

Data Center: Contrail Enterprise Multicloud for Fabric Management

Published
2023-07-13

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.

Data Center: Contrail Enterprise Multicloud for Fabric Management
Copyright © 2023 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

1

Data Center Fabric Management—Overview

About This Solutions Guide | 2

Terminology | 2

Contrail Enterprise Multicloud Architecture | 6

Contrail Enterprise Multicloud Components | 10

Contrail Command | 11

IP Fabrics | 12

Device Roles | 14

Virtual Networks | 16

Virtual Port Groups | 17

Logical Routers | 19

2

Data Center Fabric Management—Tested Implementation

Data Center Fabric Design Overview and Validated Topology | 21

Create a Greenfield Deployment For a New Data Center Network | 23

Before You Begin | 24

Creating the New Fabric and Discovering Devices | 27

Assigning Roles to Devices | 31

Applying the Role-Based Configurations to the New Fabric Devices | 31

Create a Brownfield Deployment to Add an Overlay to an Existing IP Fabric | 34

Before You Begin | 35

Adding an Existing Underlay into a Fabric and Discovering Devices | 35

Selective Onboarding of a Device | 39

Configure Virtual Networks for Multi-tenant Service Operations | 43

Create Virtual Networks | 44

Assign Interfaces to VLANs with Virtual Port Groups | 46

Enable Layer 3 Routing on Virtual Networks Using Logical Routers | 48

Verify Your Virtual Network Configuration | 50

Configure Service Chaining With PNF | 55

Service Chaining Using a PNF | 55

Service Chaining Configuration Overview | 56

Onboard an SRX Services Gateway as the PNF Device | 58

Assign Device Roles for the PNF Device | 59

Create a PNF Service Template | 60

Configure Data Center Interconnect (DCI) | 64

Data Center Interconnect Overview | 64

Data Center Interconnect Configuration Overview | 65

Assign Device Roles for Border Spine and Border Leaf Devices | 67

Manually Configure BGP Peering | 68

Configure Virtual Networks | 71

Create Virtual Port Groups | 72

Create Logical Routers | 73

Create Data Center Interconnect | 74

Verify Data Center Interconnect | 75

1

CHAPTER

Data Center Fabric Management—Overview

[About This Solutions Guide | 2](#)

[Terminology | 2](#)

[Contrail Enterprise Multicloud Architecture | 6](#)

[Contrail Enterprise Multicloud Components | 10](#)

About This Solutions Guide

The purpose of this guide is to provide networking professionals with the concepts and tools needed to build data center fabrics and multicloud networks on an EVPN/VXLAN infrastructure by using Contrail Enterprise Multicloud and QFX Series switches.

The intended audience for this guide includes system integrators, infrastructure professionals, partners, and customers.

Terminology

IN THIS SECTION

- [Glossary Terms | 2](#)

This section provides a summary of commonly used terms, protocols, and building block technologies used in creating and maintaining data center networks.

Glossary Terms

- **ARP**—Address Resolution Protocol. A protocol defined in RFC 826 for mapping a logical IP address to a physical MAC address.
- **Backbone Device**—A device in the WAN cloud that is directly connected to a spine device or devices in a data center. Backbone devices are required in this reference topology to provide physical connectivity between data centers that are interconnected using a data center interconnect (DCI).
- **Border Leaf**—A device that typically has the sole purpose of providing a connection to one or more external devices. The external devices, for example, multicast gateways or data center gateways, provide additional functionality to the IP fabric.
- **Border Spine**—A device that typically has two roles—a network underlay device and a border device that provides a connection to one or more external devices. The external devices, for example, multicast gateways or data center gateways, provide additional functionality to the IP fabric.

- **Bridged Overlay**—An Ethernet-based overlay service designed for data center environments that do not require routing within an EVPN/VXLAN fabric. IP routing can be provided externally to the fabric as needed.
- **BUM**—Broadcast, Unknown Unicast, and Multicast. The BUM acronym collectively identifies the three traffic types.
- **Centrally-Routed Bridging Overlay**—A form of IRB overlay that provides routing at a central gateway and bridging at the edge of the overlay network. In an IRB overlay, a routed overlay and one or more bridged overlays connect at one or more locations through the use of IRB interfaces.
- **Clos Network**—A multistage network topology first developed by Charles Clos for telephone networks that provides multiple paths to a destination at each stage of the topology. Non-blocking networks are possible in a Clos-based topology.
- **Collapsed Spine fabric**—An EVPN fabric design in which the overlay functions are collapsed onto the spine layer rather than distributed between spine and leaf devices. This type of fabric has no leaf layer in the EVPN core; the spine devices connect directly to the access layer.
- **Contrail Command**—Contrail Enterprise Multicloud user interface. Provides a consolidated, easy-to-use software designed to automate the creation and management of data center networks.
- **Contrail Enterprise Multicloud**—A suite of products and software that combines Contrail Command as a single point of management for private and public clouds, QFX Series switches running Junos OS as an infrastructure for data center networking, and Contrail Insights (formerly known as AppFormix) for telemetry and network visualization.
- **DCI**—Data Center Interconnect. The technology used to interconnect separate data centers.
- **Default instance**—A global instance in a Juniper Networks device that hosts the primary routing table such as `inet.0` (default routing instance) and the primary MAC address table (default switching instance).
- **DHCP relay**—A function that allows a DHCP server and client to exchange DHCP messages over the network when they are not in the same Ethernet broadcast domain. DHCP relay is typically implemented at a default gateway.
- **EBGP**—External BGP. A routing protocol used to exchange routing information between autonomous networks. It has also been used more recently in place of a traditional Interior Gateway Protocol, such as IS-IS and OSPF, for routing within an IP fabric.
- **Edge-Routed Bridging Overlay**—A form of IRB overlay that provides routing and bridging at the edge of the overlay network.
- **End System**—An endpoint device that connects into the data center. An end system can be a wide range of equipment but is often a server, a router, or another networking device in the data center.

- **ESI**—Ethernet segment identifier. An ESI is a 10-octet integer that identifies a unique Ethernet segment in EVPN. In this blueprint architecture, LAGs with member links on different access devices are assigned a unique ESI to enable Ethernet multihoming.
- **Ethernet-connected Multihoming**—An Ethernet-connected end system that connects to the network using Ethernet access interfaces on two or more devices.
- **EVPN**—Ethernet Virtual Private Network. A VPN technology that supports bridged, routed, and hybrid network overlay services. EVPN is defined in RFC 7432 with extensions defined in a number of IETF draft standards.
- **EVPN Type 2 Route**—Advertises MAC addresses and the associated IP addresses from end systems to devices participating in EVPN.
- **IBGP**—Internal BGP. In this blueprint architecture, IBGP with Multiprotocol BGP (MP-IBGP) is used for EVPN signalling between the devices in the overlay.
- **IP Fabric**—An all-IP fabric network infrastructure that provides multiple symmetric paths between all devices in the fabric. We support an IP Fabric with IPv4 (an *IPv4 Fabric*) with all architectures described in this guide, and an IP Fabric with IPv6 (an *IPv6 Fabric*) with some architectures and on some platforms.
- **IP-connected Multihoming**—An IP-connected end system that connects to the network using IP access interfaces on two or more devices.
- **IRB**—Integrated Routing and Bridging. A technique that enables routing between VLANs and allows traffic to be routed or bridged based on whether the destination is outside or inside of a bridging domain. To activate IRB, you associate a logical interface (IRB interface) with a VLAN and configure the IRB interface with an IP address for the VLAN subnet.
- **Leaf Device**—An access level network device in an IP fabric topology. End systems connect to the leaf devices in this blueprint architecture.
- **MAC-VRF instance**—A routing instance type that enables you to configure multiple customer-specific EVPN instances instead of only one instance (the default instance). MAC-VRF instances use a consistent configuration style across platforms. Different MAC-VRF instances can support different Ethernet service types (VLAN-aware and VLAN-based services) on the same device in a data center.
- **Multiservice Cloud Data Center Network**—A data center network that optimizes the use of available compute, storage, and network access interfaces by allowing them to be shared flexibly across diverse applications, tenants, and use cases.
- **NDP**—Neighbor Discovery Protocol. An IPv6 protocol defined in RFC 4861 that combines the functionality of ARP and ICMP, and adds other enhanced capabilities.
- **NVE**—As defined in RFC 8365, *A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)*, a network virtualization edge is a device that terminates a VXLAN tunnel in a network

virtualization overlay. For example, in a centrally routed bridging overlay, we consider spine and leaf devices to be NVE devices.

- **NVO**—A network virtualization overlay is a fabric in which we use EVPN as a control plane and VXLAN as a data plane.
- **Routed Overlay**—An IP-based overlay service where no Ethernet bridging is required. Also referred to as an IP VPN. In this blueprint architecture, the routed overlay is based on EVPN Type 5 routes and their associated procedures, and supported by VXLAN tunneling.
- **Spine Device**—A centrally-located device in an IP fabric topology that has a connection to each leaf device.
- **Storm Control**—Feature that prevents BUM traffic storms by monitoring BUM traffic levels and taking a specified action to limit BUM traffic forwarding when a specified traffic level is exceeded.
- **Underlay Network**—A network that provides basic network connectivity between devices. In this blueprint architecture, the underlay network is an IP Fabric that provides the basic IP connectivity, usually with IPv4. We also support an IP Fabric with an IPv6 underlay with some architecture designs on certain platforms.
- **VLAN trunking**—The ability for one interface to support multiple VLANs.
- **VNI**—VXLAN Network Identifier. Uniquely identifies a VXLAN virtual network. A VNI encoded in a VXLAN header can support 16 million virtual networks.
- **VTEP**—VXLAN Tunnel Endpoint. A loopback or virtual interface where traffic enters and exits a VXLAN tunnel. Tenant traffic is encapsulated into VXLAN packets at a source VTEP, and de-encapsulated when the traffic leaves the VXLAN tunnel at a remote VTEP.
- **VXLAN**—Virtual Extensible LAN. Network virtualization tunneling protocol defined in RFC 7348 used to build virtual networks over an IP-routed infrastructure. VXLAN is used to tunnel tenant traffic over the IP fabric underlay from a source endpoint at an ingress device to a destination endpoint at the egress device. These tunnels are established dynamically by EVPN. Each VTEP device advertises its loopback address in the underlay network for VXLAN tunnel reachability between VTEP devices.
- **VXLAN Stitching**—A Data Center Interconnect (DCI) feature that supports Layer 2 interconnection EVPN-VXLAN fabric on a per-VXLAN VNI basis.

RELATED DOCUMENTATION

| [Contrail Enterprise Multicloud Components](#) | 10

Contrail Enterprise Multicloud Architecture

IN THIS SECTION

- [Contrail Enterprise Multicloud Introduction | 6](#)
- [Benefits of the Contrail Enterprise Multicloud Solution | 8](#)
- [Benefits of Using an SDN Controller for an EVPN/VXLAN Fabric | 9](#)

Contrail Enterprise Multicloud Introduction

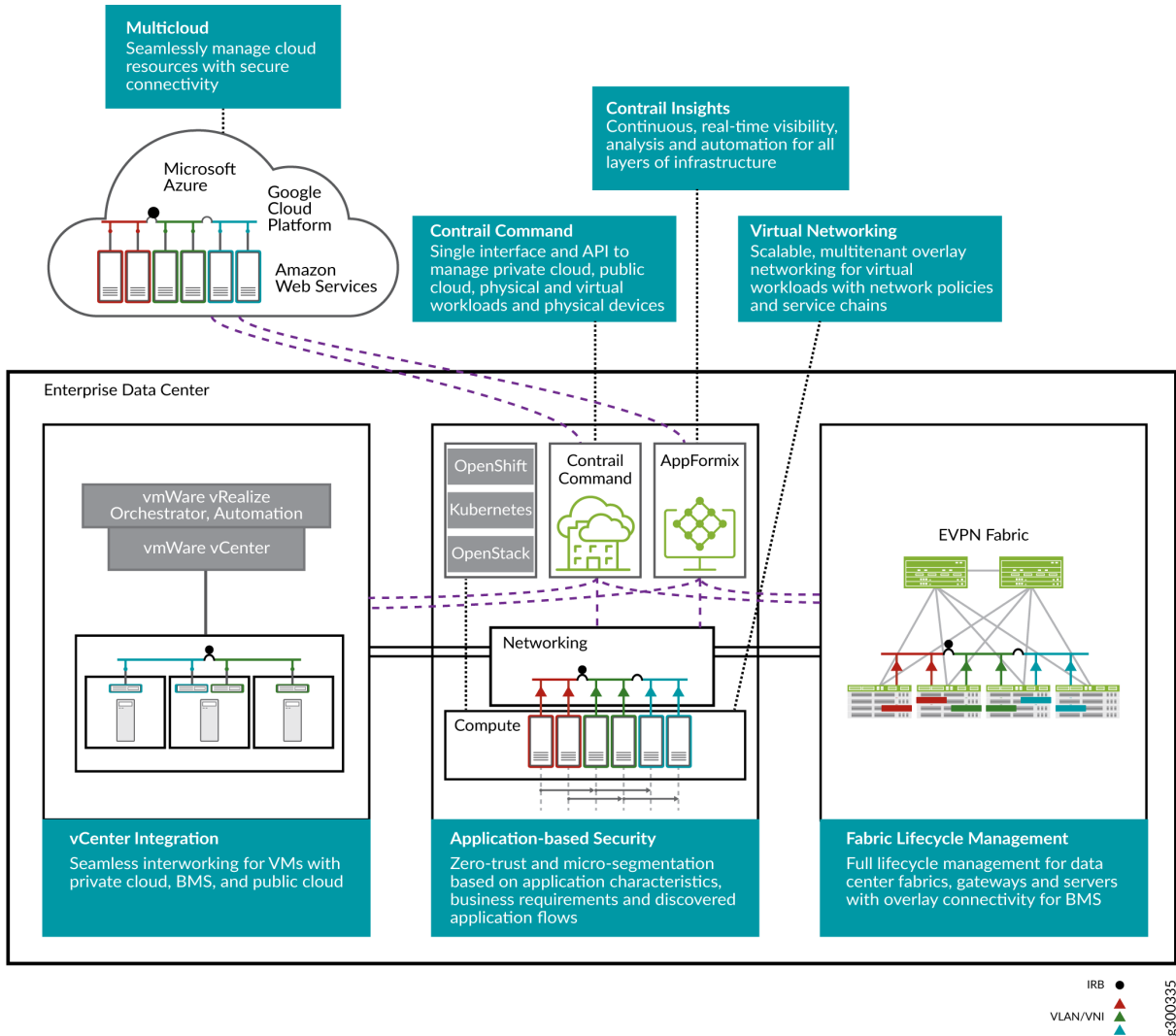
Contrail Enterprise Multicloud (CEM) is an intent-based networking system that automates the lifecycle of the infrastructure and application networking services on multicloud infrastructures that are composed of private clouds (data centers, virtualized computes) and public clouds.

For physical data center IP fabrics CEM supports the whole scope of network operations by:

- Automating Day 0 configuration of the infrastructure. This involves configuring a set of factory reset devices into a completely functional fabric or the onboarding of an existing fabric. It can also enable multitenant application networking services and perform hitless OS upgrades on devices that run Junos OS.
- Automating Day 1 service operations such as provisioning VLANs on access ports, inter-subnet routing services, advanced inter-tenant services, across the fabric, and where needed extending those services across physical and virtualized endpoints.
- Automating Day 2 maintenance and scale out procedures of the fabric (adding devices to the fabric, replacing failed devices, diverting traffic from devices).
- Collecting flow usage counters, streaming telemetry, alarms, counters from devices.
- Providing a view on how the infrastructure and multitenant services are performing, identifying capacity bottlenecks or traffic anomalies with respect to the baseline
- Providing workflows and methods to proactively identify issues, faults, correlate them and take the relevant corrective actions.

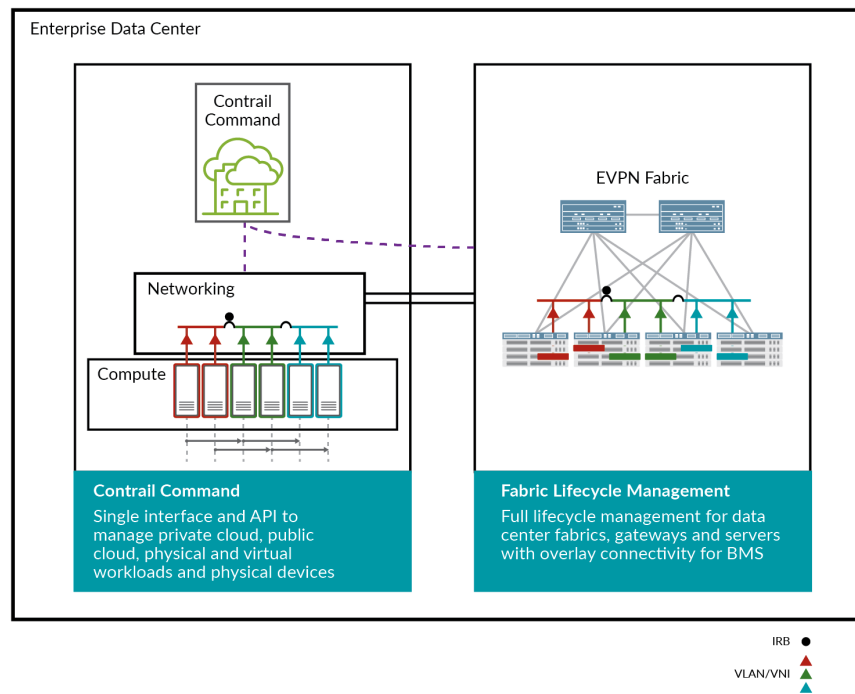
This guide focuses on Contrail Enterprise Multicloud as the central point of management of EVPN/VXLAN data center fabrics as shown in [Figure 1 on page 7](#).

Figure 1: Contrail Enterprise Multicloud



The components focused on in this guide are seen in [Figure 2 on page 8](#), namely Contrail Command as a central point of management and EVPN/VXLAN as the key data center technology.

Figure 2: Contrail Enterprise Multicloud—Data Center Fabric Management



Benefits of the Contrail Enterprise Multicloud Solution

The following points explain why Juniper Networks Contrail Enterprise Multicloud solution can meet your needs for a multicloud environment:

- Intent based automation and lifecycle management of the fabric using Contrail Command removes requirement to manually configure the fabric using the JunosOS CLI.
- Cloud ready architecture—ready to take you from private data centers all the way to the multi-cloud.
- An architecture that provides seamless integration of physical and virtual VXLAN tunnel endpoints (VTEP) by using vRouter technology.
- Built-in management security that provides end-to-end security and a uniform security posture by using Contrail Security and BMS policy management.
- Takes the dream of a self-healing, self-driven network closer to reality with help from tight integration of Contrail Command, AppFormix and Junos OS components.
- Support for Red Hat Enterprise Linux (RHEL), VMware integration, and integration with Nutanix.

- Open-standards based.

Benefits of Using an SDN Controller for an EVPN/VXLAN Fabric

When you combine an IP fabric with an EVPN/VXLAN environment, there is a clear demarcation between *underlay* operations (related to the infrastructure, devices, and software images) and *overlay* networking services (VLANs carried over VXLAN tunnels using MP-BGP EVPN protocol). Unlike proprietary fabrics, an EVPN/VXLAN fabric uses a role-definition for every device based on capabilities and location of routing between virtual networks.

EVPN is a powerful technology that can be used in a range of use cases. It brings multitenant, multiservice capabilities to production data centers, corporate branches and campuses, enterprises, and service provider wide-area networks (WANs). EVPN can be deployed in network hardware, servers, and even the public cloud. It supports networking functions from Layer 1 to Layer 4 in a relatively simple, integrated, and scalable manner. Last but not least, EVPN has been widely adopted across the networking industry.

With the context provided above, let's look at the reasons an enterprise should deploy a controller for an EVPN/VXLAN environment and why Contrail Enterprise Multicloud is the best tool for the job:

- **Provides a fast and error-free infrastructure to build operations with minimal human effort.** Contrail Enterprise Multicloud brings simple abstractions of composable service building blocks that it translates into underlying network building blocks including EVPN. Service layer building blocks include constructs such as tenants, subnets, policies, gateways, and service chains with associated service-level controls.
- **Brings day 1 plug-and-play baselining of the physical network fabric and enables an operator to perform day 2 functions at an intent/service level rather than at a technology level.** For example, Contrail Enterprise Multicloud helps create the fabric, create tenants, add subnets to tenants, attach endpoints to subnets, build and apply policies to tenants, and so on.
- **Adds smart life cycle management (LCM) capabilities to the fabric.** Contrail Enterprise Multicloud offers life cycle management of the fabric.
- **Opens endless positive business outcomes.** For example, fabric-wide visibility and control of critical operations means a is a very short lead time for daily operations, such as VLAN Tickets.
- **Simplifies network management using normalized configurations/operations for all tenant services.** Contrail Enterprise Multicloud eliminates manual procedures and complexity of performing those operations, while leaving network operators in full control of which operations should be performed in the data center fabric.

- **Adds openness at all layers.** This quality is unique to Contrail Enterprise Multicloud and makes it stand out from all other controllers in the industry. From the use of open standards technology in the network (such as EVPN/VXLAN, Ansible and Jinja2 templates, and APIs for everything), Contrail frees operators from the pitfalls of closed proprietary systems.
- **Achieves realtime visibility on the usage of infrastructure by each tenant service to minimize outages.** Contrail Enterprise Multicloud provides a single pane of glass to display the health and status of the infrastructure. Being able to use a single tool to analyze which services and tenants are impacted provides operators invaluable insights, which minimizes the impact of outages and reduces them to a minimum.

RELATED DOCUMENTATION

[Contrail Enterprise Multicloud Components | 10](#)

[Data Center Fabric Design Overview and Validated Topology | 21](#)

Contrail Enterprise Multicloud Components

IN THIS SECTION

- [Contrail Command | 11](#)
- [IP Fabrics | 12](#)
- [Device Roles | 14](#)
- [Virtual Networks | 16](#)
- [Virtual Port Groups | 17](#)
- [Logical Routers | 19](#)

This section provides an overview of the components used in this solution. The implementation of each component is covered in later sections of this guide.

Contrail Command

Contrail Command is the CEM user interface that provides a user-friendly interface that lets you provision your private data center network and extend it to the public cloud. It automates the process of building a new data center from scratch, adding an overlay to an existing IP fabric, and providing switching, routing, and security services. As a result, Contrail Command is a powerful component of the CEM solution.

The screenshot shows the Contrail Command interface with a sidebar on the left containing navigation options: Servers, Cluster, Fabrics (selected), Multi Cloud, and Networks. The main content area is titled 'Fabric Devices' and 'Topology View'. It contains a table of fabric devices and a 'Namespaces' panel on the right.

STATUS	NAME	MANAGEMENT...	LOOPBACK IP	VENDOR NAME	PRODUCT NA...	ROLE	ROUTING BRI...	INTERFACES
ACTIVE	baum	10.1.1.111	10.0.1.250	Juniper	qfx5110-32q	spine	CRB-Gateway Route-Reflect	5
ACTIVE	carroll	10.1.1.225	10.0.1.249	Juniper	qfx5110-32q	spine	CRB-Gateway Route-Reflect	5
ACTIVE	leguin	10.1.1.227	10.0.1.252	Juniper	qfx10002-36q	leaf	CRB-MCAST-G PNF-Serviced	5
ACTIVE	lengle	10.1.1.238	10.0.1.251	Juniper	qfx10002-36q	leaf	CRB-MCAST-G PNF-Serviced	5
ACTIVE	scieszka	10.1.1.181	10.0.1.248	Juniper	qfx5110-48...	leaf	CRB-Access	4
ACTIVE	silverstein	10.1.1.113	10.0.1.247	Juniper	qfx5110-48...	leaf	CRB-Access	5

NAME	VALUE
eBGP-ASN-pool	65101-65110 ASN
fabric-subnets	10.10.0.0/24 CIDR
loopback-subnets	10.0.1.0/24 CIDR
management-subnets	10.1.1.0/24 CIDR
overlay_ibgp_asn	65100 ASN

Contrail Command provides an intuitive user interface for the user—whether a network operation administrator, a cloud administrator, or a tenant administrator—to perform any infrastructure and service operations on the managed multicloud infrastructure. Some of the infrastructure and troubleshooting operations that you can perform with Contrail Command are:

- Performs Junos OS upgrades on devices in the fabric.
- Automates service operations, such as provisioning VLANs on access ports, inter-subnet routing services, advanced inter-tenant services, across the fabric, and extending those services across physical and virtualized endpoints
- Automates maintenance and scale out procedures of the fabric (adding devices to the fabric, replacing failed devices, diverting traffic from devices)
- Collects flow usage counters, streaming telemetry, alarms, counters from the devices and providing a view on how the infrastructure and the multitenant services are performing, identifying capacity bottlenecks or traffic anomalies with respect to the baseline
- Provides workflows and methods to proactively identify issues and faults, correlate them and take corrective actions.

SEE ALSO

[Create a Greenfield Deployment For a New Data Center Network | 23](#)

IP Fabrics

IN THIS SECTION

- [New IP Fabric | 12](#)
- [Existing IP Fabric | 13](#)

An IP fabric is a set of devices and physical network functions (PNFs) that fall under the same data center administrator responsibility area. You can provision new or existing fabrics using CEM.

New IP Fabric

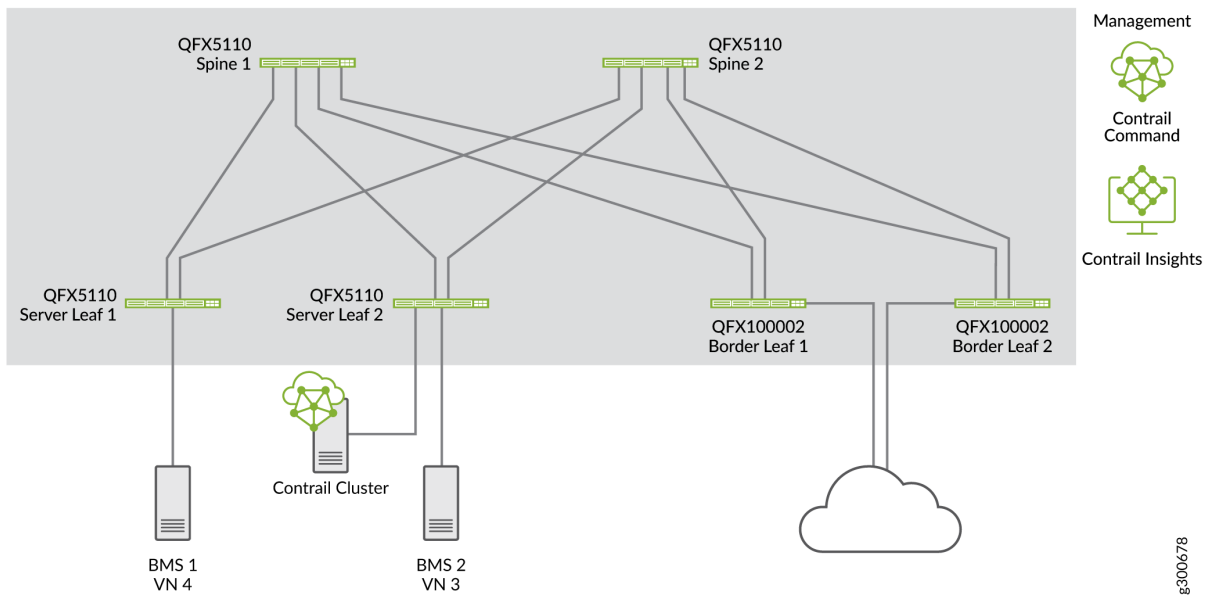
When you build a brand new data center network, you can use CEM to automate the provisioning and configuration of your fabric. The new fabric process (also known as a greenfield deployment) provisions new devices to form an IP Clos data center topology with leaf (TOR) and spine devices. Leaf switches are typically QFX5K devices and spine devices are typically QFX10K devices, but there are many variants.

CEM creates an IP fabric underlay network built on EBGP, combined with an EVPN/VXLAN overlay supported by IBGP. It discovers the data center topology, assigns IP addresses to the loopback interfaces, creates fabric subnets, loopback subnets, and management subnets, and configures the EBGP underlay and the IBGP overlay.

For IP fabric greenfield onboarding, CEM uses Zero-Touch Provisioning (ZTP) to initialize and configure factory-default devices. The shaded area of [Figure 3 on page 13](#) shows the scope of ZTP operations. These devices are connected to an out-of-band management network that is provisioned before the new fabric process is run. All of the devices must be reachable on the management network.

After you have run the initial ZTP process on your fabric, you can easily assign device roles, create device-specific configurations, and push the configurations to each device.

Figure 3: Scope of Zero Touch Provisioning



Existing IP Fabric

If you already have a deployed data center infrastructure for which you have configured the underlay of the data center fabric, your network is considered a brownfield network. To migrate to an overlay, you only need to let Contrail Command discover the existing topology of pre-connected and pre-configured spine and leaf devices, assign device roles, create device-specific configurations, and push the configurations to each device.

SEE ALSO

[Create a Greenfield Deployment For a New Data Center Network | 23](#)

[Create a Brownfield Deployment to Add an Overlay to an Existing IP Fabric | 34](#)

IP Fabric Underlay Network Design and Implementation

[Data Center EVPN-VXLAN Fabric Architecture Guide](#)

Device Roles

Assigning roles to devices tailors the data center design for distributed or centralized routing. There are two types of roles that you assign to devices in your fabric.

- Physical roles
- Routing bridging (overlay) roles

The roles define the routing and bridging responsibilities of the device. A device can have one physical role and one or more routing bridging roles.

In centrally-routed bridging (CRB) devices, when you configure the logical router to allow traffic to flow between Ethernet virtual network instances, routing occurs at the spine device. Traffic is routed from the leaf to the spine and back. IRB interfaces are configured in the overlay at each spine device to route traffic between virtual networks.

In edge-routed bridging (ERB) you can configure the ERB-UCAST-Gateway role on a border leaf device, which causes routing to occur at the leaf switch. The IRB interfaces are configured at the leaf switch to enable unicast traffic routing at the leaf switch.

[Table 1 on page 14](#) shows the routing and bridging roles that are available for each of the physical roles.

Table 1: Physical and Routing Bridging Roles in Contrail

Physical Role	Routing Bridging Role	Description
Spine	Route-Reflector	Specifies that the device acts as a route reflector for IBGP to satisfy the full-mesh requirement and enable scalability for the fabric. Usually all spine devices or gateways are given this role.
	Null	Specifies that the device is used in an IP routing environment that provides only underlay routing; does not participate in VXLAN tunnels. Applies only to spine devices when edge routing and bridging is used
	CRB-Gateway	Provides Layer 3 Unicast gateway functionality for routing between VNIs using an IRB interface. Routing is done centrally on a spine

Table 1: Physical and Routing Bridging Roles in Contrail (Continued)

Physical Role	Routing Bridging Role	Description
	CRB-MCAST-Gateway	<p>Provides Layer 3 multicast gateway for routing between VNIs using an IRB interface. Multicast routing is done centrally.</p> <p>It is not supported on QFX5100 and 5200 hardware families.</p>
	DC-Gateway	<p>Provides a routing connection for traffic to exit the data center</p> <p>Devices that provide connectivity to external networks or between fabrics.</p>
	DCI-Gateway	<p>Interconnects a logical router in one data center to a logical router in a different data center using EVPN VXLAN Type 5 routes.</p>
	PNF-Servicechain	<p>Specifies the devices where the Layer 3 PNF is attached.</p>
	AR-Replicator	<p>Specifies that the device replicates BUM traffic from one overlay tunnel to others.</p>
	AR-Client	<p>Specifies that the device sends BUM traffic to an AR replicator.</p>
Leaf	CRB-Access	<p>Specifies devices in a CRB architecture that perform only Layer 2 VXLAN functionality (bridging).</p>
	ERB-UCAST-Gateway	<p>Specifies that routing occurs at the leaf switch. IRB interfaces are configured at the leaf switch to enable unicast traffic routing.</p> <p>While unicast traffic can be routed at the leaf switches, multicast traffic routing still occurs at the spine devices. In contrast, the CRB-Gateway role at a spine is capable of routing both unicast and multicast traffic. With ERB, leaf switches route the unicast traffic, which makes the configuration of the CRB-Gateway role on the spine unnecessary since unicast traffic will never be routed to a spine device. Instead, you must configure the spine devices with the CRB-MCAST-Gateway role to route multicast traffic when required.</p>

Table 1: Physical and Routing Bridging Roles in Contrail (Continued)

Physical Role	Routing Bridging Role	Description
	CRB-MCAST-Gateway	Provides Layer 3 multicast gateway for routing between VNIs using an IRB interface. Multicast routing is done centrally. It is not supported on QFX5100 and 5200 hardware families.
	Route-Reflector	Specifies that the device acts as a route reflector for IBGP to satisfy the full-mesh requirement and enable scalability for the fabric. Usually all spine devices or gateways are given this role.
	DCI-Gateway	Interconnects a logical router from one data center to another by using EVPN VXLAN Type 5 routes. This role should be configured on all border leafs.
	PNF-Servicechain	Specifies the devices where the Layer 3 PNF is attached.
	AR-Replicator	Specifies that the device replicates BUM traffic from one overlay tunnel to others.
	AR-Client	Specifies that the device sends BUM traffic to an AR replicator.
PNF	PNF-Servicechain	Specifies the devices where the Layer 3 PNF is attached.

SEE ALSO

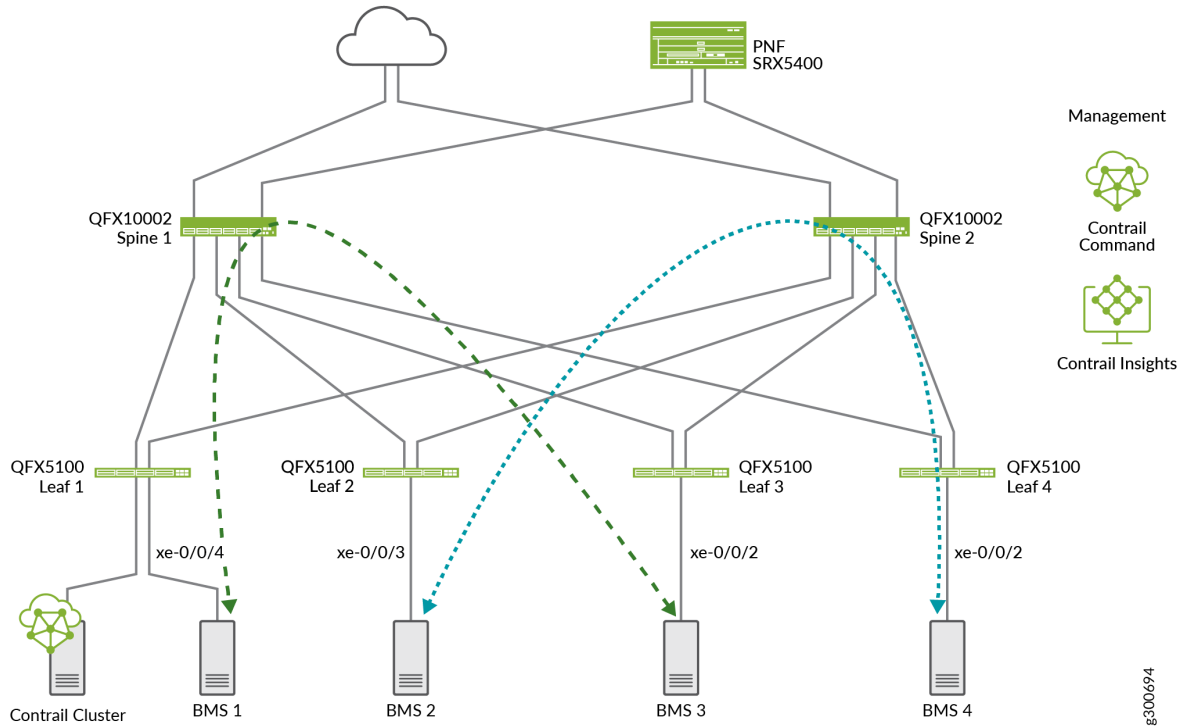
https://www.juniper.net/documentation/en_US/contrail19/topics/reference/hardware-platforms-supported-roles.html

Virtual Networks

A virtual network is a bridge domain or LAN segment. It can be associated to a subnet (prefix of hosts attached to the LAN segment), similarly to hosts connected to a LAN switch in a building. You create LAN segments to give departments, or tenants, access to servers that are spread across the VXLAN network.

To do so, you specify which servers are on the same VLAN or VNI and allow them to reach each other over VXLAN tunnels across the fabric. In this example shown in [Figure 4 on page 17](#), BMS 1 and BMS 3 servers have been added to the Green virtual network so they can reach each other. BMS 2 and BMS 4 have been added to the blue virtual network.

Figure 4: Green and Blue Virtual Networks



SEE ALSO

[Configure Virtual Networks for Multi-tenant Service Operations | 43](#)

Virtual Port Groups

VPG provides connectivity to servers that were not configured by Contrail Command. A virtual port group (VPG) is the representation of:

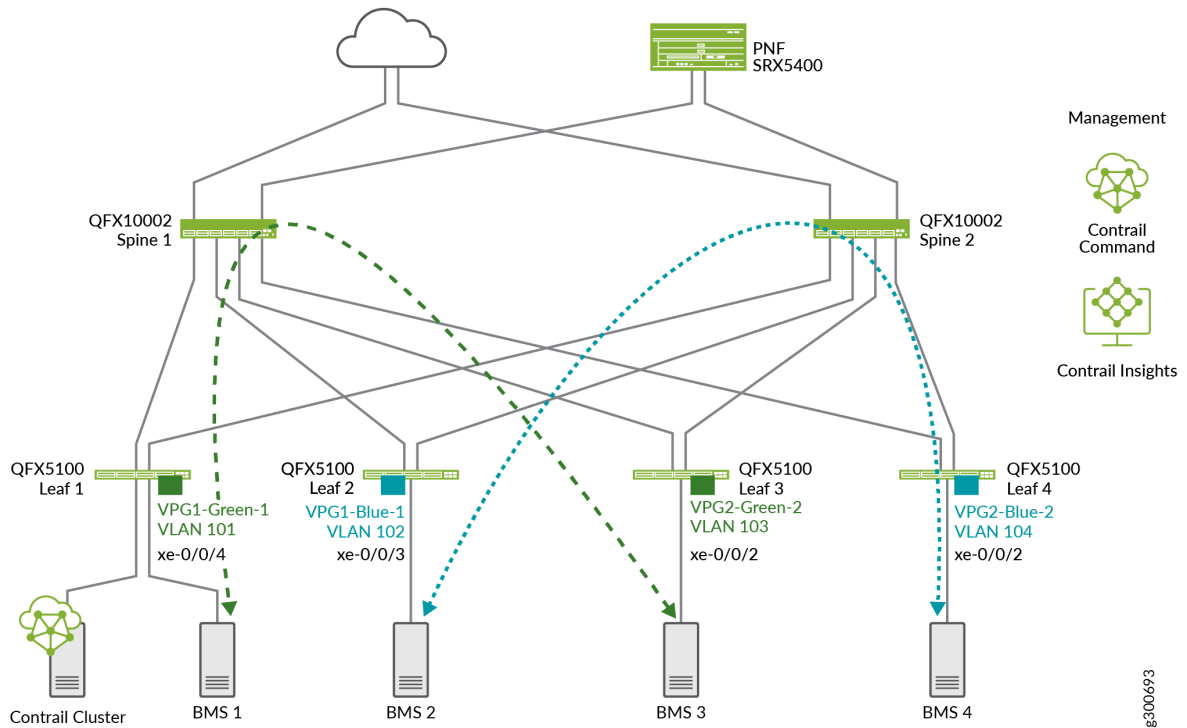
- A group of one or more physical interfaces (or ports) on one or more physical devices, and
- How these ports are used as server attachment points to the VXLAN virtual networks (VLANs)

Each VPG is assigned VXLAN Network Identifier (VNI) and is attached to a virtual network. You can select multiple interfaces on the same device or on different devices. A VPG is similar to a link aggregation group (LAG) but supports both LAG and multihoming depending on whether you select the interfaces on the same devices or on different devices. A LAG is automatically created if you select more than one interface on the same device.

When you provision a VPG, you can define a Security Group, which corresponds to a 5-tuple stateless filter or ACL, or which advanced port profile (such as for storm control) is applied on the access VLANs of this VPG.

Figure 5 on page 18 show VPGs attached to leaf devices for each end of the green and blue virtual networks.

Figure 5: Virtual Port Groups Attached to Virtual Networks



SEE ALSO

Figure 13 | 47

8300693

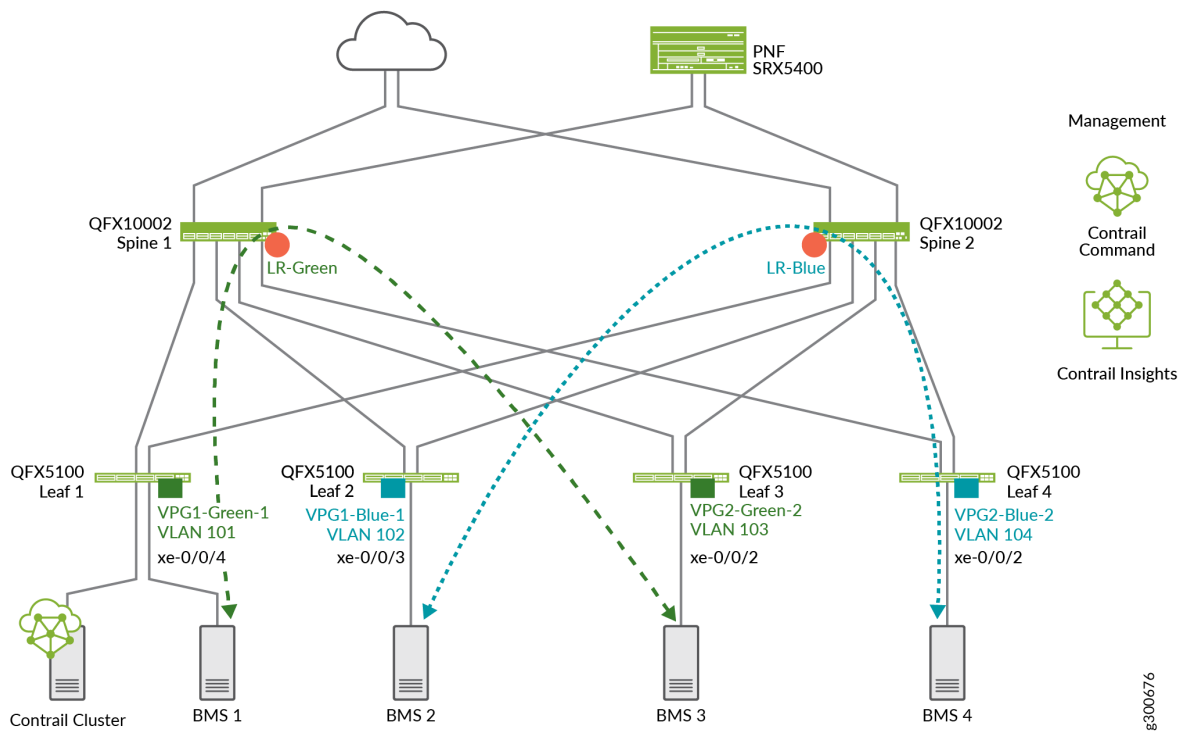
Logical Routers

In CEM a logical router is a Layer 3 virtual routing and forwarding (VRF) routing instance for a tenant that provides routed connectivity for devices in the same virtual network. The logical router represents a Layer 3 routing table and its attachment points to the Layer 2 tenant network.

In the Layer 3 routing instance, there is one IRB unit for each virtual network that is attached to the logical router. These IRBs correspond to the anycast gateway of the virtual network to which any unknown traffic is sent. Traffic from a virtual network (a Layer 2 bridge domain) that has to reach a subnet for which it doesn't have an explicit route is sent to the IRB.

Figure 6 on page 19 shows logical routers added to spines for the green and blue virtual networks shown in the previous section.

Figure 6: Logical Routers on the Spine Devices



SEE ALSO

[Enabling Routing Between Virtual Networks](#)

2

CHAPTER

Data Center Fabric Management—Tested Implementation

Data Center Fabric Design Overview and Validated Topology | 21

Create a Greenfield Deployment For a New Data Center Network | 23

Create a Brownfield Deployment to Add an Overlay to an Existing IP Fabric | 34

Selective Onboarding of a Device | 39

Configure Virtual Networks for Multi-tenant Service Operations | 43

Configure Service Chaining With PNF | 55

Configure Data Center Interconnect (DCI) | 64

Data Center Fabric Design Overview and Validated Topology

IN THIS SECTION

- [Reference Design Topologies | 21](#)
- [Software Summary | 23](#)

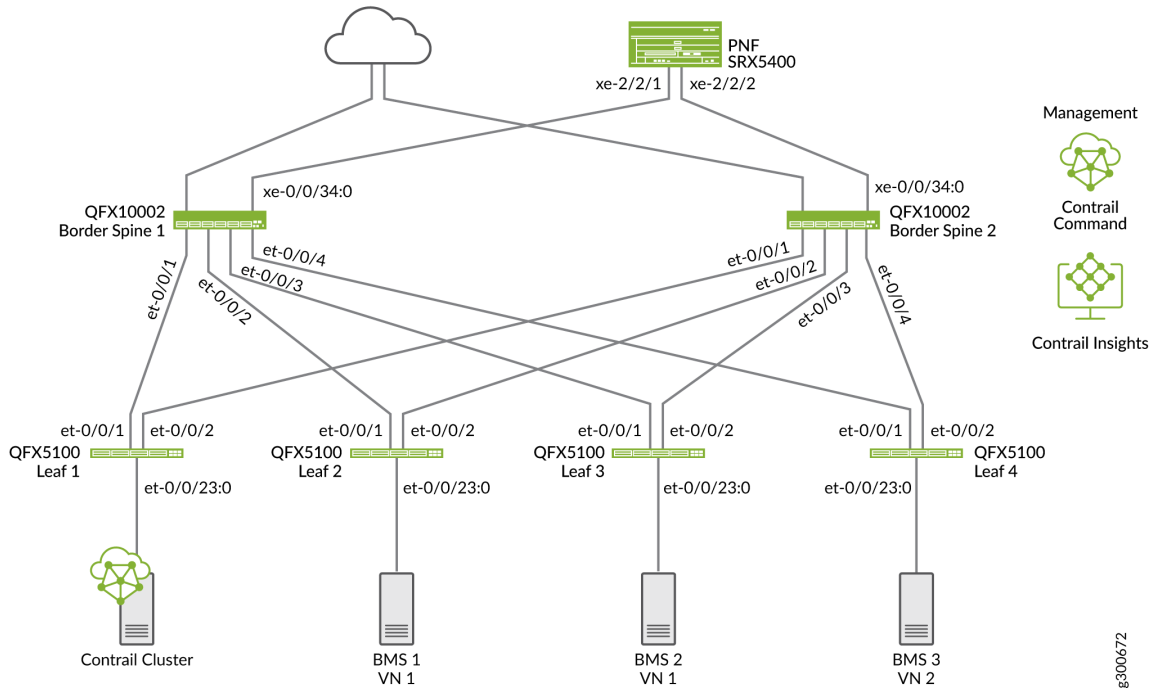
This section provides an overview of the data center fabric design used in this guide summarizes the topologies that were validated by the Juniper Networks Test Team.

Reference Design Topologies

We are using two topologies in this reference design—a centrally-routed bridging data center and an edge-routed bridging data center.

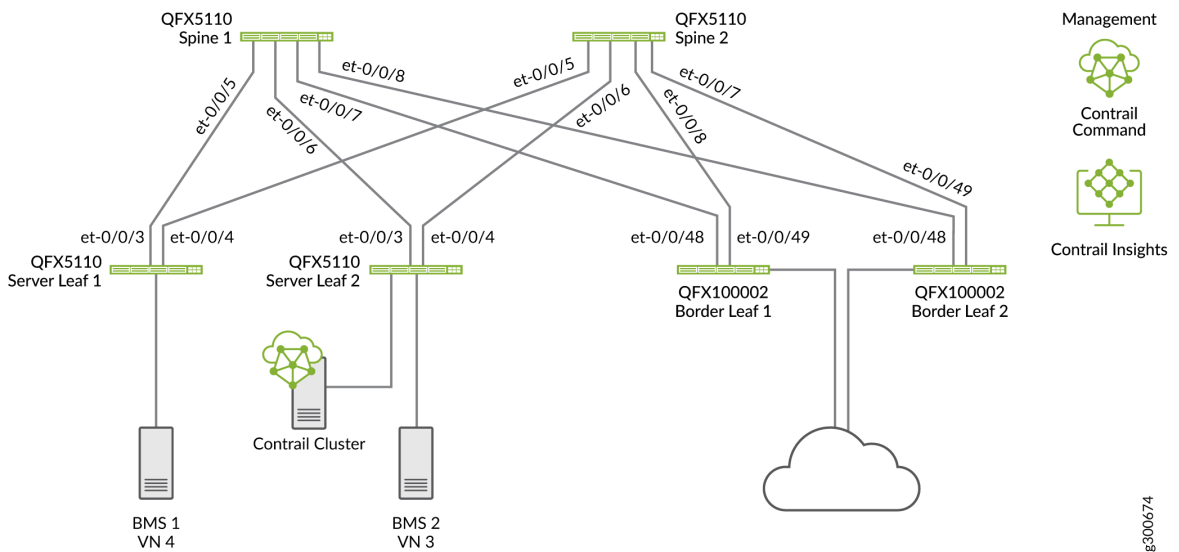
- [Figure 7 on page 22](#) shows the centrally-routed bridging topology.

Figure 7: Centrally-Routed Bridging Data Center



- [Figure 8 on page 22](#) shows the edge-routed bridging topology.

Figure 8: Edge-Routed Bridging Data Center



The Contrail-based servers (Contrail Command, controller, compute, and CSN) help to discover the data center network, create role-based device configurations (such as spine and leaf configurations), push them to the fabric devices, associate the servers and virtual machines with the network, provide switching and routing services, and coordinate with Contrail Insights (formerly known as AppFormix) to monitor and maintain the network. In summary, the components work together to simplify the onboarding, provisioning, operation, and maintenance of your data center network.

Software Summary

Table 2 on page 23 summarizes the software components that we used in this reference design.

Table 2: Reference Design Software Summary

Device	Software
Junos Release	Junos OS Release 18.4R2-S5
Contrail Command	2008

RELATED DOCUMENTATION

| [Contrail Enterprise Multicloud Components](#) | 10

Create a Greenfield Deployment For a New Data Center Network

IN THIS SECTION

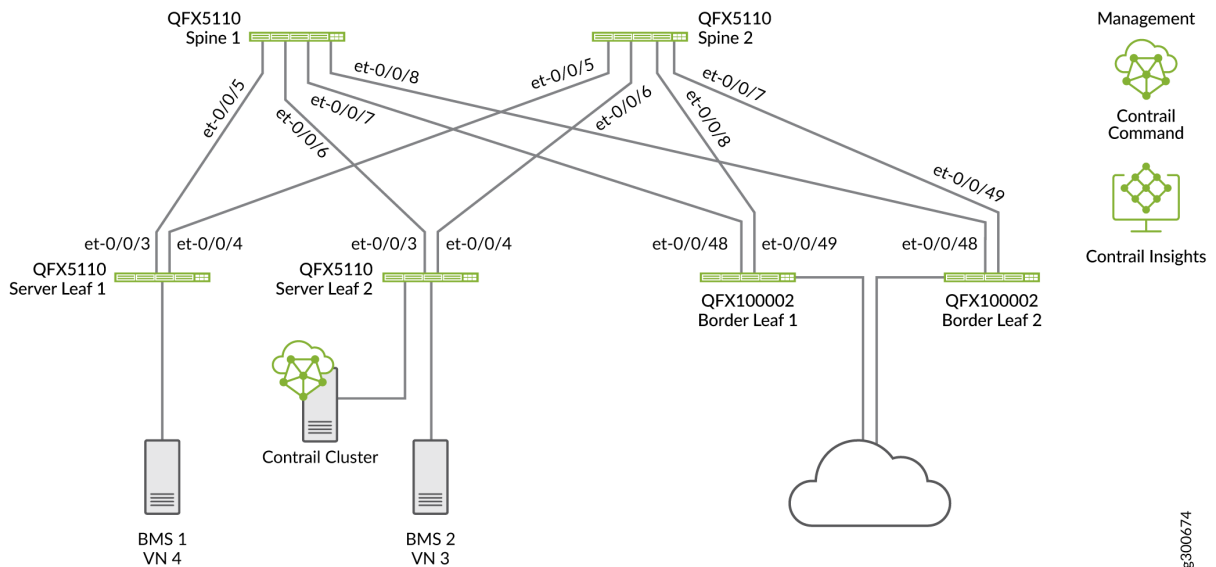
- [Before You Begin](#) | 24
- [Creating the New Fabric and Discovering Devices](#) | 27
- [Assigning Roles to Devices](#) | 31

- Applying the Role-Based Configurations to the New Fabric Devices | 31

This section shows how to perform zero-touch provisioning to build a new data center fabric from scratch (sometimes called a *greenfield deployment*). To do so, we are using Contrail Command, the user interface for CEM.

Figure 9 on page 24 shows the edge-routed bridging topology that we will use in this example.

Figure 9: Greenfield Deployment on Edge-Routed Bridging Topology



Before You Begin

IN THIS SECTION

- Information to Obtain | 25
- Cable Your Devices | 25

- Cable Your Management Network | 25
- Install Contrail Software | 25
- Create YML File | 26
- Put Fabric Devices in a Factory-Default State | 26

Before you begin building a new fabric, you need to do a few tasks.

Information to Obtain

- IP address ranges for your management network, fabric interfaces, and loopback interfaces.
- Autonomous system (AS) number for the iBGP fabric overlay
- AS number range for eBGP in the fabric underlay.
- Serial numbers of the devices in your fabric.

You can use 4-byte AS numbers. To do so, **select Infrastructure > Cluster > Advanced Options**. Then select the pencil to edit the system configuration. Changing this value to enabled causes all BGP sessions to use 4-byte ASNs.

Cable Your Devices

Connect the interfaces between the fabric devices. Make sure to connect all leaf devices to all spine devices, and all spine devices to all leaf devices.

Do not connect similar devices to each other. For example, do not connect a cable between one leaf device and another leaf device, nor between two spine devices.

Cable Your Management Network

Cable the management network including all of the devices that will be in the data center fabric. The resulting out-of-band (OoB) management network should include the fabric devices and the Contrail Cluster components.

Install Contrail Software

You need to connect a server to your management network and install Contrail software. See [Installing Contrail Command](#) and [Installing a Contrail Cluster Using Contrail Command](#).

Create YML File

You must create a file in .yml format that is uploaded to Contrail as part of the process of creating a fabric. You can use Contrail Command to first download a generic template to edit with the specifics of your installation.

The .yml file must contain the serial numbers of all devices to which ZTP is performed.

You can also include hostnames in your file, and the hostnames are assigned for your devices during ZTP. If you don't specify hostnames, Contrail Software uses the serial number of the device.

You also have the option to include loopback addresses and the ASN of the underlay.

There is a field called `to_ztp` that you can set to true or false. You can use it to include or ignore devices in the ZTP workflow.

A device information .yml file is in the following format:

```
device_to_ztp:
  - serial_number: 'WS3718030113'
    hostname: 'DC1-Access-Leaf-1'
    supplemental_day_0_cfg: ["Interface-Speed", "Base-Config"]
    device_functional_group: 'Lean-Spine-with-Route-Reflector'
    loopback_ip: "172.17.254.241"
    underlay_asn: "64641"
    mgmt_ip: "10.87.110.111"
    to_ztp: "True/False"
```

You can also specify a JunOS image release version, and devices will be upgraded to that version during ZTP.

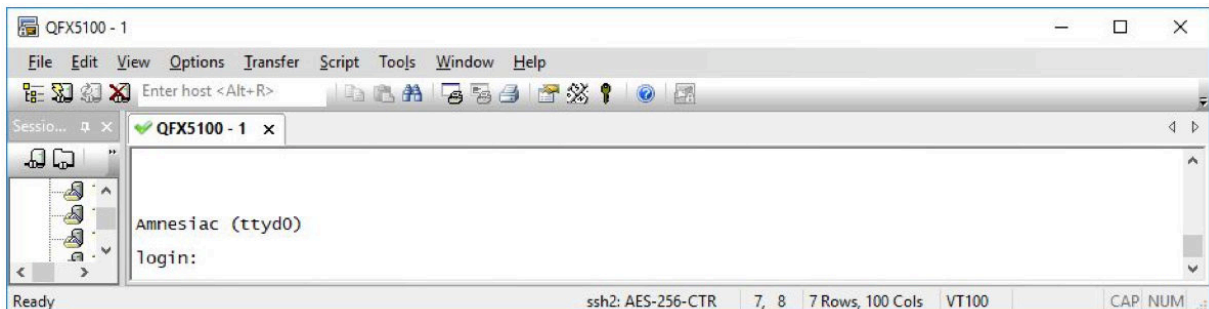
Put Fabric Devices in a Factory-Default State

Make sure the fabric devices have not been configured and are in a zeroized, factory-default state and bring them online.

To place devices in a factory-default state, enter the `request system zeroize` command at the Junos OS CLI.

Junos OS devices display `Amnesiac` on the login screen when in the proper state.

Figure 10: Junos OS in Zeroized State



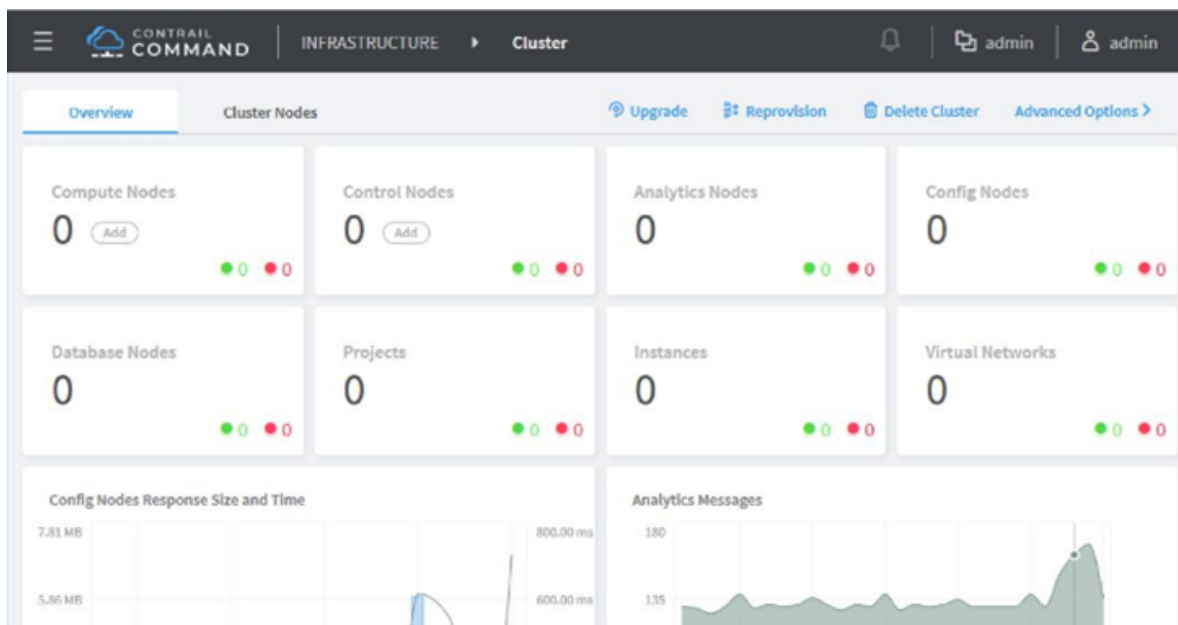
Creating the New Fabric and Discovering Devices

Once you complete the tasks in ["Before You Begin" on page 24](#) you can use zero-touch provisioning to create a new data center fabric and launch the device discovery process. To begin:

1. Open a web browser, navigate to the Contrail Command URL, enter your user name and password, and click **Log in**.

The format for the Contrail Command URL is `https://contrail-command-server-ip-address:9091`. 9091 is the port that gives you access to Contrail Command.


Contrail Command displays a status dashboard as the home page.



2. Navigate to **Infrastructure > Fabrics** and click **Create**.

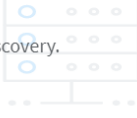
Select provisioning option

New Fabric



Wizard takes you through deployment of new devices which require discovery, zero touch provisioning(ZTP) and complete configuration.

Existing Fabric



Import existing deployed devices by discovery.

Cancel
Provision

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

4. Configure the following fields:

Field	Value used in this example
Name	DC1
Device credentials	*****
Overlay ASN (iBGP)	64512
Device Info	Upload.yml
Node profiles	Use the default, which enables all node profiles.
VLAN-ID Fabric-Wide Significance	Box is checked
Underlay ASNs (eBGP)	65501-65509
Management subnets	<ul style="list-style-type: none"> • CIDR: 10.1.1.0/24 • Gateway: 10.1.1.254
Fabric subnets (CIDR)	10.10.0.0/24


(Continued)

Field	Value used in this example
Loopback subnets (CIDR)	10.0.0.0/24

5. Click **Next**. The device discovery process begins.

The device discovery process discovers devices, physical interfaces, and logical interfaces. Expect this process to take 10 minutes or more to complete.

Device discovery progress



```
Tue Oct 08 2019 15:38:44 GMT-0400 (Eastern Daylight Time)
Starting execution for job template
"fabric_onboard_template" and execution id
"1570563519169_74b01af9-0e39-4bb4-aa72-36cf5f52c4c7"

Tue Oct 08 2019 15:38:52 GMT-0400 (Eastern Daylight Time)
Successfully onboarded fabric 'DC1'

Tue Oct 08 2019 15:39:04 GMT-0400 (Eastern Daylight Time)
Created DHCP and TFTP configuration

Tue Oct 08 2019 15:39:07 GMT-0400 (Eastern Daylight Time)
```

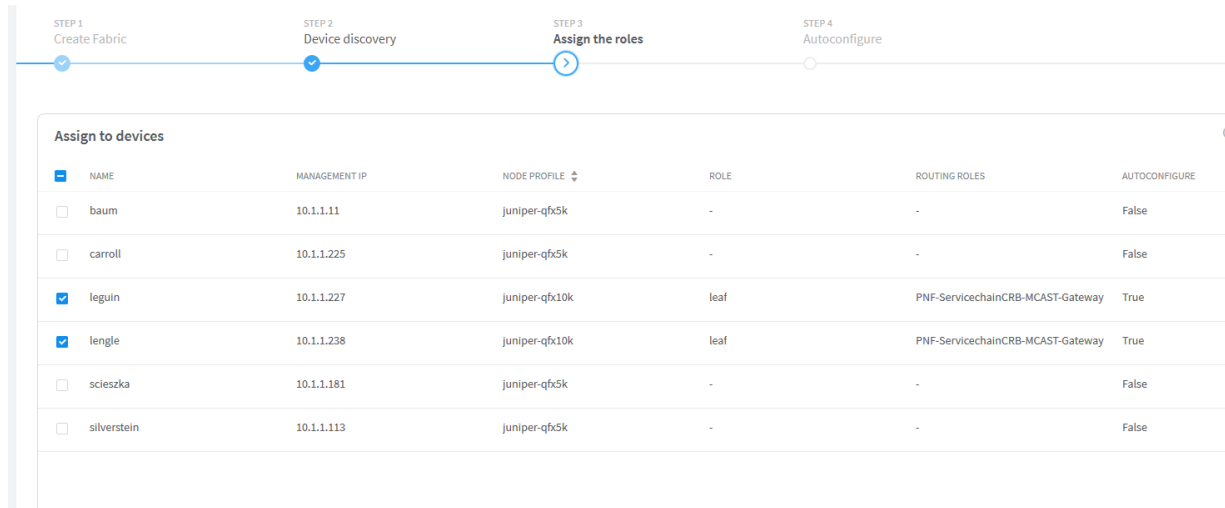
6. When the device discovery process is complete, click **Next** to begin assigning roles to your onboarded fabric devices.

Assigning Roles to Devices

After the new fabric devices are discovered, you need to assign the roles that the devices will perform in the fabric. Assigning roles to devices tailors the data center design and determines whether there is distributed or centralized routing.

To assign device roles:

Put a check in the box next to the device or devices for which you want to assign roles.



The screenshot shows a progress bar at the top with four steps: STEP 1 Create Fabric, STEP 2 Device discovery, STEP 3 Assign the roles (highlighted with a blue circle and arrow), and STEP 4 Autoconfigure. Below the progress bar is a table titled 'Assign to devices' with the following columns: NAME, MANAGEMENT IP, NODE PROFILE, ROLE, ROUTING ROLES, and AUTOCONFIGURE. The table contains seven rows of device information, with checkboxes in the first column indicating which devices have roles assigned.

<input type="checkbox"/>	NAME	MANAGEMENT IP	NODE PROFILE	ROLE	ROUTING ROLES	AUTOCONFIGURE
<input type="checkbox"/>	baum	10.1.1.11	juniper-qfx5k	-	-	False
<input type="checkbox"/>	carroll	10.1.1.225	juniper-qfx5k	-	-	False
<input checked="" type="checkbox"/>	leguin	10.1.1.227	juniper-qfx10k	leaf	PNF-ServicechainCRB-MCAST-Gateway	True
<input checked="" type="checkbox"/>	lengle	10.1.1.238	juniper-qfx10k	leaf	PNF-ServicechainCRB-MCAST-Gateway	True
<input type="checkbox"/>	scieszka	10.1.1.181	juniper-qfx5k	-	-	False
<input type="checkbox"/>	silverstein	10.1.1.113	juniper-qfx5k	-	-	False

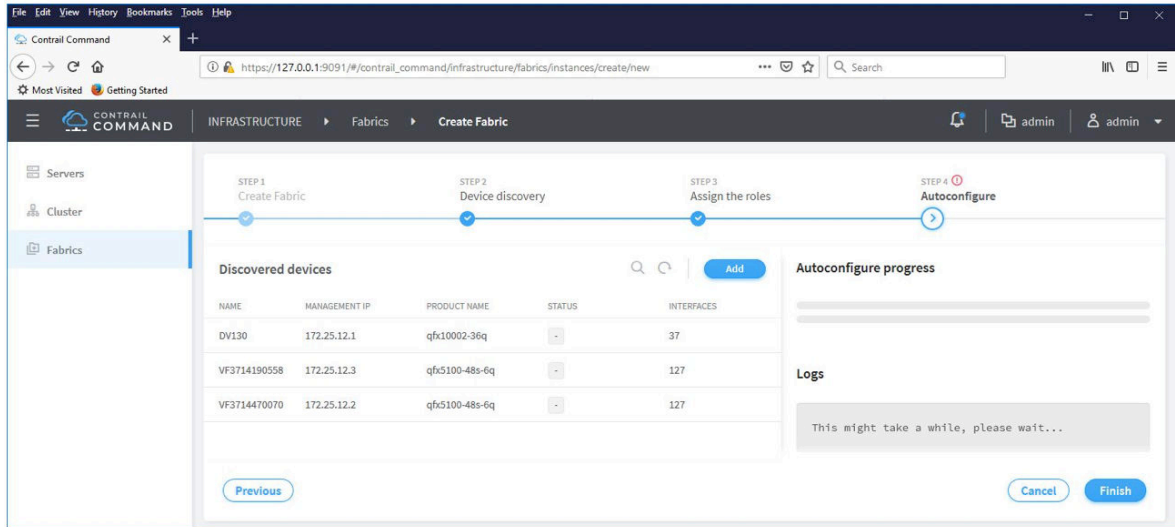
See "[Device Roles](#)" on page 14 for information about configuring roles.

Applying the Role-Based Configurations to the New Fabric Devices

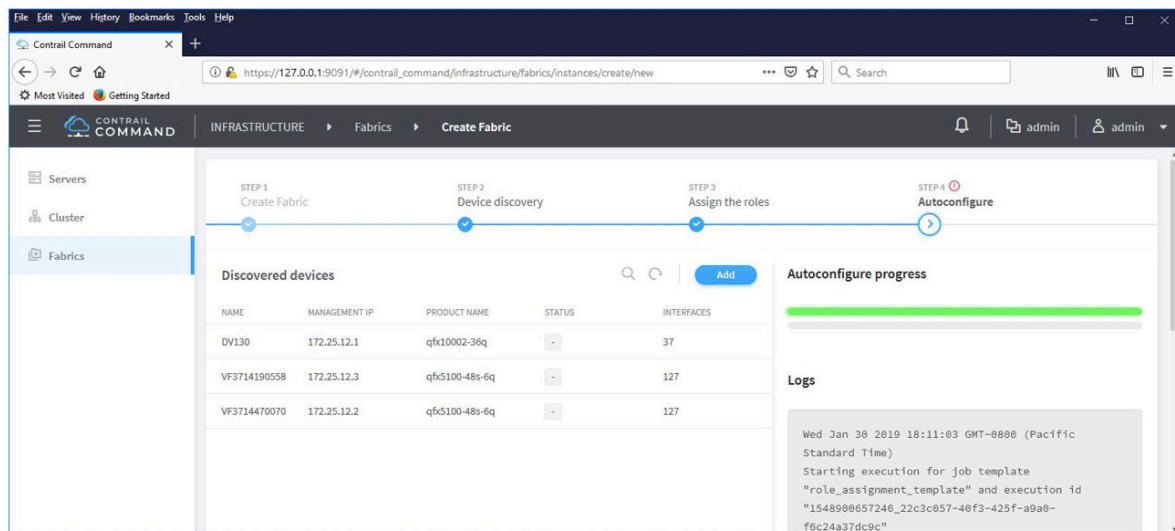
After you have assigned roles to the fabric devices, it is time to generate role-based configurations and push them to the devices. The autoconfigure process handles this task and simplifies the process of configuring the fabric devices.

To autoconfigure the fabric devices with their role-based configurations:

1. Click **Autoconfigure**.

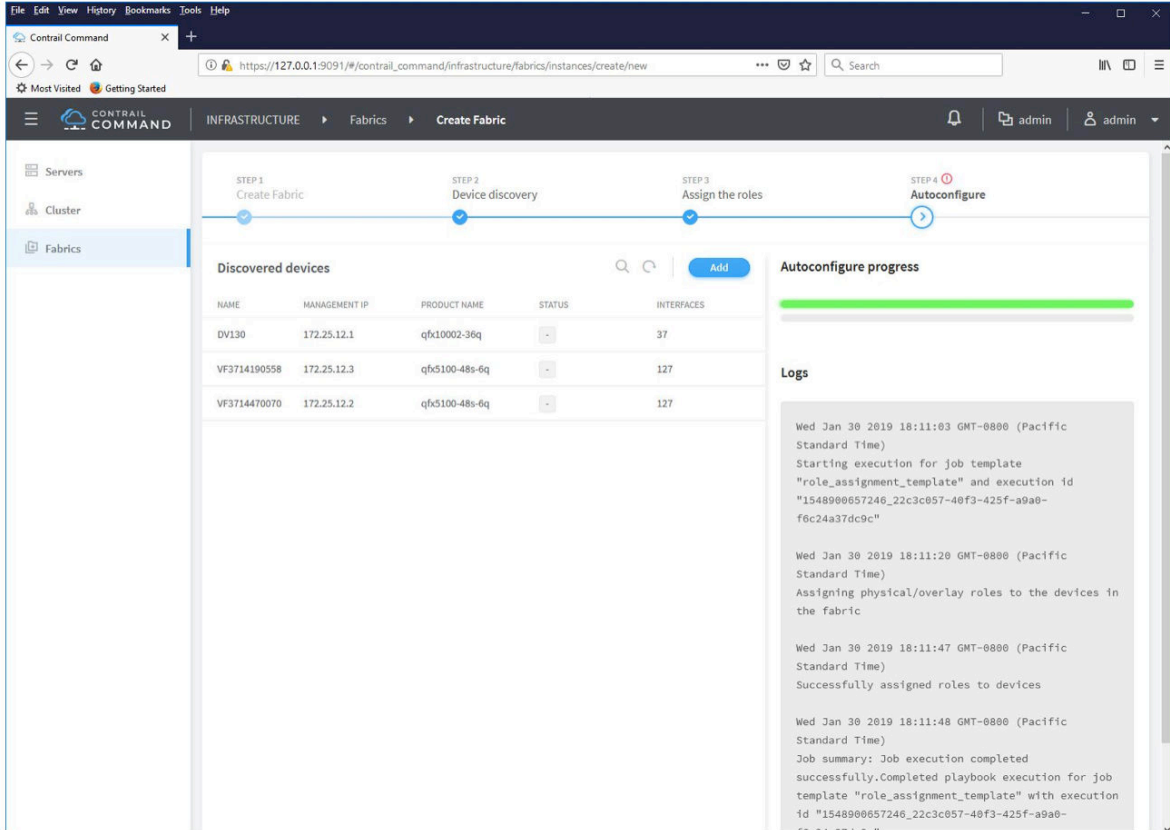


2. Monitor the status of the autoconfiguration process. The **Logs** section of the screen and the **Autoconfigure progress** status bar display the progress of this process.

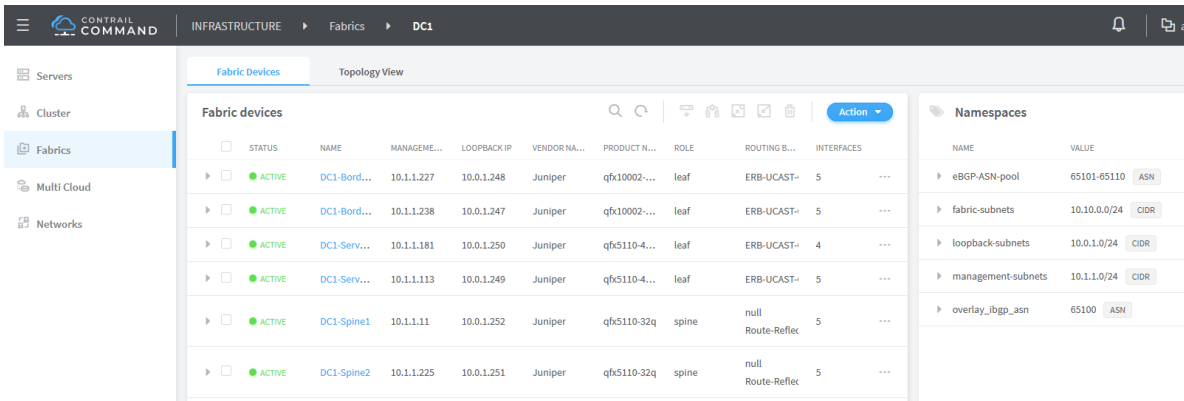


3. The autoconfiguration process completes when the device configurations are pushed to each fabric device based on their role.

When the **Autoconfigure progress** bar turns green and **Job execution completed successfully** appears in the **Logs** section (as shown below), you'll know that the process is done.



4. On the resulting screen, you can view the completed status of the new fabric. This includes the subnets for the fabric devices, loopback interfaces, and management network; along with the device roles and interfaces. To navigate to this page manually, go to **Infrastructure > Fabrics > Fabric Name**.



Create a Brownfield Deployment to Add an Overlay to an Existing IP Fabric

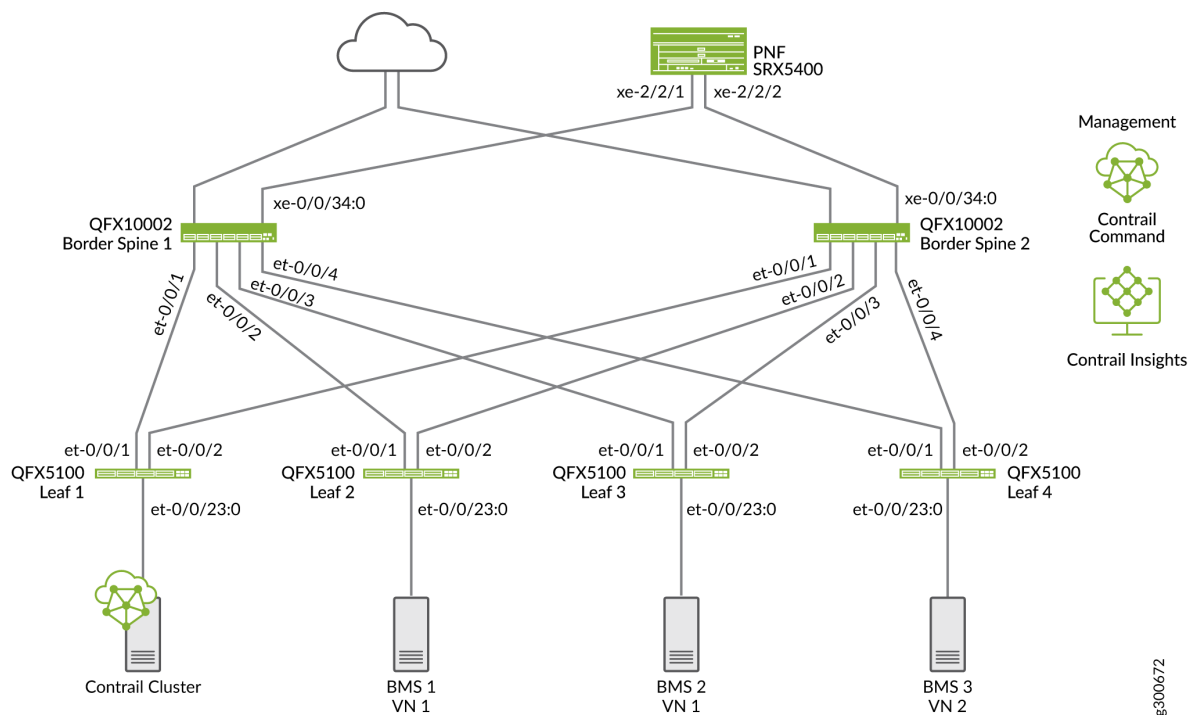
IN THIS SECTION

- Before You Begin | 35
- Adding an Existing Underlay into a Fabric and Discovering Devices | 35

When you add an overlay onto an existing data center network (sometimes called a brownfield deployment), you need to make sure the IP fabric is fully in place.

We are adding an overlay to a centrally-routed bridging (CRB) fabric as shown in figure [Figure 11](#) on [page 34](#).

Figure 11: Centrally-Routed Bridging IP Fabric



Once the underlay is in place, Contrail Command does the following to add the overlay:

- Discovery of the underlay (devices, interfaces, and management network)
- BGP configuration and EVPN-VXLAN baselined for the overlay based on configured device roles.

Before You Begin

The brownfield overlay procedure assumes that the following are established before you provision the overlay.

- Management network
- Hostname and router ID
- Remote access to fabric devices using SSH or NETCONF
- IP addresses configured on all the fabric interfaces
- Physical interfaces with LLDP between fabric devices and an MTU of at least 2000
- Loopback interfaces with IP addresses
- Underlay routing protocols

For the most successful results, we recommend that you use EBGP for the underlay and configure it as follows:

- Configure each spine and leaf device with its own AS number
- EBGP peering between all fabric devices (using local-as)
- EBGP policy to advertise BGP and direct and connected routes

It is considered good practice to tag routes with a community based on local EBGP AS number

- Routing information base (RIB) and forwarding information base (FIB) multipath with per-packet load balancing and fast reroute functionality enabled.

For more information about configuring an IP fabric, see *IP Fabric Underlay Network Design and Implementation* in the *Data Center Fabric Architecture Guide*.

Adding an Existing Underlay into a Fabric and Discovering Devices

1. Open a Web browser, navigate to the Contrail Command URL, enter your user name and password, and click Log in.

The format for the Contrail Command URL is `https://contrail-command-server-ip-address:9091`. 9091 is the port that gives you access to Contrail Command.

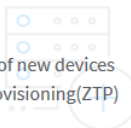
2. Navigate to **Infrastructure > Fabrics** and click **Create**.

The provision option box appears.

Select provisioning option

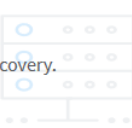
New Fabric

Wizard takes you through deployment of new devices which require discovery, zero touch provisioning (ZTP) and complete configuration.



Existing Fabric

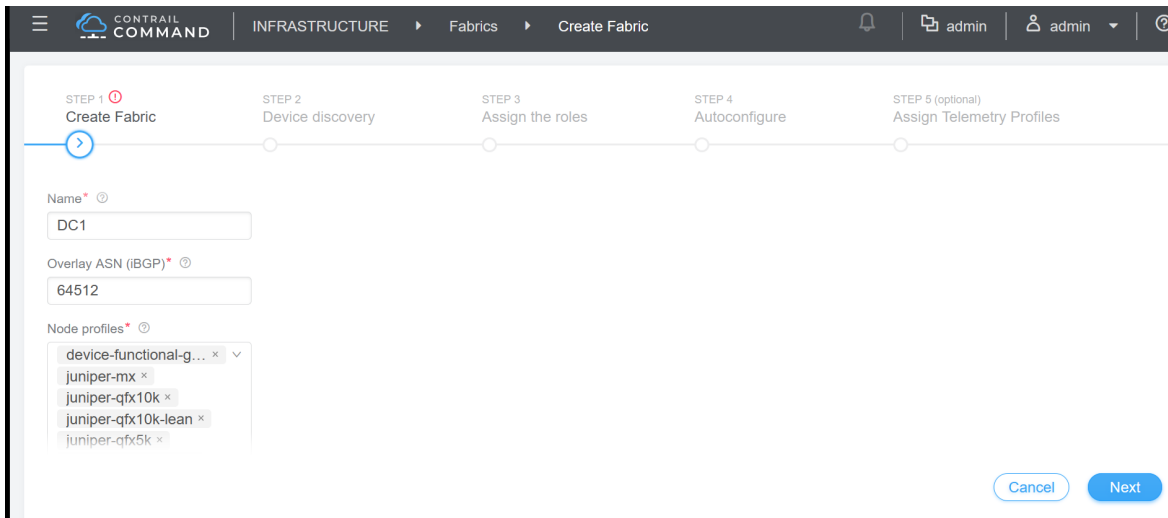
Import existing deployed devices by discovery.



Cancel
Provision

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

The Create Fabric screen displays.



4. Fill in the following fields.

Field	Value Used in This Example
Name	DC1

(Continued)

Field	Value Used in This Example
Overlay ASN (IBGP)	65100
Node Profiles	Default, which selects all device types
Disable VLAN-VN Uniqueness Check	Box is unchecked
VLAN-ID Fabric-Wide Significance	Box is checked
Device credentials	Username: lab Password: *****
Management subnets	CIDR: 10.1.1.0/27
Loopback Subnets	CIDR:10.0.1.0/24

- Click **Next**, and the Device Discovery process begins.

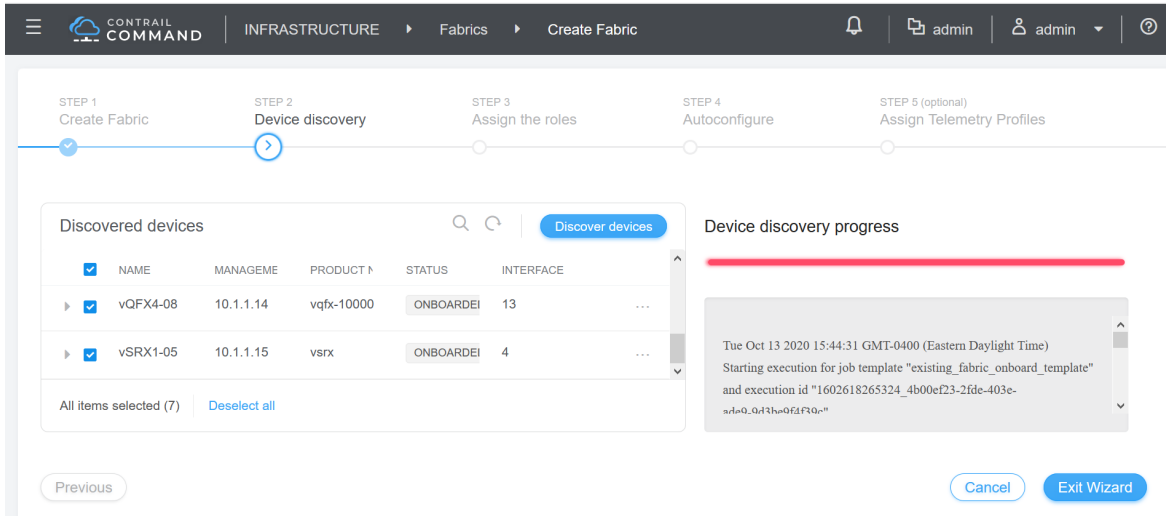
The screenshot shows the Contrail Command interface during the 'Device discovery' step. The breadcrumb navigation is 'INFRASTRUCTURE > Fabrics > Create Fabric'. The progress bar indicates that 'STEP 2 Device discovery' is the current step. Below the progress bar, there is a table of discovered devices and a progress indicator.

NAME	MANAGEMENT	PRODUCT	STATUS	INTERFACE
vQFX3-07	10.1.1.13	vqfx-10000	ONBOARDED	13
vQFX2-06	10.1.1.12	vqfx-10000	ONBOARDED	13

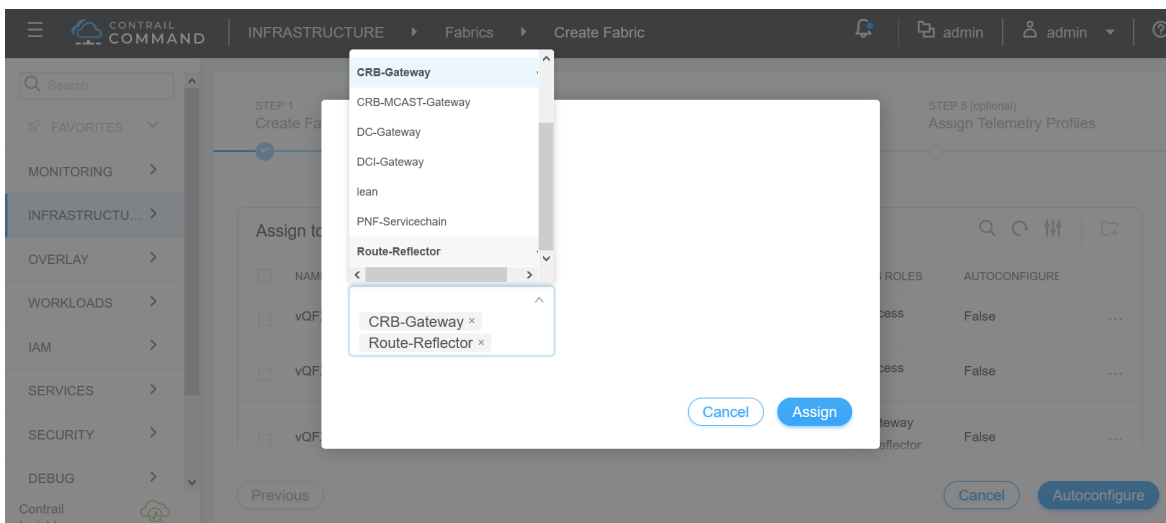
Device discovery progress

The Oct 13 2020 15:04:17 GMT-0400 (Eastern Daylight Time)
Starting execution for job template "existing_fabric_onboard_template" and execution id "1602615850748_931ae707-7b18-4e2c-9377-f6eb3332c600"

- After the new fabric devices are discovered, the Assign the roles screen displays. You need to assign the roles that the devices will perform in the fabric.



7. Put a check in the box next to the device or devices for which you want to assign roles. To save time, check the boxes for more than one device to assign the same role to multiple devices at once.
8. Next to the spine devices, select **Assign Roles**.
9. Add the following roles to the spine devices and click **Assign**.



10. Assign the CRB-Access role to the leaf devices and click **Assign**.
See "[Device Roles](#)" on page 14 for information about configuring roles.
11. When you are done assigning roles, click **Autoconfigure** to generate role-based configurations.
12. When the autoconfiguration is complete click **Finish**.
On the resulting screen, you can view the completed status of the fabric.

RELATED DOCUMENTATION

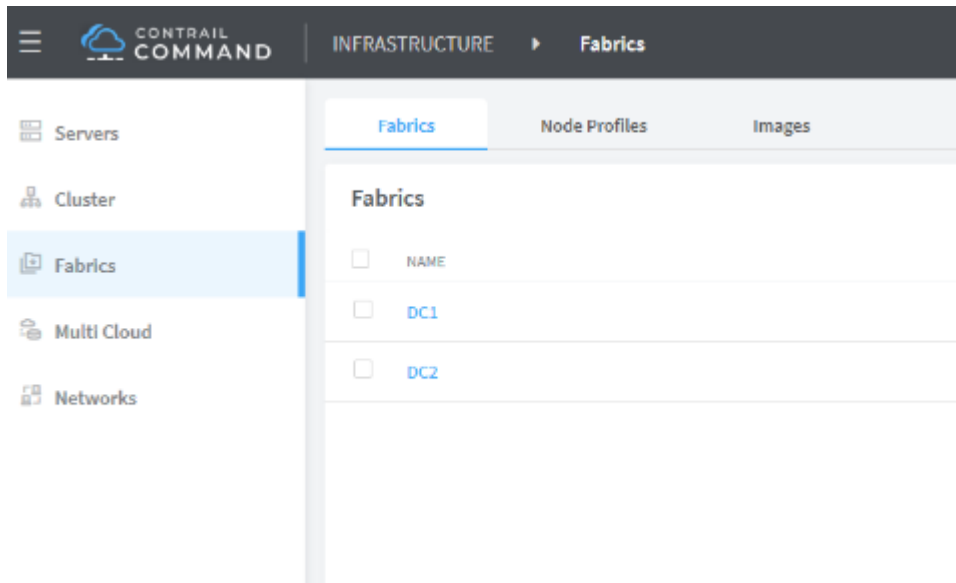
[Existing IP Fabric](#) | 13

Selective Onboarding of a Device

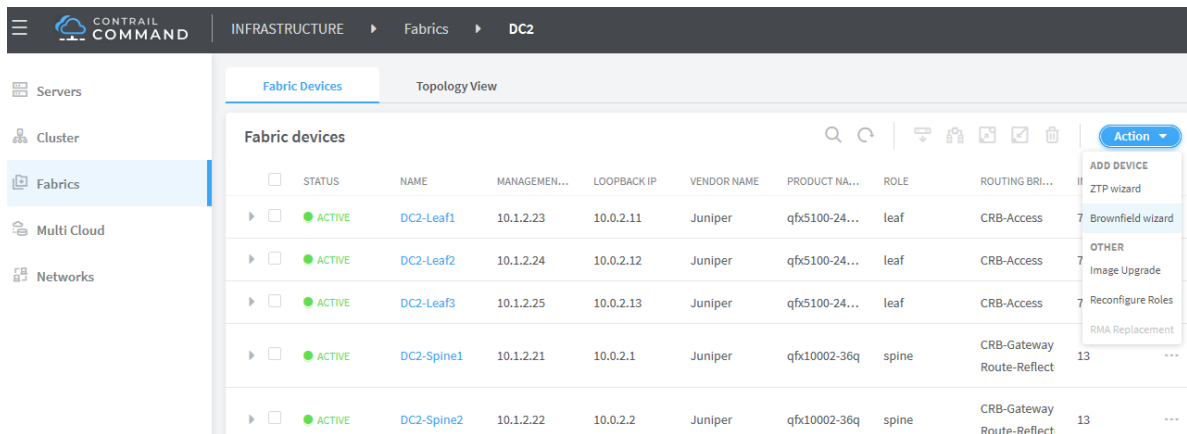
In this procedure, we will add a leaf device to the DC2 data center fabric.

To onboard a device:

1. Select **Fabrics**, and then select the fabric to which you want to add the leaf device.



2. Select **Action > Brownfield Wizard**.



The device configuration screen appears.

3. Fill in the following fields and click Next..

Field	Value Used in This Example
Name	DC1
Overlay ASN (IBGP)	65100
Node Profiles	Default, which selects all device types
VLAN-ID Fabric-Wide Significance	Box is checked
Device credentials	Username: lab Password: *****
Management subnets	CIDR: 10.1.2.0/24

4. Click **Next** and then click **Finish**.

The device discovery process begins.

The screenshot shows the 'Device discovery' step in the 'Create Fabric' process. The interface includes a navigation pane on the left with options like Servers, Cluster, Fabrics, Multi Cloud, and Networks. The main area is divided into two sections: 'Discovered devices' and 'Device discovery progress'.

NAME	MANAGEMENT IP	PRODUCT NAME	STATUS	INTERFACES
DC2-Leaf1	10.1.2.23	qfx5100-24q-2p	ONBOARDED	7
DC2-Leaf2	10.1.2.24	qfx5100-24q-2p	ONBOARDED	7
DC2-Leaf3	10.1.2.25	qfx5100-24q-2p	ONBOARDED	7
DC2-Leaf4	10.1.2.26	qfx5100-24q-2p	DISCOVERED	0
DC2-Spine1	10.1.2.21	qfx10002-36q	ONBOARDED	13
DC2-Spine2	10.1.2.22	qfx10002-36q	ONBOARDED	13

The 'Device discovery progress' section shows a log of events:

```

Wed Oct 23 2019 12:58:12 GMT-0400 (Eastern Daylight Time)
Starting execution for job template
"existing_fabric_onboard_template" and execution
id "1571849887929_6eebce71-b1f8-423f-
8793-9bf6959401c4"

Wed Oct 23 2019 12:58:19 GMT-0400 (Eastern Daylight Time)
Successfully onboarded fabric 'DC2'

Wed Oct 23 2019 12:58:32 GMT-0400 (Eastern Daylight Time)
Prefix(es) to be discovered: 10.1.2.26/32

Wed Oct 23 2019 12:58:46 GMT-0400 (Eastern Daylight Time)

```

5. Configure **CRB-Access** as the role for the leaf device.

The screenshot shows the 'Assign Telemetry Profiles' step in the 'Create Fabric' process. A dropdown menu is open, showing the selection of 'CRB-Gateway' and 'Route-Reflector' roles. The interface includes a navigation pane on the left with options like FAVORITES, MONITORING, INFRASTRUCTURE, OVERLAY, WORKLOADS, IAM, SERVICES, SECURITY, and DEBUG. The main area is divided into two sections: 'Assign Telemetry Profiles' and 'Assign Telemetry Profiles'.

The dropdown menu shows the following options:

- CRB-Gateway
- CRB-MCAST-Gateway
- DC-Gateway
- DCI-Gateway
- lean
- PNF-Servicechain
- Route-Reflector

The selected roles are 'CRB-Gateway' and 'Route-Reflector'. The interface includes 'Cancel' and 'Assign' buttons.

6. Click **Assign**.

7. Click **AutoConfigure**.



Autoconfigure progress

Wed Oct 23 2019 13:01:32 GMT-0400 (Eastern Daylight Time)
Starting execution for job template "role_assignment_template" and execution id "1571850087974_ae0baf9d-37d5-499c-b5a9-6f98cf5f71ed"

Wed Oct 23 2019 13:01:37 GMT-0400 (Eastern Daylight Time)
Assigning physical/overlay roles to the devices in the fabric

Wed Oct 23 2019 13:01:39 GMT-0400 (Eastern Daylight Time)
Successfully assigned roles to devices

Wed Oct 23 2019 13:01:40 GMT-0400 (Eastern Daylight Time)

 Fabric Autoconfiguring job for DC2 has finished 

Cancel

Proceed to Servers Discovery

Finish

Configure Virtual Networks for Multi-tenant Service Operations

IN THIS SECTION

- [Create Virtual Networks | 44](#)
- [Assign Interfaces to VLANs with Virtual Port Groups | 46](#)
- [Enable Layer 3 Routing on Virtual Networks Using Logical Routers | 48](#)
- [Verify Your Virtual Network Configuration | 50](#)

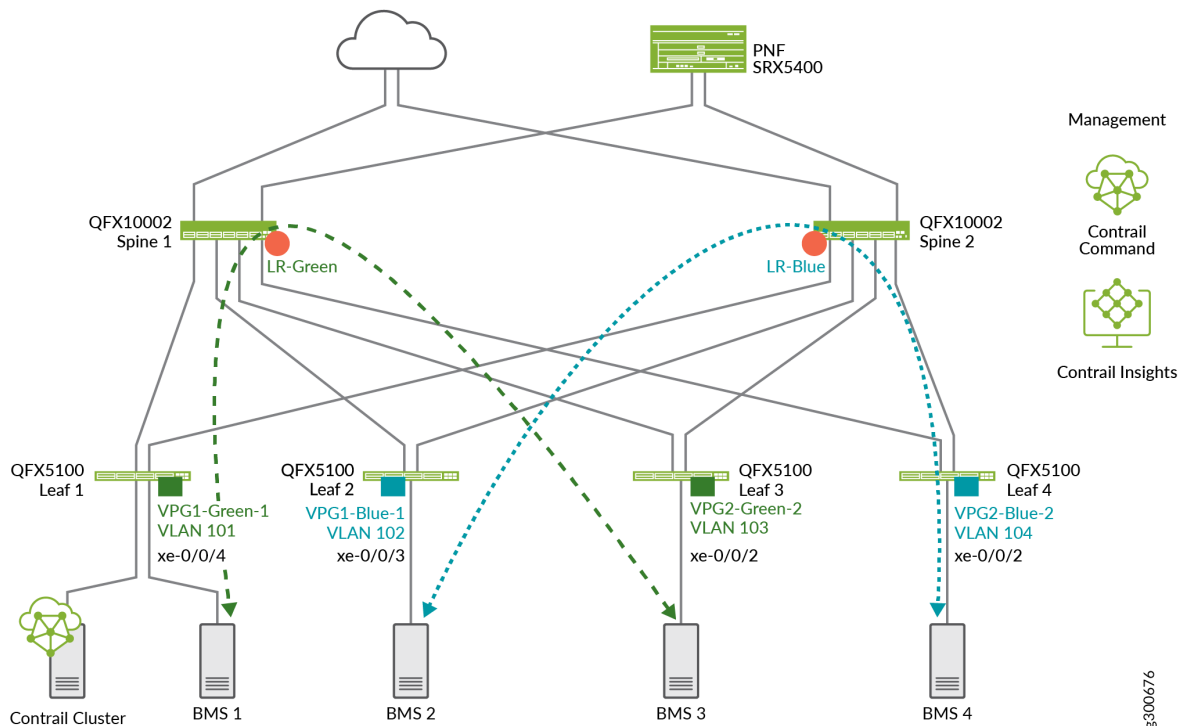
This section shows how to configure Layer 2 and Layer 3 multi-tenant network services on two virtual networks, blue and green as shown in [Figure 12 on page 44](#).

This is a typical day one operation that provides virtual network connectivity that isolates traffic between the virtual networks while allowing bridged or routed connectivity for devices in the same virtual network.

To create the Green and Blue networks in Contrail Command, we will configure the following:

- Four virtual networks, two Green and two Blue
- Four VPGs to add the access interfaces to the servers
- Two Logical Routers (LRs) for inter-VN communication, one for the Green virtual network and one for the Blue virtual network

Figure 12: Green and Blue Virtual Networks

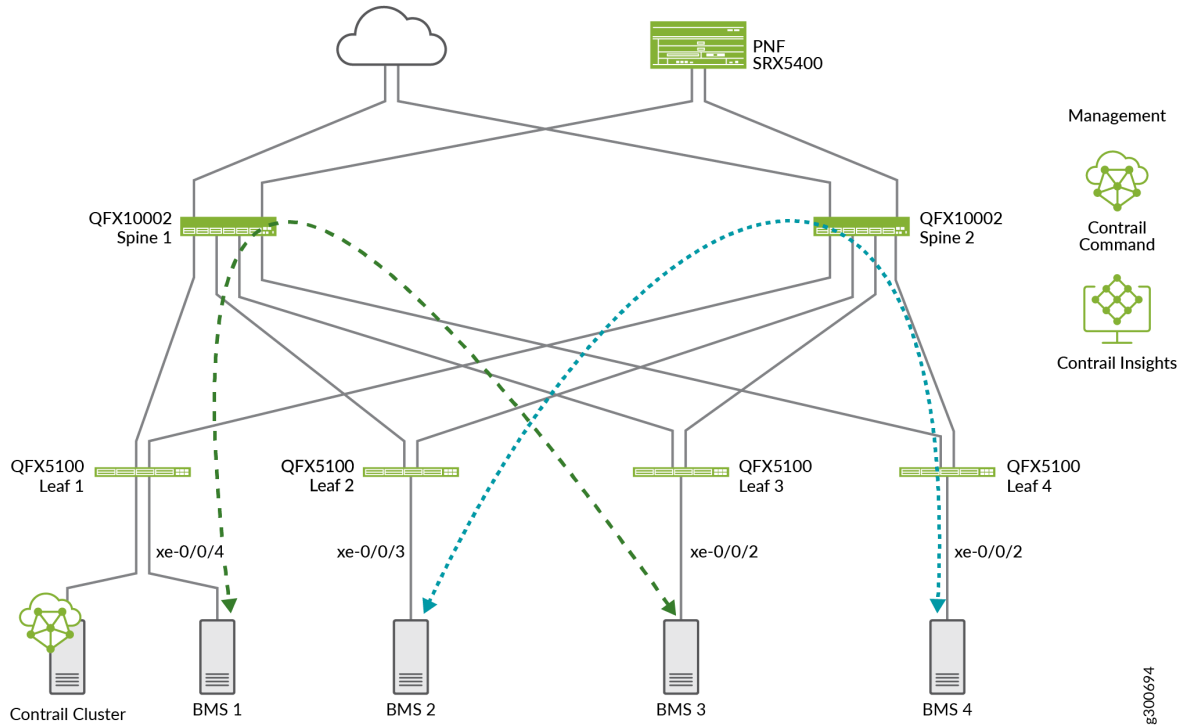


At this point we do not have communication between the green and blue networks. LRs cannot connect to other LRs. For inter-LR, or inter-tenant communication, you need to connect the LRs using service chaining. See ["Configure Service Chaining With PNF" on page 55](#).

Create Virtual Networks

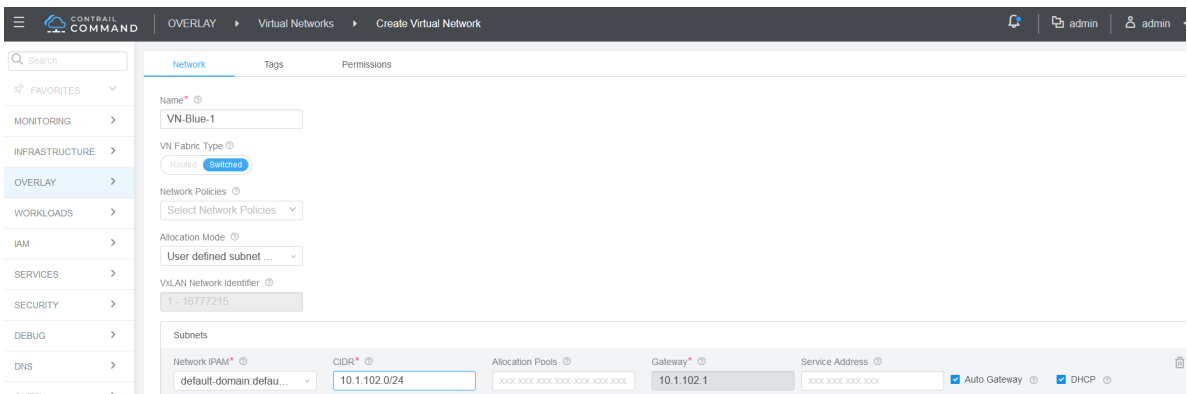
A virtual network in the Contrail environment allows hosts in the same network to communicate with each other. This is similar to assigning a VLAN to each host so that hosts on the same VLAN can reach each other.

In this section, we will create four virtual networks, two for the green network and two for the blue virtual network.



To configure a virtual network:

1. Navigate to **Overlay > Virtual Networks** and click **Create**.



2. Fill in the following fields to define four virtual networks. By default Contrail Networking uses the first available host ID in the subnet for that subnet's default gateway. As a result it's good practice to avoid assigning host ID 1 to VMs or BMSs.

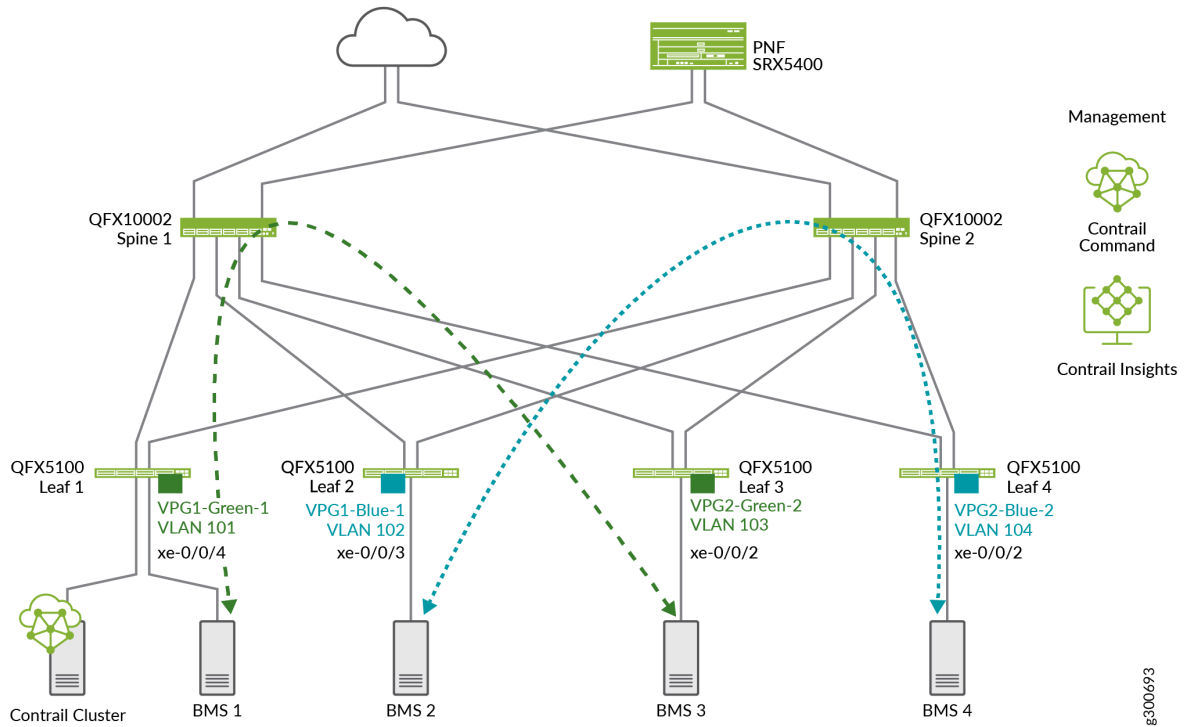
Name:	Allocation Mode	Subnets		
		Network IPAM	CIDR	Gateway
VN-Green-1	Default setting of "User defined subnet only"	Default-domain:default-project:default	10.1.101.0/24	10.2.4.1
VN-Green-2	Default setting of "User defined subnet only"	Default-domain:default-project:default	10.1.103.0/24	10.2.3.1
VN-Blue-1	Default setting of "User defined subnet only"	Default-domain:default-project:default	10.1.102.0/24	10.2.2.1
VN-Blue-2	Default setting of "User defined subnet only"	Default-domain:default-project:default	0.1.104.0/24	10.2.4.1

- When both virtual networks are created, the **Virtual Networks** screen displays. You will see that both the green and blue networks are available.

Assign Interfaces to VLANs with Virtual Port Groups

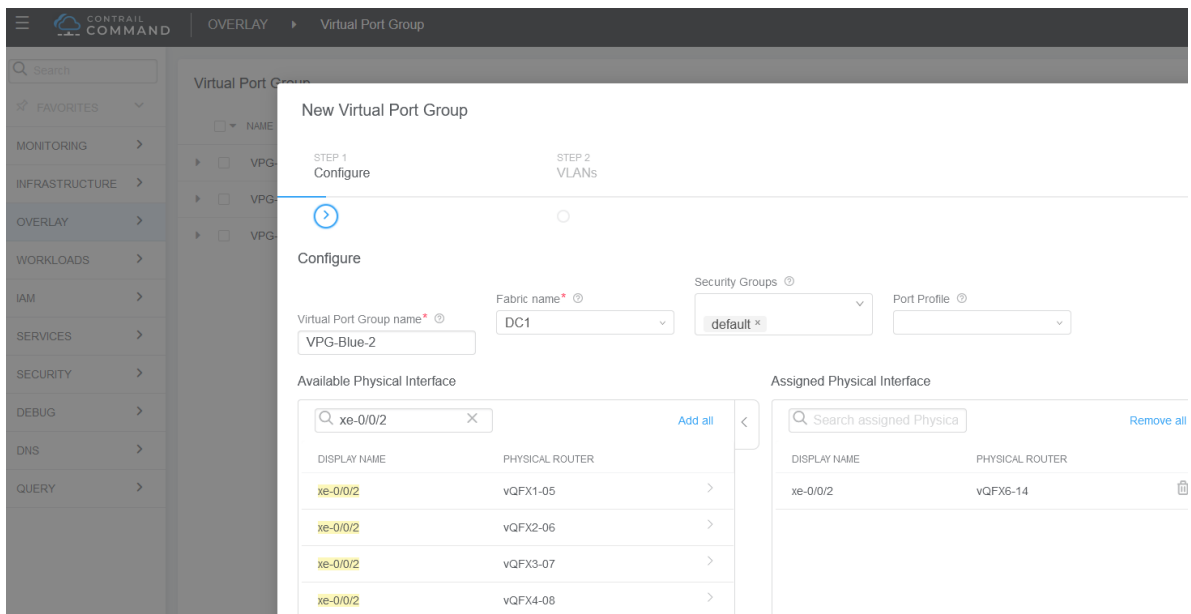
You configure VPGs to add interfaces to your virtual networks. In this section, we will add the access interfaces from the leaf devices to the servers as shown in [Figure 13 on page 47](#).

Figure 13: Adding VPGs to Virtual Networks



To create a VPG:

1. Navigate to **Overlay > Virtual Port Group** and click **Create**.



2. Create four VPGs with the values shown in the following table.

To assign a physical interface, find the interface under **Available Physical Interface**. There can be multiple pages of interfaces. To move an interface to the **Assigned Physical Interface**, click the > next to the interface.

Virtual Port Group Name	VPG1-Green-1	VPG2-Green-2	VPG1-Blue-1	VPG2-Blue-2
Fabric Name	DC1	DC1	DC1	DC1
Assigned Physical Interface	xe-0/0/4:0	xe-0/0/2:0	xe-0/0/3:0	xe-0/0/2:0

3. Click **Next**.

The screen to add VLANs appears.

4. To create VLANs on the VPGs, create the following VLANs.

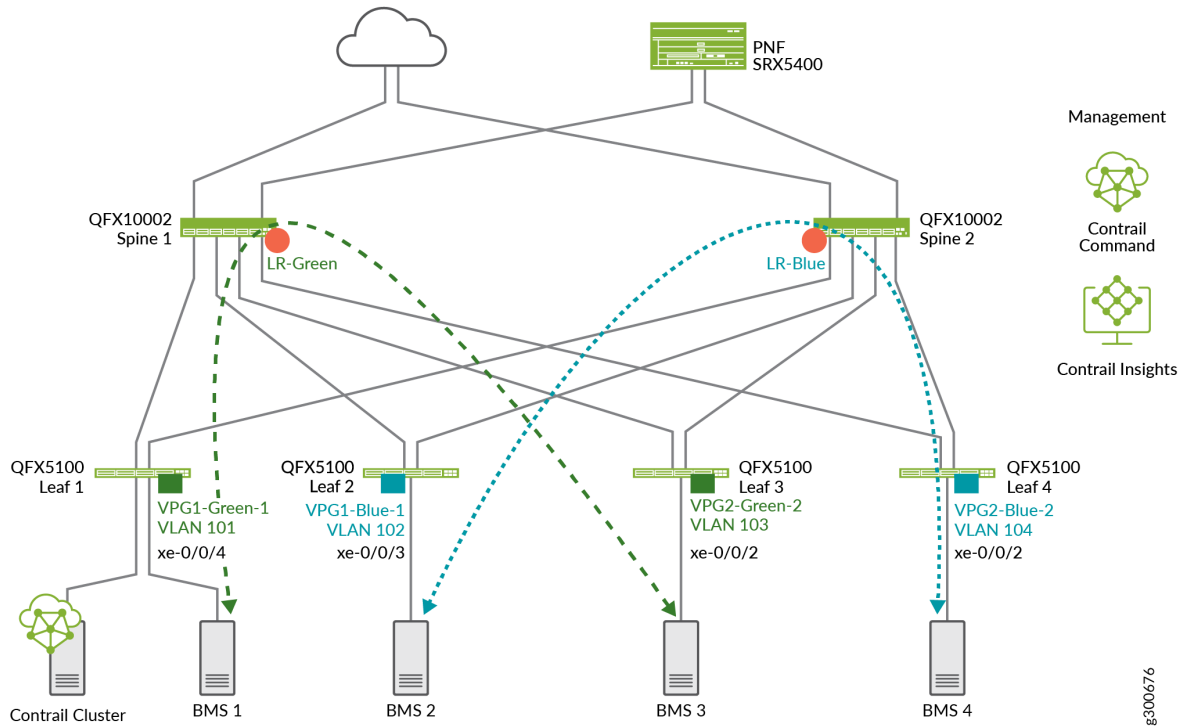
Virtual Network	VLAN IDs
VN-Green-1	101
VN-Green-2	103
VN-Blue-1	102
VN-Blue-2	104

Enable Layer 3 Routing on Virtual Networks Using Logical Routers

CEM uses logical routers (LRs) to enable routing on virtual networks. It does so by creating a VRF routing instance for each logical router with IRB interfaces on the spine devices. After CEM configures the devices, network traffic from the blue and green networks travels over a VXLAN tunnel from the leaf devices to the spine devices. At the spine devices, the traffic is routed at Layer 3.

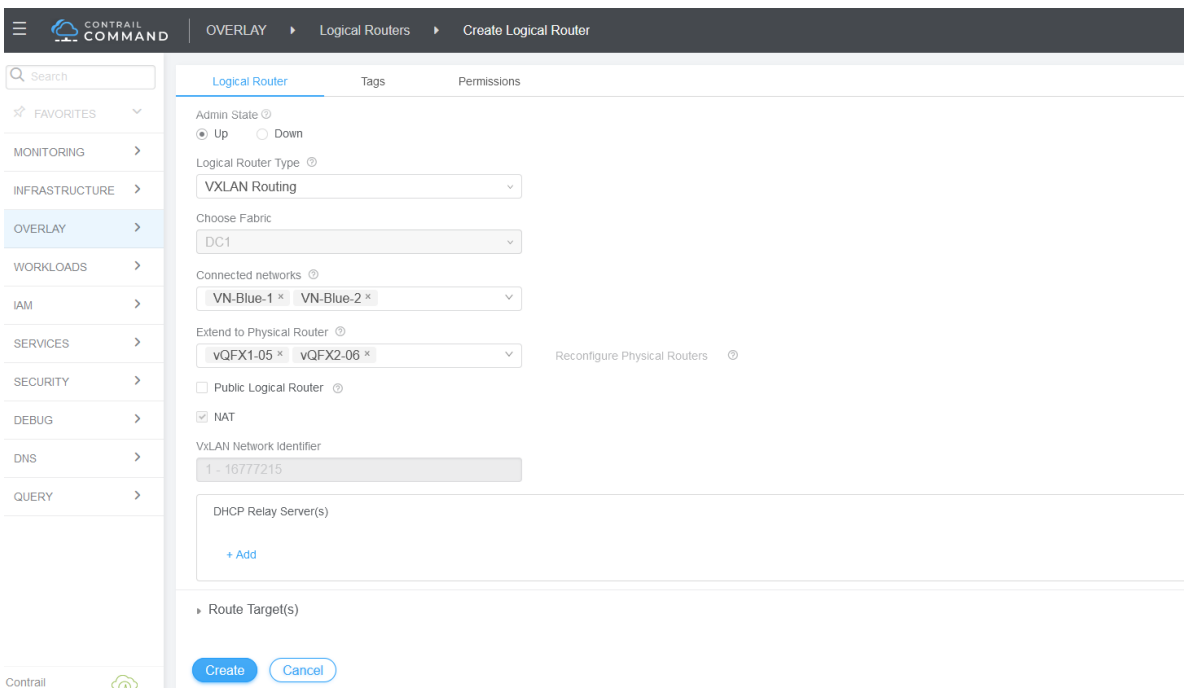
In this section, we will enable routing on the blue and the green virtual networks as shown in [Figure 14 on page 49](#).

Figure 14: Adding Logical Routers to the Virtual Networks



To configure the logical routers:

1. Navigate to **Overlay > Logical Routers**, and click **Create**.



2. Create two logical routers as shown in the following table:

Name	LR-Blue	LR-Green
Extend to Physical Router	DC2-Spine1	DC2-Spine1
	DC2-Spine2	DC2-Spine2
Logical Router Type	VXLAN Routing	VXLAN Routing
Connected Networks	Blue-1	Green-1
	Blue-2	Green-2

Verify Your Virtual Network Configuration

1. On a spine device, check that IRB interfaces are configured. There are two IRBs for each virtual network.

```

interfaces {
  irb {
    gratuitous-arp-reply;
    unit 11 {
      proxy-macip-advertisement;
      virtual-gateway-accept-data;
      family inet {
        address 10.1.104.5/24 {
          preferred;
          virtual-gateway-address 10.1.104.1;
        }
      }
      virtual-gateway-v4-mac 00:00:5e:01:00:01;
    }
    unit 10 {
      proxy-macip-advertisement;
      virtual-gateway-accept-data;
      family inet {
        address 10.1.102.5/24 {

```

```

        preferred;
        virtual-gateway-address 10.1.102.1;
    }
}
virtual-gateway-v4-mac 00:00:5e:01:00:01;
}
unit 13 {
    proxy-macip-advertisement;
    virtual-gateway-accept-data;
    family inet {
        address 10.1.101.5/24 {
            preferred;
            virtual-gateway-address 10.1.101.1;
        }
    }
    virtual-gateway-v4-mac 00:00:5e:01:00:01;
}
unit 14 {
    proxy-macip-advertisement;
    virtual-gateway-accept-data;
    family inet {
        address 10.1.103.5/24 {
            preferred;
            virtual-gateway-address 10.1.103.1;
        }
    }
    virtual-gateway-v4-mac 00:00:5e:01:00:01;
}
}
}
}

```

2. On a spine device, check that VLANs are configured.

```

vllans {
    bd-11 {
        description "Virtual Network - VN-Blue-2";
        vllan-id none;
        l3-interface irb.11;
        vxlan {
            vni 11;
        }
    }
}

```

```

bd-10 {
    description "Virtual Network - VN-Blue-1";
    vlan-id none;
    l3-interface irb.10;
    vxlan {
        vni 10;
    }
}
bd-13 {
    description "Virtual Network - VN-Green-1";
    vlan-id none;
    l3-interface irb.13;
    vxlan {
        vni 13;
    }
}
bd-14 {
    description "Virtual Network - VN-Green-2";
    vlan-id none;
    l3-interface irb.14;
    vxlan {
        vni 14;
    }
}
}

```

3. On a spine device, check that VRFs are configured, one for the green network and one for the blue network. Note that the IRB interfaces are added to the VRFs.

```

routing-instances {
    __contrail_LR-Blue_f25a81b3-41f0-4750-97cb-7fd87fc5a0bd {
        routing-options {
            rib __contrail_LR-Blue_f25a81b3-41f0-4750-97cb-7fd87fc5a0bd.inet6.0 {
                multipath;
            }
            static {
                route 172.16.0.15/32 discard;
            }
            multipath;
        }
        protocols {
            evpn {

```



```

        ip-prefix-routes {
            advertise direct-nexthop;
            encapsulation vxlan;
            vni 12;
            export type5_policy;
        }
    }
}
instance-type vrf;
interface lo0.1012;
interface irb.11;
interface irb.10;
vrf-import __contrail_LR-Blue_f25a81b3-41f0-4750-97cb-7fd87fc5a0bd-import;
vrf-export __contrail_LR-Blue_f25a81b3-41f0-4750-97cb-7fd87fc5a0bd-export;
}
__contrail_LR-Green_e11292e0-3abf-4e4c-a9b8-df84b148a2ec {
    routing-options {
        rib __contrail_LR-Green_e11292e0-3abf-4e4c-a9b8-df84b148a2ec.inet6.0 {
            multipath;
        }
        static {
            route 172.16.0.15/32 discard;
        }
        multipath;
    }
}
protocols {
    evpn {
        ip-prefix-routes {
            advertise direct-nexthop;
            encapsulation vxlan;
            vni 15;
            export type5_policy;
        }
    }
}
instance-type vrf;
interface lo0.1015;
interface irb.13;
interface irb.14;
vrf-import __contrail_LR-Green_e11292e0-3abf-4e4c-a9b8-df84b148a2ec-import;
vrf-export __contrail_LR-Green_e11292e0-3abf-4e4c-a9b8-df84b148a2ec-export;

```

```

    }
}

```

4. When you have finished your configuration, you can run ping between servers in the same virtual network. For example, run ping from BMS1 to BMS3 in the green network.

```

host@ix-centos-s3 ~]# ping 10.2.4.101

PING 10.2.4.101 (10.2.4.101) 56(84) bytes of data.
64 bytes from 10.2.4.101: icmp_seq=1 ttl=63 time=0.626 ms
64 bytes from 10.2.4.101: icmp_seq=2 ttl=63 time=0.627 ms
^C
--- 10.2.4.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.626/0.626/0.627/0.025 ms

```

5. Run ping from BMS2 to BMS4 in the blue network.

```

[root@ix-cn-centos-01 ~]# ping 10.1.104.101 -c 2
PING 10.1.104.101 (10.1.104.101) 56(84) bytes of data.
64 bytes from 10.1.104.101: icmp_seq=1 ttl=60 time=493 ms
64 bytes from 10.1.104.101: icmp_seq=2 ttl=60 time=304 ms

--- 10.1.104.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 304.216/398.664/493.113/94.450 ms

```

SEE ALSO

[Virtual Networks | 16](#)

[Virtual Port Groups | 17](#)

[Logical Routers | 19](#)

Configure Service Chaining With PNF

IN THIS SECTION

- [Service Chaining Using a PNF | 55](#)
- [Service Chaining Configuration Overview | 56](#)
- [Onboard an SRX Services Gateway as the PNF Device | 58](#)
- [Assign Device Roles for the PNF Device | 59](#)
- [Create a PNF Service Template | 60](#)

This section shows how to create Layer 3 PNF service chains for inter-LR traffic.

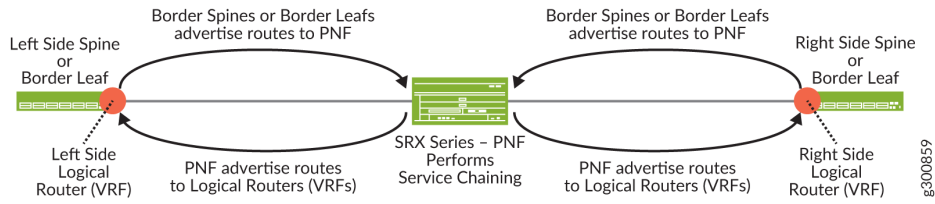
Service Chaining Using a PNF

Service Chaining provides security control and enforcement through a physical firewall on traffic between virtual networks that are attached to logical routers. By default, virtual networks attached to the same logical router can communicate only using Layer 3 routing. Virtual networks connected to different logical routers cannot communicate. Service chaining using a firewall (a physical network function) between the logical routers allows virtual networks on separate logical routers to communicate and to communicate in a secure way.

For CEM service chaining you insert a physical network function (PNF) device between two logical routers on a border spine or border leaf device. The PNF device allows for Layer 3 communication between the logical routers. Only Juniper SRX Services Gateways are supported as PNF devices.

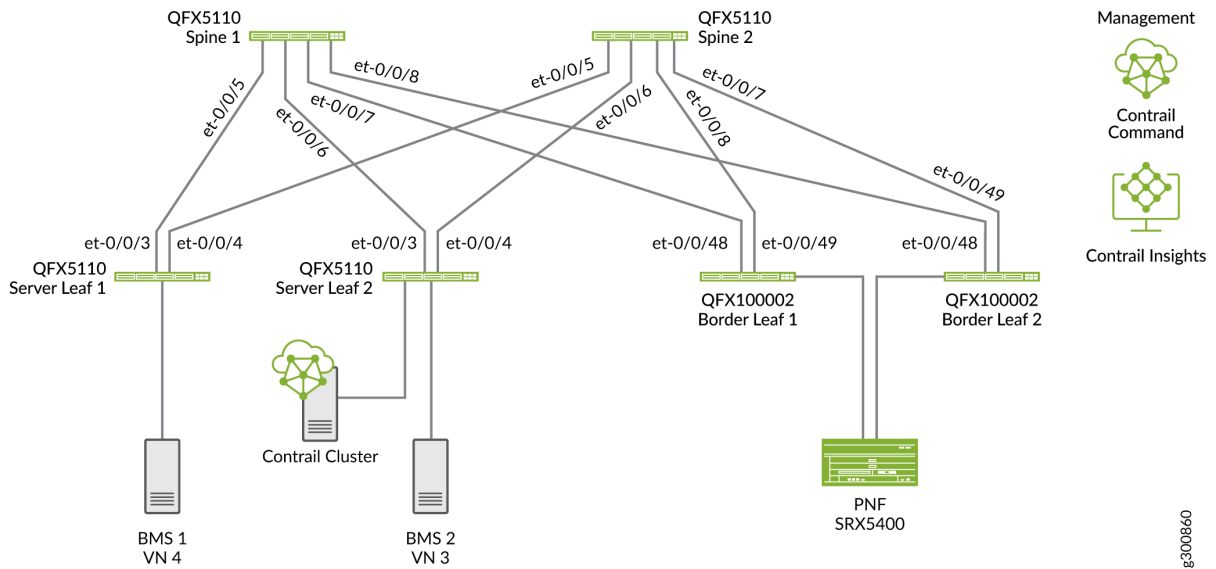
[Figure 15 on page 56](#) shows a logical view of service chaining. VLANs provide connectivity between the logical routers and the PNF device. EBGP advertises routes between the logical routers and the PNF.

Figure 15: Logical View of Service Chaining



In a topology that uses border leaf devices, attach the PNF to the border leaf devices as shown in [Figure 16 on page 56](#).

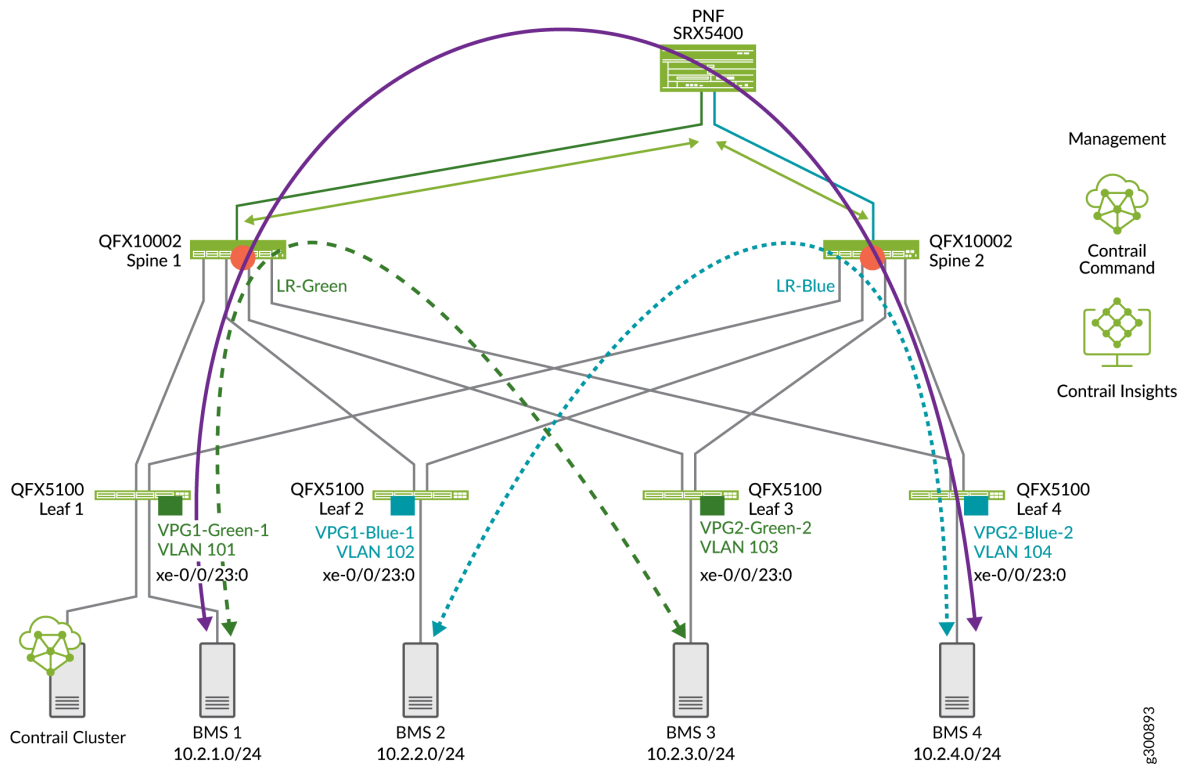
Figure 16: PNF in Topology with Border Leaf



Service Chaining Configuration Overview

In this example we are configuring service chaining in the following topology to provide inter-LR routing on the blue and green networks as shown in [Figure 17 on page 57](#). SRX4k and SRX5k Services Gateways are supported as managed PNFs. Our PNF is an SRX5400 Services Gateway.

Figure 17: Inter-LR Service Chaining



The virtual networks shown in Figure 17 on page 57 have already been configured. See "Configure Virtual Networks for Multi-tenant Service Operations" on page 43. We are adding PNF service chaining so that devices on each network can communicate with each other as shown with the purple line.

To configure service chaining for inter-LR traffic:

1. Onboard an SRX device as the PNF device connected to an existing fabric—you can connect the PNF device to a border spine or a border leaf.
2. Assign PNF service chaining device role to the PNF device and to the border spines or border leaf devices that connect to the PNF device.
3. Connect the PNF to the fabric using a PNF service template.
4. Connect the right and left LRs by configuring VLANs and EBGP peering between the PNF and the LRs using a PNF service instance.

Onboard an SRX Services Gateway as the PNF Device

This section shows how to use Contrail Command to integrate an SRX device into our data center fabric to serve as a PNF device.

This configuration assumes that you have already created your fabric. You must use the Brownfield Wizard to onboard the PNF device. You can't onboard a PNF using the Greenfield Wizard.

SRX clusters are not supported for PNF service chaining.

To selectively onboard an SRX Series router as a PNF device onto an existing fabric:

1. Select **Infrastructure** > **Fabrics**, and then select the fabric to which you want to add the SRX Series gateway.
2. Select **Action** > **Brownfield Wizard**.
3. On the Create Fabric screen, configure the Management subnet, then select Additional Configuration, and enter the PNF ServiceChain subnets.

In this example, we are assigning 10.1.1.15/32 as the Management subnet and 10.100.0.0/24 as the PNF ServiceChain subnet. The Management subnet searches for the device. The PNF ServiceChain subnet establishes the EBGP session between the PNF device and the spine.

Name	DC1
Overlay ASN	64532
Node Profile	Select the SRX device
VLAN-ID Fabric-Wide Significance	Check box

Management subnets (used to search for the device)	10.1.1.15
PNF ServiceChain subnets (subnet used to establish EBGP session between the PNF device and the spine)	10.200.0.0/24

4. Click **Next**, and then click **Finish**.

Assign Device Roles for the PNF Device

In this procedure we will assign the PNF service chaining role for the spine or border leaf devices that connect to the PNF.

To assign roles:

1. On the **Fabric Devices** summary screen, select the PNF device, and then select **Action**>**Reconfigure Roles**.

The screenshot shows the Cisco Control Plane Command Center interface. The main content area displays a table of Fabric Devices. The table has columns for Status, Name, Management IP, Loopback IP, Vendor Name, Product Name, Role, and Routing. The 'VSRX1-05' device is selected, and the 'Action' menu is open, showing options like 'ZTP wizard', 'Brownfield wizard', 'Image Upgrade', and 'Reconfigure Roles'. The 'Reconfigure Roles' option is highlighted.

STATUS	NAME	MANAGEMENT IP	LOOPBACK IP	VENDOR NAME	PRODUCT NAME	ROLE	ROUTING
ACTIVE	VSRX1-05	10.1.1.15	10.0.1.5	Juniper	vsrx		
ACTIVE	VQFX6-14	10.1.1.18	10.0.1.8	Juniper	vqfx-10000	leaf	CRB-Acc
ACTIVE	VQFX5-13	10.1.1.17	10.0.1.7	Juniper	vqfx-10000	leaf	CRB-Acc
ACTIVE	VQFX1-05	10.1.1.11	10.0.1.1	Juniper	vqfx-10000	spine	CRB-Ga CRB-HC 2 more
ACTIVE	VQFX3-07	10.1.1.13	10.0.1.3	Juniper	vqfx-10000	leaf	CRB-Access 13
ACTIVE	VQFX4-08	10.1.1.14	10.0.1.4	Juniper	vqfx-10000	leaf	CRB-Access 13
ACTIVE	VQFX2-06	10.1.1.12	10.0.1.2	Juniper	vqfx-10000	spine	CRB-Gateway CRB-MCAST-Ga 2 more

2. Next to the PNF device, select **Assign Roles**.

Assign role to 1 devices

Physical Role* ?

pnf

Routing Bridging Roles ?

PNF-Servicechain x

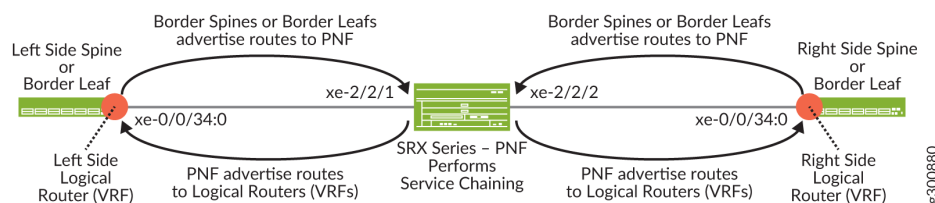
Cancel

Assign

3. Assign the **Physical Role** as **pnf** and assign the **Routing Bridging Roles** as **PNF-Servicechain** role and click **Assign**.

Create a PNF Service Template

The service template provides Contrail Command with information about how the PNF device attaches to the spine or border leaf device. In our example, we are using the following interface numbers:



To create a PNF service template:

1. Click **Services>Catalog**.
The VNF Service Instances page is displayed.
2. Click the **PNF** tab.
The Create PNF Service Template page is displayed.
3. Click **Create** and select **Instance (with Template)** from the list that appears.

The screenshot shows the 'Create PNF Service Instance' wizard in the Contrail Command interface. The 'PNF Service Template' step is selected, and the following information is entered:

- Name:** PNF
- PNF Device:** vSRX1-05
- PNF Left Interface:** ge-0/0/0
- PNF Left Fabric:** DC1
- PNF Left Attachment Points:**
 - Physical Router:** vQFX1-05
 - Left Interface:** xe-0/0/2

4. Enter the following information in the PNF Service Template pane and click **Create**.

Field	Value
Name	PNF
PNF Device	vSRX1-05
PNF Left Interface	ge-0/0/0
PNF Left Fabric	DC1
PNF Left Attachment Points (Attachment points on the spine or border leaf.)	Specify how the spine or border leaf device attaches to the left interface of the PNF device: Physical Router —QFX1-05 Left Interface —xe-0/0/1

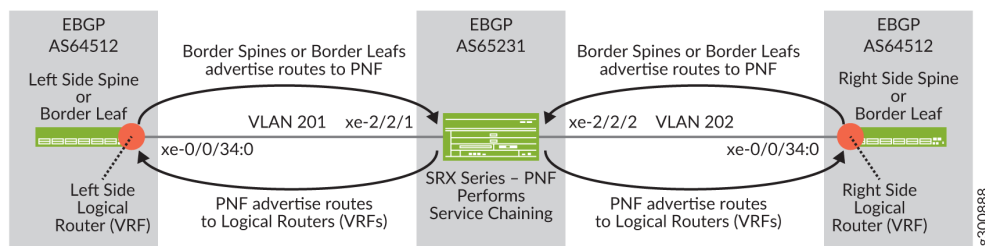
(Continued)

Field	Value
PNF Right Interface	ge-0/0/1
PNF Right Fabric	DC1
PNF Right Attachment Points (Attachment points on the spine or border leaf.)	Specify how the spine or border leaf device attaches to the right interface of the PNF device: Physical Router —QFX2-06 Right Interface —xe-0/0/2

5. Click Next and the PNF service instance configuration screen appears.

A PNF service instance defines how logical routers are interconnected and how BGP reachability is exchanged between the PNF and the logical routers. The configuration includes VLANs that are created between the PNF and the logical routers along with EBGp peering.

Figure 18: Completed PNF Configuration



To create a PNF Service Instance:

1. Navigate to **Services > Deployments**, and select the **PNF** tab.

The PNF Service Instances screen displays.

2. Select **Create Instance**.

Configure the screen as shown here:

The screenshot shows the 'Create PNF Service Instance' form in the Contrail Command interface. The form is divided into several sections:

- Name:** Spine-to-PNF
- Service Template:** PNF-template
- PNF eBGP ASN:** 65231
- RP IP Address:** Enter valid IP
- Left Tenant Logical Router:**
 - Interface Type: left
 - Left Tenant Logical Router: LR1
 - PNF Left BGP Peer ASN: 64512
 - Left Service VLAN: 201
- Right Tenant Logical Router:**
 - Interface Type: right
 - Right Tenant Logical Router: LR2
 - PNF Right BGP Peer ASN: 64512
 - Right Service VLAN: 202

At the bottom of the form, there are 'Create' and 'Cancel' buttons.

3. Enter the following information in the PNF Service Template pane and click Create.

Field	Value
Name	Spine-to-PNF
Service Template	PNF-template
PNF eBGP ASN	65231
Left Tenant Logical Router	LR1-Green
PNF Left BGP Peer ASN	64512
Left Service VLAN (VLAN between the PNF and the LR1)	201

(Continued)

Field	Value
Right Tenant Logical Router	LR2-Green
Right BGP Peer ASN	64512
Right Service VLAN (VLAN between the PNF and LR2)	202

Configure Data Center Interconnect (DCI)

IN THIS SECTION

- [Data Center Interconnect Overview | 64](#)
- [Data Center Interconnect Configuration Overview | 65](#)
- [Assign Device Roles for Border Spine and Border Leaf Devices | 67](#)
- [Manually Configure BGP Peering | 68](#)
- [Configure Virtual Networks | 71](#)
- [Create Virtual Port Groups | 72](#)
- [Create Logical Routers | 73](#)
- [Create Data Center Interconnect | 74](#)
- [Verify Data Center Interconnect | 75](#)

Data Center Interconnect Overview

You can use CEM to interconnect multiple data centers over a WAN such as the Internet or an enterprise network. We support DCI based on EVPN/VXLAN and not Layer 3 VPN and not EVPN/MPLS.

Multiple tenants connected to a logical router (VRF routing instance) in one data center can exchange routes with tenants connected to a logical router in another data center.

The implementation described in this section uses EBGp peering between the data centers.

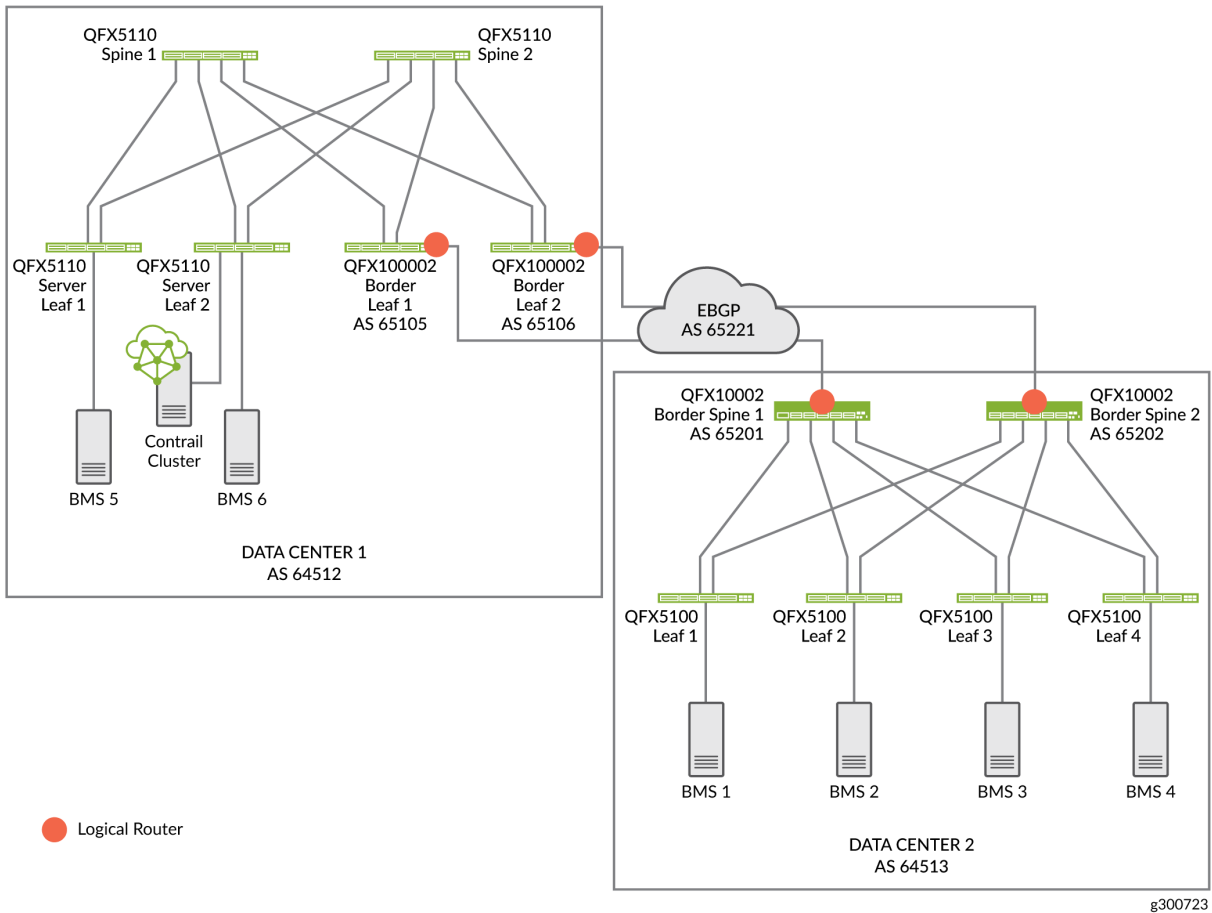
Data Center Interconnect Configuration Overview

IN THIS SECTION

- [DCI Configuration Overview | 66](#)

In this example, [Figure 19 on page 66](#) we are configuring DCI between Data Center 1 (DC1) and Data Center 2 (DC2). Physical connectivity between the data centers is provided by backbone devices in a WAN cloud. In DC1, we are connecting to the WAN cloud from the border leafs. In DCI2, we are connecting to the WAN cloud from the border spines. We are using BGP as the routing protocol between the border devices and the devices in the WAN cloud.

Figure 19: Data Center Interconnect Between DC1 and DC2



DCI Configuration Overview

With CEM, you can automate data center interconnect (DCI) of two data centers. You can use the same CEM cluster to configure multiple data centers in distinct fabrics.

To configure DCI between Data Center 1 and Data Center 2:

1. Assign device roles to the spines and border leafs used for DCI
2. Configure EBGP peering on the underlay
3. Create virtual networks
4. Create logical routers
5. Create Data Center Interconnect

- Configure BGP peers on the WAN cloud device.

Assign Device Roles for Border Spine and Border Leaf Devices

In this procedure we assign roles for the border leaf and border spine devices used for DC1.

To assign roles:

- On the Fabric Devices summary screen, select **Action > Reconfigure Roles**.

The screenshot shows the Contrail Command interface for the DC1 fabric. The 'Fabric Devices' table lists several devices with their status, name, management IP, loopback IP, vendor name, product name, and role. The 'Action' menu is open for the selected device, and 'Reconfigure Roles' is highlighted.

STATUS	NAME	MANAGEMENT IP	LOOPBACK IP	VENDOR NAME	PRODUCT NAME	ROLE	ROUTING
ACTIVE	VSRX1-05	10.1.1.15	10.0.1.5	Juniper	vsrx		
ACTIVE	VQFX6-14	10.1.1.18	10.0.1.8	Juniper	vqfx-10000	leaf	CRB-Access
ACTIVE	VQFX5-13	10.1.1.17	10.0.1.7	Juniper	vqfx-10000	leaf	CRB-Access
ACTIVE	VQFX1-05	10.1.1.11	10.0.1.1	Juniper	vqfx-10000	spine	CRB-Gateway, CRB-MCAST-Ga, CRB-MC 2 more
ACTIVE	VQFX3-07	10.1.1.13	10.0.1.3	Juniper	vqfx-10000	leaf	CRB-Access 13
ACTIVE	VQFX4-08	10.1.1.14	10.0.1.4	Juniper	vqfx-10000	leaf	CRB-Access 13
ACTIVE	VQFX2-06	10.1.1.12	10.0.1.2	Juniper	vqfx-10000	spine	CRB-Gateway, CRB-MCAST-Ga, CRB-MC 2 more

- Next to the spine devices, select **Assign Roles**.

Assign role to 1 devices

Physical Role* ⓘ

Routing Bridging Roles ⓘ

Cancel

Assign

- Be sure that the following roles are assigned.

In DC1, set the roles as follows:

- Border leaf—CRB Access, CRB Gateway, DCI Gateway
- Spine—CRB Gateway, Route Reflector
- Server leaf—CRB Access

In DC2, set the roles as follows:

- Border spine—CRB Gateway, DCI Gateway, Route Reflector
- Leaf—CRB Access

For a description of roles, see ["Device Roles" on page 14](#).

Manually Configure BGP Peering

When you assign the CRB Gateway or DCI gateway role to a device, CEM autoconfigures IBGP overlay peering between the fabrics. In our implementation, it creates BGP peering between the spine and border leaf devices on DC1 and the border spine devices on DC2.

CEM cannot always configure the underlay automatically when the data centers are not directly connected to each other. In this case, CEM requires loopback-to-loopback reachability between the two data centers on devices with the DCI Gateway role.

We are using an MX Series router as the cloud device. On the cloud device configure the border leaf devices and border spine devices as BGP peers.

1. Configure the following on the cloud device.

```
policy-options {
  policy-statement dci {
    term 1 {
      from protocol direct;
      then accept;
    }
  }
}
```

```
protocols bgp {
  group dci {
```



```

export dci;
multipath multiple-as;
neighbor 10.200.1.1 {
    peer-as 65201;
}
neighbor 10.200.2.1 {
    peer-as 65202;
}
neighbor 10.100.1.1 {
    peer-as 65105;
}
neighbor 10.100.2.1 {
    peer-as 65106;
}
}
}

```

2. On DC1 border leaf 1, configure the MX device as a BGP peer.

```

protocols bgp {
    group dci {
        local-as 65105;
        neighbor 10.100.1.2 {
            peer-as 65221;
        }
    }
}
}

```

3. On DC1 border leaf 2, configure the MX device as a BGP peer.

```

protocols bgp {
    group dci {
        local-as 65106;
        neighbor 10.100.2.2 {
            peer-as 65221;
        }
    }
}
}

```

4. On DC2 border spine 1, configure the MX device as a BGP peer.

```
policy-options {
  policy-statement dci {
    term 1 {
      from protocol direct;
      then accept;
    }
  }
}
```

```
protocols bgp {
  group dci {
    export dci;
    local-as 65201;
    neighbor 10.200.1.2 {
      peer-as 65221;
    }
  }
}
```

5. On DC2 border spine 2, configure the MX router as the peer.

```
policy-options {
  policy-statement dci {
    term 1 {
      from protocol direct;
      then accept;
    }
  }
}
```

```
protocols bgp {
  group dci {
    export dci;
    local-as 65202;
    neighbor 10.200.2.2 {
      peer-as 65221;
    }
  }
}
```

```
}
}
```

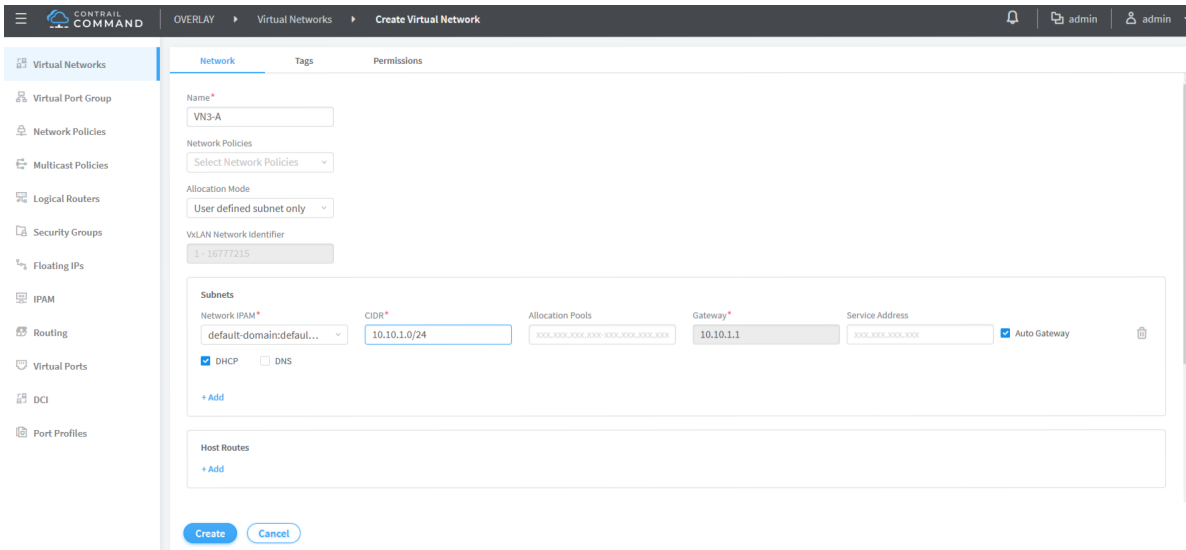
Configure Virtual Networks

We are creating a virtual network in each data center. A virtual network lets hosts in the same network communicate with each other. This is like assigning a VLAN to each host.

To create a virtual network:

1. Navigate to **Overlay > Virtual Networks** and click **Create**.

The Virtual Networks screen appears.



2. Create two virtual networks as follows:

Field	VN3-A Configuration	VN3-B Configuration
Name	VN3-A	VN3-B
Allocation Mode	User defined subnet only	User defined subnet only
Subnets		

(Continued)

Field	VN3-A Configuration	VN3-B Configuration
Network IPAM	default-domain:default-project:default...	default-domain:default-project:default...
CIDR	10.10.1.0/24	10.10.2.0/24
Gateway	10.10.1.1	10.10.2.1

Create Virtual Port Groups

You configure VPGs to add interfaces to your virtual networks. To create a VPG:

1. Navigate to **Overlay > Virtual Port Group** and click **Create**.

The Create Virtual Port Group screen appears.

The screenshot shows the 'Edit Virtual Port Group' configuration page in the Contrail Command interface. The breadcrumb navigation is 'OVERLAY > Virtual Port Group > Edit Virtual Port Group'. The left sidebar shows a navigation menu with 'Virtual Port Group' selected. The main content area is divided into several sections:

- Virtual Port Group Name***: BMS5
- Fabric name***: DC1
- Available Physical Interface**: A table with columns 'DISPLAY NAME' and 'PHYSICAL ROUTER'. It lists several interfaces: et-0/0/7 (DC1-Spine2), et-0/0/34 (DC1-Border-Leaf1), et-0/0/5 (DC1-Spine2), et-0/0/48 (DC1-Server-Leaf1), and et-0/0/8 (DC1-Spine1). Each row has a right-pointing arrow (>).
- Assigned Physical Interface**: A table with columns 'DISPLAY NAME' and 'PHYSICAL ROUTER'. It lists one interface: xe-0/0/3 (DC1-Server-Leaf1). There is a trash icon to the right of the row.
- VLAN**:
 - Network***: VN3-A
 - VLAN ID***: 111
 - Display Name***: BMS5-111-untagged
 - Auto Display Name**:
 - Security Groups**: (empty dropdown)

At the bottom, there are 'Save' and 'Cancel' buttons.

2. Create two VPGs with the values shown in the following table.

To assign a physical interface, find the interface under **Available Physical Interface**. There can be multiple pages of interfaces. To move an interface to the **Assigned Physical Interface**, click the > next to the interface.

Name	BMS5	BMS6
Assigned Physical Interface	xe-0/0/3:0 (on DC1-Server-Leaf 1)	xe-0/0/3:0 (DC1-Server-Leaf2)
Network (Virtual Network)	VN3-A	VN3-B
VLAN ID	111	112

Create Logical Routers

CEM uses logical routers (LRs) to create a virtual routing and forwarding (VRF) routing instance for each logical router with IRB interfaces on the border spine or border leaf devices.

1. Navigate to **Overlay > Logical Routers** and click **Create**.

The Logical Router screen appears:

The screenshot displays the 'Create Logical Router' configuration page in the Contrail Command Line interface. The breadcrumb navigation shows 'OVERLAY > Logical Routers > Create Logical Router'. The left sidebar lists various network management options, with 'Logical Routers' selected. The main configuration area includes the following fields and options:

- Name:** DC1-LR1
- Admin State:** Up (selected), Down
- Extend to Physical Router:** DC1-Border-Leaf1, DC1-Border-Leaf2
- Logical Router Type:** VXLAN Routing
- Connected networks:** VN3-A, VN3-B
- Public Logical Router:**
- NAT:**
- VLAN Network Identifier:** 1-16777215
- DHCP Relay Server(s):** + Add

At the bottom of the configuration area, there are 'Create' and 'Cancel' buttons.

2. On the Logical Router screen, create a logical router:

Field	DC1-LR1 Configuration
Name	DC1-LR1
Extend to Physical Router	DC1-Border-Leaf1 DC1-Border-Leaf2
Logical Router Type	VXLAN Routing
Connected Networks	VN3-A VN3-B

Create Data Center Interconnect

The DCI configuration sets up the connection between two data centers. Once you add DCI, CEM adds family EVPN to the BGP peers between the border leaf and border spine devices in DC1 and DC2.

1. Click **Overlay > DCI Interconnect**.

The Edit DCI screen appears.

2. Fill in the screen as shown:

Verify Data Center Interconnect

To verify that DCI is working, we will ping from a server on a virtual network in one data center to a server on a virtual network in the other data center.

1. Run ping from BMS6 (DC1 Server Leaf 2) to BMS3 (DC2 Leaf 3)

```

ping 10.2.3.101 -c 5
PING 10.2.3.101 (10.2.3.101) 56(84) bytes of data.
64 bytes from 10.2.3.101: icmp_seq=1 ttl=62 time=0.512 ms
64 bytes from 10.2.3.101: icmp_seq=2 ttl=62 time=0.506 ms
64 bytes from 10.2.3.101: icmp_seq=3 ttl=62 time=0.481 ms
64 bytes from 10.2.3.101: icmp_seq=4 ttl=62 time=0.478 ms
64 bytes from 10.2.3.101: icmp_seq=5 ttl=62 time=0.409 ms

--- 10.2.3.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.409/0.477/0.512/0.039 ms

```

2. Run ping from BMS6 (DC1 server Leaf 2) to BMS1 (DC2 Leaf 1)

```
ping 10.2.1.101 -c 5
PING 10.2.1.101 (10.2.1.101) 56(84) bytes of data.
64 bytes from 10.2.1.101: icmp_seq=1 ttl=62 time=0.462 ms
64 bytes from 10.2.1.101: icmp_seq=2 ttl=62 time=0.535 ms
64 bytes from 10.2.1.101: icmp_seq=3 ttl=62 time=0.535 ms
64 bytes from 10.2.1.101: icmp_seq=4 ttl=62 time=0.571 ms
64 bytes from 10.2.1.101: icmp_seq=5 ttl=62 time=0.467 ms

--- 10.2.1.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.462/0.514/0.571/0.042 ms
```