F5 BIG-IP Device Package for Cisco APIC User and Troubleshooting Guide

Welcome to the Cisco® Application Policy Infrastructure Controller (APIC) and F5® BIG-IP® Device Package for Cisco APIC User and Troubleshooting Guide. This document describes the features, configuration procedures, and troubleshooting steps for using the F5 BIG-IP Device Package for Cisco APIC with Cisco APIC.

The F5 Synthesis™ architecture and Cisco Application Centric Infrastructure (ACI) are focused on efficiently delivering applications by taking a fabric-based approach to networking and services architectures. Cisco ACI is designed to translate application requirements into services required for successfully deploying applications in a simplified and automated fashion.

For detailed information about Cisco ACI, see
http://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html.
For detailed information about Cisco APIC, see
http://www.cisco.com/c/en/us/products/cloud-systems-management/application-policy-infrastructure-controller-apic/index.html.

For detailed information about F5 Synthesis, see *https://synthesis.f5.com/*.

Products and applicable versions

Product	Versions
F5 BIG-IP Device Package for Cisco APIC	1.0.0(78)
BIG-IP system	11.4.1 or later (Virtual Edition or physical appliance)
Cisco APIC	APIC version 1.0(1e), Switch version 11.0(1b)
Guide version	1.0 (see *Document Revision History on page 31*)

Important: *Make sure you are using the most recent version of this guide, available at*
http://www.f5.com/pdf/deployment-guides/f5-cisco-apic-dg.pdf.

To provide feedback about this guide or other F5 solution documents, contact us at *solutionsfeedback@f5.com*.

Contents

Related documentation

The following F5 and Cisco documentation provides additional details on this solution.

F5 documentation

➤ For known issues and information for a specific release of the F5 BIG-IP Device Package for Cisco APIC, refer to the F5 BIG-IP Device Package for Cisco APIC Release Notes for the applicable version of the device package.

➤ For a condensed list of the steps required to configure your first Service Graph using the BIG-IP system with Cisco APIC, refer to the *F5 BIG-IP Device Package for Cisco APIC Quick Start Guide*. All of the information in the Quick Start guide is contained (and expanded on) in this guide.

Cisco documentation

➤ For an overview of APIC, refer to the *Cisco APIC Getting Started Guide*.

➤ For details on how to configure Layer 4 to Layer 7 services on APIC, refer to the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*.

➤ Cisco also provides several other documents for APIC, refer to your Cisco APIC documentation set for additional details.

F5 and Cisco APIC Integration Overview

F5 integrates with APIC using a Device Package. The F5 BIG-IP Device Package for Cisco APIC is available for download from F5 as a ZIP file and then is imported into APIC (as described in this document). The file contains the following:

• A device model, which describes the features and functions available to APIC on the BIG-IP system.

• A device script, which implements the features and functions described by the device model.

APIC is built with a standard API used to configure services implemented by integrated vendor devices, such as F5. The F5 BIG-IP Device Package for Cisco APIC implements the API specific to the semantics of the BIG-IP system.

The following diagram illustrates the logical flow between Cisco APIC and the BIG-IP system.
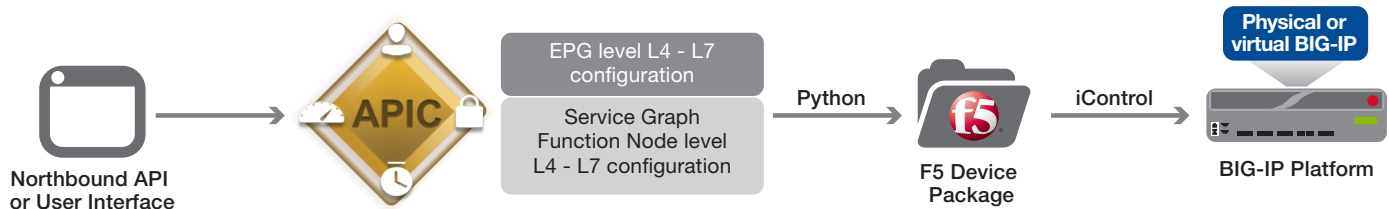
Figure 1: *Logical configuration example*

An administrator uses the northbound API or the user interface on APIC for configuration. Service Graphs created with the F5 BIG-IP Device Package for Cisco APIC cause APIC to call the F5 BIG-IP Device Package for Cisco APIC to push configuration to the BIG-IP system, ascertain health, and obtain statistics (interface counters). The APIC API for L4 - L7 services is implemented by the F5 device script. The device script translates the standard API calls into BIG-IP system specific iControl/SOAP calls to implement the service. Status and information from the iControl/SOAP calls are packaged and returned to APIC for processing.

Network Topologies with the BIG-IP system

The following diagram shows a typical network topology using the BIG-IP system integrated with Cisco ACI.
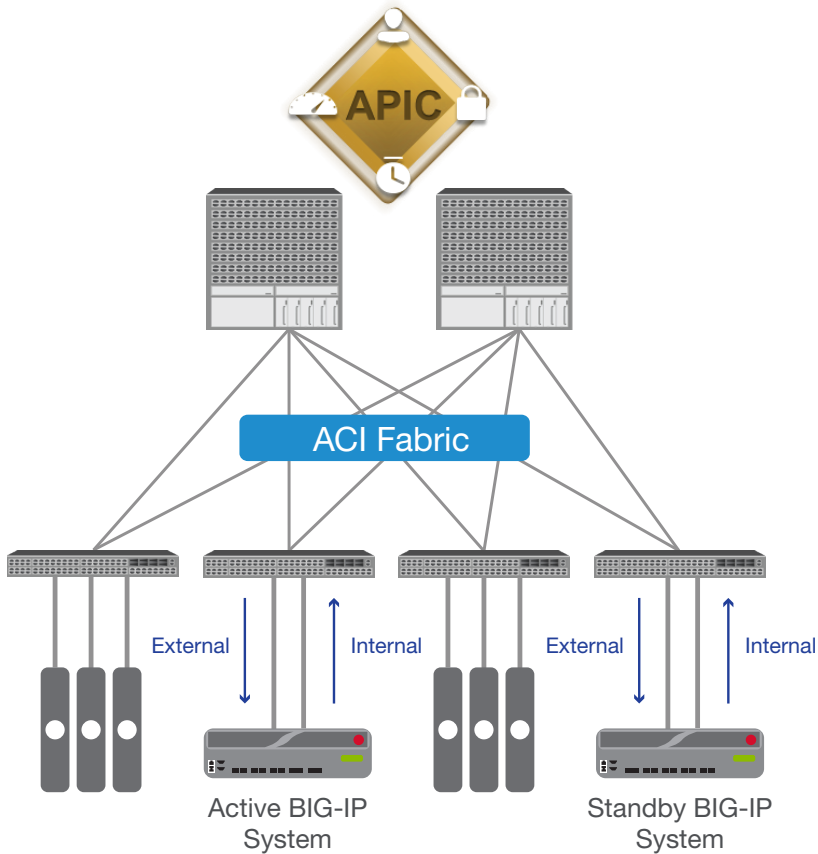
Figure 2: *Network topology example*

The internal and external interfaces on the BIG-IP system are connected to leaf nodes in the ACI architecture. Items such as web servers, database engines, and application tiers are also connected to leaf nodes. Spine nodes handle the routing between the BIG-IP system and the various other end points necessary to deliver an application service.

The management port of the BIG-IP system is connected out-of-band to a switch outside of the ACI architecture (not shown in the diagram) to provide management access.

This diagram is not meant to illustrate all possible architectures but rather communicate a typical architecture showing where the BIG-IP system fits into the Cisco ACI architecture.

Preparing the environment

Use this section to prepare the environment for deploying services using Cisco APIC and the F5 BIG-IP Device Package for Cisco APIC.

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this implementation. Be sure your environment meets or exceeds the requirements described in the following sections prior to using the F5 BIG-IP Device Package for Cisco APIC.

➤ **Minimum version requirements**
  Your environment must meet the following minimum version requirements:
  » Cisco APIC v1.0(1e) and Switch software 11.0(1b).
  » BIG-IP version 11.4.1 or later, running as a standalone BIG-IP system or in a BIG-IP cluster. This can be a physical appliance or a BIG-IP Virtual Edition (VE).
  » F5 BIG-IP Device Package v1.0.0 for Cisco APIC v1.0(1e).

➤ **Minimum Cisco APIC requirements**
  The Cisco APIC environment must meet the following requirements. Refer to the ***Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*** for specific details on how to configure APIC.
  » The initial configuration of APIC and ACI must be complete. This includes racking and cabling the hardware, powering on the devices, installing the Cisco APIC v1.0(1e) and Switch 11.0(1b) software, configuring the management IP address and verifying it is reachable.
  » The Layer 3 networks must be defined and operational.
  » The AAA configuration (such as RADIUS or LDAP) must be completed and operational. You may need to create an Application EPG to reach external AAA servers to verify the AAA configuration is functioning properly.
  » Any APIC tenants, Security Domains, private network(s), bridge domain(s), and related objects must be configured and operational.
  » You must have access to an administrator-level account on the Cisco APIC.
  » If you are testing multi-tenancy, you must have access to an account assigned to a tenant.
  » If you plan on using the BIG-IP virtual edition in your environment, you must have created a Virtual Machine Mobility (VMM) domain and configured vCenter integration.
  » If you plan on using a physical BIG-IP appliance in your environment, you must have created a Physical Domain.
  » Any inter-EPG application filters, Contracts, and application profiles (if needed) to facilitate traffic flow between EPGs must be created.
  » You must have created a management EPG, which is required for APIC to reach the management IP addresses of your BIG-IP system(s).
  » All external network configuration must be complete.

➤ **Minimum F5 BIG-IP requirements**
  The BIG-IP system must meet the following requirements before you are able to use it with Cisco APIC. Refer to the BIG-IP documentation on the F5 technical support site (*http://support.f5.com/kb/en-us/products/big-ip_ltm.html*) for specific information about how to configure BIG-IP system to meet the minimum requirements.
  » The BIG-IP system must be cabled to a leaf switch and powered on (if using an appliance) or started in a VMware environment (if using a Virtual Edition).
  » The BIG-IP system must be running version 11.4.1 or later.
  » You must have configured a management IP address and it must be accessible by the APIC environment.
  » You must have access to an administrator-level account on the BIG-IP system.

Downloading the F5 BIG-IP Device Package for Cisco APIC

The F5 BIG-IP Device Package for Cisco APIC is available on http://downloads.f5.com. If you do not already have an account with F5 technical support, you must register for a free account to obtain the software.

To download the F5 BIG-IP Device Package for Cisco APIC

1. Open a web browser and go to *https://downloads.f5.com*.

2. Use your credentials to login. If you do not have an account, click **Register for an Account** to create one.

3. After successfully logging in, click **Find a Download**.

4. In the **Third-Party-Integrations** row, click **Cisco APIC**.

5. From the **Product Version** list, select a version. Remember this must be 11.4.1 or later.

6. Read and accept the End User License Agreement.

7. Click the README file to familiarize yourself with the files available.

8. Click **F5-BIG-IP-Device-Package-for-Cisco-APIC.zip** to download the F5 BIG-IP Device Package for Cisco APIC file. Save the file to a location accessible from the Cisco APIC user interface. We recommend you also download and read the associated documentation.
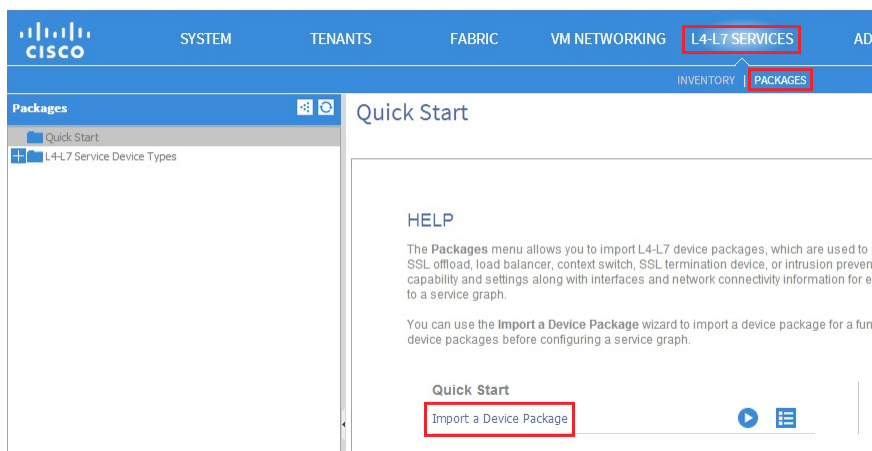
Installing the F5 BIG-IP Device Package for Cisco APIC on Cisco APIC

The next task is to import and install the F5 BIG-IP Device Package for Cisco APIC you just downloaded on Cisco APIC. Prior to loading the F5 BIG-IP Device Package for Cisco APIC into your Cisco APIC, we recommend reading the F5 release notes, which contain useful information regarding this F5 BIG-IP Device Package for Cisco APIC release.

Use the following procedure to import the F5 BIG-IP Device Package for Cisco APIC using the Cisco APIC user interface.

To import the F5 BIG-IP Device Package for Cisco APIC using the APIC user interface

1. Log into Cisco APIC as an administrator.

2. On the menu bar, click **L4-L7 SERVICES**, and then click **PACKAGES**.

3. In the right pane, click **Import a Device Package**.

Figure 3: *Importing the Device Package*

4. Click **BROWSE**, and then navigate to the location where you saved the F5 BIG-IP Device Package for Cisco APIC you downloaded.

5. Click **SUBMIT** to start the installation process.

6. Once the installation is complete, verify the device package has been accepted by APIC.

   a. From the left pane, click **L4-L7 Service Device Types** to open the folder.

   b. Click **F5-BIGIP-1.0.0** to expand the F5 BIG-IP Device Package for Cisco APIC.

   c. Click **L4-L7 Service Functions**.
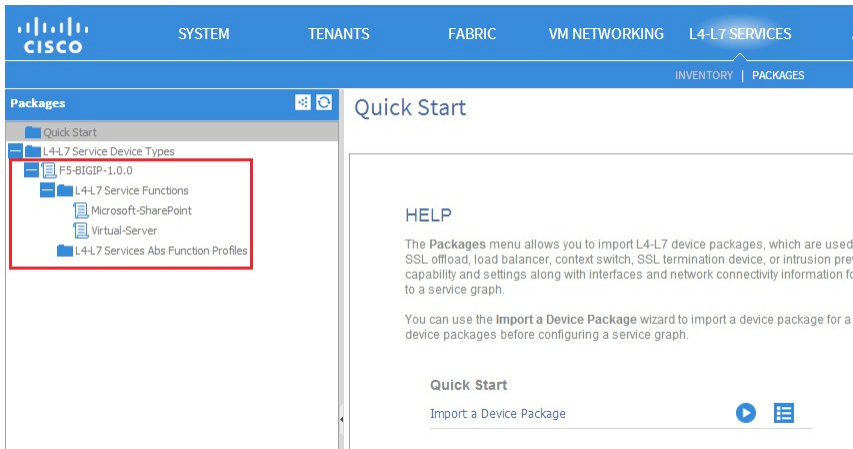
Figure 4: *Verifying the package has been imported*

Once the F5 BIG-IP Device Package for Cisco APIC has been successfully installed, you are ready to use Cisco APIC to deploy services supported by the F5 BIG-IP Device Package for Cisco APIC.

➡ **Note**

Cisco APIC can support multiple versions of the F5 BIG-IP Device Package. For example, a newer version may be installed to take advantage of new functionality without disrupting Service Graphs deployed with an older version.

A single version of the F5 BIG-IP Device Package for Cisco APIC may be used for any number of BIG-IP systems, providing they meet the prerequisites detailed on page 5.

Configuring services using Cisco APIC

This section describes how to configure a Service Graph using the F5 BIG-IP Device Package for Cisco APIC, and contains the following:

- *Creating a Device Cluster on this page*
- *Exporting the Device Cluster to a Tenant on page 11*
- *Creating a Service Graph on page 12*
- *Locating the Service Graph Edit Page on page 13*

At any time during the APIC configuration process, you can click the information icon (i) in the upper-right corner of the UI for help on the current screen.

Creating a Device Cluster

A Device Cluster is a logical representation of one or more Concrete Devices acting as a single device. Concrete Devices are physical (or virtual) BIG-IP devices added to the Device Cluster. For more information about Device Clusters and Concrete Devices, refer to the Cisco APIC documentation.

Before you create a Device Cluster, you must decide if the BIG-IP devices are shared between tenants in a multi-tenant environment, or if the BIG-IP devices are used by a single tenant. In the following procedure, our example uses a Device Cluster that shares the BIG-IP devices between tenants.

To create a Device Cluster for your BIG-IP systems

1. On the menu bar, click **TENANTS**.

2. From the sub menu, select the tenant in which you want to create the Device Cluster.

    a. If the BIG-IP devices are to be shared between tenants, click the pre-configured **mgmt** tenant.

    b. If the BIG-IP devices are to be used by a single tenant, click the single tenant you want to use.

    For the rest of this procedure, we use the **mgmt** tenant (BIG-IP devices are shared between two or more tenants). Later, you can export the Device Cluster to other tenants as needed.

3. In the left pane, expand **Tenant mgmt**, and then expand the **L4-L7 Services** folder.

4. Right-click **Device Clusters**, and then click **Create Device Cluster**. The Create Device Cluster page opens.
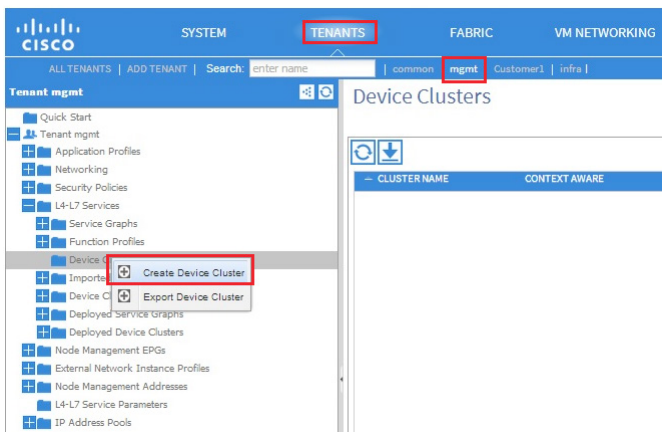
Figure 5: *Initiating Device Cluster creation*

5. On the Create Device Cluster page, in the **Name** field, type a name for the cluster. In our example, we use **F5-2**.

6. From the **Device Package** list, select the F5 BIG-IP Device Package for Cisco APIC you imported.

7. For the **Content Aware** option, click **Multiple**.

8. For the **Device Type** option, click the button for the type of BIG-IP system you are using: **Physical** or **Virtual**.

    - If you select Physical, you must have already created a Physical Domain. Refer to the Cisco APIC documentation for instructions.

    - If you select Virtual, you must have already created a VMM domain and integration with vCenter. Refer to the Cisco APIC documentation for instructions.

9. From the **Physical Domain** or **Virtual Domain** list, select the appropriate domain.

10. In the Cluster Management Interface area of the screen, do not specify an EPG. Inband management is not currently supported.

11. In the **Virtual IP Address** field, type virtual IP address. This must be a management IP address from one of the BIG-IP systems you intend to add to the cluster.

12. In the **Port** field, type the appropriate port number, for example, **443** (SSL).

13. In the **Username** and **Password** fields, type the BIG-IP user name and password of a user with administrative privileges.

    (i) *Important*

    The user name and password must be the same for each BIG-IP system you intend to add to the Device Cluster instance. Cisco APIC uses this user name and password to issue iControl/SOAP calls to the BIG-IP system.

13. In the Logical Interfaces area, click the Add (**+**) button to add a logical interface.

    a. In the **Name** field, type **external**.

    b. From the **Type** list, select **external**.

    c. Click **UPDATE** to save.

    d. Click the Add (**+**) button to add another logical interface.

    e. In the **Name** field, type **internal**.

    f. From the **Type** list, select **internal**.

    g. Click **UPDATE** to save. You do not need to configure the management interface here prior to clicking UPDATE.

Figure 6: *Creating the Device Cluster*

14. Click the **NEXT** button to proceed to the Concrete Device creation.

15. In the Create L4-L7 Devices area, click Add (**+**) to add a new Concrete Device. We use physical BIG-IP systems in this example.

   a. In the **Name** field, type a name for the device. As a best practice, use the host name of the BIG-IP system you are adding.

   b. In the **Context Label** field, you can optionally type a label.

   c. In the Management Interface area, in the **IP Address** field, type the management IP address for the BIG-IP device you are adding.

   d. In the **Username** and **Password** fields, type the BIG-IP user name and password of a user with administrative privileges. All operations from APIC use this user name and password for configuration operations on the BIG-IP system.

   e. In the Interfaces area, click the Add (**+**) button to add the internal interface.

      i). In the **Name** field, type a name, such as **1_1**.
      Important: The format of this name is critical, as it must map to the physical interfaces on the BIG-IP system. In APIC, the format is **x_y**; in the BIG-IP system, the interface format is **x.y**. Thus, **1_1** in APIC corresponds to interface **1.1** on the BIG-IP system; **1_2** in APIC corresponds to **1.2** on the BIG-IP system, and so on.   If you want to have your internal Self IP on BIG-IP interface 1.1, then you must specify **1_1** in APIC, and then choose **internal** from the **Logical Interface** list in step iii.

      ii). From the **Path** list, select the physical interface. This must be the physical port on the leaf node where the internal interface of the BIG-IP is physically connected.

      iii). From the **Logical Interface** list, select **internal**.

      iv). Click **UPDATE** to save.

      v). Click the Add (**+**) button to add the external interface.

      vi). In the **Name** field, type a name, such as **1_2**. In this example, **1_2** corresponds to interface **1.2** on the BIG-IP system. See the Important note in step 15.e.i for details.

      vii). From the **Path** list, select the physical interface. This must be the physical port on the leaf node where the external interface of the BIG-IP is physically connected.

      viii). From the **Logical Interface** list, select **external**.

      ix). Click **UPDATE** to save.

Figure 7:   *Creating the Concrete Devices*

16. Click the **NEXT** button to go to the Parameters screen.

17. There is no configuration needed on the Parameters screen. Click **OK** to complete adding the Concrete Device.

18. Repeat step 15 if you want to add a second Concrete Device. The F5 BIG-IP Device Package for Cisco APIC and APIC only supports two Concrete Devices per Device Cluster for high availability configurations.

19. When you have finished adding the Concrete Devices, click **NEXT**. The Create Device Cluster > Parameters screen opens.

20. Click **FINISH** to complete the Device Cluster configuration procedure.

You can create multiple Device Clusters by repeating this entire procedure for additional Device Clusters.

When you are finished, after expanding your Device Cluster in the left pane, the APIC UI looks similar to Figure 8.
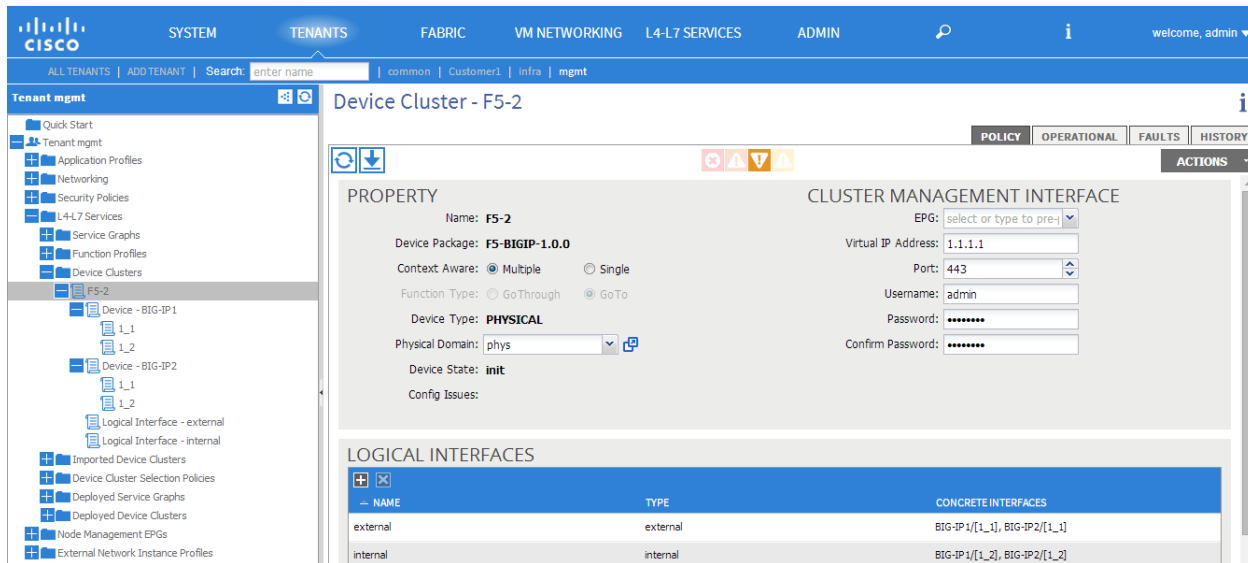
Figure 8:   *Reviewing the Device Cluster properties*

Exporting the Device Cluster to a Tenant

An APIC administrator can choose which tenant(s) are permitted to use the Device Clusters created in APIC. Use the following procedure to export a Device Cluster to a tenant.

To export a Device Cluster to a tenant

1. On the menu bar, click **TENANTS**.

2. From the sub-menu, click the tenant where the Device Cluster was created. In our example, we created the Device Cluster in the mgmt Tenant, so we click **mgmt**.

3. In the left pane, expand the **Tenant** folder and then the **L4-L7 Services** folder.

4. Click **Device Clusters**.

5. From the **ACTIONS** list, click **Export Device Cluster**.

6. From the **Device Cluster** list, select the Device Cluster you want to export.

7. From the **Tenant** list, select the tenant to which you want to export the Device Cluster.

8. In the **Description** field, you can optionally type a description (see *Figure 9: Exporting the Device Cluster on page 12*).

9. Click **SUBMIT**.

You can repeat this procedure if you want to export the same Device Cluster to multiple tenants. This functionality is useful for assigning BIG-IP resources in your network to meet your end-user's requirements.

> **➡ Note**
>
> *As of APIC v1.0(1e), you must refresh the screen to see any newly-exported Device Clusters.*

Figure 9: *Exporting the Device Cluster*

To view the Device Cluster you exported

1. On the menu bar, click **TENANTS**, and then click the Tenant where the Device Cluster was created.

2. In the left pane, expand the **Tenant** folder and then the **L4-L7 Services** folder.

3. Click **Imported Device Clusters**. The screen looks similar to Figure 10.

Figure 10: *Viewing the Device Cluster*

Creating a Service Graph

Use the following procedure to create a Service Graph.

To create a Service Graph

1. On the menu bar, click **TENANTS**.

2. From the sub menu, click the tenant in which you want to create the Service Graph, for example, Customer1.

3. In the left pane, expand the **Tenant** folder and then the **L4-L7 Services** folder.

4. Right-click **Service Graphs**, and then click **Create L4-L7 Service Graph**.

5. In the **Name** field, type a name for the service.

6. In the **Description** field, you can optionally type a description.

7. Drag and drop the appropriate L4-L7 Service Function to the white space on the right pane.

   • If your service is an L4 or L7 server load balancing use case, drag and drop the **Virtual-Server** function.

   • If your service is a Microsoft SharePoint use case, drag and drop the **Microsoft-SharePoint** function.

8. In the **Name** field, you can optionally type a name for the BIG-IP node created. This is your only opportunity to provide a name, as you cannot edit this field after completing this procedure. This field has a 10 character limit.

9. Connect **To Consumer EPG** to the block labeled **E** on the F5 node in the center using your mouse.

   a. In the **Adjacency Type** area, click **L2** or **L3**. If your clients originate on a different VLAN, choose **L3**.

   b. Click **OK**.

10. Connect the block labeled **I** on the F5 node to **To Provider EPG**.

    a. In the **Adjacency Type** area, click **L2**.

    b. Click **OK**. The right pane should look like one of the examples in Figure 11, depending on whether you selected SharePoint or Virtual server.
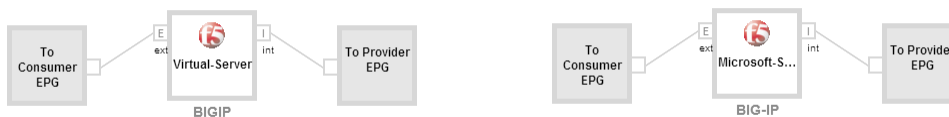
11. Click **Submit**.

Figure 11: *Visual representation of the Service Graphs*

At this point, no configuration has been pushed to the BIG-IP system(s); this occurs later.

Locating the Service Graph Edit Page

Use the following procedure to find the page where you can edit the Service Graph parameters.

To locate the Service Graph edit page

1. On the menu bar, click **TENANTS**.

2. From the sub menu, click the tenant that contains the Service Graph.

3. In the left pane, expand the **Tenant** folder and then the **L4-L7 Services** folder.

4. Expand the **Service Graphs** folder, and then expand the service you created in the previous section.

5. Click **Function Node – *name*** where *name* is the name you used in step 8 in the previous section. The configuration parameters for this service display in the right pane. Figure 12 shows our example.

Figure 12: *Service Graph properties*

Configuring Service Parameters

Use this section for editing the parameters exposed to APIC though the F5 package. This section contains the following categories:
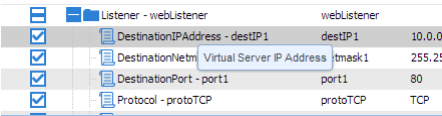
- *Helpful Hints When Editing Parameters* on this page
- *Choosing the function for your application on page 16*
    - » *Configuring Service Parameters for L4-L7 Service Load Balancing Use Cases on page 16*
    - » *Configuring Service Parameters for Microsoft SharePoint Use Cases on page 22*

Helpful Hints When Editing Parameters

Use the following guidance to improve your experience when editing parameters.

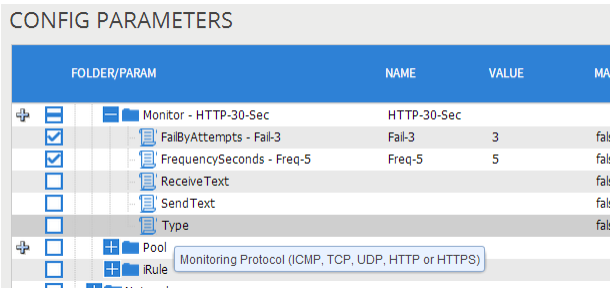#### Viewing mouseover hints for parameters

If you hover your mouse over a parameter, a hint displays with a summary description. The following image shows the hint for **DestinationIPAddress - destIP1**.

Figure 13: *Mouseover hint*

You can also use the hints to view the valid values available for a particular field. In the Figure 14, you can see that the valid monitor **Type** values are ICMP, TCP, UDP, HTTP or HTTPS.

Figure 14: *Mouseover hint showing valid values*

Adding Additional Instances of a Folder or Parameter

Some folders and parameters allow for multiple instances. When a plus (**+**) icon is present in the far left of the row (seen in the following image), it indicates the F5 BIG-IP Device Package for Cisco APIC supports multiple instances of the folder or parameter.

Figure 15: *Icon signifying the ability to add multiple instances*

In this example, you can configure multiple **ExternalSelfIP** folders, and multiple instances of the parameters inside; this is not permitted for **SNATPool**, as it does not have the icon.

Preventing error messages

One common error message you may encounter when configuring a value states **Please Update the parent folder first**.

This occurs when a required value on a parent folder is not set. The value on the parent folder must be set prior to configuring values in the folder. In the following example, attempting to update the **SelfIPAddress** field causes the error because the **ExternalSelfIP** folder does not have a value for Name. Once you give **ExternalSelfIP** a name, you can edit any of the parameters in the folder.

Figure 16: *Error message because the Name value on the folder is not set*
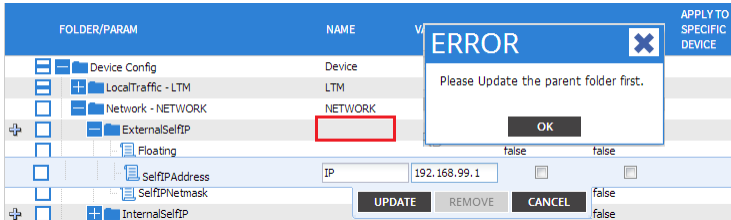
Providing a folder name is necessary because it is possible to have parameters relate to a specific folder and parameter in another part of the configuration. For example, you may create an object in **Device Config/LocalTraffic/Pool** and the Functional Config may have a parameter designed to refer to it. These are called *relations* and this is the method for addressing and/or referring to those objects from another part of the configuration. The following sections show examples of this type of configuration.

Parameter and Folder Names

When configuring a Service Graph, you need to supply a name for each parameters and folder that is a part of your configuration. This occurs in the APIC UI. You can see the location of the Name column in the following image.

Figure 17:   *Config Parameters Name column*

There is no strict naming convention for these names– you are free to name objects in a manner suiting your environment. The F5 BIG-IP Device Package for Cisco APIC does not have a dependency on the names. For referential parameters, Cisco APIC uses the name to make the path to the reference.

Configuration Order

There are two top-level folders for the F5 BIG-IP Device Package for Cisco APIC functions: Device Config and Function Config.

Figure 18:   *Top-level folders*

The Device Config folder contains device-level objects that could be shared between one or more Service Graphs for a given tenant.

The Function Config folder contains configuration objects local to a Service Graph. These objects may have explicit parameters you can specify (a virtual IP address for example) or may have references to device-level configuration objects (such as a Pool).

You modify parameters first in the Device Config section and then in the Function Config. All configuration tasks occur in the CONFIG PARAMETERS pane.

For more details on Device Config and Function Config, see Chapter 7 of the **Cisco APIC Layer 4 to Layer 7 Services Deployment Guide**.

Choosing the function for your application

The F5 BIG-IP Device Package for Cisco APIC supports two functions:

➤ **Virtual-server**
Use this function when you want to create an L4-L7 load balancing application on the BIG-IP system through Cisco APIC. This function permits you to specify the essential configuration elements of these service types.

➤ **Microsoft-SharePoint**
Use this function when you want to create a Microsoft SharePoint service. This service is tailored specifically for SharePoint and uses the SharePoint iApp template on the BIG-IP system for managing the configuration.

Each service graph has a one-to-one mapping to a F5 BIG-IP Device Package for Cisco APIC function. This means you cannot create a service with two functions in the same node – you must choose one.

The following sections provide specific descriptions and steps for each of the two functions offered in the F5 BIG-IP Device Package for Cisco APIC. Be sure to use the correct section when you are ready to configure your service.

Configuring Service Parameters for L4-L7 Service Load Balancing Use Cases

This section describes how to configure the parameters that are exposed for the L4-L7 service load-balancing use case. If you are using the SharePoint use case, see *Configuring Service Parameters for Microsoft SharePoint Use Cases on page 22.*

Summary of Parameters Available for Configuration
The following table shows the parameters that are exposed to APIC through the F5 BIG-IP Device Package for Cisco APIC. Refer to the BIG-IP documentation, such as **BIG-IP TMOS: Concepts** or **BIG-IP Local Traffic Manager: Concepts**, if you are unfamiliar with any of the F5 terms.

➡ *Note*

This table contains a subset of the parameters available on the BIG-IP system. In future versions of the F5 BIG-IP Device Package, additional parameters may be exposed. If a parameter is not exposed via APIC, the BIG-IP system uses the default setting.

Folder Path	Parameter Name	Description
Device Config -> LocalTraffic -> ClientSSL	Certificate	Client SSL certificate file name. It must be present on the BIG-IP system prior to deploying the Service Graph
	Key	Client SSL key file name. It must be present on the BIG-IP system prior to deploying the Service Graph
	KeySecret	Client SSL password used to decrypt the Client SSL key file
Device Config -> LocalTraffic -> FastL4	IdleTimeout	Connection idle time (in seconds) required to make a connection a candidate for deletion
Device Config -> LocalTraffic -> HTTP	Pipelining	Allow pipelining of HTTP requests
	XForwardedFor	Insert the X-Forwarded-For header in HTTP connections

Folder Path	Parameter Name	Description
Device Config -> LocalTraffic -> Monitor	FailByAttempts	Number of times a monitor must fail in order to trigger a service down event
	FrequencySeconds	Monitoring frequency, in seconds
	ReceiveText	Monitor receive string
	SendText	Monitor send string
	Type	Monitor type
Device Config -> LocalTraffic -> Pool	ActionOnServiceDown	Action to take when a pool member has a state of Down.
	LBMethod	Load balancing algorithm
Device Config -> LocalTraffic -> Pool -> Member	ConnectRateLimit	Connect rate limit
	ConnectionLimit	Connection limit
	IPAddress	Pool member IP address
	Port	Pool member port
	Ratio	Ratio for load balancing algorithm
Device Config -> LocalTraffic -> Pool -> PoolMonitor	PoolMonitorRel	Reference to pool monitor to use for this pool definition. Note the path consists of the name of your LocalTraffic folder, a forward slash (**/**), and then the name of your Monitor folder. For example, *LTM/monitor*.
Device Config -> LocalTraffic -> iRule	iRuleName	Name of the iRule to use. Note the iRule must exist on the BIG-IP system prior to deploying a Service Graph.
Device Config -> Network -> ExternalSelfIP	Floating	Enable floating for Self IP. Must be **YES** or **NO**.
	SelfIPAddress	External Self IP address
	SelfIPMask	External Self IP mask
Device Config -> Network -> InternalSelfIP	Floating	Enable floating for Self IP. Must be **YES** or **NO**.
	SelfIPAddress	Internal Self IP address
	SelfIPMask	Internal Self IP mask
Device Config -> Network -> Route	DestinationIPAddress	Destination IP address
	DestinationNetmask	Destination network mask
	NextHopIPAddress	Next hop router IP address
Device Config -> Network -> SNATPool	SNATIPAddress	Source IP address for SNAT
Function Config -> ClientSSL	ClientSSLRel	Reference to the Client SSL object to use. Note the path consists of the name of your LocalTraffic folder, a forward slash (**/**), and then the name of your Device Config -> LocalTraffic -> ClientSSL folder. For example, *LTM/ssl*.
Function Config -> FastL4	FastL4Rel	Reference to the FastL4 object to use. Note the path consists of the name of your LocalTraffic folder, a forward slash (**/**), and then the name of your Device Config -> LocalTraffic -> FastL4 folder. For example, *LTM/l4.*
Function Config -> HTTP	HTTPRel	Reference to the HTTP object to use. Note the path consists of the name of your LocalTraffic folder, a forward slash (**/**), and then the name of your Device Config -> LocalTraffic -> HTTP folder. For example, *LTM/http.*
Function Config -> HTTPRedirect	HTTPRedirectRel	Reference to the HTTPRedirect object to use. Note the path consists of the name of your LocalTraffic folder, a forward slash (**/**), and then the name of your Device Config -> LocalTraffic -> HTTPRedirect folder. For example, *LTM/http-redirect.*

Folder Path	Parameter Name	Description
Function Config -> Listener	DestinationIPAddress	Virtual service IP address
	DestinationNetmask	Virtual service network mask
	DestinationPort	Virtual service port
	Protocol	Virtual server protocol, valid values are **TCP** or **UDP**
	SourceIPAddress	Allowed client source address or network
	SourceNetmark	Allowed client source netmask
Function Config -> NetworkRelation	NetworkRel	Reference to the Network object to use. Note the path consists of the name of your Device Config-> Network folder
Function Config -> Pool	EPGConnectRateLimit	Connect rate limit
	EPGConnectionLimit	Connection limit
	EPGDestinationPort	Destination port for endpoint pool members
	EPGRatio	Ratio for load balancing algorithm
	PoolRel	Reference to the Pool object to use. Note the path consists of the name of your LocalTraffic folder, a forward slash (**/**), and then the name of your Device Config -> LocalTraffic -> Pool folder. For example, *LTM/http-redirect*
Function Config -> iRule	iRuleRel	Reference to the iRule object to use. Note the path consists of the name of your LocalTraffic folder, a forward slash (**/**), and then the name of your Device Config -> LocalTraffic -> iRule folder. For example, *LTM/my-irule*

Configuration Steps

In this section, we provide guidance for a minimal configuration, which includes Device Config and Function Config parameters. You may specify additional parameters as necessary to ensure your application behaves as desired. If you are familiar with the BIG-IP system, the parameters exposed in APIC are designed to mirror those available directly on the BIG-IP system. For detailed description of these parameters, please refer to the BIG-IP documentation.

Device Config Parameters
Use the following section to configure the Device Config parameters for the L4-L7 Service Load Balancing use case.

To configure the Device Config parameters

1. Expand the **Device Config** folder.

2. Double-click **LocalTraffic**.

    a. In the **Name** field, type a name. We use **LTM**.

    b. Click **UPDATE** to save.

3. Expand **LocalTraffic**. All the parameters for the Device portion of the configuration appear.

4. Double-click **Monitor**.

    a. In the **Name** field, type a name. We use **MONITOR**.

    b. Click **UPDATE** to save.

5. Under Monitor, double-click **FailByAttempts**.

    a. In the **Name** field, type a name. We use **FailedAttempts**.

    b. In the **Value** field, type a number value. We use **3**.

    c. Click **UPDATE** to save.

6. Under Monitor, double-click **FrequencySeconds**.

a. In the **Name** field, type a name. We use **FrequencySeconds**.

b. In the **Value** field, type a number value. We use **2**.

c. Click **UPDATE** to save.

7. Under Monitor, double-click **Type**.

a. In the **Name** field, type a name. We use **TCP**.

b. In the **Value** field, type a value. We use **TCP**.

c. Click **UPDATE** to save.

8. Under **Device Config** -> **LocalTraffic**, double-click **Pool**.

a. In the **Name** field, type a name for the pool. We use **WebServers**.

b. Click **UPDATE**.

9. Under **Pool**, double-click **Member** to add the pool members. The pool member configuration uses the same general pattern as the monitor parameters you just completed.

a. In the **Name** field, type a name for the pool member. We use **S1**.

b. Click **UPDATE**.

c. Click the expand icon (+) to expand the pool member you just added. We expand **S1**.

d. Double-click **IPAddress**.

i). In the **Name** field, type a name. We use **IP**.

ii). In the **Value** field, type the IP address for the pool member.

iii). Click **UPDATE**.

e. Double-click **Port**.

i). In the **Name** field, type a name. We use **Port**.

ii). In the **Value** field, type the port number for the pool member.

iii). Click **UPDATE**.

f. To include additional pool members, click the plus (**+**) icon to the far right of the member you just created, and then return to step **a** to repeat this procedure. Repeat for each pool member you want to add.
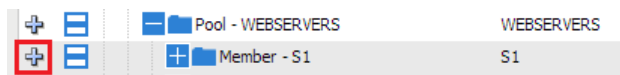
Figure 19: *Add icon for additional pool members*

10. Collapse the **LocalTraffic** folder under **Device Config**.

11. Expand **Device Config** -> **Network**.

12. Double-click the **Network** folder.

a. In the **Name** field, type a name for the network. We use **Network**. Make note of the name you use here, as you need to recall it in the Function Config procedure.

b. Click **UPDATE**.

13. Double-click the **ExternalSelfIP** parameter in the Network folder.

a. In the **Name** field, type a name.

b. Click **UPDATE**.

      c.   Double-click **SelfIPAddress**.

          i).   In the **Name** field, type a name. We use **ExSelfIP**.

          ii).   In the **Value** field, type the IP address you want to use for the BIG-IP external self IP address.

          iii).   Click **UPDATE**.

      d.   Double-click **SelfIPmask**.

          i).   In the **Name** field, type a name. We use **ExSelfIPmask**.

          ii).   In the **Value** field, type the network mask for the external self IP address.

          iii).   Click **UPDATE**.

14. Double-click the **InternalSelfIP** parameter in the Network folder.

      a.   In the **Name** field, type a name.

      b.   Click **UPDATE**.

      c.   Double-click **SelfIPAddress**.

          i).   In the **Name** field, type a name. We use **InSelfIP**.

          ii).   In the **Value** field, type the IP address you want to use for the internal self IP address.

          iii).   Click **UPDATE**.

      d.   Double-click **SelfIPmask**.

          i).   In the **Name** field, type a name. We use **InSelfIPmask**.

          ii).   In the **Value** field, type the network mask for the internal self IP address.

          iii).   Click **UPDATE**.

15. Close the **Device Config** folder.

This completes the Device Config portion of the configuration.

Function Config Parameters

Use the following section to configure the Function Config Parameters for the L4-L7 Service Load Balancing use case.

To configure the Function Config parameters

1.   Expand the **Function Config** folder.

2.   Double-click the **Listener** folder. The Listener is the virtual IP address hosted on the BIG-IP system.

      a.   In the **Name** field, type a name.

      b.   Click **UPDATE**.

      c.   Double-click **DestinationIPAddress**.

          i).   In the **Name** field, type a name. We use **DestIP**.

          ii).   In the **Value** field, type the IP address for the BIG-IP virtual server.

          iii).   Click **UPDATE**.

      d.   Double-click **DestinationNetmask**.

          i).   In the **Name** field, type a name. We use **DestMask**.

          ii).   In the **Value** field, type the network mask for the virtual server.

          iii).   Click **UPDATE**.

      e.   Double-click **DestinationPort**.

          i).   In the **Name** field, type a name. We use **DestPort**.

ii). In the **Value** field, type the service port for the virtual server.

iii). Click **UPDATE**.

f. Double-click **Protocol**.

i). In the **Name** field, type a name. We use **TCP**.

ii). In the **Value** field, type either **TCP** or **UDP**. We use **TCP**.

iii). Click **UPDATE**.

g. You can optionally include additional properties. Refer to the *Summary of Parameters Available for Configuration on page 16* for a list of available parameters.

When you are finished, this should look like similar to the following:

	Listener - Listener	Listener				false
☑	DestinationIPAddress - IP	IP	10.10.99.100	false		false
☑	DestinationNetmask - Mask	Mask	255.255.255.0	false		false
☑	DestinationPort - Port	Port	80	false		false
☑	Protocol - Protocol	Protocol	TCP	false		false
☐	SourceIPAddress			false		false
☐	SourceNetmask			false		false

Figure 20: *Listener and associated configuration*

3. Double-click **NetworkRelation**.

a. In the **Name** field, type a name. We use **NetworkRelation**.

b. Click **UPDATE**.

4. In the **NetworkRelation** folder, double click **NetworkRel**.

a. In the **Name** field, type a name.

b. In the **Value** field, type a value. This must be the same as the name provided for the **Device Config -> Network** folder you used in step 12a in the preceding procedure. We use **Network**.

c. Click **UPDATE**.

➡ **Note**

As a reminder, the Device Config contains device-level configuration and the Function config contains Service Graph local configuration. Because network information can be shared between Service Graphs, it is specified in the Device Config section, and the Function Config section refers to that object.

2. Double-click the **Pool** folder.

a. In the **Name** field, type a name. We use **Pool**.

b. Click **UPDATE**.

3. In the **Pool** folder, double click **PoolRel**.

a. In the **Name** field, type a name. We use **LBPoolrel**.

b. In the **Value** field, type a value. This must be the path to the pool name configured in the Device Config section. This path is formed by the name provided to Device Config -> LocalTraffic (in step 2a), a forward slash (**/**), and then the name provided to Device Config -> LocalTraffic -> Pool (in step 8a). For example, if the name given to LocalTraffic is **LTM** and the name given the Pool is **WebServers**, the value for PoolRel is **LTM/WebServers**. The values are case sensitive, so make sure they match.

c. Click **UPDATE**.

This completes our example of a basic L7 server load balancing service. You can use the *Summary of Parameters Available for Configuration on page 16* for a list of additional parameters not included in our example. Note that at this point, the configuration has not been sent to the BIG-IP system.

Continue with *Configuring a Device Cluster Selection Policy on page 25*.

Configuring Service Parameters for Microsoft SharePoint Use Cases

This section describes the how to configure the parameters for the Microsoft SharePoint use case. The F5 BIG-IP Device Package for Cisco APIC deploys the Microsoft SharePoint using the **f5.microsoft_sharepoint_2010** iApp template (for information about iApps® templates, see
http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf and *https://devcentral.f5.com/wiki/iapp.homepage.ashx*).

Summary of Parameters Available for Configuration
The following table shows the parameters that are exposed to APIC through the F5 BIG-IP Device Package for Cisco APIC. Refer to the BIG-IP documentation, such as **BIG-IP TMOS: Concepts** or **BIG-IP Local Traffic Manager: Concepts**, if you are unfamiliar with any of the F5 terms.

➡ **Note**

This table contains a subset of what is available in the iApp – in future versions of the F5 BIG-IP Device Package, additional parameters may be exposed. If a parameter is not exposed via APIC, the BIG-IP system uses the default setting.

Folder Path	Parameter Name	Description
Device Config -> Network -> ExternalSelfIP	**Floating**	Enable floating for Self IP. Must be **YES** or **NO**
	SelfIPAddress	External Self IP address
	SelfIPMask	External Self IP mask
Device Config -> Network -> InternalSelfIP	**Floating**	Enable floating for Self IP. Must be **YES** or **NO**
	SelfIPAddress	Internal Self IP address
	SelfIPMask	Internal Self IP mask
Device Config -> Network -> Route	**DestinationIPAddress**	Destination IP address
	DestinationNetmask	Destination network mask
	NextHopIPAddress	Next hop router IP address
Function Config -> NetworkRelation	**NetworkRel**	Reference to the Network object to use. Note the path consists of the name of your Device Config-> Network folder
Function Config -> SharePoint2010	**FQDN**	Fully-qualified domain name to use for the SharePoint service
	VirtualAddress	Virtual server address for the SharePoint service
Function Config -> SharePoint2010 Member	**ConnectionLimit**	Number of connections permitted on the pool member
	IPAddress	IP address of the pool member
	Port	Port to use when accessing the pool member

Configuration Steps
In this section, we provide guidance for a minimal configuration for the SharePoint use case, which includes Device Config and Function Config parameters. You may specify additional parameters as necessary to ensure your application behaves as desired. If you are familiar with the SharePoint iApp template, the parameters exposed in APIC are designed to mirror those available directly on the BIG-IP system. For detailed description of these parameters, please refer to the BIG-IP documentation, or the SharePoint iApp deployment guide (*http://www.f5.com/pdf/deployment-guides/iapp-sharepoint-2010-2013-dg.pdf*).

Device Config Parameters

Use the following section to configure the Device Config Parameters for the Microsoft SharePoint use case.

To configure the Device Config parameters

1. Expand the **Device Config** folder, and then double-click the **Network** folder.

    a. In the **Name** field, type a name for the network. Make note of the name you use here, as you need to recall it in the Function Config procedure.

    b. Click **UPDATE**.

2. Double-click the **ExternalSelfIP** parameter in the Network folder.

    a. In the **Name** field, type a name.

    b. Click **UPDATE**.

    c. Double-click **SelfIPAddress**.

        i).   In the **Name** field, type a name.

        ii). In the **Value** field, type the IP address you want to use for the external self IP address.

        iii). Click **UPDATE**.

    d. Double-click **SelfIPmask**.

        i).   In the **Name** field, type a name.

        ii). In the **Value** field, type the network mask for the external self IP address.

        iii). Click **UPDATE**.

3. Double-click the **InternalSelfIP** parameter in the Network folder.

    a. In the **Name** field, type a name.

    b. Click **UPDATE**.

    c. Double-click **SelfIPAddress**.

        i).   In the **Name** field, type a name.

        ii). In the **Value** field, type the IP address you want to use for the internal self IP address.

        iii). Click **UPDATE**.

    d. Double-click **SelfIPmask**.

        i).   In the **Name** field, type a name.

        ii). In the **Value** field, type the network mask for the internal self IP address.

        iii). Click **UPDATE**.

4. Close the **Device Config** folder.

This completes the Device Config portion of the configuration.

Function Config Parameters

Use the following section to configure the Function Config Parameters for the Microsoft SharePoint use case.

To configure the Function Config parameters

1. Expand the **Function Config** folder, and then double-click **NetworkRelation**.

    a. In the **Name** field, type a name.

      b.   Click **UPDATE**.

2.   In the **NetworkRelation** folder, double click **NetworkRel**.

      a.   In the **Name** field, type a name.

      b.   In the **Value** field, type a value. This must be the same as the name provided for the **Device Config -> Network** folder you used in step 1a in the preceding procedure.

      c.   Click **UPDATE**.

3.   Double-click the **SharePoint2010** folder in the Function Config folder.

      a.   In the **Name** field, type a name.

      b.   Click **UPDATE**.

4.   Open the **SharePoint2010** folder and then double-click the **FQDN** parameter.

      a.   In the **Name** field, type a name.

      b.   In the **Value** field, type the FQDN of your SharePoint service.

      c.   Click **UPDATE**.

5.   Double-click the **VirtualAddress** parameter.

      a.   In the **Name** field, type a name.

      b.   In the **Value** field, type the IP address you want to use for the BIG-IP virtual server.

      c.   Click **UPDATE**.

6.   Open the **Member** folder inside the SharePoint2010 folder.

      a.   Double-click the **IPAddress** parameter.

           i).   In the **Name** field, type a name.

           ii).   In the **Value** field, type the IP address of a SharePoint server.

           iii).   Click **UPDATE**.

      b.   Double-click the **Port** parameter.

           i).   In the **Name** field, type a name.

           ii).   In the **Value** field, type the port your SharePoint servers use.

           iii).   Click **UPDATE**.

      c.   To include additional pool members, click the plus (**+**) icon to the far right of the member you just created, and then return to step **a** to repeat this procedure. Repeat for each pool member that you want to add.

This completes the SharePoint parameter configuration. At this point, the parameters of your SharePoint service have been specified to APIC and are ready for deployment to the BIG-IP system. Continue with the following section.

Configuring a Device Cluster Selection Policy

In some cases, you may want to direct intensive traffic to high-performance hardware-based BIG-IP systems, or low-performance traffic to BIG-IP virtual edition instances. In APIC, you can configure device cluster selection policies to steer specific Service Graphs to specific BIG-IP clusters in your environment.

To create a device cluster selection policy

1. On the top menu bar, click **TENANTS**.

2. On the sub-menu, click the name of the Tenant you are using.

3. Open the **Tenant** folder, and then open the **L4-L7 Services** folder.

4. Right-click the **Device Cluster Selection Policies** folder.

5. Select **Create Logical Device Context**. The Create Logical Device Context page opens.

6. From the **Contract Name**, **Graph Name**, and/or **Node Name** fields, you can choose where to place the Service Graphs. You can choose **any** as a wild card (to match all).

7. From the **Device Cluster** list, choose the BIG-IP cluster to use.
    Figure 20 shows two device clusters as possible targets for the graphs matching the selection criteria:

8. Click **SUBMIT** when your configuration is complete. Refer to the APIC documentation for additional details.

Figure 21: *Selecting the Service Graph to associate with the Contract*

Using the Logical Interface Contexts, you can specific networking information to configure on BIG-IP when the service graph is deployed.
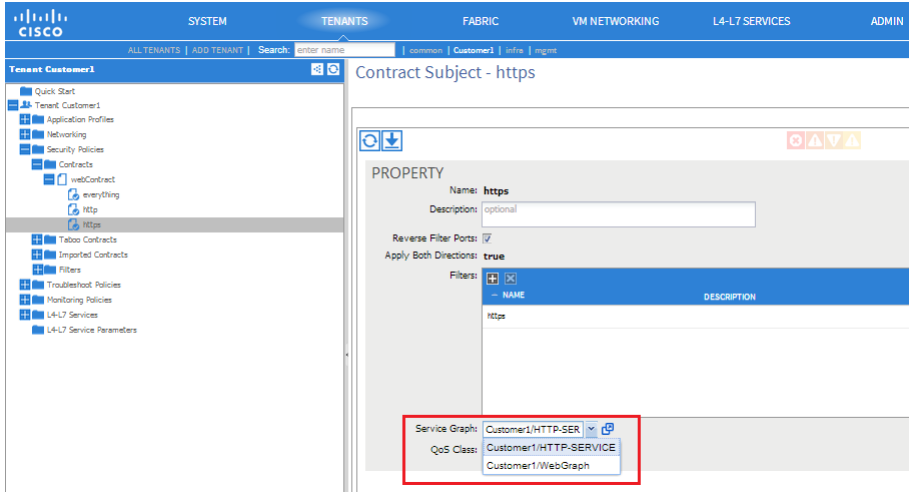
Attaching a Service Graph to a Contract

No matter which of the use cases you configured, the next task is to attach the Service Graph to a Contract. As stated in *Minimum Cisco APIC requirements on page 5*, you must have an existing Contract already configured on APIC. Refer to the **Cisco APIC Layer 4 to Layer 7 Services Deployment Guide** for more information about how to configure Contracts.

To attach a Service Graph to a contract

1. Open the **Tenant** folder, and then open the **Security Policies** folder.

2. Open the **Contracts** folder, and then open the contract to which you want to assign the Service Graph.

3. Under the Contract, click the Subject you want to assign to the Service Graph. For information about Subjects, refer to the APIC documentation.

4.   In the main pane, from the **Service Graph** list, select the Service Graph you created in *Creating a Service Graph on page 12*.

5.   Click **SUBMIT**.

Figure 22: *Selecting the Service Graph to associate with the Contract*

After completing this procedure, the configuration is pushed to the BIG-IP system.
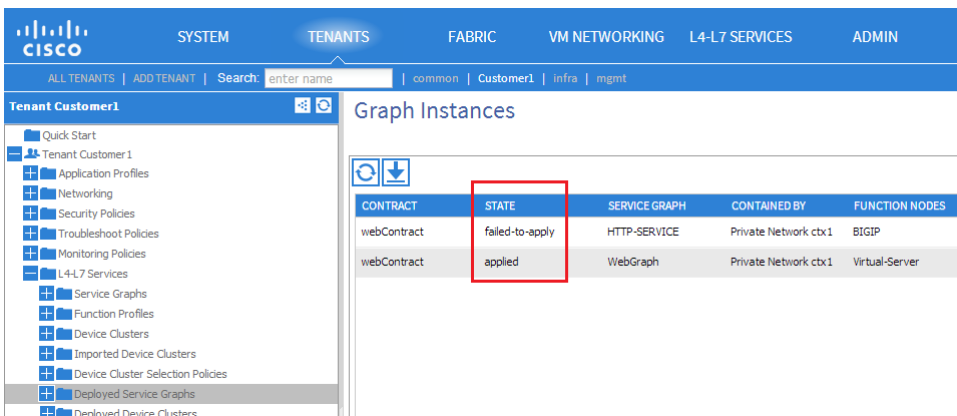
Checking the status of a Service Graph Deployment

The final task is to check the status of the Service Graph deployment, from APIC and from the BIG-IP system.

Checking the status of a Service Graph deployment from APIC

Use the following procedure to check the status of a Service Graph deployment using APIC.

1.   On the top menu bar, click **TENANTS**.

2.   On the sub-menu, click the name of the Tenant you are using.

3.   Open the **Tenant** folder, and then open the **L4-L7 Services** folder.

4.   Click the **Deployed Service Graphs** folder.

This causes the Graph Instances to show in the right pane.   The status of the deployment is shown under the STATE column. If the state is **applied**, it indicates the graph was successfully deployed to the BIG-IP system. The following image shows both a graph that failed (**failed-to-apply**) and a graph that succeeded (**applied**).

Figure 23: *Checking the status of the Service Graph*

Checking the Status of a Service Graph Deployment – from the BIG-IP system

If your Service Graph is showing a state of *applied* in APIC, you can log into your BIG-IP system to check the configuration. This allows you to verify it is in sync with the configuration you specified using the APIC UI.

Each Tenant in APIC with a Service Graph deployed to the BIG-IP system is assigned a partition in the form of **xxxx_apic**, where xxxx is an APIC tenant ID. To view the Partition list, on the Main tab, click **System > Users > Partition List**.
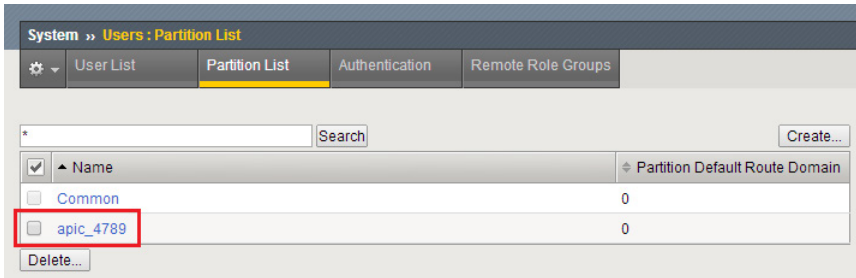

Figure 24: *BIG-IP Partition list showing the APIC tenant ID*

Each tenant with a deployed Service Graph is assigned a randomly-generated route domain ID. To view the list of Route Domains, on the Main tab, click **Network > Route Domains**.
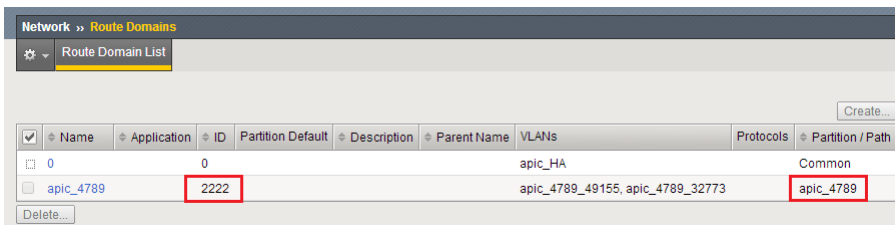

Figure 25: *BIG-IP Route Domain list*

You can check to see the correct Self IP addresses were programmed as configured on APIC. To view the Self IP list, on the Main tab, click **Network > Self IPs**.
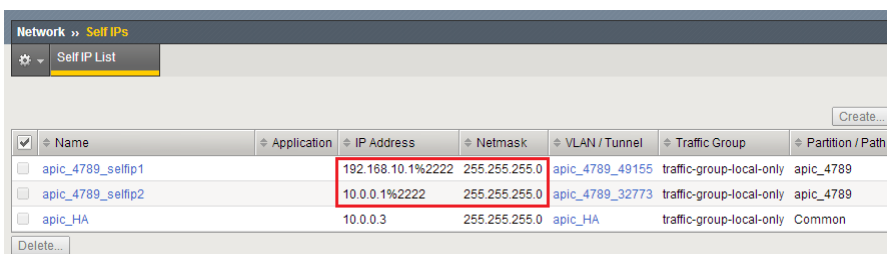

Figure 26: *BIG-IP Self IP list*

If you return to the APIC UI, you can see the external Self IP of 10.0.0.1 mask 255.255.255.0 matches the BIG-IP system configuration.
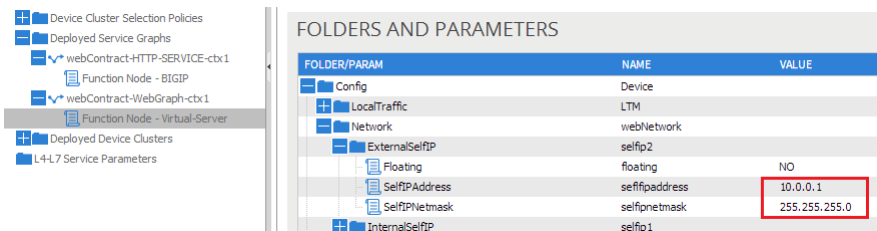

Figure 27: *Verifying the Self IP and Mask values match the BIG-IP configuration*

You can check other aspects of your L7 configuration on the BIG-IP system, such as virtual servers, pool members and so on. As you change the parameters of the graph, APIC automatically configures the BIG-IP system with the changes.

This completes the configuration. If you are having any issues, see *Troubleshooting on page 29* and *Frequently Asked Questions on page 30.*

Troubleshooting

This section describes troubleshooting steps you can take to resolve issues.

Ensuring your configuration is in sync

Cisco APIC maintains a representation of your configuration as specified using the user interface or the northbound API (using XML POSTs, for example). As configuration changes on Cisco APIC, it is pushed to the BIG-IP system by the F5 BIG-IP Device Package for Cisco APIC.

If a configuration change is not occurring on the BIG-IP system as expected, follow these steps:

1. Log into APIC, and then locate the Service Graph exhibiting the problem.

2. Log into the BIG-IP system(s) to which the Service Graph is deployed.

3. Validate the BIG-IP systems, if using a redundant pair, are in sync. You can see the Configuration State in the upper left corner of the screen near the F5 logo. For more information about the Configuration state and synchronization, see the BIG-IP system documentation.

4. Validate the parameters configured on Cisco APIC match those configured on the BIG-IP system.

Health Score Calculation

Cisco APIC makes use of health scores to communicate the high-level status of the components in the ACI architecture. The F5 BIG-IP Device Package for Cisco APIC implements the health score assessment (i.e., determining the value). Using the Cisco APIC UI, you can examine specific parts of the Service Graph to obtain deeper detail, allowing you to correct issue affecting your application.

The F5 BIG-IP Device Package for Cisco APIC calculates two health scores.

> ➤ **Overall device health**
> For the overall device, the health is based on a weighted measure consisting of CPU usage, memory usage, and connections per second. As CPU and memory usage goes up, the health score goes down. As the rate of connections/second goes up, the health score goes down.

> ➤ **Virtual Server health**
> For virtual servers, the health score is calculated based on the pool status. If all pool members are reachable, the health score for a virtual server is reported as 100.   If two out five pool members are down, the health score for the virtual server is reported as 60.   Each virtual server's health score is computed separately.

Frequently Asked Questions

This section contains frequently-asked questions and answers.

Is the F5 BIG-IP Device Package for Cisco APIC provided at no charge to F5 customers?

Yes; currently, there are no plans to charge for use of the F5 BIG-IP Device Package for Cisco APIC.

If an issue is encountered with the F5 BIG-IP Device Package for Cisco APIC, how do customers obtain support from F5?

Customers using the F5 BIG-IP Device Package for Cisco APIC with the BIG-IP system receive support via their BIG-IP system support contract.

If I open a support case, what information is required?

You need to provide the following information to open a case:

- Version of your F5 BIG-IP Device Package for Cisco APIC

- Generate qkview(s) from your BIG-IP devices (one for each device in the target Device Cluster). For instructions on generating a qkview, see *http://support.f5.com/kb/en-us/solutions/public/12000/800/sol12878.html*.

Is there a forum where customers can discuss their experience, share POSTs, seek advice, and more?

Yes, go to *http://devcentral.f5.com/cisco* for the F5 forum about Cisco.

Document Revision History

Version	Description	Date
1.0	Initial release of this guide	08-11-2014