment • 48 GB RAM • 500 GB hard disk storage

Table 7: Details of VMs for CSO Deployment *(Continued)*

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required
contrailanalytics3	Contrail Analytics for a distributed deployment.	1. 16 vCPUs for ESXi deployment 2. 12 vCPUs for KVM deployment • 48 GB RAM • 500 GB hard disk storage
proxy1	Proxy VM	• 2 vCPUs • 8 GB RAM • 500 GB hard disk storage
proxy2	Proxy VM	• 2 vCPUs • 8 GB RAM • 500 GB hard disk storage
k8master1	Kubernetes master node	• 2 vCPUs • 4 GB RAM • 500 GB hard disk storage
k8master2	Kubernetes master node	• 2 vCPUs • 4 GB RAM • 500 GB hard disk storage
k8master3	Kubernetes master node	• 2 vCPUs • 4 GB RAM • 500 GB hard disk storage

Table 7: Details of VMs for CSO Deployment *(Continued)*

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required
vrr1	Virtual route reflector (VRR) VM	• 4 vCPUs • 32 GB RAM
vrr2	Virtual route reflector (VRR) VM	• 4 vCPUs • 32 GB RAM
sblb1	Proxy VM—Southbound	• 2 vCPUs • 8 GB RAM • 500 GB hard disk storage
sblb2	Proxy VM—Southbound	• 2 vCPUs • 8GB RAM • 500 GB hard disk storage
The following VMs are available only if you installed streaming services.		
streaming1	syslog streaming applications	• 32 vCPUs • 64 GB RAM • 2 TB hard disk storage
streaming2	syslog streaming applications	• 32 vCPUs • 64 GB RAM • 2 TB hard disk storage

Table 7: Details of VMs for CSO Deployment *(Continued)*

Name of VM or Microservice Collection	Components That Installer Places in VM	Resources Required
streaming3	syslog streaming applications	• 32 vCPUs • 64 GB RAM • 2 TB 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 GB.

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 8 on page 18 and Table 9 on page 19 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 8: 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
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.

Table 8: Ports to Open on CSO VMs *(Continued)*

Port Number	Protocol	CSO Communication Type	Port Function
NAT_IP:1947	TCP	External	Icinga UI
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:8529	TCP	External	ArangoDB

Table 9: 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

Hardware and Software Requirements for Contrail Service Orchestration | 5

Provision VMs on Contrail Service Orchestration Servers | 23

CHAPTER 3

Install Contrail Service Orchestration

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 23.

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 <CSO folder>
root@host:~/# rm -rf /root/disks
root@host:~/# cd /root/ubuntu_vm
root@host:~/# rm -rf <vm directory>
```

2. Clear the Ubuntu cache.

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

RELATED DOCUMENTATION

Provision VMs on Contrail Service Orchestration Servers | 23

Provision VMs on Contrail Service Orchestration Servers

IN THIS SECTION

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 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, except Contrail Analytics VMs, where CSO components are deployed must have Ubuntu 16.04.5 LTS OS installed.
- All the Contrail Analytics VMs where CSO components are deployed must have CentOS version 7.7.1908 installed.

- Ensure that the VMs and associated resources meet the requirements as given at "Minimum Requirements for Servers and VMs" on page 10.
- 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 10.

  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.

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
* apt-get install dnsutils
```

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. Modify the main Apt sources configuration file on the new physical servers to connect the Debian sources.list to internet.

```
root@host:~/# cp /etc/apt/orig-sources.list /etc/apt/sources.list
```

You do not need to modify the file if Debian sources.list is connected to the Ubuntu repository.

6. 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_6.3.0/ci_cd# ls -ltr setup_bms.sh
-rwxr-xr-x 1 root root 877 Jun 15 11:50 setup_bms.sh
root@host:~/Contrail_Service_Orchestration_6.3.0/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.

Verify that the `libguestfs-tools` package is installed successfully.

```
root@host:~/# dpkg -l |grep libguestfs-tools
```

NOTE: If you run the `setup_bms.sh` script after creating the bridge interface, you might see an error-`device br0 already exists; can't create bridge with the same name`. You can ignore the error message.

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.

   Example output for CSO deployment on KVM hypervisor—

```
root@host:~/Contrail_Service_Orchestration_6.3.0./ deploy.sh
*********************************************
Generic Questions
*********************************************
Do you need a Standalone/HA deployment (1/2) [2]:2
Would you like to install streaming feature? (y/n) [y]:

*********************************************
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]:
Provide bridge interface for VMs [br0]:
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><nslookup of dns IP should be resolved>]:
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 VRR2 []: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) #It 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 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) []:cso.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
Do you use IPV6 (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-6.3.0.tgz* under the **/Artifacts** folder.

   Extract the *ESXi-6.3.0.tgz* package.

   The *ESXi-6.3.0.tgz* package contains the **ubuntu-16.04-server-cloudimg-amd64.ova** file, the **junos-vrr-x86-64-19.4R1.12.ova** file, and the **centos-77.ova** file.
3. Provision the VMs (except the VRR and contrail_analytics 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 10.

   The default username is *root*.

   NOTE: Provision the streaming VMs only if you want to opt for the streaming services feature during the install or upgrade.
4. Provision the VRR VMs using the **junos-vrr-x86-64-19.4R1.12.ova** file.

   Enable NETCONF for the VRR VMs.

Base config example for VRR VM:

```
delete groups global system services ssh root-login deny-password
set system root-authentication plain-text-password [pass] [pass]
set system services ssh
set system services netconf ssh
set routing-options rib inet.3 static route 0.0.0.0/0 discard
set system services ssh root-login allow set protocols bgp advertise-peer-as
set groups vrr-base-config protocols bgp group ibgp family inet-vpn unicast loops 3
set interfaces em0 unit 0 family inet address 192.168.x.30/24
set routing-options static route 0.0.0.0/0 next-hop 192.168.x.1
set system services ssh sftp-server
set routing-options autonomous-system <as-number> #default value for as-number is 64512
set routing-options autonomous-system loops 10
commit and-quit exit
```

5. Provision the contrail_analytics VMs using the **centos-77.ova** file.

   The default username is *root*.

After you provision the VMs:

1. Assign an IP address to the logical interface (*ens192*) associated with each VM, except contrail_analytics VMs.

   For example:

```
vi /etc/network/interfaces
auto ens192
iface ens192 inet static
address 192.168.10.47 Juniper Business Use Only

netmask 255.255.255.0
network 192.168.x.0
broadcast 192.168.x.255
gateway 192.168.x.1
dns-nameservers x.x.x.x
dns-search example.net
```

NOTE: The file must contain only the entries listed above. Remove all other entries in the file.

2. Assign an IP address to the logical interface (ens192) associated with the contrail_analytics VM.

```
vi /etc/sysconfig/network-scripts/ifcfg-ens192
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="none"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="ens192"
DEVICE="ens192"
ONBOOT="yes"
IPADDR="192.168.x.15"
PREFIX="24"
GATEWAY="192.168.x.1"
DNS1="x.x.x.x"
NETWORK="192.168.x.0"
NETMASK="255.255.255.0"
BROADCAST="192.168.x.255"
DOMAIN="example.net"
IPV6_PRIVACY="no"
```

3. Configure a valid hostname for all 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.

4. Update the **/etc/hosts** file on all the VMs.

   For example:127.0.0.1 <hostname>.<domain-name> <hostname>

> **NOTE**: The file must contain only the entry listed above. Remove all other entries in the file.

5. Add a valid DNS IP address in the **/etc/resolve.conf** file on all the VMs.

   ```
   nameserver <nameserver-ip-address>

   search <domain-name>
   ```

6. Reboot all 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

NOTE: Before you start the deployment, ensure that there is Internet connectivity on all the VMs. Internet connectivity is needed to verify the ESM license.

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 cso<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 k8-master, k8-infra and k8-microservices node for replacement in KVM]
     ```

   - For ESXi hypervisor:

     Run the `deploy.sh` script. Use the interactive script to create configuration files for the environment specific topology. Select option 1 (Deploy CSO) to deploy the CSO infrastructure, Option 2 (Replace VM) is not applicable for ESXi hypervisors.

     Example output for CSO deployment on ESXi hypervisor—

     ```
     root@host:~/Contrail_Service_Orchestration_6.3.0./ deploy.sh
     Enter the number for operation to be performed:
     1. Deploy CSO
     2. Replace VM
     0. Exit
     Your choice: 1


     ********************************************
     Generic Questions
     ```

```
*********************************************
Do you need a Standalone/HA deployment (1/2) [2]:
Would you like to install streaming feature? (y/n) [y]:y


*********************************************
Server Details
*********************************************
Please select hypervisor (kvm/esxi) [kvm]:esxi
Enter the number of cluster groups []:3
Do all your VMs have same password for root(y/n) []:y
Enter the password common for all the VMs:
Confirm Password:
Provide the list/comma separated VM IPs for cluster group 1(except VRR)
[]:192.168.x.2-192.168.x.7,192.168.x.9
Provide the list/comma separated VM IPs for cluster group 2(except VRR)
[]:192.168.x.10-192.168.x.15,192.168.x.17
Provide the list/comma separated VM IPs for cluster group 3(except VRR)
[]:192.168.x.22-192.168.x.29,192.168.x.30
Provide VIP (for admin portal and SBLB usage) for VMs []:10.x.x.183
Please provide the CSO reachable subnet for device communication []:10.x.0.0/20
Provide password for VRR VMs:
Confirm Password:
Number of VRR instances : 2
Redundancy group for VRR0 : 0
Provide routable IP for VRR1 []:10.x.x.234
Provide private IP for VRR1 []:192.168.x.8
Redundancy group for VRR1 : 1
Provide routable IP for VRR2 []:10.x.x.235
Provide private IP for VRR2 []:192.168.x.16


*********************************************
Authentication and Other Questions
*********************************************
Provide list/comma separated 10 IPs to be used for load balancers
[]:192.168.x.42-192.168.x.53
Provide Email Address for cspadmin user []:nutans@juniper.net
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) []:
CSO certificate validity (in days): [365]:
DNS name of CSO Customer Portal []:jcs.juniper.net
```

```
DNS name of CSO Admin Portal (can be same as Customer Portal) []:jcs.juniper.net
Timezone for the servers in topology [America/Los_Angeles]:
List of ntp servers (comma separated) []:
Do you use IPV6 (y/n) [n]:n
Specify additional disk for Swift storage [/dev/vdc]:/dev/sdb
```

5. Confirm if you have the Ubuntu ESM license. This license is required to obtain the security updates. If you do not have the license, contact Juniper support.

```
Do you have Ubuntu ESM (Extended Security Maintenance) license? (y/n): y #recommended
```

6. Deploy microservices.

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

7. Apply NAT rules. To review the details of the ports, see Minimum Requirements for Servers and VMs on page 18.

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

```
root@startupserver1:~/Contrail_Service_Orchestration_6.3.0# ./get_vm_details.sh
Load Balancer IP:
                    nginx : 192.168.10.16
                    keystone : 192.168.10.20
                    haproxy_confd : 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:

     NAT configuration

```
## 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
set security nat static rule-set cso rule icinga-1947 match destination-address-name
public
set security nat static rule-set cso rule icinga-1947 match destination-port 1947
set security nat static rule-set cso rule icinga-1947 then static-nat prefix-name nginx
set security nat static rule-set cso rule icinga-1947 then static-nat prefix-name
mapped-port 1947
```

- 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.

  Sample SRX config

```
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_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 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 icinga-1947 match destination-address-name
public
```

```
set security nat static rule-set cso rule icinga-1947 match destination-port 1947
set security nat static rule-set cso rule icinga-1947 then static-nat prefix-name nginx
set security nat static rule-set cso rule icinga-1947 then static-nat prefix-name
mapped-port 1947
set security nat static rule-set cso rule vrr-1 match destination-address-name vrr-1-
public
set security nat static rule-set cso rule vrr-1 then static-nat prefix-name vrr-1
set security nat static rule-set cso rule vrr-2 match destination-address-name vrr-2-
public
set security nat static rule-set cso rule vrr-2 then static-nat prefix-name vrr-2

set security policies from-zone trust to-zone trust policy trust-to-trust match source-
address any
set security policies from-zone trust to-zone trust policy trust-to-trust match
destination-address any
set security policies from-zone trust to-zone trust policy trust-to-trust match
application any
set security policies from-zone trust to-zone trust policy trust-to-trust then permit
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
source-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
destination-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
application any
set security policies from-zone trust to-zone untrust policy trust-to-untrust then
permit
set security policies from-zone untrust to-zone untrust policy default-permit match
source-address any
set security policies from-zone untrust to-zone untrust policy default-permit match
destination-address any
set security policies from-zone untrust to-zone untrust policy default-permit match
application any
set security policies from-zone untrust to-zone untrust policy default-permit then
permit
set security policies from-zone untrust to-zone trust policy default-permit match
source-address any
set security policies from-zone untrust to-zone trust policy default-permit match
destination-address any
set security policies from-zone untrust to-zone trust policy default-permit match
application any
set security policies from-zone untrust to-zone trust policy default-permit then permit
set security policies default-policy deny-all
set security zones security-zone trust host-inbound-traffic system-services all
```

```
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces irb.0
set security zones security-zone untrust screen untrust-screen
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/2.0
set interfaces ge-0/0/1 description "Public Facing"
set interfaces ge-0/0/1 unit 0 proxy-arp restricted
set interfaces ge-0/0/1 unit 0 family inet address 10.x.x.2/24
set interfaces ge-0/0/5 description Host-1
set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/6 description Host-2
set interfaces ge-0/0/6 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/7 description Host-3
set interfaces ge-0/0/7 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces irb unit 0 family inet address 192.168.10.1/24
set vlans vlan-trust vlan-id 3
set vlans vlan-trust l3-interface irb.0
set protocols l2-learning global-mode switching
set protocols lldp interface all
set protocols rstp interface all
set routing-options static route 0.0.0.0/0 next-hop 10.x.x.254
```

8. 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 | 23

Perform a Health Check of Infrastructure Components

IN THIS SECTION

Perform a Health Check of Infrastructure Components

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

- SaltStack
- Cassandra
- MariaDB
- Swift
- Redis
- ArangoDb
- Keystone
- Elasticsearch
- Elk Elasticsearch
- Icinga
- RabbitMQ
- Etcd
- Rsyslog
- Kubernetes

- ELK Logstash
- ELK Kibana
- ZooKeeper
- Contrail Analytics
- VRR
- Microservices
- Kafka
- Kafka Zookeeper
- Streaming Cassandra

To check the status of infrastructure components:

1. Log in to the startupserver_1 VM as root.
2. Navigate to the CSO directory in the startupserver_1 VM.
   For example:

```
root@host:~/# cd Contrail_Service_Orchestration_6.3.0
root@host:~/Contrail_Service_Orchestration_6.3.0#
```

3. Run the **components_health.sh** script.
   To check the status of one of infrastructure components, run the following command:

```
root@startupserver_1:/opt/Contrail_Service_Orchestration_6.3.0# ./components_health.sh --
component=<component_name>
For Example:
root@startupserver_1:/opt/Contrail_Service_Orchestration_6.3.0# ./components_health.sh --
component=elasticsearch
```

   Run the following command to check the health of all the infrastructure components.

```
root@startupserver_1:/opt/Contrail_Service_Orchestration_6.3.0# ./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 Etcd Started
INFO     The Infrastructure Component Etcd is Healthy

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

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

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

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

INFO     Health Check for Infrastructure Component Redirect_Server Started
WARNING  No redirect server information is available for this CSO setup
INFO     The Infrastructure Component Redirect_Server is Healthy

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

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

INFO     Health Check for Infrastructure Component Kafka_Zookeeper Started
INFO     The Infrastructure Component Kafka_Zookeeper 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 Streaming_Cassandra Started
INFO     The Infrastructure Component Streaming_Cassandra is Healthy

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

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

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

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

INFO     Overall result:
INFO      The following Infrastructure Components are Healthy:
INFO                      ['Saltstack', 'Etcd', 'Mariadb', 'Keystone', 'Swift', 'Redis',
'Zookeeper', 'Kafka', 'Rsyslog', 'Elk_Kibana', 'Elk_Elasticsearch', 'Icinga', 'Arangodb',
'Redirect_Server', 'Cassandra', 'Vrr', 'Kafka_Zookeeper', 'Kubernetes', 'Elk_Logstash',
```

```
'Streaming_Cassandra', 'Rabbitmq', 'Elasticsearch', 'Contrail_Analytics', 'Microservices']
INFO     All nodes are healthy!
```

RELATED DOCUMENTATION

Retrieve Passwords for Infrastructure Components | 51

4

CHAPTER

Post Installation Tasks

Retrieve Passwords for Infrastructure Components

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

- Cassandra or Streaming 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 23.

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 components, 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_6.3.0
root@host:~/Contrail_Service_Orchestration_6.3.0#
```

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

```
root@startupserver1:/opt/Contrail_Service_Orchestration_6.3.0# ./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.

For details, see *Resetting Your Password*

RELATED DOCUMENTATION

Install Contrail Service Orchestration | 32

Functions of Microservices

IN THIS SECTION

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 10 on page 53 provides the basic functions of each microservice. The list is limited to some of the public microservices.

Table 10: 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.
Device management service (central)	• 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.

Table 10: Functions of Microservices *(Continued)*

Microservice	Description
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	• 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 10: 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	• 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—Jinga2, 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.
Syslog Processor	Provides REST API and WebSocket streaming interfaces to access device syslogs.

RELATED DOCUMENTATION

- Contrail Service Orchestration Monitoring and Troubleshooting Guide

5
CHAPTER

Upgrade Contrail Service Orchestration

Upgrade Contrail Service Orchestration from Release 6.1.0 to Release 6.3.0

IN THIS SECTION

Contrail Analytics Nodes (CAN) for CSO Release 6.3.0 run on CentOS version 7.7.1908.

NOTE: Before you upgrade an on-premise deployment to CSO Release 6.3.0, ensure that

- All sites are running version 6.1.0 and the supported Junos OS release.
- All VMs have Internet connectivity. Internet connectivity is needed to verify the ESM license.

Upgrade Contrail Service Orchestration for KVM and ESXi Hypervisors

Prerequisites

- For ESXi hypervisors, create three new VMs for the streaming feature. See "Provision VMs on Contrail Service Orchestration Servers" on page 23.
- You must have at least 40 GB in the / partition in the startupserver1 VM to run the upgrade script.
- You must not delete previously installed CSO 6.1.0 folder from the *startupserver* VM.

If you opted for the streaming feature, then complete the following steps:

- Configure the three physical servers for HA setup (if streaming is opted). Ensure that all the prerequisites are met. For details, see "Provision VMs on Contrail Service Orchestration Servers" on page 23. Ensure that these three physical servers can connect to the existing CSO servers.
- Create a bridge interface for KVM hypervisors. For details, see "Create a Bridge Interface for KVM Hypervisors" on page 24. You must assign new IP addresses.

- Modify the main Apt sources configuration file on the new physical servers to connect the Debian sources.list to the Internet.

  ```
  root@host:~/# cp /etc/apt/orig-sources.list /etc/apt/sources.list
  ```

  You do not need to modify the file if Debian sources.list is connected to the Ubuntu repository.

- Run the **setup_bms.sh** script on all the three new physical servers.

- Run the following commands from the CSO folder:

  ```
  root@host:~/Contrail_Service_Orchestration_6.3.0# cd ci_cd
  ```

  ```
  root@host:~/Contrail_Service_Orchestration_6.3.0# ./setup_bms.sh
  ```

  > **NOTE**: If you run the **setup_bms.sh** script after creating the bridge interface, you might see the error meesage `device br0 already exists; can't create bridge with the same name`. You can ignore the error message.

Follow this procedure to upgrade from CSO Release 6.1.0 to CSO Release 6.3.0.

1. Download the CSO Release 6.3.0 installer package from the CSO Downloads page to the *startupserver1* VM.
2. Log in to the *startupserver1* VM as root.
3. On the *startupserver1* VM, extract the installer package.

   For example, if the name of the installer package is **Contrail_Service_Orchestration_6.3.0.tar.gz**,

   ```
   root@host:~/# tar -xvzf Contrail_Service_Orchestration_6.3.0.tar.gz
   ```

   The contents of the installer package are extracted in a directory with the same name as the installer package.
4. Navigate to the **Contrail_Service_Orchestration_6.3.0** directory and remove the csp-routing-manager option from the ms_execution_sequence file.

   ```
   root@host:~/# cd Contrail_Service_Orchestration_6.3.0
   root@host:~/Contrail_Service_Orchestration_6.3.0# sed -i '/csp-routing-manager/d' upgrade/
   migration_scripts/630/ms_execution_sequence
   ```

Verify that the csp-routing-manager option is removed from the ms_execution_sequence file.

```
root@host:~/Contrail_Service_Orchestration_6.3.0# cat upgrade/migration_scripts/630/
ms_execution_sequence
csp-appvisibility-manager-nowait
csp-data-view-central
csp-secmgt-sm
```

5. Back up the Elasticsearch data.

   The upgrade script retains all microservice data, and a day's data of junoslogs and joblogs. You must back up and restore other data (older joblogs and junoslogs). To back up the data, you need the esm and es_migration files. These files are available in the Contrail_Service_Orchestration_6.3.0 directory.

   a. Copy the esm and es_migration files to **/usr/local/bin**.

   ```
   root@host:~/# cp /root/Contrail_Service_Orchestration_6.3.0/artifacts/
   elk_esm-1.0.0.tgz /usr/local/bin/
   root@host:~/# cp /root/Contrail_Service_Orchestration_6.3.0/salt/file_root/elasticsearch/
   configs/es_migration /usr/local/bin/
   ```

   b. Navigate to the **/usr/local/bin** folder and extract the esm file.

   ```
   root@host:~/# cd /usr/local/bin
   root@host:~/usr/local/bin# tar -xvzf elk_esm-1.0.0.tgz
   ```

   c. Change the permission for both the files to 755.

   ```
   root@host:~/usr/local/bin# chmod 755 esm
   root@host:~/usr/local/bin# chmod 755 es_migration
   ```

   d. Back up junoslogs and joblogs data older than one day.

   ```
   root@host:~/usr/local/bin# es_migration -a backup -u admin -p '<es_admin_pwd>' -h
   '<haproxy-ip>' -o 'beforeupgrade'
   ```

6. Navigate to the CSO Release 6.3.0 directory in the *startupserver1* VM.

```
root@host:~/# cd Contrail_Service_Orchestration_6.3.0
root@host:~/Contrail_Service_Orchestration_6.3.0#
```

7. You can view the list of files in the Contrail_Service_Orchestration_6.3.0.

```
root@host:~/Contrail_Service_Orchestration_6.3.0# ls
```

The Contrail_Service_Orchestration_6.3.0.tar.tz file includes the `upgrade.sh` script.

8. Run the `upgrade.sh` script.

WARNING: Before you upgrade ensure that all ongoing jobs in the Administration Portal and Customer Portal are stopped; otherwise, the upgrade process will fail.

Confirm if you have the Ubuntu ESM license. This license is required to obtain the security updates. If you do not have the license, contact Juniper support.

```
Do you have Ubuntu ESM (Extended Security Maintenance) license? (y/n): y #recommended
```

Enter the IP addresses and password for the three new physical servers when prompted. This prompt appears only if you opted for the streaming services feature.

For ESXi hypervisors, enter the IP addresses of the VMs.

For KVM hypervisors, enter the host IP addresses.

```
root@host:~/Contrail_Service_Orchestration_6.3.0# ./upgrade.sh

INFO ====================================================
INFO              Overall Upgrade Summary
INFO     ====================================================
INFO     config_update : success
INFO     CSO Health-Check Before Upgrade : success
INFO     deploy_streaming_feature : success
INFO     can_upgrade : success
INFO     infra_upgrade : success
INFO     Kernel Upgrade : success
INFO     Central Microservices Upgrade : success
```

```
INFO     Regional Microservices upgrade : success
INFO     CSO Elasticsearch Restore : success
INFO     Load Microservices Data : success
INFO     CSO Health-Check after Upgrade : success
INFO     ======================================================
INFO     CSO is successfully upgraded to Release Contrail_Service_Orchestration_6.3.0
INFO     ======================================================
```

Depending on your deployment, it may take 60 minutes to 120 minutes to complete this task.

You can view the **upgrade.log** file which is available at **root/Contrail_Service_Orchestration_6.3.0/logs** folder.

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

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

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

9. Restore the Elasticsearch logs that you backed up in Step 5.

```
root@host:~/Contrail_Service_Orchestration_6.3.0# es_migration -a restore -u admin -p
'<es_admin_pwd>' -h '<haproxy-ip>' -o 'afterupgrade'
```

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

RELATED DOCUMENTATION

- Contrail Service Orchestration Administration Portal User Guide