JUNIPER NETWORKS | Engineering Simplicity

Day One+

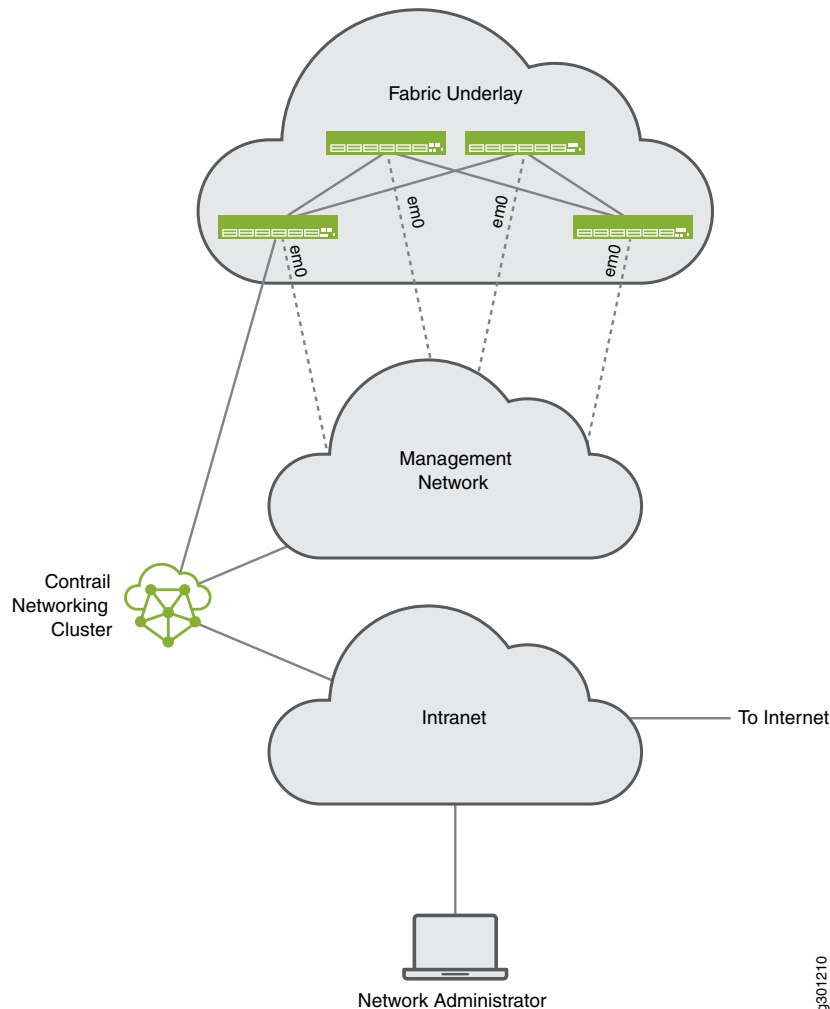# Contrail Networking

Step 1: Begin

You can use Contrail Networking, a full-featured software-defined networking (SDN) solution, to manage and configure your underlay and overlay networks all from a single user interface, Contrail Command. Contrail Command provides a central dashboard that makes it easy to configure networks, administer network policies, and create service chains for services such as load balancing, firewall, and NAT.

First, we'll show you how to install Contrail Command and set up a Contrail Networking cluster for Release 2005.1. Then, we'll show you how to set up the underlay network on a greenfield fabric, and create the overlay networks that interconnect the compute endpoints. The compute endpoints are the bare-metal servers or virtual machine (VM) workloads that the compute administrator configures and attaches to the leaf or top-of-rack switches.

Install and Deploy Workflow

To install Contrail Command, first you download and run the Contrail Command deployer. This deploys Contrail Command as a set of Docker containers. Then, you use Contrail Command to set up your Contrail Networking cluster. A Contrail Networking cluster is the set of controllers and supporting applications that manage the underlay and overlay networks.

Here's the example Contrail Networking cluster you'll be setting up:

> **NOTE:** The installation instructions that we provide assume that you're sitting at the network administrator's station. We refer to this station as *your local machine*.
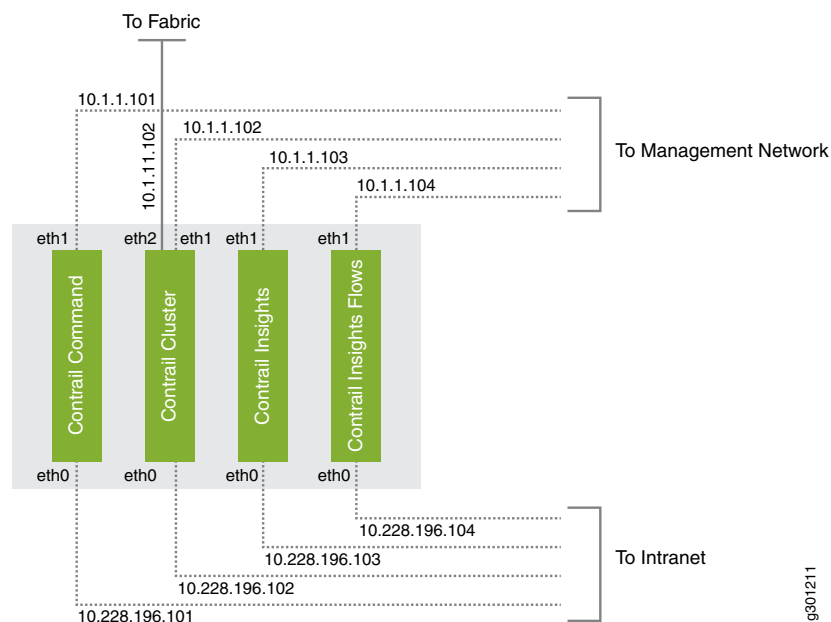
To minimize the number of servers used in this example, you'll set up a cluster of collocated servers, which is different from a typical deployment. In a typical deployment, the cluster components are implemented as discrete nodes that can be distributed over multiple leaf switches to provide higher performance and availability.

Here's a description of the networks shown:

Network	Description
Fabric underlay	The regular IP spine-and-leaf network made up of switches and routers.
Management	The out-of-band management network that the Contrail Networking controller uses to discover and configure the switches in the fabric underlay network.
Intranet	A general network that provides access for the network administrator to the Contrail Networking cluster, and for the cluster to the Internet. This can be the corporate intranet, or a lab network connected to the corporate intranet, or any other scheme that provides external management connectivity to the cluster.

The Contrail Networking cluster consists of a number of servers or VMs providing the Contrail Networking and Contrail Insights functionality. You can create a cluster with any number of servers or VMs, depending on your needs.

Here's an example of a cluster made up of four servers followed by a description of the components running on the servers.

Servers	Description	Connectivity
Contrail Command	Contains the Contrail Command application, which provides the UI that translates user intents to internal API calls to the other components.	Connects to the external network on eth0, reachable from the network administrator's browser.
		Connects to the fabric management network on eth1 to configure the other Contrail Networking components.

Servers	Description	Connectivity
Contrail Cluster	Contains the collection of containers that provide the main Contrail Networking functionality, including the control, orchestration, service, and compute node roles. In this example, we're placing most of the functionality into one server to reduce the number of servers you require.	Connects to the external network on eth0. Connects to the fabric management network on eth1 to configure the switches in the fabric. Connects to the fabric underlay on eth2. This is the main interface to the fabric to exchange routes and to provide and receive services.
Contrail Insights	Contains the Contrail Insights application, formerly called *AppFormix*, which is an optional software application that allows you to monitor and troubleshoot VMs, containers, and physical switches and routers.	Connects to the external network on eth0. Connects to the fabric management network on eth1 to communicate with the other Contrail Networking components.
Contrail Insights Flows	Contains the Contrail Insights Flows application, an optional software application that enables you to view sFlow-derived telemetry for devices in the fabric.	Connects to the external network on eth0. Connects to the fabric management network on eth1 for out-of-band flow monitoring. **NOTE:** If you want to support in-band flow monitoring, then connect the server directly to the fabric underlay.

NOTE: All servers in this example have at least four cores, 64-GB memory, 300-GB hard drive with at least 100 GB in the "/" partition, and Internet access for downloading software packages.

This component breakdown represents just one possible example. You can create a cluster that has a different number of servers and a different distribution of components and roles.

We refer to this network configuration and this component breakdown in various examples later. All IP addresses shown are /24.

Before You Begin

In preparation for installation, look through the Contrail Networking Supported Platforms List for the compatible OS and prerequisite software versions for the Contrail Networking release you want to set up, and the README Access to Contrail Registry 20XX file for the container tag to use.

Here are the software versions and container tag that we use in this example:

Software	Version
Contrail Networking	2005.1
Container tag	2005.1.66
OpenStack	Queens
OS	CentOS 7.8 with Linux kernel version 3.10.0-1127
Docker	Docker Community Edition 18.03.1

Additionally, you'll need access to the Juniper Networks container registry (hub.juniper.net). If you don't have access to the registry, e-mail contrail-registry@juniper.net to get your username and password.

Finally:

1. Make all the physical connections:

    a. Connect the leaf and spine switches together in the fabric underlay.

    b. Connect the management interface of each switch to the management network.

    c. Connect the Contrail Networking servers to the management network and to the intranet.

    d. Connect the Contrail Cluster server to a leaf switch in the fabric underlay.

2. Prepare the servers:

    a. Install a fresh OS on each server. If you're installing CentOS, you can select the minimal CentOS install, which installs much faster than the full CentOS install.

    b. Assign static IP addresses to each interface, ensuring that the IP addresses are within the proper subnets. You can assign the IP addresses during OS installation (easiest), or after. If you assign IP addresses after the OS installation, you'll need to make the changes directly in **/etc/sysconfig/network-scripts/ifcfg-xxx**.

    c. Assign meaningful non-FQDN hostnames to each server (for example, contrail-command, contrail-cluster, contrail-insights, contrail-insights-flows). You can assign the hostnames during OS installation (easiest), or you can assign hostnames after. If you assign hostnames after the OS installation, you'll need to make the changes directly in **/etc/hosts** and use the **hostnamectl set-hostname** command. If you add an entry into the**/etc/hosts** file, use the IP address of the management interface (that is, the IP address for eth1 in this example).

    d. Create a root user and set a root password as part of OS installation.

For more details on how to prepare the servers, see How to Install Contrail Command and Provision Your Contrail Cluster.

3. Prepare the switches:

    a. Attach a terminal or laptop to the serial console port of the switch and log in to the CLI. You'll need console access in this phase because the next step resets the switches, resulting in loss of management port configuration. Most laptops no longer have serial ports so if you're using a laptop, you'll likely need an RJ-45 to DB-9 adapter and a USB to DB-9 adapter.

    b. Reset the switch to zero (**request system zeroize**).

    c. Repeat Step a and Step b for all switches in the fabric underlay.

Install Contrail Command

To install Contrail Command, first you'll install the prerequisite software packages on the Contrail Command server. Next, you'll create a YAML file containing the Contrail Command server information. Finally, you'll download and run the Contrail Command deployer image.

The server or VM where you run the Contrail Command deployer image can be different from the server or VM where you install Contrail Command. This example runs the Contrail Command deployer on the same server that later runs Contrail Command.

1. From your local machine, log in to the Contrail Command server or VM using SSH.

2. Install and start Docker.

    a. Install the prerequisite software used by YUM and Docker.

    ```
    yum install -y yum-utils device-mapper-persistent-data lvm2
    ```

    b. Add the Docker Community Edition repository to the list of YUM repositories for this machine.

    ```
    yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo
    ```

    c. Install the version of Docker supported by the release of Contrail you are installing. We install Docker Community Edition 18.03.1 here as an example.

    ```
    yum install -y docker-ce-18.03.1.ce
    ```

    d. Start Docker.

```
systemctl start docker
```

e. Enable Docker so that it automatically restarts when the server or VM reboots.

```
systemctl enable docker
```

3. Retrieve the Contrail Command deployer image from the Juniper Networks container registry.

a. Log in to the registry.

```
docker login hub.juniper.net
```

Enter your hub.juniper.net credentials when prompted.

b. Pull the Contrail Command deployer image for the release you are installing. For example:

```
docker pull hub.juniper.net/contrail/contrail-command-deployer:2005.1.66
```

4. Create the **command_servers.yml** configuration file on the Contrail Command server. This file provides the following information to the Contrail Command deployer:

- The IP address and login credentials of the server where you want to install Contrail Command. This is the Contrail Command server that you just set up.

- The URL and login credentials of the Juniper Networks container registry and the container tag to use.

- The passwords that you want to set for Contrail Command, including the main (keystone admin) password to log in to the UI.

Here's a basic but fully functional example:

```
---

command_servers:
    server1:
        ip: 10.228.196.101
        connection: ssh
        ssh_user: root
        ssh_pass: <password>
        sudo_pass: <password>
        ntpserver: <ntp-server>

        registry_insecure: false
        container_registry: hub.juniper.net/contrail
        container_tag: 2005.1.66
```

```
container_registry_username: <registry-username>
container_registry_password: <registry-password>
config_dir: /etc/contrail

contrail_config:
    database:
        type: postgres
        dialect: postgres
        password: <password>
    keystone:
        assignment:
            data:
                users:
                    admin:
                        password: <password>
    insecure: true
    client:
      password: <password>
```

5. Run the **contrail-command-deployer** container to deploy the Contrail Command containers. In this example, the **command_servers.yml** file is located in the **/root** directory.

```
docker run -td --net host -v /root/command_servers.yml:/command_servers.yml --privileged
--name contrail_command_deployer hub.juniper.net/contrail/contrail-command-deployer:2005.1.66
```

This command runs in the background (detached mode) and returns right away. To track the progress of the command:

```
docker logs -f contrail_command_deployer
```

6. Verify that the Contrail Command containers are running.

```
[root@contrail-command ~]# docker ps -a
CONTAINER ID   IMAGE      <trimmed>   STATUS   <trimmed>   NAMES
2e62e778aa91   hub.juniper.net/...   Up       <trimmed>   contrail_command
c8442860e462   circleci/postgre...   Up       <trimmed>   contrail_psql
57a666e93d1a   hub.juniper.net/...   Exited   <trimmed>   contrail_command_deployer
```

The **contrail_command** container is the GUI and the **contrail_psql** container is the database. Both containers should have a status of **Up**.

The **contrail_command_deployer** container should have a status of **Exited** because it exits when the installation is complete.

Create the Contrail Networking Cluster

Now that you've installed Contrail Command, let's use it to create the Contrail Networking cluster.

1. Open a browser on your local machine and navigate to Contrail Command on port 9091 (for example, **https://10.228.196.101:9091**). Use the Contrail Command server IP address that is reachable from your local machine, which in this example is the eth0 IP address.

   Leave the Select Cluster field blank and log in using the **admin** credentials you specified in the **keystone** section of the **command_servers.yml** file.

   When you log in to Contrail Command and there is no preexisting cluster, which is the case for a fresh install, you start in the Inventory step of the Setup wizard that guides you through cluster creation. The left-nav bar tracks your progress through these steps.

2. Let Contrail Command know about the login credentials you use for the Contrail Cluster, Contrail Insights, and Contrail Insights Flows servers or VMs. You will reference these credentials in Step 3 when you add those servers.

   a. Click the **Credentials** tab and click **Add** to bring up the Add dialog box. You are adding the usernames and passwords for the Contrail Cluster, Contrail Insights, and Contrail Insights Flows servers or VMs that you set up earlier. You need to add unique credentials only. For example, if you set up two servers with the same username and password, you need to add them only once.

   b. Specify a name for these credentials and the username and password. Click **Add** to add the credentials.

   c. If you use the same username and password to log in to all servers, then proceed to Step 3. Otherwise, repeat Step a and Step b until you've finished adding all unique credentials.

3. Let Contrail Command know about the Contrail Cluster, Contrail Insights, and Contrail Insights Flows servers.

   a. Click the **Server** tab and click **Add** to bring up the Create Server dialog box.

   b. Select **Detailed** mode.

   c. Fill in the remaining fields and then click **Create**. Here are the settings used for each server in this example:

Field	Contrail Cluster	Contrail Insights	Contrail Insights Flows
Workload Type	Physical/Virtual Node	Physical/Virtual Node	Physical/Virtual Node
Hostname	contrail-cluster	contrail-insights	contrail-insights-flows
Management IP	10.1.1.102	10.1.1.103	10.1.1.104
Management Interface	eth1	eth1	eth1
Credentials	<select from drop-down list>	<select from drop-down list>	<select from drop-down list>

Field	Contrail Cluster	Contrail Insights	Contrail Insights Flows
Network Interfaces (click **Add**)	Name: eth0 IP Address: 10.228.196.102	Name: eth0 IP Address: 10.228.196.103	Name: eth0 IP Address: 10.228.196.104
	Name: eth1 IP Address: 10.1.1.102	Name: eth1 IP Address: 10.1.1.103	Name: eth1 IP Address: 10.1.1.104
	Name: eth2 IP Address: 10.1.11.102	–	–

d. Repeat Step a through Step c until you've added information about all servers.

e. Click **Next** to move to the Provisioning Options step of the Setup wizard.

4. Fill in the provisioning options fields. When you are done, click **Next** to move to the Control Nodes step of the Setup wizard.

Here are the values used in this example:

Field	Value	Notes
Provisioning Manager	Contrail Enterprise Multicloud	The only supported selection.
Cluster Name	my-cluster	–
Container Registry	hub.juniper.net/contrail	Juniper Networks main Contrail registry.
Insecure	Unchecked	–
Container Registry Username	<registry-username>	–
Container Registry Password	<registry-password>	–
Contrail Version	2005.1.66	Container tag.
Domain Suffix	local	Contrail Networking adds this suffix to the server non-FQDN hostname.
NTP Server	<ntp-server>	–

Field	Value	Notes
Default Vrouter Gateway	10.1.11.2	The IP address of the interface on the leaf switch that connects to the Contrail Cluster server's fabric underlay interface. Because this switch has been reset to zero, you'll need to configure the switch interface with this IP address later.
Encapsulation Priority	VXLAN,MPLSoUDP,MPLSoGRE	The only supported encapsulation.
Fabric Management	Checked	–
Contrail Configuration (click Add)	Key: CONTROL_NODES Value: 10.1.11.102	Specifies the fabric underlay interface IP address of the Contrail Control node. In this example, you'll be installing the control node on the Contrail Cluster server. This IP address is therefore the IP address that connects the Contrail Cluster server to the fabric underlay.
	Key: PHYSICAL_INTERFACE Value: eth2	Name of the interface that connects to the fabric underlay.
	Key: TSN_NODES Value: 10.1.11.102	Specifies the fabric underlay interface IP address of the Contrail Service node. In this example, you will be installing the service node on the Contrail Cluster server. This IP address is therefore the IP address that connects the Contrail Cluster server to the fabric underlay.

5. Assign a server for the Contrail Control node. In this example, the Contrail Cluster server contains the control node.

    a. Select **contrail-cluster** from the Available servers list and move it to the Assigned Control nodes list.

    b. Click **Next** to move to the Orchestrator Nodes step of the Setup wizard.

6. Assign a server for the OpenStack orchestrator node and configure the OpenStack Kolla parameters. In this example, the Contrail Cluster server contains the orchestrator node.

    You're required to assign an OpenStack orchestrator node even if you're using a different orchestrator for instantiating compute endpoints. The OpenStack orchestrator node is used by the cluster.

    a. Select **contrail-cluster** from the Available servers list and move it to the Assigned Openstack nodes list.

    b. Select **Show Advanced** to view additional provisioning parameters.

    c. Scroll down to Kolla Globals and click **Add**.

d. Add the following key/value pairs to disable ironic bare-metal server provisioning and to enable swift storage.

Key	Value
enable_haproxy	no
enable_ironic	no
enable_swift	yes
swift_disk_partition_size	20GB

> **NOTE:** We won't be changing any of the default Kolla passwords. By default, the Contrail Networking cluster username is **admin** and the password is **contrail123**.

e. Click **Next** to move to the Compute Nodes step of the Setup wizard.

7. Assign a server for the compute node. The compute node is used by the cluster. In this example, the Contrail Networking cluster contains a single compute node that resides on the Contrail Cluster server.

a. Select **contrail-cluster** from the Available servers list and move it to the Assigned Compute nodes list.

b. Specify the Default Vrouter Gateway. In this example, the gateway is 10.1.11.2 as explained in Step 4.

c. Click **Next** to move to the Contrail Service Nodes step of the Setup wizard.

8. Assign a server for the service node. In this example, the Contrail Cluster server contains the service node.

a. Select **contrail-cluster** from the Available servers list and move it to the Assigned Service nodes list.

b. Specify the Default Vrouter Gateway. In this example, the gateway is 10.1.11.2 as explained in Step 4.

c. Click **Next** to move to the AppFormix Nodes step of the Setup wizard.

9. Assign your AppFormix node servers.

> **NOTE:** Appformix was renamed Contrail Insights. The Appformix name is still used in the UI.

The AppFormix node consists of the Contrail Insights server and the Contrail Insights Flows server.

a. Select **contrail-insights** from the Available servers list and move it to the Assigned AppFormix nodes list.

b. Select **contrail-insights-flows** from the Available servers list and move it to the Assigned AppFormix nodes list.

c. Scroll down to the Roles field for the contrail-insights-flows server and use the drop-down list to change the role to **appformix_bare_host_node**.

d. Click **Next** to move to the AppFormix Flows step of the Setup wizard.

10. Assign your AppFormix Flows node servers. In this example, the AppFormix Flows node is the Contrail Insights Flows server.

a. Select **contrail-insights-flows** from the Available servers list and move it to the Assigned AppFormix Flows nodes list.

b. Select **Out of Band** as the provisioning type.

c. Specify the Virtual IP Address. This is the virtual IP address that devices use to reach the Contrail Insights Flows node from the fabric management network. This must be an unused IP address in the fabric management subnet (for example, 10.1.1.105).

d. Click **Next** to move to the Summary step of the Setup wizard.

11. Review your settings. Click **Provision** after verifying your settings.

The cluster provisioning process begins. The provisioning process time varies by environment and deployment, and can take 90 minutes or more.

12. (Optional) Monitor the provisioning process by logging in to the Contrail Command server and entering the **docker exec contrail-command tail /var/log/contrail/deploy.log** command at the Linux prompt.

13. When the provisioning process finishes, click **Proceed to Login** from Contrail Command.

You are redirected to the Contrail Command login screen.

14. Log in to the cluster:

- **Select Cluster**: Select the Contrail Networking cluster you just created from the drop-down list. The cluster is shown by the cluster name followed by a random string.
- **Username**: Enter the username for the cluster. The default username is **admin**.
- **Password**: Enter the password for the cluster. The default password is **contrail123**.

Step 2: Up and Running

Now that you've created the cluster, let's use Contrail Command to configure all your data center network equipment to be part of the same IP underlay network. This is referred to as *onboarding your fabric*. After onboarding the fabric, you'll then use Contrail Command to create the overlay networks that run on top of this fabric.

Onboard a New Fabric (Greenfield)

Before you onboard the fabric, you need to tell the Contrail Networking controller about the devices in the fabric. You do this by creating a device YAML file that contains the list of chassis serial numbers of the switches in the fabric. You create this file on your local machine and then upload it using Contrail Command in a later step. Contrail Networking uses the device YAML file to discover the devices that match the listed serial numbers.

> **NOTE:** To get the chassis serial number from your device, issue the **show chassis hardware** command from the Junos CLI on the device. Alternatively, you can get the chassis serial number from the label affixed to your device. See Locating the Serial Number on a QFX10000 Switch or Component and Locating the Serial Number on a QFX5110 Device or Component.

This file can contain other configuration parameters as well. Here's an example of a file that lists the serial numbers and configures the hostnames of the switches.

```
device_to_ztp:
  - serial_number: '111111111111'
    hostname: 'Access-Leaf-1'
  - serial_number: '222222222222'
    hostname: 'Access-Leaf-2'
  - serial_number: '333333333333'
    hostname: 'Border-Spine-1'
  - serial_number: '444444444444'
    hostname: 'Border-Spine-2'
```

To onboard a fabric, launch the Create Fabric wizard. It will ask you for the underlay and overlay configuration and the device YAML file you just created.

1. Log in to the cluster.

2. Select **INFRASTRUCTURE>Fabrics** to bring up the Fabrics page and then click **Create** to create the fabric.

   The Select provisioning option window appears.

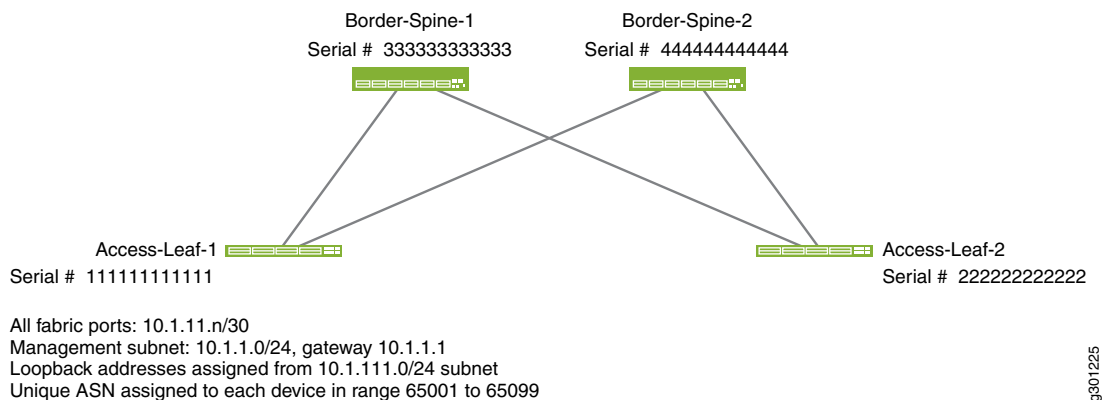3. Select **New Fabric** and click **Provision**.

   This launches the Create Fabric wizard for a new (greenfield) fabric.

4. Fill in the fields on this page according to your desired setup. Here are the mandatory fields along with example values:

Fields	Meaning	Example
Name	The name of the fabric.	my-fabric
Device credentials	The root password that you want to set for all devices in the fabric. **NOTE:** Type the password carefully. Contrail Command does not ask you to verify or confirm the password that you type in.	<password>
Overlay ASN (iBGP)	The autonomous system number for the overlay iBGP network. All devices in the overlay belong to the same autonomous system.	65000
Device Info	The device YAML file.	Select the YAML file you just created on your local computer.
Underlay ASNs (eBGP)	Specify the ASN range that you want to assign to the underlay devices. Contrail Networking assigns each device with its own AS number in the underlay.	65001 to 65099
Management subnets	Specify the management subnet and gateway for the underlay devices. Contrail Networking discovers all devices connected to the management subnet.	cidr: 10.1.1.0/24 gateway: <gateway IP>
Fabric subnets	Specify the fabric subnet for the underlay. Contrail Networking assigns IP addresses from this subnet to all fabric ports.	10.1.11.0/24
Loopback subnets	Specify the loopback subnet. The loopback IP address is used by the overlay BGP. Contrail Networking assigns IP addresses from this subnet to the loopback interfaces on all fabric devices.	10.1.111.0/24

Fields	Meaning	Example
PNF Servicechain subnets	Specify the physical network function (PNF) service chain subnets. These are the subnets for the PNF devices that you want to add to the service chain. You need a PNF service chain if you want to allow communications between devices on the different overlay networks that you later create. PNF service chains are covered in a later section.	10.1.222.0/24

Here's the resulting fabric configuration:

Border-Spine-1
Serial # 333333333333

Border-Spine-2
Serial # 444444444444

Access-Leaf-1
Serial # 111111111111

Access-Leaf-2
Serial # 222222222222

All fabric ports: 10.1.11.n/30
Management subnet: 10.1.1.0/24, gateway 10.1.1.1
Loopback addresses assigned from 10.1.111.0/24 subnet
Unique ASN assigned to each device in range 65001 to 65099

g301225

5. Click **Next** to launch the device discovery process. The process might take a few minutes.

6. When you see the message **Job summary: Job execution completed successfully** in the log section, Contrail Networking has brought up all the fabric devices and has built the fabric topology. Click **Next** to progress to role assignment.

   The Assign to devices window appears.

7. Assign roles to each switch. When you assign a role to a switch, you are telling Contrail Networking the switch's function. Contrail Networking then configures the switch for that role.

   There are two types of roles that you assign to a device. The physical (underlay) role describes whether a device is a spine device or a leaf device. The routing (overlay) role describes the overlay routing functions that a device supports. A device has one physical role and one or more routing roles.

   a. Select the row for the switch.

   b. Click the **Assign Role** icon on the far right of the row. The Assign role to devices window appears.

c. Set the roles. The roles differ depending on whether the switch is a spine switch or a leaf switch. The following tables provide examples of role settings for a basic but fully functional configuration. For more information about roles, see Device Roles.

Role	Example	Meaning
Role	leaf	Leaf switch.
Routing Roles	CRB-Access	This switch is a centrally routed and bridged access device. It tunnels user traffic to the CRB-Gateway for routing.
	AR-Client	An assisted replication client device.

Role	Example	Meaning
Role	spine	Spine switch.
Routing Roles	CRB-Gateway	This switch is a centrally routed and bridged gateway device. It provides routing between virtual networks using IRB interfaces.
	PNF-Servicechain	This switch is part of a service chain. Service chains are covered in a later section.
	Route-Reflector	This switch acts as an (overlay) route reflector.

d. Repeat Step a through Step c for each switch in the fabric.

e. Click **Autoconfigure** to push the overlay configuration onto the fabric devices based on their assigned roles.

8. When you see the message **Job summary: Job execution completed successfully** in the log section, click **Next**.

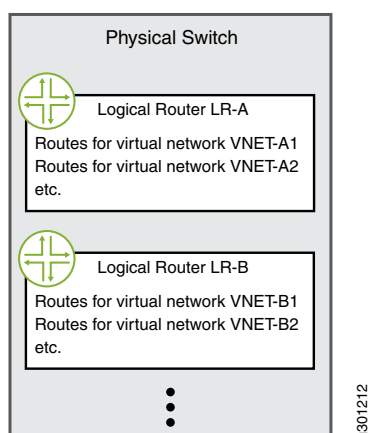9. On the Assign Telemetry Profiles page, click **Finish**.

Congratulations! You have now fully onboarded the fabric and performed the initial overlay configuration. Now you can log in to the leaf switch that connects to the Contrail Cluster server and configure the IP address of the IRB interface or connected port to match the default vrouter gateway that you specified earlier (for example, 10.1.11.2).

Create the Overlay Networks

Now that you've onboarded the fabric, you can start creating the overlay segmented networks that run on top of the fabric. Before starting, let's go over the terminology that Contrail Networking uses to create overlay networks.

Overlay networks are created by using virtual routing and forwarding (VRF) instances, which are called *logical routers*. A physical switch contains multiple logical routers. Each logical router contains routes for *virtual networks*. A virtual network, in its most basic form, is a subnet.

Here's the relationship between physical switches, logical routers, and virtual networks:

To create an overlay network, you first create the virtual networks (subnets) in that overlay and then you create the logical router (VRF instance). When you create the logical router, you assign the virtual networks you just created and specify the physical device where you want to instantiate the logical router. In a centrally routed and bridged model, you instantiate the logical router onto the spine switches. In an edge routed and bridged model, you instantiate the logical router onto the edge switches.

1. Create the virtual networks.

    a. Select **OVERLAY>Virtual Networks** and click **Create**.

    The Create Virtual Network window appears.

    b. Fill in the fields on this page according to your desired setup and click **Create**. Here are the mandatory fields along with example values. You can leave all other settings at their default values.

Field	Meaning	Example
Name	The name that you want to call this virtual network.	VNET-A1
Subnets>Network IPAM	The IP address allocation instance to use.	default-domain:default:default-project:default-network-ipam This is the default IPAM instance. **NOTE:** If you use the same IPAM instance for all virtual networks, then all IP addresses have global scope within the enterprise.
Subnets>CIDR	The virtual network subnets.	10.1.3.0/24

    c. Optionally, go to **MONITORING>Jobs** to bring up the Jobs page and click a job to see details about the configuration being pushed to the device for that job.

    d. Repeat Step a through Step c to create all the virtual networks that you want in your overlay.

2. Create the logical routers.

    a. Navigate to **OVERLAY > Logical Routers** and click **Create**.

    b. Fill in the fields on this page according to your desired setup and click **Create**. Here are the mandatory fields along with example values. You can leave all other settings at their default values.

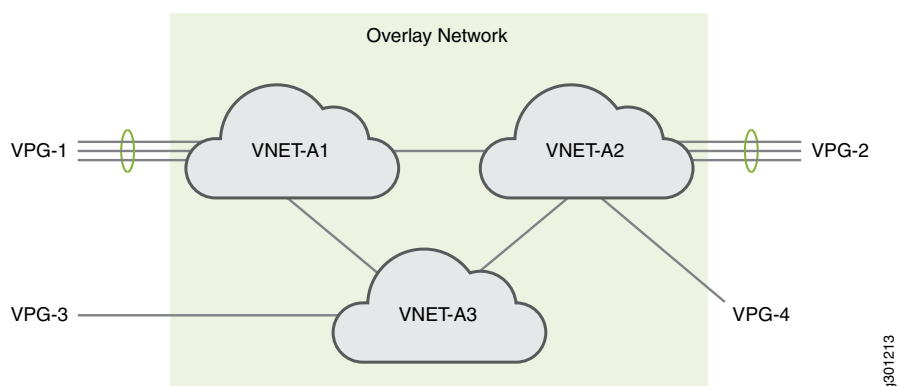| Field	Meaning	Example
Name	The name you want to call this logical router.	LR-A
Logical Router Type	The type of routing you want this logical router to perform.	VXLAN Routing
Choose Fabric	The name of the fabric underlay you onboarded earlier.	my-fabric
Connected networks	The virtual networks you want to connect to this logical router.	VNET-A1 VNET-A2
Extend to Physical Router	The actual physical routers where you want to instantiate this logical router. In a centrally routed and bridged model, these are your spine switches.	Border-Spine-1 Border-Spine-2

    c. Optionally, go to **MONITORING>Jobs** to bring up the Jobs page and click a job to see details about the configuration being pushed to the device for that job.

3. Repeat Step 1 and Step 2 to create other overlay networks.

Create the Network Endpoints of the Overlay Network

After you create the overlay network, you need to specify which network ports belong to the overlay. These are the network ports that the compute endpoints attach to. You do this at the virtual network layer by using virtual port groups.

Here's an overlay network consisting of three virtual networks along with four virtual port groups that represent the network endpoint ports. A virtual port group consists of one or more network ports. If a virtual port group contains more

than one port, it is similar in concept to a LAG. If a virtual port group contains more than one port and if the ports are on different devices, then it is similar in concept to an MC-LAG.

1. Select **OVERLAY>Virtual Port Group** to bring up the Virtual Port Group page and click **Create**.

   The Create Virtual Port Group page appears.

2. Fill in the fields on this page according to your desired setup and click **Create**. Here are the mandatory fields along with example values. You can leave all other settings at their default values.

Field	Meaning	Example
Virtual Port Group Name	The name you want to call this virtual port group.	VPG-1
Fabric name	The fabric where this virtual port group resides.	my-fabric
Physical Interface	The interface members of this virtual port group. Find the desired device and port in the Available Physical Interface list and move it to the Assigned Interface List. The Available Physical Interface panel lists all the physical interfaces in the network that are available for assignment. Search for the interfaces using the case-insensitive search box.	xe-0/0/2 on Access-Leaf-1 xe-0/0/3 on Access-Leaf-1 xe-0/0/4 on Access-Leaf-1
VLAN>Network	The virtual network that you want the virtual port group to belong to.	VNET-A1

Field	Meaning	Example
VLAN>VLAN ID	The VLAN ID to use for the specified virtual network. If this is the first time you are attaching any virtual port group to the specified virtual network, you need to specify the VLAN ID you want to use. When you subsequently attach other virtual port groups to this same virtual network, Contrail Networking automatically assigns the same VLAN ID. If the interface is untagged, select the Native/untagged checkbox. In this case, the VLAN ID represents the native VLAN.	11

3. Repeat Step 1 and Step 2 to create more virtual port groups as needed.

Congratulations! You've onboarded your fabric and created your overlay networks. Once the compute administrator instantiates the compute endpoints that are attached to the virtual port groups, the endpoints within the same overlay network will be able to communicate with each other. If that is all you want to do, then you're done.

If you want to allow users in the different overlay networks to communicate with each other, then you'll want to keep going!

Step 3: Keep Going

IN THIS SECTION

The overlay networks you just created all share the same physical infrastructure, but are completely separate from each other. Users in one overlay network won't be able to communicate with users in another overlay network.
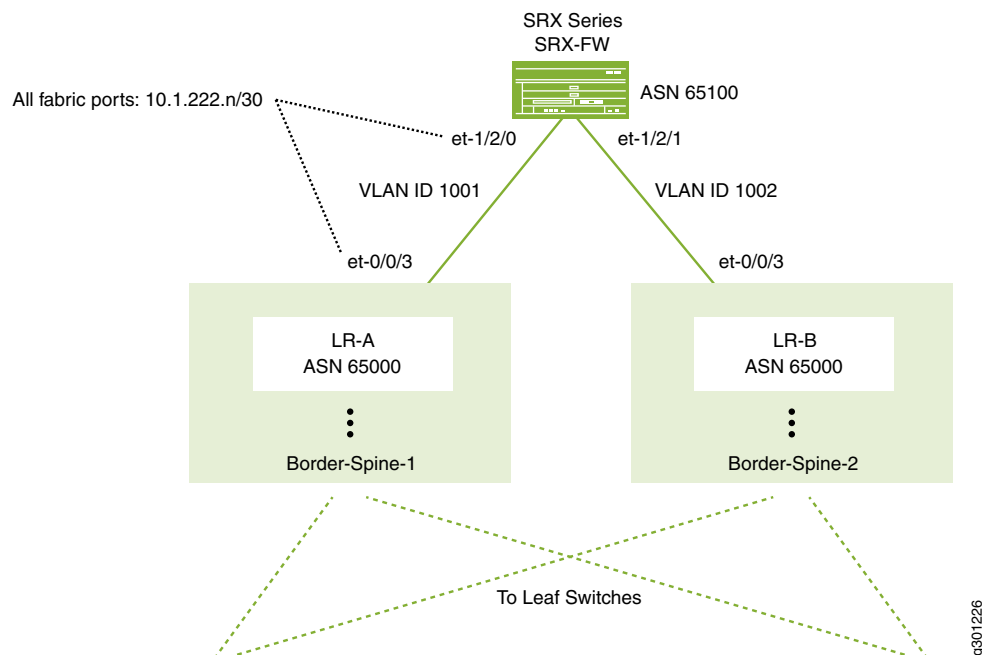
We'll show you how to open a path between networks through a physical network function (PNF), in this case, an SRX Series firewall. You do this by creating a PNF service chain that runs from one logical router to another through the firewall.

Onboard the PNF Device

To create a PNF service chain, you first have to onboard the PNF device. You do this by using the same Create Fabric wizard you used when you onboarded the fabric underlay, but this time you're discovering an existing (brownfield, already configured) device. By onboarding this device, you're telling Contrail Networking to add this device to the fabric.

Contrail Networking then assigns IP addresses to the fabric ports on the SRX Series device and on the attached switches from the PNF service chain subnet you specified earlier when you onboarded the fabric (Step 4 in "Onboard a New Fabric (Greenfield)" on page 14). Contrail Networking also configures the routing protocols to allow the SRX Series device to exchange routes with the fabric.

Here's the PNF device you'll be onboarding and the PNF service chain you'll be setting up:

Before you begin, physically connect the SRX Series firewall to both spine switches (in a centrally routed and bridged model). Make sure the SRX Series device is already up and running and contains basic configuration such as a username and password, hostname, management and loopback IP addresses, but no IP addresses on the interfaces that you'll use to connect to the fabric nor any policies that govern traffic to and from the fabric.

1. Select **INFRASTRUCTURE>Fabrics** and click the fabric underlay that you onboarded previously.

   The Fabric devices window appears listing all the devices in the fabric.

2. Select **Action>Brownfield wizard**.

   The Create Fabric wizard is launched, but you're not creating a fabric in this procedure. You're using the wizard to add a PNF device to the fabric you onboarded earlier.

3. Fill in the PNF configuration. Here are mandatory fields along with example values. Because this is an existing SRX Series device, you supply the existing login credentials and the existing management IP address. You can leave all other settings at their default values.

Fields	Meaning	Example
Device credentials>Username	The username to log in to the device.	<existing-username>
Device credentials>Password	The password to log in to the device.	<existing-password>
Management subnets>CIDR	The IP address of the device on the management network.	<existing-management-IP-address> This is a /32 address.

4. Click **Next** to launch the device discovery process.

5. When you see the message **Job execution completed successfully** in the log section, click **Next** to progress to role assignment.

6. Select the row for the PNF device you just discovered and click the **Assign Role** icon on the far right of the row.

    The Assign role to devices window appears.

7. Set the role for the SRX Series device and click **Assign**.

Role	Setting
Physical	pnf
Routing Bridging Roles	PNF-Servicechain **NOTE:** You had set this same role on the spine switches earlier.

8. Click **Autoconfigure** to push the new configuration onto the devices based on their assigned roles.

9. When the progress panel displays **Job summary: Job execution completed successfully**, click **Next** and then click **Finish** to skip the assignment of telemetry profiles.

Create the PNF Service Chain

With the PNF device now part of the fabric, you can logically insert it between two overlay networks. You insert the PNF device by setting up a PNF service chain.

To create the service chain, you first create a template that describes how the PNF device is connected to the fabric. The PNF device can be reused for multiple overlay applications. Creating a template saves you from configuring this information for future service chains.

1. Create the service chain template.

    a. Select **SERVICES>Catalog** to bring up the Catalog page.

    b. Click the **PNF** tab to bring up the PNF Service Templates window and click **Create>Template**.

    The Create PNF Service Template page appears.

    c. Fill in the fields on this page according to your desired setup. Here are the mandatory fields along with values that match our example PNF configuration.

Field	Meaning	Example
Name	The name you want to call this service template.	my-service-chain
PNF Device	The name of the device. This is the existing hostname of the SRX Series device.	SRX-FW
PNF Left Interface	The interface on one side of the SRX Series device.	et-1/2/0
PNF Left Fabric	The name of the fabric on one side of the SRX Series device.	my-fabric
PNF Left Attachment Points>Physical Router	The router attached to the left interface of the SRX Series device.	Border-Spine-1
PNF Left Attachment Points>Left Interface	The interface on the router attached to the left interface of the SRX Series device.	et-0/0/3
PNF Right Interface	The interface on the other side of the SRX Series device.	et-1/2/1
PNF Right Fabric	The name of the fabric on the other side of the SRX Series device.	my-fabric
PNF Right Attachment Points>Physical Router	The router attached to the right interface of the SRX Series device.	Border-Spine-2
PNF Right Attachment Points>Right Interface	The interface on the router attached to the right interface of the SRX Series device.	et-0/0/3

    d. Click **Create** to create the template. The name of the template is the name you specified appended by the template designation (for example, my-service-chain-template).

2. Create the service chain using this template.

   a. Select **SERVICES>Deployments** to bring up the Deployments page.

   b. Click the **PNF** tab to bring up the PNF Service Instances window and click **Create>Instance**.

      The Create PNF Service Instance page appears.

   c. Fill in the fields on this page according to your desired setup. Here are the mandatory fields along with values that match our example PNF configuration.

Fields	Meaning	Example
Name	The name you want to call this service chain instance.	my-service-chain
Service Template	The service template you want to use. This is the name of the service template you created earlier.	my-service-chain-template
PNF eBGP ASN	The ASN for the PNF device. This is used by eBGP to exchange routes in the overlay.	65100
Left Tenant Logical Router	The logical router attached to the left interface. Deciding which is the left logical router and which is the right logical router is arbitrary because each spine switch has the same two logical routers instantiated.	LR-A
PNF Left BGP Peer ASN	The ASN for the left overlay network. There is one ASN for the entire overlay.	65000
Left Service VLAN	The VLAN ID for the left interface.	1001
Right Tenant Logical Router	The logical router attached to the right interface. This is the other logical router.	LR-B
PNF Right BGP Peer ASN	The ASN for the right overlay network. There is one ASN for the entire overlay.	65000
Right Service VLAN	The VLAN ID for the right interface.	1002

   d. Click **Create** to push the configuration to the devices.

You have now created the service chain. The SRX Series device uses eBGP to learn routes from one logical router and advertises the routes to the other logical router. Once the routes are known, internetwork traffic begins to traverse the SRX Series device.

By default, Contrail Networking configures the SRX Series device to be permissive (that is, an <any>-<any>-<any> permit policy). To change the policy, log in to the SRX Series device and configure the policy as you normally do.

What's Next

Now that you've set up Contrail Networking with a basic configuration, here are some things you can do next.

If you want to	Then
See all documentation available for Contrail Networking	Visit Contrail Networking Documentation
See all documentation available for Contrail Insights	Visit Contrail Insights Documentation
See a Contrail Networking use case with a deeper explanation of the steps you've just learned	See In Focus: How to Onboard a Fabric and Create an Overlay
See a cheatsheet of the steps you've just learned	See Contrail Enterprise Multicloud Getting Started Guide - Fabric Management
See a solutions guide for fabric management	See Data Center: Contrail Enterprise Multicloud for Fabric Management
Configure advanced fabric management features	See the Contrail Networking Fabric Lifecycle Management Guide
Stay up-to-date with new and changed features and known and resolved issues	See the Contrail Networking Release Notes