



How to Add F5 Application Delivery Services to OpenStack

Advanced F5 application delivery services can be flexibly designed into an OpenStack cloud architecture with a variety of deployment and orchestration options.

WHITE PAPER
by F5



WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

Introduction

OpenStack, which is rapidly becoming the dominant cloud platform for delivering Infrastructure as a Service (IaaS), is now powering private, public, and managed private clouds. As OpenStack clouds increasingly host mission-critical production applications, advanced application delivery services for layers 4 through 7 are becoming essential. These services provide additional security, scaling, and optimization to ensure those mission-critical applications remain secure, fast, and available. F5 is the leading supplier of advanced application delivery services across data center, public, and private clouds—including those powered by OpenStack. F5 application delivery services may be designed into an OpenStack cloud, and advance consideration of the available options is useful in efficiently planning an OpenStack architecture and deployment.

What Is OpenStack?

OpenStack is an open-source software platform used to deliver cloud computing. OpenStack, which started as joint project between NASA and RackSpace Hosting, is currently managed by the OpenStack foundation with the mandate to promote the software and OpenStack community.

Several commercial organizations now either produce their own OpenStack distribution or offer additional services such as support, consulting, or pre-configured appliances.

OpenStack is composed of a number of components that provide the various services required to create a cloud computing environment. These components are [amply documented](#) elsewhere. There are, however, a number of modules that are directly relevant to an F5 OpenStack deployment.

Function	Component	Description
Computing	Nova	Manages pools of computer resources across various virtualization and bare-metal configurations
Networking	Neutron	Manages networks, overlays, IP addressing, and application network services such as load balancing
Orchestration	Heat	Orchestrates other OpenStack components using templates and APIs



WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

A foundational element of OpenStack is the [RESTful API](#), through which infrastructure components can be configured and automated. In many OpenStack use cases—such as building a multi-tenant, self-service cloud or creating an infrastructure to support DevOps practices—API-driven orchestration is essential. The ability to cut deployment times from weeks to minutes, or to deploy hundreds of services per day, is often the driving force behind the move to a cloud platform. For this to be effective, all components of the infrastructure must be part of the automation framework. Many applications will require advanced application delivery services (such as application security or access control) to be truly production ready, so it's vital that application delivery services integrate with the OpenStack orchestration and provisioning tools.

Projects, tenants, and networks

Multi-tenancy is an important concept in OpenStack. Within OpenStack, a group of users is referred to as a project or tenant. (The two terms are interchangeable.) Projects can be assigned quotas for resources such as compute, storage, or images. One of the most significant decision points, when architecting for multi-tenancy, is how networking is designed for tenants. F5® BIG-IP® platforms offer [a range of multi-tenancy and network separation](#) options to enable interoperability with OpenStack multi-tenancy.

Provider networking

Provider networks generally either use flat (untagged) or, more commonly, VLAN (802.1Q tagged) networks. These closely map to traditional data center networking. OpenStack networks are defined and created by the administrator and shared among tenants.

In some cases, a tenant's compute instances will have interfaces directly onto the provider network. Tenants don't define their own networks but simply connect to the configured provider networks using IP address ranges as defined by the provider's administrator. In other cases, tenants will create virtual network configurations within the provider networks.



WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

Tenant networking

Administrators can enable tenants to create their own specific network architectures, which are most frequently controlled by OpenStack Neutron using Open vSwitch instances on compute nodes, although other software-defined networking (SDN) solutions can also be used. Either VLANs or transparent Ethernet tunnels using [GRE](#) or [VXLAN](#) technology allow communication between tenant compute instances and isolate them from other tenants. As of early 2016, GRE tunneling has been the most common deployment method. Tenants can create their own networks and IP address ranges, which may well overlap between tenants. Each tenant may have an OpenStack router to enable communication outside of its networks. This is accomplished by allocating to the tenant one or more floating IP addresses, which the tenant router translates to the configured tenant private IP address. (Note that OpenStack Neutron and BIG-IP floating IP addresses are different things; how the BIG-IP platform manages tenant isolation will be discussed later.)

F5 Application Delivery Services

F5 products provide a spectrum of advanced application delivery services that are designed to provide scalability, availability, and multi-layered security. Some key (but not exhaustive) examples include:

Security	<p>Advanced Network Firewall Services</p> <ul style="list-style-type: none">• Decisions about traffic control using criteria beyond simply IP:port:protocol, such as geographical location or endpoint reputation• HTTP protocol validation• Day and time schedules <p>Web Application Firewall Services</p> <ul style="list-style-type: none">• Comprehensive tools to identify web application threats and block malicious traffic• Outbound data loss prevention (DLP) services <p>Access and Identity Services</p> <ul style="list-style-type: none">• Advanced authentication services such as two-factor tokens, CAPTCHA, or geographical restrictions• Client certificate checking and endpoint inspection• SAML service provider (SP) and identity provider (IdP) services <p>Denial-of-Service (DoS) Mitigation</p> <ul style="list-style-type: none">• Proactive bot defense• Layer 7 DoS detection and mitigation <p>SSL and Encryption</p> <ul style="list-style-type: none">• SSL decryption, traffic inspection, and re-encryption• Offloading of SSL workloads from compute node resources
Availability	<p>Application-Level Monitoring</p>



WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

- Advanced application health checks (using a multiple-step monitor)
- Multi-level health checks (such as checking that both the database and application are available)
- Non-HTTP health checks (such as SIP, Microsoft Windows SQL Server, and FTP,)
- Advanced algorithms to better distribute traffic to the servers functioning best

Global Availability

- Application availability across a heterogeneous mix of different cloud providers or data centers
- Integration with BIG-IP advanced monitors
- DNSSEC support

Performance

Network and Transport Optimization

- A configurable TCP stack that can be optimized to deliver across WAN and cellular networks
- An HTTP/2 gateway that brings the advantages of additional compression and request multiplexing without altering the back-end infrastructure

Application and Data Optimization

- Selective image optimization for on-the-fly optimization dependent on detected network or client characteristics
- WAN acceleration over SSL encrypted tunnels with adaptive compression and TCP optimization

Flexibility

Data Path Programmability

- Complete programmatic control of application traffic
- The ability to read, write, and inspect all aspects of application data
- Event-driven and comprehensive language

Control Plane Programmability

- The ability to modify configuration in response to events such as changes to server load, application behavior, or infrastructure
- Fully autonomous or external API-driven triggers

The BIG-IP platform

The [BIG-IP](#) platform is available in physical, virtual, and cloud editions. The platform delivers application services through BIG-IP [software modules](#). A BIG-IP platform can run one or more software modules to suit the needs of the applications, and the platform can be deployed as a stand-alone unit or in highly available clusters.



WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

	Function	F5 Software Module
Security	Network layer security	BIG-IP® Advanced Firewall Manager™ (AFM)
	Application layer security	BIG-IP® Application Security Manager™ (ASM)
	Identity and access	BIG-IP® Access Policy Manager® (APM)
Availability	Application availability and traffic optimization	BIG-IP® Local Traffic Manager™ (LTM)
	Global availability and DNS	BIG-IP® DNS
Performance	Application and network optimization	BIG-IP® Application Acceleration Manager™ (AAM)

The BIG-IP platform is a very high performance, stateful, bidirectional, zero-copy proxy. Understanding this basic architectural principle can help illuminate how the BIG-IP platform delivers services and clarify architectural choices.

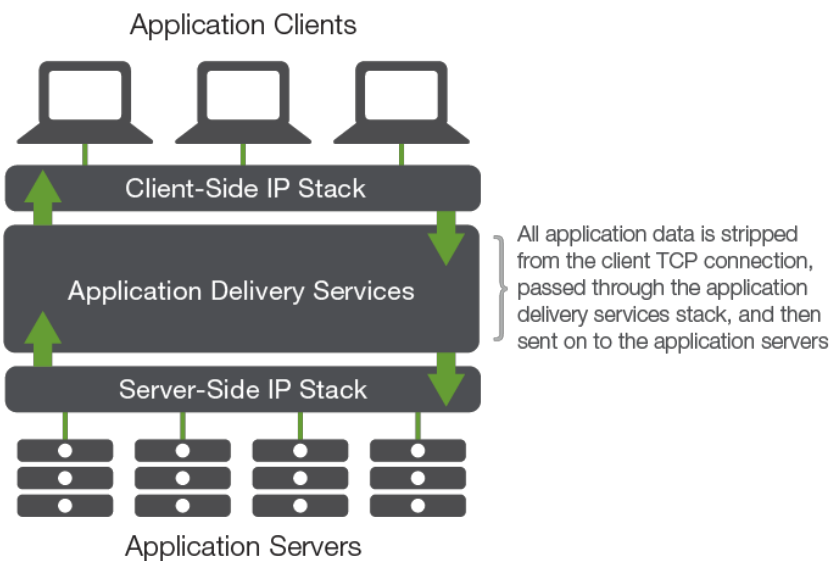


Figure 1: The BIG-IP platform architecture



WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

Clients connect to the BIG-IP device or instance, which connects to back-end servers (or in some cases, such as DNS services, handles the application traffic and responds back to the client directly). This creates a TCP “air gap,” with complete TCP session regeneration between the client and the server. Within this logical gap, the BIG-IP platform provides application delivery services. As application traffic transits the platform, it can be inspected, altered, and controlled, so the BIG-IP platform gives complete control of both inbound and outbound application traffic.

The BIG-IP platform also carries [ICSA Labs certification](#) for both network and web application firewalls, for which traffic separation and platform security are rigorously tested, providing additional platform security assurance.

Putting It Together: F5 and OpenStack

OpenStack and F5 application delivery services and platforms combine to bring production grade services to OpenStack hosted applications. F5 application delivery services can be accessed in two ways within OpenStack: The Neutron Load Balancing as a Service (LBaaS) version 2 service and Heat orchestration. (F5 also supports LBaaS version 1 integration with Neutron, but the OpenStack community has deprecated the version 1 API starting with the Liberty release of OpenStack.)

LBaaS

Neutron LBaaS enables basic load balancing services for compute (and hence application) instances. These services are limited to a core subset of functions and features that are common across a wide range of load balancing platforms.

The LBaaS service delivery model abstracts the resources providing the service away from the services themselves. The resources providing the services exist as part of the OpenStack infrastructure rather than within the OpenStack tenant resources. This model is sometimes referred to as “under the cloud.”

WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

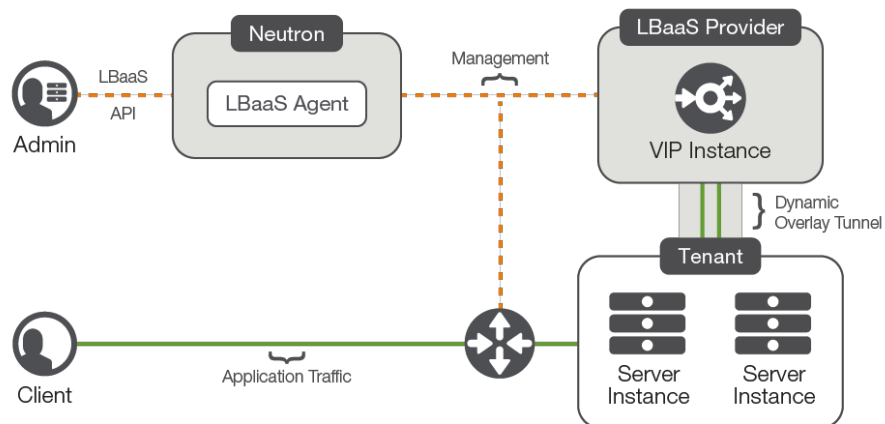


Figure 2: Under the cloud LBaaS deployment

OpenStack LBaaS relies on a number of logical objects to create a load balancing configuration.

Object	Description
loadbalancer	The root object. Specifies the subnet of the virtual IP (VIP)—which can be statically assigned or allocated—the tenant, and the provider
listener	A listener on a specific port of the load balancer VIP. Specifies the port and a limited number of protocol types
pool	A pool the listener will send traffic to. Specifies the protocol, parent listener, and load balancing algorithm
member	A member of the pool. Specifies the IP address, port number, and (optionally) subnet of an instance of the application that traffic can be directed to
health_monitor	Creates a health monitor tied to a pool. Specifies the type of monitor, frequency, and timeouts, along with options for HTTP path, methods, and expected codes
lbaas_sessionpersistence	Defines how session persistence should be handled (such as limited to cookie or source IP persistence)

WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

The object model is shown in Figure 3.

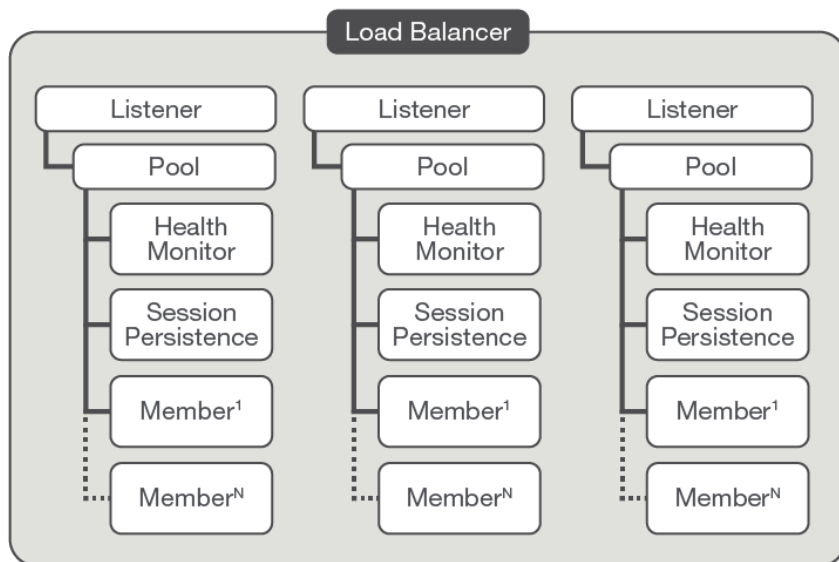


Figure 3: The OpenStack LBaaS object model

As in all OpenStack operations, LBaaS is managed via a RESTful API. The API allows tenants to make REST calls to create, update, and delete LBaaS objects, with a number of steps between a tenant's API call and a configuration change occurring on a BIG-IP instance.

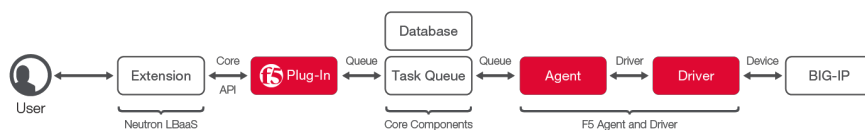


Figure 4: The OpenStack LBaaS architecture

The mapping between LBaaS objects and the API calls to create or update them into a configuration on a BIG-IP instance is handled by the [F5 OpenStack LBaaS driver](#). The LBaaS driver enables a BIG-IP instance to become a provider of load balancing services within an OpenStack powered cloud.



WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

The F5 LBaaS driver is really two separate components:

- The F5 LBaaS plug-in, which is installed on a server running the Neutron API service
- The F5 LBaaS agent process (which includes the driver), which is installed on the host that will run the agent process. Each device service group (a collection of BIG-IP devices in a cluster) requires a separate agent process.

The LBaaS driver receives tasks as a result of LBaaS API calls made by the tenant and translates them into F5 iControl® API calls to create or update configuration objects on the BIG-IP device or virtual edition. Where tenants are using isolated tenant networks and network overlay tunnels or VLANs, the LBaaS driver allows multiple tenants to be serviced from a single BIG-IP instance or high availability (HA) configuration. The F5 LBaaS plug-in creates the necessary API calls to the BIG-IP instance and to Nova to ensure that tenant traffic is routed to the tenant-isolated listener object (VIP in BIG-IP terms) on the shared BIG-IP instance.

Tenant isolation

In multi-tenant environments, a key part of Nova is ensuring that tenants are isolated from each other. The BIG-IP LBaaS components use a number of BIG-IP multi-tenancy features to ensure separation of tenant traffic.

Component	Notes
Network Overlay Support	Support for VXLAN and GRE tunnels: Tenant traffic is fully encapsulated into and out of the BIG-IP system
Route Domains	Strictly defined address spaces within the platform. Each route domain isolates IP address spaces and routing information. IP address spaces can be duplicated between domains, allowing easy reuse of RFC 1918 private addressing for multiple tenants
Administrative Partitions	Create administratively separate configurations. Each tenant configuration is contained within a separate administrative partition

To understand in more detail how and when these multi-tenancy features are used, consult the [F5 OpenStack LBaaS Driver and Agent Readme](#).

LBaaS provides a simple, API-driven system to deploy load balancing services within OpenStack, providing basic load balancing for a large number of clients. The API does, however, deliver only a subset of the functions of a comprehensive Application Delivery Controller (ADC). This table compares LBaaS and native BIG-IP services across some key application delivery properties such as protocol support, additional services, and health monitors.



WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

Property	BIG-IP services via LBaaS	Native BIG-IP ADC Services
Protocols	TCP only	TCP, UDP, SCTP
L7 Protocols	HTTP, HTTPS	HTTP, HTTP/2, HTTPS, FTP, RTSP, Diameter, FIX, SIP, PCoIP, RDP
Application layer security	None	Full web application firewall (WAF)
Network layer security	None	Full network firewall
Application layer access	None	Full authentication and SSO capabilities
Traffic distribution algorithms	3	17
Application acceleration	None	Full suite of caching, compression, and content manipulation tools, including TCP optimization
Health monitors	3	20+ (including SMTP, database, SNMP, SIP, FTP, DNS)
Data path programmability	None	F5 iRules® give full visibility and control of all application data

Where the advanced capabilities of a full-fledged application layer proxy are required, deploying F5 application delivery services using the OpenStack Heat orchestration service and the associated templates can combine simple, automated service creation with more complex service configurations.

Heat orchestration service and templates

OpenStack Heat is an orchestration service that generates running applications based on templates. The Heat template describes the infrastructure in one or more text files and the Heat service executes the appropriate API calls to create the required components. The Heat service can be extended beyond the core modules through the use of custom plug-ins.

The [F5 Heat plug-in](#) allows [Heat templates](#) to create advanced application delivery configurations on any BIG-IP device or virtual edition with network access that is reachable from the server running the Heat service. The BIG-IP instance will also need connectivity and routing to the tenant instances, as that connectivity is not configured by the Heat plug-in.

WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

Heat templates use a simple mark-up language, YAML, which is designed to be human readable and easy to work with. Heat templates are declarative, which means you simply define your desired infrastructure components and rely on the underlying providers to create the configuration you have defined.

Heat templates allow the creation of more advanced application delivery scenarios, especially when combined with the F5 iApps® template system. iApps templates allow the repeatable creation of application delivery configurations by simply passing in the required template and instance-specific values. Complex delivery configurations using advanced features such as web application firewall services, application acceleration, and advanced load balancing algorithms can be implemented with [simple API calls](#).

Heat templates work with instances of BIG-IP virtual editions within the individual tenant network environment (“over the cloud”) as well as BIG-IP appliances deployed in the underlying physical network. The BIG-IP device does not need to participate in any Neutron networking API calls, since it is treated as any other compute node within the tenant.

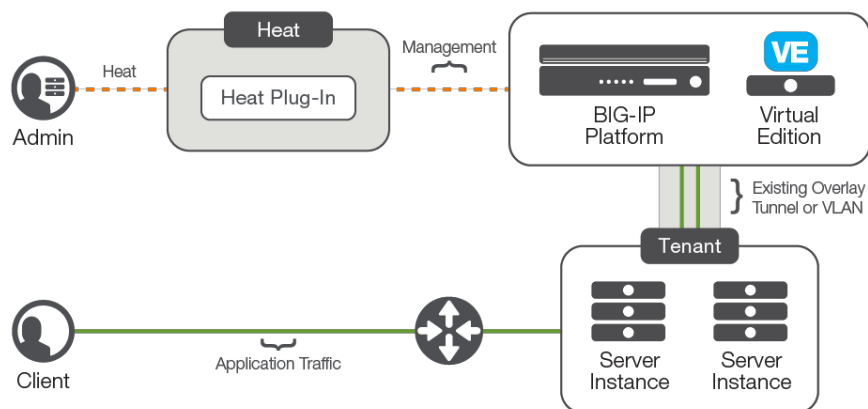


Figure 5: Over the cloud deployment with a BIG-IP appliance



WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

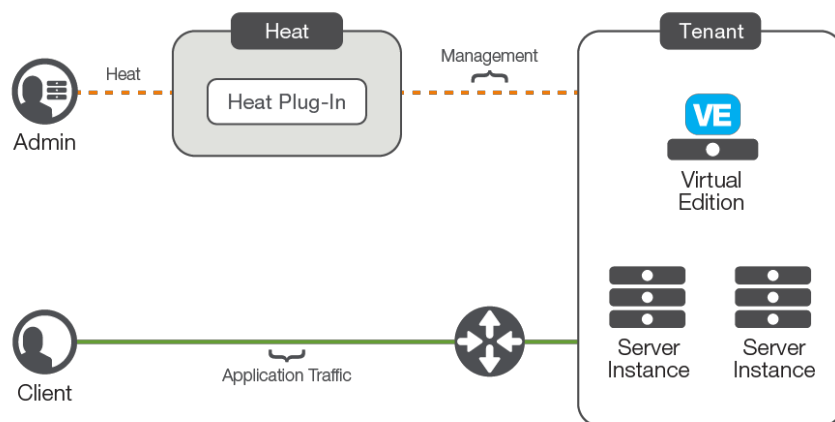


Figure 6: Over the cloud deployment with a BIG-IP virtual edition

The F5 Heat plug-in is available from the [F5 Github](#) repository. This repository contains both the Heat plug-in—which is installed on the server running the Heat engine—and sample [Heat templates](#).

Flexible platform options

F5 application delivery services are available in a number of platforms, all of which offer the same application delivery capabilities, as they run the same core operating system and F5 microkernel.

F5 appliances and F5 VIPRION® chassis

F5 hardware platforms offer high performance and massive scalability for environments requiring a large number of clients or tenants or high throughput use cases. A single HA pair can service many hundreds of tenants and millions of clients. F5 hardware devices provide connection rate service level agreements (SLAs) and significant offloading for the underlying compute environment through the use of specialized hardware for both SSL and TCP processing. Where network security services and distributed denial-of-service (DDoS) mitigation is required, F5 hardware platforms offer excellent performance and high levels of protection. Support for multiple overlapping address spaces and network overlay protocols enables hardware devices to be used in most multi-tenant environments.



WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

F5 BIG-IP virtual editions

F5 BIG-IP virtual editions are available for most hypervisors (including KVM) and for use in public cloud Infrastructure as a Service (IaaS) providers such as Amazon AWS and Microsoft Azure. BIG-IP virtual editions (VEs) also are available in a range of capacities, from a lab edition to production-ready versions with pay-as-you-grow upgrades for throughputs ranging from 25 Mb to 10 Gb. Volume licensing and flexible license pools enable dynamic lifecycle management of BIG-IP instances in test and development environments. Utility billing is also available in public cloud environments. BIG-IP virtual editions offer the same application delivery services as the hardware platforms but lack the specialized hardware and scale of the appliances.

BIG-IP virtual editions can be entirely contained within a tenant network. Seen by OpenStack as simply another compute instance, they're configured by Heat templates or can be used as a provider for LBaaS.

Use Case	Tenant Isolation	Possible Architectures
LBaaS configuration, isolation of thousands of tenants, millions of clients	VLAN, VXLAN, or GRE	Consolidated BIG-IP hardware platforms
LBaaS configuration, isolation of thousands of tenants, millions of clients	GRE, VXLAN	High throughput BIG-IP virtual editions, scaled out as needed ¹
LBaaS configuration, lower scale requirements	GRE, VXLAN	Lower throughput BIG-IP virtual editions ¹
Heat configuration, advanced application delivery services	None	BIG-IP virtual edition(s) within a tenant

¹Consult the [F5 and OpenStack Integration Guide](#) for detailed information.

Since the F5 LBaaS plug-in can accommodate multiple F5 agent and driver instances, it is possible to mix hardware devices and BIG-IP virtual editions within the same LBaaS configuration.

As with all architectural decisions, the right option is the one that best suits the individual requirements of the solution. High performance, scalable solutions can be built using BIG-IP hardware or virtual editions. The overall requirements for scale and services should help guide infrastructure architects toward hardware, software, or a combination of the two. For a consumer or tenant who just wants to provision services, the choice between LBaaS or Heat is more significant than the delivery platform itself.



WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

High availability

High availability is key in mission-critical network and application stacks, and as expected, the BIG-IP platform has a robust HA architecture. BIG-IP devices and virtual editions can be deployed as standalone devices (for example, for test and development environments), highly available pairs, or in N-way active device groups of up to four devices. All of these deployment types are supported within OpenStack platforms.

Scalability

Being able to add additional capacity to LBaaS or tenant BIG-IP resources enables administrators or tenants to cope with increases in application throughput or tenant numbers. Scaling up or out without disruption to services is essential to building an agile and scalable cloud.

The BIG-IP platform can scale both up and out: Appliances and virtual editions can scale up via license upgrades, and the VIPRION chassis can scale up through the addition of additional hardware blades. The BIG-IP LBaaS plug-in will manage multiple agents and drivers (each of which manage a single BIG-IP instance or cluster), allowing for horizontal scale. Where multiple agents are in use, the F5 LBaaS plug-in will, by default, keep all LBaaS load balancer objects for a particular tenant assigned to a BIG-IP device (or cluster).

When using BIG-IP VE instances within a tenant, the instances can again be scaled up via license or additional instances added to cover new workloads.

Conclusion

As OpenStack deployments increasingly host critical production applications, the need for robust, high quality application delivery services within OpenStack grows. F5 application delivery services provide the capacity, security, and advanced capabilities that these critical applications need, coupled with the agility and low operational overhead that an OpenStack-powered cloud delivers.



WHITE PAPER

How to Add F5 Application Delivery Services to OpenStack

Additional Resources

[F5 Github](#)

[F5 OpenStack Documentation](#)

[F5 Multi-Tenancy Designs](#)

[F5 OpenStack Integration Guide](#)

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. WP-CLOUD-81384976-ads-openstack-Haynes 0113