Cisco Application Policy Infrastructure Controller Driver for OpenStack Group-Based Policy

Product Description

The Cisco® Application Policy Infrastructure Controller (APIC) was designed based on open APIs, allowing it to be tightly integrated with cloud orchestration platforms such as OpenStack.

In addition to support for the OpenStack Neutron Modular Layer 2 (ML2) interface, the Cisco APIC supports integration with OpenStack using Group-Based Policy (GBP). GBP was created by OpenStack developers to offer declarative abstractions for achieving scalable, intent-based infrastructure automation within OpenStack. It supports a plug-in architecture that connects its policy API to a broad range of open-source and vendor solutions, including the APIC.

The combined solution, including OpenStack GBP with the GBP APIC driver, offers an end-to-end policy-based infrastructure that exposes the full power of the application-centric policy model supported by Cisco Application Centric Infrastructure (Cisco ACI™).

Group-Based Policy API

GBP offers a command-line interface (CLI) and OpenStack Heat and Horizon interfaces for defining policy abstractions. This policy is mapped to APIC constructs through an APIC driver, and virtual machines are automatically connected to the corresponding APIC endpoint group (EPG) as they are provisioned (Table 1). Each GBP object can be either private to a particular OpenStack tenant or shared among projects.

Table 1. GBP and Cisco APIC Mapping

GBP Object	Cisco APIC Mapping	Description
Policy target	Endpoint	A basic addressable unit in the architecture. It corresponds to an individual network endpoint (generally a virtual network interface card [vNIC]).
Policy group	Endpoint group (fvAEPg)	A basic unit of isolation consisting of a set of policy targets with the same policy.
Policy classifier	Filter (vzFilter)	A means of filtering network traffic including protocol, port range, and direction (in or out or bidirectional).
Policy action	-	An action to take when a particular rule is applied. The APIC driver supports **Allow** as well as **Redirect** actions.
Policy rule	Subject (vzSubj)	A classifier-action pair defining a specific policy behavior.
Policy rule set	Contract (vzBrCP)	A group of policy rules that can be provided or consumed by a number of policy groups.
Layer 2 policy	Bridge domain (fvBD)	A set of groups within the same switching domain. Layer 2 policies can contain one or more subnets.
Layer 3 policy	Context (fvCtx)	Private network containing a potentially overlapping set of IP addresses. Layer 3 policies in GBP contain IP supernets that are divided into subnets.

When GBP is being used with OpenStack and the APIC GBP driver, it supersedes many of the Neutron APIs, including the network, router, subnet, and security group APIs, and these Neutron APIs should not be used directly.

OpFlex and Open vSwitch Support

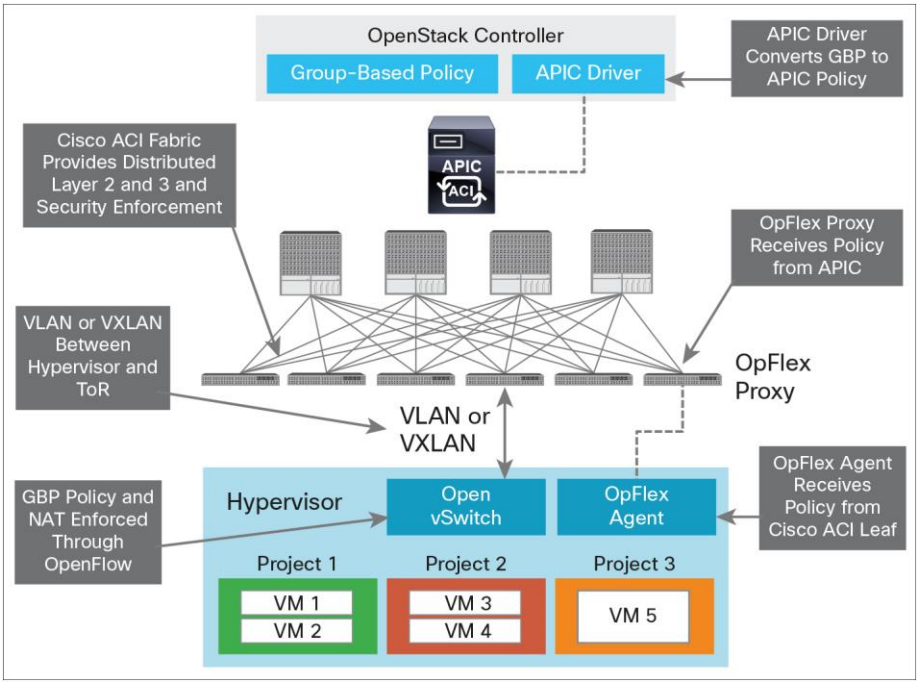
The APIC can manage Open vSwitch (OVS) in an OpenStack environment using the OpFlex protocol. The OpFlex agent, an open-source software component running on each hypervisor, communicates with one or more physical leaf switches within the Cisco ACI fabric and manages a local instance of OVS.

This approach allows tight integration between the APIC and OpenStack using the controller's native virtual machine networking tools and interfaces. This link between OpenStack and the APIC offers a number of advantages:

- It enables local enforcement of GBP within each hypervisor, avoiding unnecessary hair-pinning of traffic to the top-of-rack (ToR) switch.
- It allows the APIC to track each OpenStack computing node, including its virtual machines, internal networking configuration, and traffic metrics.
- It provides operational visibility into the OpenStack environment and simplifies troubleshooting across the physical and virtual environments.
- It offers fully distributed Neutron services. This includes local response to Dynamic Host Configuration Protocol (DHCP) and metadata requests on each OpenStack computing node rather than relying on responses through a centralized network node.
- It enables efficient virtual machine migration by automatically sending Address Resolution Protocol (ARP) requests.

Figure 1 shows how the APIC GBP driver works in an OpenStack environment along with Cisco ACI and APIC.

Figure 1. Cisco APIC GBP Architecture



Layer 2 and 3 Policy Management

The GBP APIC driver supports multiple ways of managing Layer 2 and 3 policies.

A Layer 2 policy is an independent switching domain that may or may not enable broadcast semantics. In Cisco ACI, it maps to a bridge domain.

A Layer 3 policy represents an independent address space and a collection of Layer 2 policies. In Cisco ACI, it maps to a private network (or Virtual Routing and Forwarding [VRF] instance).

GBP offers several options for managing Layer 2 and 3 policies:

- By default, GBP creates and manages Layer 2 and 3 policies automatically. As each policy group is created, a corresponding Layer 2 policy is matched to it and placed in a default Layer 3 policy.
- A user can create Layer 2 and 3 policies through GBP and use them for policy groups.
- An administrator can register preconfigured APIC bridge domains and contexts as Layer 2 and 3 policies to be used for different policy groups.

The GBP APIC driver supports the configuration of multiple tenant-specific private networks within the APIC.

Floating IP and Network Address Translation

Cisco ACI, with the GBP APIC driver, supports the capability to create floating IP addresses and dynamically assign them to virtual machines. Using OpFlex and OVS, the floating IP address capability is fully distributed within each hypervisor host. The solution also allows virtual machines within private tenant networks to access external networks through Source Network Address Translation (SNAT).

High Availability

The GBP APIC driver is designed for high availability. It supports connections to multiple APICs within the Cisco ACI fabric and is designed to synchronize the state if a failure occurs in the OpenStack or APIC deployment. The GBP APIC driver also supports multihomed hosts using virtual PortChannels (vPCs).

Licensing

GBP is an open-source project that includes a number of drivers, including the GBP APIC driver. It is available without additional licensing when run with Cisco ACI and APIC.

Platform Requirements

- The GBP APIC driver is supported on OpenStack Juno and later releases. The GBP APIC driver is compatible with any server hardware capable of supporting Juno.
- The Cisco ACI fabric consists of Cisco Nexus® 9500 and 9300 platform switches, which support Cisco ACI, and APICs. The GBP APIC driver is supported on APIC Release 1.1(4e) and later.

GBP APIC Driver Features and Capabilities

Table 2 summarizes the main features and functions of the GBP APIC driver.

Table 2. Main Features

Features	Description
GBP policy API	Supported; automatic configuration of APIC through GBP.
Hypervisor	Kernel-based Virtual Machine (KVM) - based hypervisor (multiple versions of Ubuntu, RHEL, and

Features	Description
	Centos).
Neutron plug-in API	Not supported when using the GBP APIC driver.
GBP API client interfaces	CLI, Horizon, and Heat
GBP Layer 2 and 3 capabilities	• Multiple policy groups mapped to same Layer 2 policy • Multiple Layer 3 policies per project (that is, overlapping IP address spaces)
GBP enforcement	• Policies enforced within hypervisor for local traffic • Policies enforced within Cisco ACI fabric for traffic across hypervisors
Encapsulation to Cisco ACI fabric from hypervisor	VLAN or Virtual Extensible LAN (VXLAN).
Automatic hypervisor discovery	This feature is optional and requires Link-Layer Discovery Protocol (LLDP). The driver automatically discovers hypervisor physical connectivity to the top of the rack using LLDP and dynamically provisions the Cisco ACI fabric. This behavior allows physical topology changes without the need for any reconfiguration.
Scalability	Scalability limits are set by the capabilities of the ACI fabric. Please check the scalability guide for each ACI release.
Floating IP and sNAT	Distributed Floating IP and sNAT support implemented through OpFlex and Open vSwitch.
Neutron Node HA	Distributed meta-data proxy and DHCP implemented through OpFlex and Open vSwitch.
Support for multiple APICs	The driver communicates with multiple APICs and is resilient to failure of any specific APIC.
Dual-homed servers	The driver supports dual-homed servers using the vPC function of the Cisco ACI fabric's ToR switches.
Licensing	The GBP APIC driver is open source and is available without additional licensing on the APIC or Cisco ACI fabric.
Supported versions	• The GBP APIC driver is supported on OpenStack Juno and later releases. • GBP is supported by commercial distributions from Red Hat and Mirantis. Packages are available for Ubuntu platforms as well. Check with Cisco for specific vendor versions. • Cisco ACI Release 1.1(4e) BMR2 or later is required.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For More Information

- Read more about Cisco ACI at http://www.cisco.com/go/aci.
- Read more about GBP at https://wiki.openstack.org/wiki/GroupBasedPolicy.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-734181-02 02/17