JUNIPER NETWORKS® | Engineering Simplicity

THE MULTICLOUD DATA CENTER

Controller-based EVPN-VXLAN simplifies and secures multicloud connectivity

Challenge

Data centers are shifting from vendor-proprietary solutions to standards-based EVPN-VXLAN fabrics that are difficult to understand and hard for traditional operations staff to manage.

Solution

Contrail Enterprise Multicloud is a scalable, controller-based solution that simplifies and automates the deployment and day-to-day management of an EVPN-VXLAN-based fabric.

Benefits

- *Provides tools to automate and simplify greenfield or brownfield (pre-existing) underlay deployments*
- *Automates EVPN-VXLAN overlay based on desired connectivity*
- *Integrates with popular VM orchestration and container management systems such as VMware vCenter, Red Hat OpenStack Platform, Kubernetes, and Mesos*
- *Provides secure multicloud connectivity*

The industry-wide move towards cloud-based networking and cloud-native applications presents a considerable challenge to today's data center. The velocity of change is increasing, and downtime—caused by a manual and highly complex provisioning process—is extremely costly in terms of customer satisfaction and lost revenue. A trend towards multicloud connectivity, which involves interconnecting multiple data center fabrics or connecting private data centers to a public cloud, further compounds the problem.

Juniper® Contrail® Enterprise Multicloud reduces the complexity of data center fabric management, starting with the IP fabric itself (the underlay) through the Ethernet VPN (EVPN)-Virtual Extensible LAN (VXLAN) logical overlay that provides secure virtual networking, all the way to the secure extension of your data center into public cloud offerings.

The Challenge

The network is critical to the success of any modern enterprise needing high-performance access to applications. A fast and reliable data center that can be extended into remote locations, including public clouds for on-demand computing, is no longer a luxury—it is a requirement.

Enterprise networks around the world are adopting cloud and cloud-based applications to improve their competitiveness, lower IT costs, and provide users with anytime, anywhere access to resources and data. A growing number of network endpoints, coupled with rapidly evolving business needs, is driving demand for highly flexible networks that are not only scalable, programmable, and simple to operate, but are also built on a standards-based architecture that spans the campus, data center, and public cloud.

Security is also of paramount concern; enterprise data centers want security to be embedded into their network architectures through segmentation, tenant separation, and policies extended across the entire organization. Mobile workloads that use ephemeral geographic locations and floating IP addresses pose a unique security challenge; static access control lists (ACLs) no longer suffice when a compute load can shift in and out of a public cloud. Modern enterprises need security that is linked to these dynamic workloads in a simple and intuitive manner—that is, through application-level tags that can be reused as policies to extend security across the entire organization.

The shift from vendor-proprietary data center solutions to a standards-based IP fabric underlay with an EVPN-VXLAN overlay is often perceived as highly complex and hard to manage. Your staff should focus on providing the necessary connectivity and meeting performance SLAs, not on arcane implementation details or complicated troubleshooting procedures to recover from provisioning errors. Connectivity changes must be efficient and reliable, not tied to vendor-specific devices, complex operations, or manual configuration changes prone to human error and delays. The network should also be easy to visualize, with end-to-end telemetry monitoring how the network and applications are performing, with AI and alarms simplifying fault isolation when problems occur.

What's needed is a solution that will help you build out a new data center based on scalable open standards—one with the ability to keep pace with the increasing velocity of additions, moves, and changes while supporting legacy L2 protocols and applications.

This data center build-out must include end-to-end security and performance analytics to secure the network and help you understand how applications are performing, whether they are running locally, extended to a remote fabric, or in the public cloud.

The Juniper Contrail Enterprise Multicloud Solution

Contrail Enterprise Multicloud is based on a centralized controller driven by an intent-based UI that manages both the data center fabric—a collection of switches and links that form the basic IP connectivity underlay—and the Multiprotocol IBGP (MP-IBGP) overlay. This overlay advertises EVPN routes that instantiate VXLAN tunnels, isolating tenants or extending the data center into public cloud offerings.

The Juniper Contrail Networking™ Controller itself does not enable EVPN-VXLAN features; Juniper offers similar capabilities in a controllerless solution (see The **Enterprise Data Center** solution brief). The Contrail Networking Controller merely simplifies and automates traditionally complex and error-prone configuration tasks, giving the operator a single point of control while offering a standards-based fabric and network virtualization overlay manager that supports fabrics comprised of multiple vendor devices.

Features and Benefits

Contrail Enterprise Multicloud offers a multicloud-enabled platform for policy orchestration and advanced analytics. It is built with intent-based methodology for high-performance connectivity, application security, and unified operations, and includes the following features.

Fabric Management

Contrail Enterprise Multicloud contains an embedded manager that saves considerable time when building out a new data center fabric underlay (greenfield), or when migrating an existing IP-based underlay (brownfield) to support the VXLAN overlay. The fabric underlay refers to a Clos-based switching fabric that offers the IP connectivity needed to support the logical overly, which is based on MP-IBGP and EVPN route exchanges to establish VXLAN tunnels. These tunnels support flexible tenant options like L2 or L3 adjacencies, Data Center Interconnect (DCI), broadcast isolation, and multihoming to top-of-rack switches for high availability. Contrail Enterprise Multicloud supports Zero Touch Provisioning (ZTP) in the Greenfield Underlay (GrU) case, automatically discovering and configuring the underlay based on a small set of parameters provided by the user. In the Brownfield Underlay (BrU) case, a wizard helps you "onboard" the existing IP fabric to prepare it for the logical overlay.

Network Virtualization and Overlay Management

Once the underlay is handled, the Contrail Networking Controller automatically configures the EVPN-VXLAN overlay that provides logical connectivity between your clients and workloads. Contrail Networking Controller greatly simplifies the process; the user simply interacts with the UI to declare a few parameters, such as BGP Autonomous System Number (ASN) range, and assign roles to fabric devices, such as "leaf with bridging" or "spine with routing." It then applies your "overlay intent" to the device (and role-specific) configurations, which are pushed out to establish the overlay. As part of the configuration process, users determine whether their data center architecture will be based on edge routing (often associated with a "lean-spine") or edge bridging with a centrally routed spine. Both architectures are supported by Contrail Enterprise Multicloud.

Once the overlay is up and running, the Contrail Networking Controller simplifies Day 2 functions at a service rather than a technology level—for example, "create tenant," "bind subnet to tenant," "attach endpoint to subnet," "build and apply policy to tenant," and so on. These "intent-level" operations are defined using the Contrail Networking Controller's UI without having to interact with low-level vendor-specific CLI commands.

Integration with Orchestration Systems and vRouter Support for VM Network Connectivity

Understanding how the Contrail Networking Controller interacts with the fabric and virtualized devices to rapidly provide the desired network connectivity, all while shielding your staff from device-level details, is key to realizing the value of the solution. To better understand the operation, consider the case of a new VM that needs to be connected to an existing bare-metal server (BMS). Figure 1 shows how the Contrail
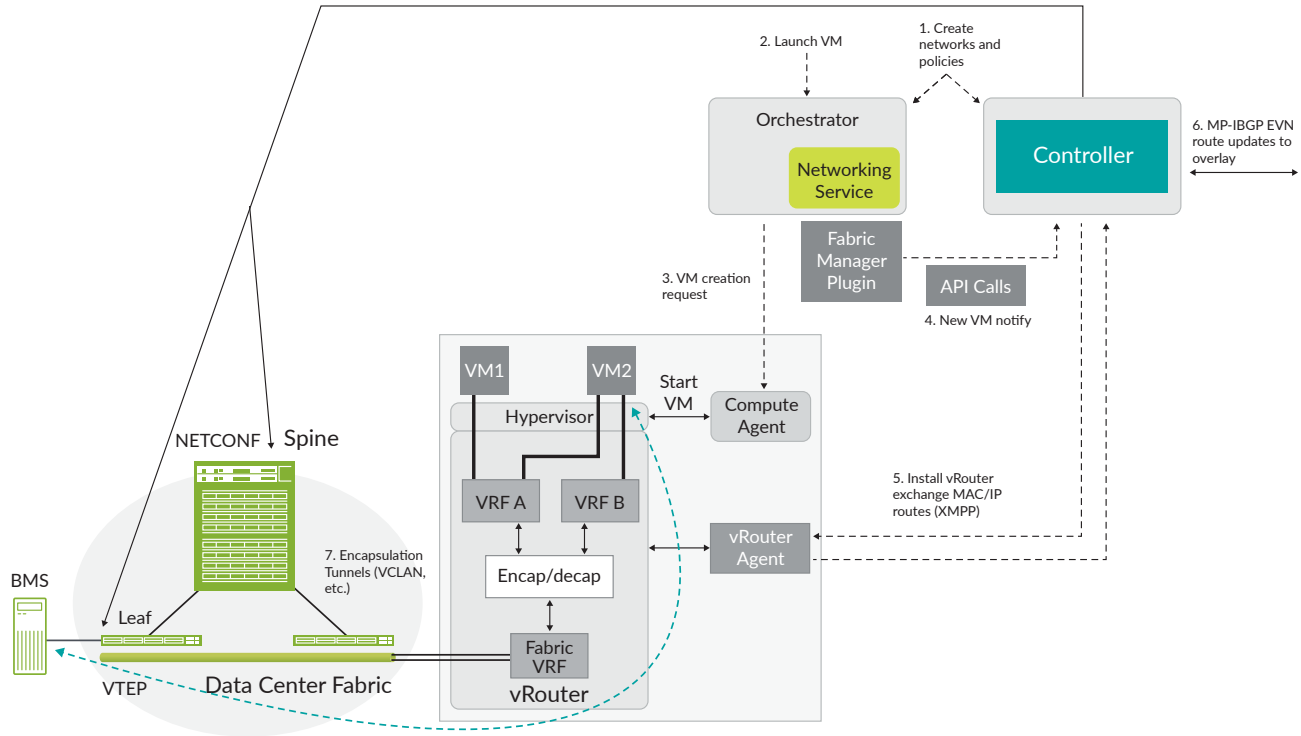
Figure 1: Integration of orchestration and VXLAN connectivity

Networking Controller interacts with your orchestration system, which manages VM life cycles, and the EVPN-VXLAN fabric to provide secure networking services. The virtual tunnel endpoint (VTEP) functionality for the BMS side of the VXLAN tunnel is performed by a fabric leaf—that is, a top-of-rack switch. This contrasts with how VTEP processing is typically handled by a vRouter in such a scenario, and how both ends handle configuration changes pushed out by the Contrail Networking Controller.

Step 1 in Figure 1 shows a new VM being defined on the orchestrator. The desired connectivity, via the assignment of a virtual network identifier (VNI)/VLAN and related security policies, are defined separately on the Contrail Networking Controller.

In Steps 2 and 3, the orchestration system signals the instantiation of the new VM (VM2), which is created in the hypervisor host. In Step 4, the orchestrator starts the new VM and notifies the controller of its existence through a fabric manager plugin. Now that the Contrail Networking Controller knows the VM's specifics, in Step 5, it installs (or updates) a virtual router (vRouter) and, using the Extensible Messaging and Presence Protocol (XMPP), populates its L2/L3 virtual routing and forwarding (VRF) tables with the desired connectivity—in this case, edge bridging between members of the same VN/VLAN.

Step 6 shows the Contrail Networking Controller using the MP-IBGP overlay to advertise the associated EVPN routes to

update reachability for the new VM, allowing other devices to form VXLAN tunnels when policies allow such connectivity. The process ends with Step 7, once the VXLAN data plane tunnel is established between the leaf and the vRouter-housed VTEPs, where the dotted line represents the edge bridged traffic flowing between the BMS and VM2.

In this example, the BMS does not use a vRouter; this is typical given that a BMS is not virtualized and is dedicated to a single tenant so that its internal connectivity does not need to be managed or controlled. The VTEP functionality that handles the VXLAN tunneling for the BMS is offloaded to the attached leaf device, which is configured by the Contrail Networking Controller through the Network Configuration Protocol (NETCONF). During this process, changes may also be pushed to the spine switch in order to influence central routing or data center gateway services.

Data Center Interconnect and Multicloud Connectivity

Contrail Enterprise Multicloud supports DCI that extends the EVPN-VXLAN overlay between fabrics managed by the same controller. You can also extend connectivity between the local fabric and a public cloud using a multicloud gateway (MC-GW) wizard, starting with release 5.1 of Contrail Enterprise Multicloud. The vRouter is a key component of the solution's multicloud capabilities, given that they are installed in VMs that reside within a public cloud to support networking and telemetry in the same manner as local compute nodes.
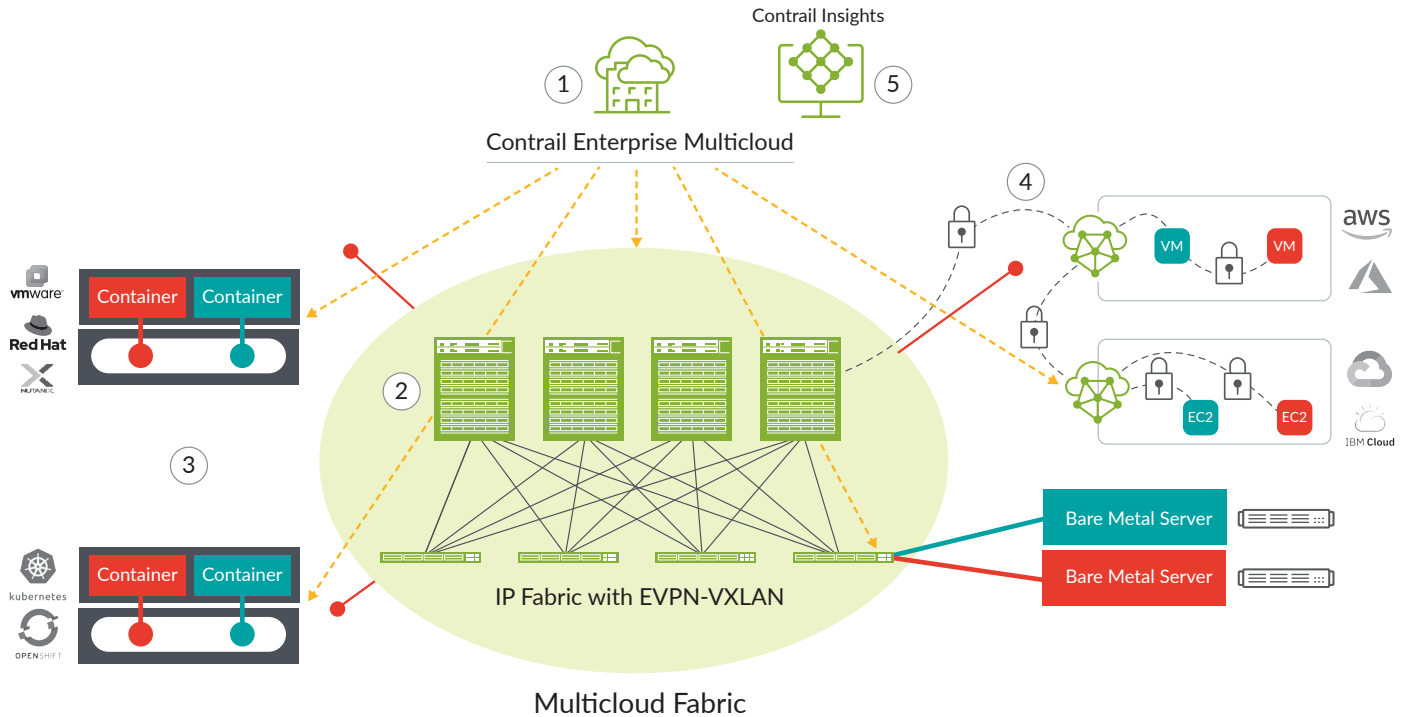
Figure 2: The Contrail Enterprise Multicloud reference architecture

Application-Based Security

Contrail Enterprise Multicloud provides security through an application-based tagging (also referred to as labeling) model that protects your application workloads regardless of their physical location or IP addressing. This feature is increasingly critical as microservices-based containerized applications grow more popular. These applications are typically deployed rapidly and tend to expose more inter-process traffic, a double whammy that requires complicated access control rules compared to securing a traditional monolithic application.

End-to-End Telemetry

Integration of the Juniper Contrail Platform with Juniper Networks Contrail Insights provides detailed telemetry and alarming, as well as the ability to leverage AI and machine learning to support self-driving networks. This integration yields a complete view of your network and applications, from the fabric all the way to the compute loads—whether BMS, VMs, or containerized.

Juniper Contrail Enterprise Multicloud Components

Contrail Enterprise Multicloud makes it easy to manage a complex problem by using a standards-based architecture that can scale to global levels. Figure 2 provides an overview of the solution's building blocks and summarizes the role they play in simplifying your data center operations—from tools to manage the fabric, to an intent-based UI for managing logical connectivity in the overlay (both locally and with extension to remote sites), to integrated end-to-end visibility, so you always know how your network and applications are performing.

The numbered areas in Figure 2 detail key aspects of the Contrail Enterprise Multicloud architecture:

1. The Contrail Networking Controller and Contrail Command UI enable intuitive intent-based control of the network and logical connectivity.

2. Juniper Contrail Networking™ provides data center fabric management for greenfield or brownfield deployments.

3. Contrail Networking/security allows VXLAN data plane and vRouter integration with orchestration systems, as well as application/tag-based security.

4. Contrail Networking supports DCI for multiple sites and extension to public cloud (multicloud) with secure tunnels.

5. Contrail Insights delivers end-to-end multicloud telemetry and reporting.

Summary—EVPN-VXLAN Data Centers Elevated to a New Level

Contrail Enterprise Multicloud simplifies and automates building, configuring, managing, securing, and visualizing your data center while letting you extend your private cloud into public cloud offerings. The highly scalable controller-based solution's UI simplifies all aspects of managing a modern data center based on EVPN-VXLAN technology.

Next Steps

For more information, please contact your Juniper sales representative.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

Fax: +1.408.745.2100

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.0.207.125.700

Fax: +31.0.207.125.701