JUNIPER NETWORKS | Engineering Simplicity

Contrail Service Orchestration Monitoring and Troubleshooting Guide

Published
2022-01-26

RELEASE
6.2.0

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

Contrail Service Orchestration Monitoring and Troubleshooting Guide
6.2.0

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 monitor CSO infrastructure services and microservices and troubleshoot CSO installation, login, site activation, license, and deployment-related issues.

PART 1

Troubleshooting Contrail Service Orchestration Issues

CHAPTER 1

Identifying Connectivity Issues for Cloud-based Deployments

IN THIS CHAPTER

Identifying Connectivity Issues by Using Ping

You can use Contrail Service Orchestration (CSO) to perform a ping operation from a device (provider hub, tenant device, CPE device, enterprise hubs, or next-generation firewall device) to a remote host for identifying issues in connectivity with the remote host.

When you ping a remote host from a device, an Internet Control Message Protocol (ICMP) packet is sent to the remote host. By analyzing the results of the ping operation, you can identify the possible device connectivity issues between the remote host and the device.

NOTE: In Contrail Service Orchestration (CSO) Release 6.1, the following devices support ping:

- NFX Series: NFX150, NFX250
- SRX Series: SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600
- vSRX

To perform the ping operation:

1. Do one of the following:
   - To initiate a ping from a provider hub device, select **Resources** > **Provider Hub Devices**.

     The :Provider Hub Devices page appears.

- To initiate a ping from a tenant device, select **Resources** > **Tenant Devices**.

  The Tenant Devices page appears.

2. Select a device from the list of devices displayed and click **More** > **Ping**.

   The Ping page appears.

   NOTE: You can initiate a ping from a device only when its operational status (in CSO) is Up.

3. Complete the configuration according to the guidelines provided in Table 1 on page 3.

   NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **Ping** to initiate the ping request.

   A job is created and a Ping Progress page appears. After the host sends the ping packets, the Ping Result page appears. If the ping operation is successful, the Ping Result page displays the parameters specified in Table 2 on page 5.

   If the ping operation fails, the Ping Result page displays an appropriate error message (such as `No response` or `No route to host`), indicating that there is an issue in the connectivity to the remote host.

Table 1: Fields on the Ping page

Field	Description
Remote Host	Enter the IPv4 address or hostname of the remote host.
Ping Request Packets	Enter the number of ping request packets to be sent to the remote host. Default: 5. Range: 1 through 300.
Advanced	
Source Interface	Select the source interface on the device through which you want to send the ping request to the remote host. If you do not select a source interface, ping requests are sent on all interfaces. To clear the selected interface, click **Clear All** and select another interface.

Table 1: Fields on the Ping page *(Continued)*

Field	Description
Hostname Resolution	Click the toggle button to enable or disable (default) the display of hostname of the hops along the path to the remote host.
Rapid Ping	Click the toggle button to enable or disable (default) sending ping requests rapidly. If you enable this option, the device sends a minimum of 100 ping request packets per second or sends a packet as soon as a response to the previous packet is received, whichever is greater. • If the source device does not receive a response for 500 ms, timeout is considered. • If the source device receives a response within 500 ms, the next ping request packet is sent immediately. **NOTE**: The ping results are displayed in a single consolidated message instead of individual messages for each ping request packet sent.
Packet Fragmentation	Click the toggle button to enable or disable (default) the fragmenting of ping request packets. If packet fragmentation is disabled, ping packets with the maximum transmission unit (MTU) greater than 1500 bytes are dropped.
Packet Size (bytes)	Enter the size (in bytes) of the ping request packet. Default: 56 bytes. Range: • 1 through 1,472 bytes, if packet fragmentation is disabled. • 1 through 65,468 bytes, if packet fragmentation is enabled.

Table 1: Fields on the Ping page *(Continued)*

Field	Description
Wait Time (seconds)	Enter the time (in seconds) for which the source device waits for a response to the ping request packet. The source device considers the remote host as not reachable after the wait time elapses. Default: 10 seconds. Range: 0 through 600 seconds.
Incoming Interface	Click the toggle button to include or exclude (default) information (on the Ping Result page) about the interface on the source device that receives the ping responses..
Routing Instance	Select a specific routing instance that the ping request packets can use to reach the remote host. The ping result displays the information about the connectivity between the source device and the remote host based on the selected routing instance. To clear the selected routing instance, click **Clear All** and select another routing instance.

Table 2: Fields on the Ping Result page

Field	Description
Packet Loss	Displays the percentage of ping packets sent for which the source device did not receive a response.

Table 2: Fields on the Ping Result page *(Continued)*

Field	Description
Round Trip Time Taken (in µs)	Displays the following information about the duration (in microseconds) between the time when the device sends the ping request and the time when the device receives a response from the remote host. Displays the following: • Minimum: The minimum time taken to receive a response for a ping request packet. • Maximum: The maximum time taken to receive a response for a ping request packet. • Average: The average time taken to receive a response for all the ping request packets sent in a ping operation. • Standard Deviation: The variation of the round trip time from the mean round trip time.
Details	
Sequence	Sequence number of all the ping request packets.
Result	Result of the ping request packets—Success or Failure.
Incoming Interface	Interface on the source device on which the responses are received for the ping requests. This data appears if you have enabled the Incoming Interface option on the Ping page.
Time Taken	Time taken (in microseconds) to receive response to a ping request packet.

Identifying Connectivity Issues by Using Traceroute

You can use Contrail Service Orchestration (CSO) to perform a traceroute operation from a device (provider hub, tenant device, CPE device, enterprise hubs, or next-generation firewall device) to the remote host. Traceroute helps you view the path that a packet travels to reach the remote host. The result is useful in identifying the point of network failure in the path between the source device and remote host.

NOTE: In Contrail Service Orchestration (CSO) Release 6.1, the following devices support traceroute:

- NFX Series: NFX150, NFX250
- SRX Series: SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600
- vSRX

To perform traceroute operation:

1. Do one of the following:
   - To initiate traceroute from a provider hub device, select **Resources** > **Provider Hub Devices**.

     The Provider Hub Devices page appears.
   - To initiate traceroute from a tenant device, select **Resources** > **Tenant Devices**.

     The Tenant Devices page appears.
2. Select a device from the list of devices displayed and click **More** > **Traceroute**.

   The Traceroute page appears.
3. Complete the configuration according to the guidelines provided in Table 3 on page 7.

   NOTE: Fields marked with an asterisk (*) are mandatory.
4. Click **Traceroute** to initiate the traceroute operation.

   A job is created and a traceroute progress page appears. If the traceroute operation is successful, the Traceroute Result page displays the traceroute parameters specified in Table 4 on page 9.

   If the traceroute operation fails, the Traceroute Result page displays an appropriate error message (such as `No response` or `No route to host`).

Table 3: Fields on the Traceroute page

Field	Description
Remote Host	Enter the IPv4 address or hostname of the remote host.

Table 3: Fields on the Traceroute page *(Continued)*

Field	Description
Maximum Hops	Specify the maximum number of network devices that a packet can pass through to reach the remote host. Default: 30. Range: 1 through 255. If the number of hops to reach the remote host exceeds the set value, the traceroute packet is dropped.
Advanced	
Source Interface	Select a source interface on the device from which you want to send the packets to the remote host. Click **Clear All** to remove the selected interface and select another interface.
Hostname Resolution	Click the toggle button to enable or disable (default) the display of hostname of the hops in the path to the remote host.
Wait Time (seconds)	Enter the time until which the device waits for a response from the remote host to a packet sent before considering timeout. Default: 10 seconds. Range: 0 through 86,399 seconds.
Routing Instance	Select a routing instance that the traceroute request packets can use to reach the remote host. The trace result displays the route information based on the configured routing instance type. To clear the selected routing instance, click **Clear All** and select another routing instance.

Table 4 on page 9 lists the parameters on the Traceroute Result page when the traceroute operation is successful.

Table 4: Fields on the Traceroute Result page

Field	Description
Hop	Hostname or IPv4 address of the network devices that the packet passed through to reach the remote host.
Time Taken by Packet 1 Time Taken by Packet 2 Time Taken by Packet 3	Duration (in microseconds) between the time from when the source device sends a packet, and the time it received a response from the hops and the remote host.

CHAPTER 2

Troubleshooting Site Activation Issues for Cloud-based Deployments

IN THIS CHAPTER

Troubleshooting Site Activation Issues

IN THIS SECTION

Prerequisites to Activate a Site

IN THIS SECTION

Problem

Description

User was unable to activate a site. Specify the prerequisites to activate a site.

Solution

The prerequisites to activate a site are as follows:

- Check the spoke connectivity to Internet.
- Check the firewall policies between the CPE device and the CSO. The hub or spoke must be able to communicate to CSO through ports 443 (activation), 444 (activation for small and medium deployments), 7804 (outbound-ssh), 3514(app-track logs), 514 (syslog), and 2216 (telemetry agent). See Deployment Guide

Site activation process is stuck in device detected state

IN THIS SECTION

Problem

Description

Site activation process is stuck in device detected state; how do I proceed?

Solution

Do the following:

- Verify that your device can reach the Internet.
- Verify the date and time on the device.
- Verify that the DHCP server and the device are connected to the ge-0/0/0 port.
- Reboot the device.

Site activation process is stuck in bootstrap state

IN THIS SECTION

Problem

Description

Site activation process is stuck in bootstrap state; how do I proceed?

Solution

If the site activation proces is stuck for more than 15 minutes, then do the following:

- Verify that your network firewall allows UDP ports 500 and 4500 for the SD-WAN site.
- Verify that your network firewall allows TCP port 7804 for the next-generation firewall site.
- Reboot the device.

Site activation process failed in bootstrap state

IN THIS SECTION

Problem

Description

Site activation process failed in bootstrap state; how do I proceed?

Solution

Verify that the device is zeroized or running the factory-default configuration. If the device is pre-staged, then ensure that the configuration is not overlapping with the CSO stage-1 configuration. Reboot the device.

Site activation process failed during provisioning

IN THIS SECTION

Problem

Description

Site activation process failed during provisioning; how do I proceed?

Solution

Verify the device connectivity to the Internet. Retry the failed job in CSO. Navigate to **Monitor > Jobs**, select the failed job, and click **Retry Job**.

CHAPTER 3

Troubleshooting Image, License, and Policy Deployment Issues for Cloud-based Deployments

IN THIS CHAPTER

Troubleshooting Image, License, and Policy Deployment Issues

IN THIS SECTION

Unable to find device image version

IN THIS SECTION

Problem

Description

How do I find my device image version without console access to the device?

Solution

Use the J-Web interface to find the device image version.

To access the J-Web interface of the device:

1. Connect your laptop or workstation to any port (except ge-0/0/0) that is available on the device.
2. Enable DHCP on the laptop or workstation and acquire the IP address and gateway information from the device.
3. Use the gateway address (also known as the device address) in the Web browser to connect to the J-Web interface.
4. Log in with the default username **root**. As the root user, you don't need a password to log in.

   The Welcome page appears displaying the device image version.

Upgrade device image using J-Web

IN THIS SECTION

Problem

Description

Device image version is 15.1X49-D110; how do I upgrade the device image before site onboarding?

Solution

Use the J-Web interface to upgrade the device image.

To upgrade the device image using J-Web:

1. Download the recommended image or the software version from the Juniper Networks website to your local machine.
2. Log in to the J-Web interface.
3. Select **Maintain > Software > Upload Package**.
4. Navigate to the device image file location and select the file.
5. Click **Upload and Install Package** to upgrade the device image.

Unable to connect to the device

IN THIS SECTION

Problem

Description

I am not able to log in to the device through the J-Web interface or through the device console. How do I proceed?

Solution

Press and hold the Reset Config button on the device for 15 seconds. Wait for two minutes for the device to restore the factory-default settings. Log in to the device as the root user (no password is required for the root user). If you are still not able to access the device, then reboot the device.

Device image version is different from the recommended version

IN THIS SECTION

Problem

Description

The device image version at the site is 15.1X49D110, but the recommended image version is 15.1X49D170.*x*. Should I upgrade the device image manually before site onboarding?

Solution

You don't' need to upgrade the device image manually before site onboarding. You can do either of the following:

- Upgrade the device image during site activation in CSO—While you are in the site configuration or onboarding workflow, select the device image from the drop-down list.

  NOTE: Device image upgrade during site activation delays the site activation process.

- Upgrade the device image post site activation in CSO—Navigate to **Resources > Images**, select the image, and click **Deploy**.

Policy deployment failed

IN THIS SECTION

Problem

Description

Policy deployment failed; how do I proceed?

Solution

Verify the device connectivity to the Internet. Retry the policy deployment.

No data for next-generation firewall site

IN THIS SECTION

Problem

Description

Application Visibility Monitoring page shows no data for the next-generation firewall site; how do I proceed?

Solution

Do the following:

- Verify that your network firewall allows the UDP port 514.

- Verify the application visibility monitoring page after multiple application sessions (in the time range of 3–5 minutes) traffic.
- Use an appropriate time interval for the query. For example, if you are querying for the traffic sent in the last 10 minutes, then try using a 15-minute query (minimum time interval).

No data for SD-WAN site

IN THIS SECTION

Problem

Description

Application visibility and WAN performance data on the Site Management page shows no data for the SD-WAN site; how do I proceed?

Solution

Do the following:

- Verify the application visibility and WAN performance data after multiple application sessions (in the time range of 3-5 minutes) traffic.
- Use an appropriate time interval for the query. For example, if you are querying for the traffic sent in the last 10 minutes, then try using a 15-minute query (minimum time interval).

Traffic from Spoke Sites Are Dropped or Are Not Reaching Internet or Destination

IN THIS SECTION

Problem

Description

Traffic from spoke sites are dropped or are not reaching the Internet or their specified destinations.

Solution

1. Verify the alerts for overlay or underlay connections, and check whether BGP is active.

   Log in to Administration portal, and select **Monitor > Alerts and Alarm > Alerts**.

2. Check whether the firewall policies are successfully deployed to the CPE device and that the traffic or applications are matching the policies to permit the traffic to Internet or to other sites.

   In Administration Portal, select **Sites > Site-Name > Policies**.

   Or log in to the CPE device and verify that the next-generation firewall policies are deployed.

3. Check the routes in the default VRF route table in the CPE device.

4. Trace the route and verify the reachability from the hub to the destination. If the hub cannot reach the Internet, then verify whether the firewall and NAT policies are set up properly in the hub.

5. For further troubleshooting, collect the logs and output results and contact Juniper Networks Technical Support team.

SLA Violation-Original Link Recovered After SLA Violation

IN THIS SECTION

Problem

Description

The original link is recovered after a service-level agreement (SLA) violation but the application traffic does not switch back to the original link.

Solution

Applications change links only on an SLA violation, because applications are not tied to a specific link and are based on SLA type, such as path preference or link performance metrics.

All WAN links are Up But Not All Links Are Utilized

IN THIS SECTION

Problem

Description

All WAN links are up but not all links are being utilized.

Solution

It is possible that all SD-WAN policies can select the same WAN link if they match the SLAs. If the CPE receives a lot of matching and non-matching application traffic for SD-WAN policies, but not all WAN links are being used, then ensure the following:

1. Check that the CPE device receives multiple flows per application.
2. Check that all the WAN overlays are up (IPsec, GRE) in the CPE device and the hub device.
3. Check the SLA performance data or real-time performance monitoring (RPM) probe results in the CPE device for all links.

   Log in to the Administration Portal, and select **Monitor > Applications > SLA Performance**.

CHAPTER 4

Troubleshooting SMTP Issues for Cloud-based Deployments

IN THIS CHAPTER

Troubleshooting SMTP Issues

IN THIS SECTION

Basic Configuration for SMTP Server

IN THIS SECTION

Problem

Description

User was unable to configure the SMTP e-mail server.

Solution

1. Check the SMTP server settings.

   - SMTP server address—Check the host name or network address of the SMTP e-mail server. Typical SMTP server addresses or host names are as follows:
     - smtp.juniper.net
     - smtp.gmail.com
     - smtp.mail.yahoo.com
     - AWS
   - TLS—Check whether Transport Layer Security (TLS) option is enabled. This setting ensures that the information is transmitted over an encrypted channel. Not all SMTP servers support encryption. If TLS option is enabled for an SMTP server that does not support TLS, then disable the TLS option.
   - Port—Check with your e-mail service provider for the port number that the SMTP server listens to. Generally, port number 587 is used for a TLS connection and port number 25 is used for unencrypted connections.

   Typical SMTP server settings are as follows:

   - smtp.juniper.net—Set TLS to No and port number to 25
   - smtp.gmail.com—Set TLS to Yes and port number to 587
   - smtp.mail.yahoo.com—Set TLS to Yes and port number to 465 or 587

2. Check the SMTP authentication settings.

   - Check whether the e-mail server requires authentication. If yes, then specify the following options.
     - From Name
     - User Name
     - Password
     - From E-mail Address

> **NOTE**: If Gmail blocks SMTP e-mails, then log in to Gmail account, navigate to **Advanced Settings > Security > Less secure app access** and click the toggle button to turn on **Allow less secure apps** option.

3. Test SMTP settings by sending a test e-mail.

   If you are unable to send a test e-mail:

   a. Check the SMTP server settings to see if they match the SMTP server provider's settings.

   b. Check authentication credentials.

   c. Check the SMTP server provider's security settings for SMTP (for example: Gmail blocks SMTP email unless user selects less secure app settings on their gmail account).

   d. Check whether there is network access from CSO to the SMTP server.

   e. Check whether the firewall is blocking SMTP traffic to SMTP server or whether the ports are blocked. If the server settings and authentication settings are correct, check whether the firewall is blocking port 587 and 465 and SMTP traffic. If it is a case of the firewall blocking, then work with the network administrator to unblock ports 465, 587, and SMTP traffic.

RELATED DOCUMENTATION

Configuring SMTP Settings

CHAPTER 5

Recovering an Installation

IN THIS CHAPTER

CSO Disaster Recovery

In case of any failures you can recover CSO Release 6.2.0. To recover CSO Release 6.2.0 you must have already taken a backup and saved the backup file.

To recover CSO Release 6.2.0:

1. Based on the hypervisor you are using, do one of the following:
   - If you are using KVM as the hypervisor:
     a. Copy the CSO 6.2.0 backup folder to the bare metal server.
     b. From the backup folder, copy the **_topology.conf** file to the **Contrail_Service_Orchestration_6.2.0/topology/** folder.

        For example:

        ```
        cp /root/backups/backupfordr/2020-06-19T17:27:05/config_backups/_topology.conf /root/
        Contrail_Service_Orchestration_6.2.0/topology/
        ```

     c. Provision the VMs. For information on provisioning KVM hypervisor, see *Provision VMs on Contrail Service Orchestration Servers* in *CSO Installation and Upgrade Guide*.
     d. Copy the backup folder file from the bare metal server to the startupserver1 VM.

        ```
        user@server>scp -r /root/backups/backupfordr/ startupserver1:
        ```

     e. Log in to the startupserver1 VM as the root user.

f. Expand the installer package.

```
root@startupserver1:~/# tar -xvzf Contrail_Service_Orchestration_6.2.0.tar.gz
```

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

g. From the backup folder, copy the **_topology.conf** file to the **Contrail_Service_Orchestration_6.2.0/topology/** folder.

```
cp /root/backups/backupfordr/2020-06-19T17:27:05/config_backups/_topology.conf /root/
Contrail_Service_Orchestration_6.2.0/topology/
```

- If you are using ESXi as the hypervisor:

a. Copy the backup folder to the startupserver1 VM.

b. Expand the installer package.

```
root@startupserver1:~/# tar -xvzf Contrail_Service_Orchestration_6.2.0.tar.gz
```

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

c. From the backup folder, copy the **_topology.conf** file to the **Contrail_Service_Orchestration_6.2.0/topology/** folder in the startupserver1 VM.

For example:

```
cp /root/backups/backupfordr/2020-06-19T17:27:05/config_backups/_topology.conf /root/
Contrail_Service_Orchestration_6.2.0/topology/
```

2. Run the **deploy.sh** command.

```
root@host:~/Contrail_Service_Orchestration_6.2.0./deploy.sh
```

3. Run the following command:

```
cso_backupnrestore -b backup -s backup62new
```

4. Run the pre_disaster recovery script.

   python /usr/local/bin/pre_disaster_recovery.py

```
Enter the old backup path: /root/backups/backupfordr/2020-10-29T06:45:11:45:11
Enter the new backup path: /backups/backup62new/2020-10-30T03:47:51
COMPONENTS: ('cassandra', 'elasticsearch', 'etcd', 'arangodb', 'icinga', 'swift',
'config_backups') Start cassandra pre restore task...
Get old and new backup path for component cassandra
cassandra pre restore task successfully done
*Do you want to redeploy cassandra container to apply tokens.
*This process will delete all the existing data from cassnadra
Please enter yes to process [yes/no]:
```

   Enter **yes** at the prompt.

```
Start elasticsearch pre restore task...
Get old and new backup path for component elasticsearch
Get Elasticsearch user id for permission
Set permission for elasticsearch dir.
elasticsearch pre restore task successfully done
Start etcd pre restore task...
Get old and new backup path for component etcd
etcd pre restore task successfully done
Start arangodb pre restore task...
Get old and new backup path for component arangodb
arangodb pre restore task successfully done
Start mariadb pre restore task...
Get old and new backup path for component mariadb
mariadb pre restore task successfully done
Start icinga pre restore task...
Get old and new backup path for component icinga
icinga pre restore task successfully done
Start swift pre restore task...
Get old and new backup path for component swift
swift pre restore task successfully done
Start config_backups pre restore task...
config_backups pre restore task successfully done
Pre restore task completed for all components.
```

5. Restore the data from the new backup created in step 3 by using the **cso_backupnrestore** script.

```
#cso_backupnrestore -b restore -s backuppath -t '*' -c ‘cassandra' -r ‘yes’

#cso_backupnrestore -b restore -s backuppath -t '*' -c ‘elasticsearch' -r ‘yes’

#cso_backupnrestore -b restore -s backuppath -t '*' -c ‘arangodb' -r ‘yes’

#cso_backupnrestore -b restore -s backuppath -t '*' -c ‘icinga' -r ‘yes’

#cso_backupnrestore -b restore -s backuppath -t '*' -c ‘swift' -r ‘yes’

#cso_backupnrestore -b restore -s backuppath -t '*' -c ‘mariadb' -r ‘yes’
```

where `backuppath` is the new backup path.

If the restore procedure fails for any of the above components, you must retry to restore only those components. At times, restore of mariadb fails at the first attempt but is successful at the second attempt.

6. Synchronize the data between nodes.

```
cso_backupnrestore -b nodetool_repair
```

```
IF Cluster nodetool status is UP/Normal(UN) please proceed for nodetool repair (Y/n):
```

Enter **y** at the prompt.

7. Copy the certificate from the backup folder to SDN-based load balancing (SBLB) HA Proxy.

```
salt-cp -G "roles:haproxy_confd_sblb" /root/backups/backupfordr/2020-06-19T17:27:05/
config_backups/haproxycerts/minions/minions/csp-central-proxy_sblb1.NH5XCS.central/
files/etc/pki/tls/certs/ssl_cert.pem /etc/pki/tls/certs
```

```
salt-cp -G "roles:haproxy_confd_sblb" /root/backups/backupfordr/2020-06-19T17:27:05/
config_backups/haproxycerts/minions/minions/csp-central-proxy_sblb1.NH5XCS.central/
files/etc/pki/tls/certs/ssl_cert.crt /etc/pki/tls/certs
```

8. Restart the SBLB HA Proxy.

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

9. Copy the certificate from the backup folder to Central HA Proxy.

```
salt-cp -G "roles:haproxy_confd" /root/backups/backupfordr/2020-06-19T17:27:05/
config_backups/haproxycerts/minions/minions/csp-central-proxy1.NH5XCS.central/
files/etc/pki/tls/certs/ssl_cert.pem /etc/pki/tls/certs
```

```
salt-cp -G "roles:haproxy_confd" /root/backups/backupfordr/2020-10-29T06:45:11/
config_backups/haproxycerts/minions/minions/csp-central-proxy1.NH5XCS.central/
files/etc/pki/tls/certs/ssl_cert.crt /etc/pki/tls/certs
```

10. Restart the Central HA Proxy.

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

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

```
kubectl get secret -n central | grep cso-ingress-tls
cso-ingress-tls kubernetes.io/tls                    2      17d
kubectl delete secret cso-ingress-tls -n central kubectl create secret tls cso-ingress-tls
--key /root/backups/backupfordr/2020-10-29T06:45:11/config_backups/haproxycerts/minions/
minions/csp-central-proxy1.NH5XCS.central/files/etc/pki/tls/certs/ssl_cert.key --cert /root/
backups/backupfordr/2020-10-29T06:45:11/config_backups/haproxycerts/minions/minions/csp-
central-proxy1.NH5XCS.central/files/etc/pki/tls/certs/ssl_cert.crt -n central
```

12. Deploy microservices.

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

13. Reindex the elastic search.

    a. Open the csp.csp-ems-regional deployment file.

```
kubectl edit deployment -n regional csp.csp-ems-regional
```

b. Change the replicas to 2 and increase the memory from 500Mi to 2048Mi (2Gi).

c. Save the file.

d. Start the reindex process.

```
cso_backuprestore -b reindex
```

e. Using the admin token, run the following API to build the policy indices:

```
curl --location --request POST 'https://AdminPortalIP/policy-mgmt/_index' \ --header 'x-auth-token: XXXXXXX‘\ --data-raw ‘'
```

14. Create the RabbitMQ FMPM queue.

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

15. Load the data.

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

16. Synchronize the Virtual Route Reflector (VRR). Use the admin token. Do not use the cspadmin token.

a. Obtain the topo-uuid for the VRR.

```
GET: https://<IP Address>/topology-service/device
```

b. Synchronize the VRR using the POST https://<ip>/routing-manager/synchronize-vrr API.

```
{
  "input": {
    "recover_vrr": true,
    "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
  }
}
```

17. Restore the SD-WAN and security reports.

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

where `backuppath` is the new backup path.

18. Restart all fmpm-provider-api and fmpm-provider-core pods by deleting the existing pods.

```
root@startupserver1:~# kubectl get pods -n central|grep fmpm-provider
csp.csp-fmpm-provider-6644bc8b94-7pvfn                    1/1     Running   0          9d
csp.csp-fmpm-provider-6644bc8b94-c2psl                    1/1     Running   0          9d
csp.csp-fmpm-provider-6644bc8b94-gzkht                    1/1     Running   1          9d
csp.csp-fmpm-provider-6644bc8b94-hz8f5                    1/1     Running   0          9d
csp.csp-fmpm-provider-6644bc8b94-nsqfs                    1/1     Running   0          9d
csp.csp-fmpm-provider-6644bc8b94-rq9xq                    1/1     Running   0          9d
csp.csp-fmpm-provider-core-797f7c48c9-7nm8q               1/1     Running   0          9d
csp.csp-fmpm-provider-core-797f7c48c9-7zj67               1/1     Running   0          9d
csp.csp-fmpm-provider-core-797f7c48c9-8njsq               1/1     Running   0          9d
csp.csp-fmpm-provider-core-797f7c48c9-rh2jr               1/1     Running   0          9d
csp.csp-fmpm-provider-core-797f7c48c9-sswbg               1/1     Running   0          9d
csp.csp-fmpm-provider-core-797f7c48c9-zvhps               1/1     Running   0          9d
```

19. Delete all the pods displayed in the previous step.

```
kubectl delete pods csp.csp-fmpm-provider-6644bc8b94-7pvfn csp.csp-fmpm-provider-6644bc8b94-
c2psl csp.csp-fmpm-provider-6644bc8b94-gzkht csp.csp-fmpm-provider-6644bc8b94-hz8f5csp.csp-
fmpm-provider-6644bc8b94-nsqfs csp.csp-fmpm-provider-6644bc8b94-rq9xq csp.csp-fmpm-provider-
core-797f7c48c9-7nm8q csp.csp-fmpm-provider-core-797f7c48c9-7zj67 csp.csp-fmpm-provider-
core-797f7c48c9-8njsq csp.csp-fmpm-provider-core-797f7c48c9-rh2jr csp.csp-fmpm-provider-
core-797f7c48c9-sswbg csp.csp-fmpm-provider-core-797f7c48c9-zvhps
```

20. Restore the Contrail Analytics Node (CAN) database.

NOTE: You can restore the database only if a backup is available. CAN backup is disabled by default. To include CAN data in the backup, comment out `contrail_analytics` in the following configuration:

```
root@startupserver1:~# cat /etc/salt/master.d/backup.conf
backups:
```

```
keep: 10
timeout: 1200
path: /backups
enabled_roles:
    - cassandra
    - mariadb
    - kubemaster
    - elasticsearch
# - redis
    - icinga
    - helm_manager
# - contrail_analytics
```

To restore the CAN configuration database, run the following script:

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

To restore the CAN analytics database, perform the following steps:

The **analyticsdb** backup files are located at **/backups/daily/2021-06-07T06:46:37/central/can/contrail_analytics<x>**, where x indicates the contrail analytics node number. The value of x ranges from 1 through 3.

On all the three contrail analytics nodes:

- Copy the CAN backup files from the startupserver to each CAN VM:

  ```
  rsync -a<can-backup-files>root@<can-ip>:<created-backup-folder>
  ```

- Run the following command on the CAN VMs:

  ```
  docker cp 0000/ analytics_database_cassandra_1:/root
  ```

  ```
  docker exec -it analytics_database_cassandra_1 bash
  mv /root/mc-* /var/lib/cassandra/data/ContrailAnalyticsCql/statstablev4-
  d5b63590a7f011eba080c3eb6817d254
  ```

#The path might be different based on uuid.

```
cd /var/lib/cassandra/data/ContrailAnalyticsCql/statstablev4-
d5b63590a7f011eba080c3eb6817d254
chown -R cassandra:cassandra *
nodetool -p 7200 refresh -- ContrailAnalyticsCql statstablev4
```

After a successful upgrade, CSO Release 6.2.0 is functional and you can log in to the Administrator Portal and the Customer Portal.

CHAPTER 6

Renewing Certificates

IN THIS CHAPTER

How to Renew Certificates for CSO Components

IN THIS SECTION

You can renew or view the certificates of CSO components by using the **manage_certificate.sh** script.

NOTE: Actual output might vary from the sample output shown based on your deployment scenario.

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

   For example:

```
root@startupserver1:~/# cd Contrail_Service_Orchestration_6.2.0
root@host:~/Contrail_Service_Orchestration_6.2.0#
```

3. Run the **manage_certificate.sh** script to check the status or renew the certificates of the CSO components.

```
root@startupserver1:~/Contrail_Service_Orchestration_6.2.0# ./manage_certificate.sh

************************************************************
 This tool assists you to renew CSO components certificate
************************************************************

Certificate renew sequence need to be followed:

     Kubernetes -> Haproxy -> Elasticsearch

     0: List all certificate expiry date
     1: Schedule cron for email notification

Following component's certificate can be renewed

     2: Haproxy, Nginx, Rsyslog
     3: Telemetry Agent

Select a option (In Number) :
```

NOTE: To check the options that you can use with the **manage_certificate.sh** script, enter `manage_certificate.sh -h` or `manage_certificate.sh --help`.

```
root@startupserver1:~/Contrail_Service_Orchestration_6.2.0# ./manage_certificate.sh -h
Usage:
  ./manage_certificate.sh -> to check/renew CSO components's certificate
  ./manage_certificate.sh [options]

  options:

    -c | --check     to only check and list expiry dates of CSO components
    -n | --notify    to list and send email notification with CSO components and its
expiry dates
    --cron           to schedule cron job
    -h | --help      this help
```

4. You can choose to perform any of the following tasks:

- To view the certificate expiry dates, see "How to View the Certificate Expiry Dates" on page 36.
- To schedule a cron job, see "How to Schedule a Cron Job" on page 36.
- To renew a component's certificate, see "How to Renew a Certificate" on page 38.

How to View the Certificate Expiry Dates

To list all the certificates and their expiry dates, type **0** at the prompt and press Enter. You can also view the same output by using **./manage_certificate.sh -c** or **./manage_certificate.sh --check**.

```
Select a option (In Number) : 0
INFO     Fetching certificate details...
+----------------+---------------------+----------------+-------------+
| Component Name |     Expiry Date     | Days to Expire |    Status   |
+----------------+---------------------+----------------+-------------+
|    Haproxy     | 2022-08-24 09:58:20 |      240       | Not Expired |
|     Nginx      | 2022-08-24 09:58:20 |      240       | Not Expired |
|    Rsyslog     | 2022-08-24 09:58:20 |      240       | Not Expired |
+----------------+---------------------+----------------+-------------+
```

How to Schedule a Cron Job

To schedule a cron job:

1. To schedule a cron job for e-mail notifications about certificate expiry, type **1** at the prompt and press Enter. We recommend that you configure the SMTP server information in the **/usr/local/etc/smtp_server_details.json** file before proceeding to schedule the cron job.

   You can also schedule a cron job by using **./manage_certificate.sh -n** or **./manage_certificate.sh --notify**.

   ```
   Select a option (In Number) : 1

   Is /usr/local/etc/smtp_server_details.json file configured with proper SMTP server details?
   (y/n):
   ```

   - If you did not configure an SMTP server, type **n** and press Enter.

     ```
     Is /usr/local/etc/smtp_server_details.json file configured with proper SMTP server
     details? (y/n): n

     Kindly configure /usr/local/etc/smtp_server_details.json file with proper SMTP server
     ```

```
details.
Then retry scheduling cron job
```

Configure the SMTP server and run the manage_certificate.sh again to schedule the cron job.

- If an SMTP server is configured, type **y** and press Enter.

```
Is /usr/local/etc/smtp_server_details.json file configured with proper SMTP server
details? (y/n): y

Please select the cron tab operation

     1: list
     2: create
     3: delete

Select a option (In Number) :
```

Select any of the options available. You can choose to list all the cron jobs, create a new cron job, or delete a cron job.

2. To create a cron job, type 2 at the prompt and press Enter.

   Define a schedule for the cron job using the format * * * * *, which is a set of five values (that is *Minute, Hour, Day of the Month, Month, and Day of the Week*) in a line separated by spaces. Here are a few sample schedules:

   - Every hour: 0 * * * *
   - Every Monday at 10 PM: 0 22 * * 1

   The e-mail notification contains information such as component name, certificate expiry date, number of days left for certificate expiry, and status of the certificate.

```
Select a option (In Number) : 2
Please provide a cron schedule time in below format (space separated)

* * * * *
1 2 3 4 5

1. Minute (0 - 59)
2. Hour (0 - 23)
3. Day of month (1 - 31)
4. Month (1 - 12)
```

```
5. Day of week (0 - 7) (Sunday=0 or 7)
Schedule time: 0 * * * *
INFO     Scheduling cron job: 0 * * * * cd ~/Contrail_Service_Orchestration_6.2.0 && ./
manage_certificate.sh -n > /var/log/certificate.log
INFO     Successfully scheduled cron job
INFO     Current cron tab list:

0 * * * * cd ~/Contrail_Service_Orchestration_6.2.0 && ./manage_certificate.sh -n > /var/log/
certificate.log
```

3. To delete a cron job, type 3 at the prompt and press Enter.

```
Please select the cron tab operation

     1: list
     2: create
     3: delete

Select a option (In Number) : 3
INFO     Current cron tab list:

0 * * * * cd ~/Contrail_Service_Orchestration_6.2.0 && ./manage_certificate.sh -n > /var/log/
certificate.log

Please copy-paste the cron tab line here which you wants to delete:
```

At the prompt, copy and paste the cron schedule that you want to delete and press Enter.

```
Please copy-paste the cron tab line here which you wants to delete: 0 * * * * cd ~/
Contrail_Service_Orchestration_6.2.0 && ./manage_certificate.sh -n > /var/log/certificate.log
'0 * * * * cd ~/Contrail_Service_Orchestration_6.2.0 && ./manage_certificate.sh -n > /var/log/
certificate.log' will be deleted. Do you wish to continue ? (y/n): y
INFO     Successfully deleted cron job
INFO     Current cron tab list:
```

How to Renew a Certificate

You can renew a certificate only if its status is Expired or About to Expire.

NOTE: You can renew only self-signed certificates. Third-party certificates cannot be renewed.

At the prompt that appears when you run the **manage_certificate.sh** script, type the number representing the component for which you want to renew the certificate and press Enter.

```
Following component's certificate can be renewed

     2: Haproxy, Nginx, Rsyslog
     3: Telemetry Agent
Select a option (In Number) :
```

The system checks the status of the certificate:

- If the status is Expired or About to Expire, then the certificate renewal process is initiated. After the certificate renewal, the system performs a health check.

  NOTE: When HA proxy certificate is renewed, the telemetry agent certificate for all devices provisioned on CSO is automatically renewed.

  If HA proxy certificate is renewed and if the telemetry agent renewal cannot be completed due to a failure, then you can renew the telemetry agent certificate separately. Run the **manage_certificate.sh** script and provide the number corresponding to the Telemetry Agent (3 in the sample output) to renew the certificate.

- If the status is Not Expired, then the certificate is not renewed.

  Sample output if the status of a certificate is Not Expired:

```
************************************************************
 This tool assists you to renew CSO components certificate
************************************************************

Certificate renew sequence need to be followed:

     Kubernetes -> Haproxy -> Elasticsearch

     0: List all certificate expiry date
     1: Schedule cron for email notification
```

```
Following component's certificate can be renewed

     2: Haproxy, Nginx, Rsyslog
     3: Telemetry Agent

Select a option (In Number) : 2
INFO     Started check and renew haproxy component's certificate at 2021-12-27
02:19:10.974535 ...
INFO     Checking haproxy certificate expiry date
INFO     Checking nginx certificate expiry date
INFO     Checking rsyslog certificate expiry date
INFO     Haproxy certificate is Not Expired
INFO     Nginx certificate is Not Expired
INFO     Rsyslog certificate is Not Expired
INFO     Certificate is not about to expire, So renewal is not required
INFO     Completed check and renew haproxy component's certificate at 2021-12-27
02:19:13.638765 .
INFO     Time taken to renew haproxy component's certificate : 0:00:02.664230
```