

Contrail® Networking

Contrail Networking Getting Started Guide

Published
2025-08-18

RELEASE
2011

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

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

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Contrail® Networking Contrail Networking Getting Started Guide
2011

Copyright © 2025 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About This Guide | iv

1

Contrail Networking Getting Started Guide

Contrail Networking Getting Started Guide | 2

About This Guide

Use this guide to get started with Contrail Networking solution. This guide explains the general workflow to setup your data center fabric using Contrail Enterprise Multicloud (CEM).

Contrail Networking product documentation is organized into multiple guides, according to the task you want to perform or the deployment scenario.

Table 1: Contrail Networking Guides

Guide Name	Description
Contrail Networking for Container Networking Environments User Guide	Provides information about installing and using Contrail Networking in containerized environments using Kubernetes orchestration.
Contrail Networking Cloud-Native User Guide	Provides information about installing and using Contrail Networking in cloud-native environments using Kubernetes orchestration.
Contrail Networking Fabric Lifecycle Management Guide	Provides information about Contrail underlay management and data center automation.
Contrail Networking and Security User Guide	Provides information about creating and orchestrating highly secure virtual networks.
Contrail Networking Service Provider Focused Features Guide	Provides information about the features that are used by service providers.
Contrail Networking Monitoring and Troubleshooting Guide	Provides information about Contrail Insights and Contrail analytics.

RELATED DOCUMENTATION

[README Access to Contrail Networking Registry 20XX](#)

[Contrail Networking Release Notes 20XX](#)

[Tungsten Fabric Architecture Guide](#)

1

CHAPTER

Conrail Networking Getting Started Guide

IN THIS CHAPTER

- [Conrail Networking Getting Started Guide | 2](#)
-

Contrail Networking Getting Started Guide

IN THIS SECTION

- [Before You Begin | 2](#)
- [BUILD and DESIGN: Onboard a Fabric and Assign Roles | 3](#)
- [OPERATE: Add Virtual Networks | 6](#)
- [OPERATE: Add Logical Routers | 7](#)
- [OPERATE: Add Endpoints/BMSs | 7](#)
- [OPERATE: \(Optional\) Add Physical Network Function | 10](#)
- [What's Next | 14](#)

Use this guide to get started with Contrail Enterprise Multicloud. Let's go!

Before You Begin

The general workflow to setup your data center fabric using Contrail Enterprise Multicloud (CEM) is as follows:

Figure 1: General Workflow to Setup Datacenter Fabric



This workflow assumes:

- All CEM components are installed and running
- Leaf-spine physical cabling and connections are in place
- Management network connectivity to all fabric devices and CEM components

BUILD and DESIGN: Onboard a Fabric and Assign Roles

You have two options for onboarding the IP fabric devices:

Onboard a New Fabric (Greenfield)

Use the Contrail Command UI to discover devices to create a new IP fabric underlay, and assign device roles.

Before you Begin

This workflow assumes:

- Fabric devices are in a zeroized, factory-default state
- You know the following information for the devices:
 - Desired device host names
 - Desired management subnet from which to assign management interface IP addressing
 - Management subnet gateway address
 - Desired loopback subnet from which to assign loopback interface IP addressing
 - Desired 'master' subnet from which to assign fabric device in-band interface IP addressing
 - Desired ASN range from which to assign device underlay ASNs
 - Desired overlay ASN (default is 64512)
- You have a YAML file that defines device serial numbers and other details (see sample [here](#))
 - Minimum configuration is device serial numbers
 - Adding host names is recommended, otherwise serial numbers are used as host names
- You know which role(s) to assign to the devices (for more information on roles, see [here](#))

Procedure - Onboard new fabric

1. Navigate to **INFRASTRUCTURE > Fabrics** and click **Create**.
2. Select **New Fabric** and click **Provision**.
3. Configure the following fields:
 - Name (give the fabric a name)

- Device credentials (specify the desired root user password)
- Overlay ASN (suggest using default but can change if desired)
- Device Info (upload the YAML file)
- Underlay ASNs (specify range)
- Management subnet and gateway address
- Fabric subnet (specify a single 'master' subnet block for all in-band connections; the system will use it to create /30 subnets between fabric devices)
- Loopback subnet

4. Click **Next**. The device discovery process begins. The process may take a few minutes.
5. When you see the message 'Job summary: Job execution completed successfully' in the log section and the Next button turns from grey to blue, click **Next**.

Procedure - Assign roles

1. On the **Assign the roles** page, select the checkboxes for all spine devices and click the **Assign Role** icon at upper right.
2. In the pop-up window that appears, select Physical Role of **spine** and select Routing Bridging Roles as appropriate for your environment. Then click **Assign**.
3. Back on the **Assign the roles** page, uncheck the boxes for the spine devices.
4. Now select the checkboxes for all leaf devices and again click the **Assign Role** icon.
5. In the pop-up window that appears, select Physical Role of **leaf** and select Routing Bridging Roles as appropriate for your environment. Then click **Assign**.
6. Back on the **Assign the roles** page, uncheck the boxes for the leaf devices, and click the **Autoconfigure** button to push the overlay configuration onto the fabric devices based on their assigned roles.
7. When the device roles are configured, and the progress panel says 'Job summary: Job execution completed successfully', click **Next**.
8. On the **Assign Telemetry Profiles** page, click **Finish**.
9. Back on the **Fabric Devices** page, review the summary details for the fabric.

At this point the EVPN-VXLAN overlay should be successfully deployed.

Onboard an Existing Fabric (Brownfield)

Use the Contrail Command UI to onboard an existing IP fabric underlay, and assign device roles.

Before you Begin

This workflow assumes:

- Fabric devices are preconfigured with an underlay configuration that includes:
 - A common user account
 - Host name
 - Management, loopback, and fabric interfaces with IP addressing
 - EBGp-based IP fabric
 - Load balancing
 - Routing policy that advertises lo0 addresses throughout the fabric
- You know the desired overlay ASN (default is 64512)
- You know which role(s) to assign to the devices (for more information on roles, see [here](#))

Procedure - Onboard existing fabric

1. Navigate to **INFRASTRUCTURE > Fabrics** and click **Create**.
2. Select **Existing Fabric** and click **Provision**.
3. Configure the following fields:
 - Name (give the fabric a name)
 - Overlay ASN (suggest using default but can change if desired)
 - Device credentials (enter existing username and password to access the devices)
 - Management subnet
 - Loopback subnet
4. Click **Next**. The device discovery process begins. The process may take a few minutes.
5. When you see the message 'Job summary: Job execution completed successfully' in the log section and the Next button turns from grey to blue, click **Next**.

Procedure - Assign roles

1. On the **Assign the roles** page, select the checkboxes for all spine devices and click the **Assign Role** icon at upper right.
2. In the pop-up window that appears, select Physical Role of **spine** and select Routing Bridging Roles as appropriate for your environment. Then click **Assign**.
3. Back on the **Assign the roles** page, uncheck the boxes for the spine devices.
4. Now select the checkboxes for all leaf devices and again click the **Assign Role** icon.
5. In the pop-up window that appears, select Physical Role of **leaf** and select Routing Bridging Roles as appropriate for your environment. Then click **Assign**.
6. Back on the **Assign the roles** page, uncheck the boxes for the leaf devices, and click the **Autoconfigure** button to push the overlay configuration onto the fabric devices based on their assigned roles.
7. When the device roles are configured, and the progress panel says 'Job summary: Job execution completed successfully', click **Next**.
8. On the **Assign Telemetry Profiles** page, click **Finish**.
9. Back on the **Fabric Devices** page, review the summary details for the fabric.

At this point the EVPN-VXLAN overlay should be successfully deployed.

OPERATE: Add Virtual Networks

Configure virtual networks (VNs). A VN is a subnet; end hosts on the same VN can communicate.

Before you Begin

This workflow assumes that you know:

- Name for each VN
- Subnet information for each VN

Procedure

1. Navigate to **OVERLAY > Virtual Networks** and click **Create**.
2. On the **Create Virtual Network** page:
 - Enter a **Name**.
 - Add a **Subnet**; select the available **Network IPAM** option, and define the subnet in the **CIDR** field.

- Click **Create**.
3. (Optional) Repeat these steps to create more VNs as needed.

OPERATE: Add Logical Routers

Configure a logical router (LR) to interconnect VNs.

Before you Begin

This workflow assumes that you know:

- Name for each LR
- Which VNs to assign to each LR

Procedure

1. Navigate to **OVERLAY > Logical Routers** and click **Create**.
2. On the **Create Logical Router** page:
 - Enter a **Name**.
 - Click the **Extend to Physical Router** drop-down menu and select the fabric devices that perform inter-VN routing.
 - Click the **Logical Router Type** drop-down menu and select **VXLAN Routing**.
 - Click the **Connected Networks** drop-down menu and select the VNs you want to be able to communicate.
 - Click **Create**.
3. (Optional) Repeat these steps to create more LRs as needed.

OPERATE: Add Endpoints/BMSs

You have two options for adding endpoints:

Add Endpoints using Virtual Port Groups

Configure virtual port groups (VPGs). A VPG defines leaf device interfaces attached to end hosts. Use this option when

- you don't need to view the BMSs as entities in CEM
- the BMSs use static IP addressing
- the BMSs use dynamic IP addressing provided by an external DHCP server

Before you Begin

This workflow assumes that you know:

- Name for each VPG (suggest using a name related to the attached BMS)
- Associated leaf device/port information
- Server VLAN ID information (if the endpoints use VLAN tagging)

Procedure

1. Navigate to **OVERLAY > Virtual Port Group** and click **Create**.
2. On the **Create Virtual Port Group** page:
 - Enter a **Name**.
 - Select the **Fabric name** that contains the leaf device attached to the BMS
 - Find the desired device and port in the **Available Physical Interface** list and move it to the **Assigned Interface List**.
 - In the **VLAN** section, select the (virtual) **Network** this BMS should belong to, enter a **VLAN ID** (to be used by the leaf device), and if the BMS itself is not configured with a VLAN tag click the **Native/untagged** checkbox.
 - Click **Create**.
3. (Optional) Repeat these steps to create more VPGs as needed.

Verify connectivity

Your network should now be up and running. To verify connectivity, perform ping testing as follows:

- Intra-VN: Ping from an endpoint to its VN gateway (.1 on the subnet), then to another endpoint in the VN
- Inter-VN: Ping from an endpoint to an endpoint in another VN within the same LR

Add Endpoints using Servers/Instances

Define a BMS in CEM and then create a BMS instance that defines which leaf device interface it is attached to. Use this option when

- you want to view the BMSs as entities in CEM
- the BMSs use static IP addressing
- the BMSs use dynamic IP addressing with CEM as the DHCP server

Before you Begin

This workflow assumes that you know:

- BMS host name
- BMS in-band interface name, IP address, and MAC address
- BMS VLAN ID information (if the endpoints use VLAN tagging)
- Associated leaf device/port information
- Which VN each BMS belongs to

Procedure

This configuration option includes two elements:

- Create BMS profile
- Create BMS instance

Create BMS profile

1. Navigate to **INFRASTRUCTURE > Servers**, and click **Create**.
2. On the **Create Server** page, select mode **Detailed**, then select workload **Baremetal**.
3. Configure the following fields:
 - Hostname (of the BMS)
 - Network interfaces (enter name and MAC address of the server interface attached to the leaf device; select leaf device and attached interface)
 - Click **Create**.
4. (Optional) Repeat these steps to create more BMS profiles as needed.

Create BMS instance

1. Navigate to **WORKLOADS > Instances**, and click **Create**.
2. On the **Create Instance** page, select server type **Existing Baremetal Server** and configure the following fields:
 - Instance name
 - Baremetal node (select the BMS you defined above)
 - Associate interfaces (select server interface defined above; enter IP address; select VN BMS attaches to; specify VLAN ID or enter 0 if untagged)
 - Click **Create**.
3. (Optional) Repeat these steps to create more BMS instances as needed.

Verify connectivity

Your network should now be up and running. To verify connectivity, perform ping testing as follows:

- Intra-VN: Ping from an endpoint to its VN gateway (.1 on the subnet), then to another endpoint in the VN
- Inter-VN: Ping from an endpoint to an endpoint in another VN within the same LR

OPERATE: (Optional) Add Physical Network Function

Add an SRX device to provide physical network function (PNF) capabilities. The PNF provides interconnectivity between LRs, as well as the ability to implement security policy.

Before You Begin

This workflow assumes:

- The SRX device has a basic configuration, including:
 - User account(s)
 - Host name
 - Management and loopback interfaces and IP addressing
- The SRX device has two physical connections to one or more fabric devices



NOTE: Do not preconfigure any elements related to PNF functionality, such as interfaces connecting to the fabric devices, zones and policies related to inter-LR traffic, and so on.

- You know the following details:
 - Which two interfaces on the PNF device connect to the fabric device(s), and vice-versa
 - The two unique VLAN IDs to assign to the PNF-to-fabric-device connections
 - The /24 subnet to use to connect the PNF device to the fabric
 - The ASN to assign to the PNF device
 - Which LR to interconnect

Procedure

PNF configuration includes four elements:

Onboard the SRX/PNF device

1. Navigate to **INFRASTRUCTURE > Fabrics** and select the fabric you created above.
2. On the **Fabric devices** page, click the **Action** button and select **Brownfield wizard**.
3. On the **Create Fabric** page, configure the following fields:
 - Device credentials (existing username and password to access the devices)
 - Management subnet (use a /32 to specifically identify the SRX device)
 - Loopback subnet
 - Additional configuration - PNF Servicechain subnets (specify a /24 network; CEM will use it to create two /29 subnets during configuration)
4. Click **Next**. The device discovery process begins. The process may take a few minutes.
5. When you see the message 'Job execution completed successfully' in the log section and the Next button turns from grey to blue, click **Next**.

Assign overlay roles

1. On the **Assign the roles** page, select the checkbox for the SRX device and click the **Assign Role** icon at upper right.
2. In the pop-up window that appears, select the Physical Role of **pnf** and select the Routing Bridging Role **PNF-servicechain**. Then click **Assign**.
3. Back on the **Assign the roles** page, uncheck the box for the SRX device.
4. Now select the checkboxes for the device(s) that attach to the PNF. Note the currently assigned roles, and again click the **Assign Role** icon.
5. In the pop-up window that appears:
 - Select the Physical Role of **leaf** or **spine**, as appropriate
 - Re-select the devices' existing Routing Bridging Roles
 - Additionally, select **PNF-Servicechain** and **CRB-MCAST-Gateway**
 - Click **Assign**
6. Back on the **Assign the Roles** page, uncheck the boxes for the devices, and click the **Autoconfigure** button to push new configuration onto the devices based on their assigned roles.
7. When the device roles are configured, and the progress panel says 'Job summary: Job execution completed successfully', click **Next**.
8. On the **Assign Telemetry Profiles** page, click **Finish**.
9. Back on the **Fabric Devices** page, review the summary details to verify PNF elements are in place.

Configure a PNF Service Template

The PNF service template defines the physical connectivity of the PNF to the fabric.

1. Navigate to **SERVICES > Catalog**, click the **PNF** tab, and click **Create > Template**.
2. On the **Create PNF Service Template** page, configure the following fields:
 - Name
 - PNF device (select the SRX device)
 - PNF Left Interface (select one of the interfaces connecting to the fabric)
 - PNF Left Fabric (select the fabric to attach to)

- PNF Left Attachment Points > Physical Router (select the related fabric device connecting to the PNF 'left' interface above)
- PNF Left Attachment Points > Left Interface (select the related interface connecting to the PNF 'left' interface above)
- PNF Right Interface (select the second interface connecting to the fabric)
- PNF Right Fabric (as above, select the fabric to attach to)
- PNF Right Attachment Points > Physical Router (select the related fabric device connecting to the PNF 'right' interface above)
- PNF Right Attachment Points > Right Interface (select the related interface connecting to the PNF 'right' interface above)

3. Click **Create**.

Configure a PNF Service Instance

The PNF service instance uses the template to interconnect the LRs.

1. Navigate to **SERVICES > Deployments**, click the **PNF** tab, and click **Create > Instance**.
2. On the **Create PNF Service Instance** page, configure the following fields:
 - Name
 - Service Template (select the template created above)
 - PNF eBGP ASN (specify a unique ASN for peering between the fabric and PNF)
 - Left Tenant Logical Router (select an LR)
 - Left Service VLAN (assign a unique VLAN ID for the 'left' interconnection between the PNF and related fabric device)
 - Right Tenant Logical Router (select another LR to connect to the LR above)
 - Right Service VLAN (assign another unique VLAN ID for the 'right' interconnection between the PNF and related fabric device)
3. Click **Create**. CEM pushes the configuration elements to the devices; the process may take a few minutes.

Verify Connectivity

The SRX device should now be tied into the fabric to provide PNF services. To verify functionality:

- Connectivity: Ping from an endpoint in one LR to and endpoint in the other LR
- PNF: Add security policy configuration to the SRX device to allow or block traffic as desired

What's Next

- [Hitless Software Upgrades](#)
- [Return Material Authorization](#)