F5 BIG-IP Service Insertion with Cisco Application Centric Infrastructure using iWorkflow

August, 2016
**DEPLOYMENT GUIDE**  
F5 BIG-IP Service Insertion with Cisco ACI using iWorkflow

**Introduction** ........................................................................................................................................... 4

**PREFACE** .............................................................................................................................................. 4

**AUDIENCE** ........................................................................................................................................... 4

**SCOPE** .................................................................................................................................................. 4

**Cisco APIC OVERVIEW** ....................................................................................................................... 4

**Hardware and Software Support** ........................................................................................................ 6

**Cisco ACI** .............................................................................................................................................. 6

**F5 iWORKFLOW** ................................................................................................................................... 6

**F5 BIG-IP** ............................................................................................................................................... 7

**F5 iAPPS** .............................................................................................................................................. 7

**F5 iWorkflow Dynamic Device Package** ............................................................................................ 9

**F5 iWorkflow + Cisco ACI Supported Features** ................................................................................ 9

**F5 iWorkflow Dynamic Device Package** ............................................................................................ 9

**Cisco ACI L4-L7 Service Insertion Prerequisites** .......................................................................... 13

**Prerequisites** ....................................................................................................................................... 13

**F5 BIG-IP** .............................................................................................................................................. 13

**Access the Management IP Address** ............................................................................................... 13

**Install the License** .............................................................................................................................. 13

**F5 iWorkflow** ....................................................................................................................................... 15

**Cisco ACI** .............................................................................................................................................. 15

**Integrating the Virtual Machine Manager When Using Virtual Machines** .................................. 15

**Defining Fabric Access Policies to Communicate with F5 Hardware** ........................................ 15

**Creating Tenants** ................................................................................................................................. 16

**Create the VRF and Bridge Domain** ................................................................................................... 16

**Create the Application Profile and EPG** ............................................................................................ 16

**F5 BIG-IP Service Insertion with Cisco ACI using iWorkflow** ......................................................... 17

**Deployment Workflow** ....................................................................................................................... 17

**Cisco ACI, F5 iWorkflow And BIG-IP Terminologies** ..................................................................... 17

**BIG-IP: Import App Services iAPPS** ................................................................................................ 20

**iWorkflow Cloud: Device Discovery** .................................................................................................. 20

**iWorkflow Cloud: Create APIC Cloud Connector** .......................................................................... 22

**iWorkflow Cloud: Create Application Template** ............................................................................. 23

**iWorkflow Cloud: Dynamic Creation of Customized F5 Device Package** .................................... 29

**APIC: Import F5 Device Package** ...................................................................................................... 30

**APIC: Device Manager Configuration** ............................................................................................... 32

**(Optional) APIC: Chassis Manager Configuration** ............................................................................. 35

**APIC: Create L4-L7 Device With F5 VCMP Guests** ......................................................................... 39

**Assign APIC “Context Label” to BIG-IP Concrete Device** ............................................................ 47

**Export F5 L4-L7 Device** ..................................................................................................................... 48

**APIC: Create L4-L7 Device With F5 BIG-IP Appliance** ................................................................... 50

**APIC: Create L4-L7 Device With F5 BIG-IP Virtual Edition (VE)** .................................................. 54

**APIC: Create Service Graph Template** .............................................................................................. 54
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>APIC Function Profiles</td>
<td>55</td>
</tr>
<tr>
<td>APIC: CREATE ONE-ARM SERVICE GRAPH TEMPLATE</td>
<td>59</td>
</tr>
<tr>
<td>APIC: CREATE TWO-ARM SERVICE GRAPH TEMPLATE</td>
<td>61</td>
</tr>
<tr>
<td>APIC: ENABLE DYNAMIC ENDPOINTS ATTACH/DETACH</td>
<td>62</td>
</tr>
<tr>
<td>APIC: DEPLOY ONE-ARM SERVICE GRAPH TEMPLATE</td>
<td>64</td>
</tr>
<tr>
<td>APIC: DEPLOY TWO-ARM SERVICE GRAPH TEMPLATE WITH FUNCTION PROFILE AND DYNAMIC ENDPOINTS</td>
<td>75</td>
</tr>
<tr>
<td>F5 BIG-IP as Unmanaged Device in Cisco ACI</td>
<td>81</td>
</tr>
<tr>
<td>DEPLOYMENT WORKFLOW</td>
<td>81</td>
</tr>
<tr>
<td>APIC: CREATE UNMANAGED L4-L7 DEVICE</td>
<td>82</td>
</tr>
<tr>
<td>APIC: CREATE SERVICE GRAPH TEMPLATE USING UNMANAGED DEVICE</td>
<td>84</td>
</tr>
<tr>
<td>APIC: DEPLOY SERVICE GRAPH TEMPLATE USING UNMANAGED DEVICE</td>
<td>85</td>
</tr>
<tr>
<td>BIG-IP: CONFIGURE NETWORK PARAMETERS</td>
<td>86</td>
</tr>
<tr>
<td>BIG-IP: CONFIGURE VIRTUAL SERVERS</td>
<td>89</td>
</tr>
<tr>
<td>iWORKFLOW: DISCOVER DEVICE</td>
<td>89</td>
</tr>
<tr>
<td>iWORKFLOW: CREATE BIG-IP CLOUD CONNECTOR</td>
<td>91</td>
</tr>
<tr>
<td>iWORKFLOW: CREATE TEMPLATE FOR “ALL CLOUDS”</td>
<td>91</td>
</tr>
<tr>
<td>iWORKFLOW: CREATE APPLICATION USER / TENANT / ROLE</td>
<td>92</td>
</tr>
<tr>
<td>iWORKFLOW: LOGIN AS APPLICATION USER</td>
<td>94</td>
</tr>
<tr>
<td>iWORKFLOW: DEPLOY SERVICES BASED ON CATALOG TEMPLATE</td>
<td>96</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>101</td>
</tr>
<tr>
<td>APIC</td>
<td>101</td>
</tr>
<tr>
<td>iWORKFLOW</td>
<td>101</td>
</tr>
<tr>
<td>BIG-IP</td>
<td>101</td>
</tr>
</tbody>
</table>
Introduction

Preface
This document discusses how to deploy F5 BIG-IP Service Insertion with the Cisco® Application Centric Infrastructure (Cisco ACI™) using a customized device package generated by F5 iWorkflow. F5 iWorkflow manages application service catalog life cycle; and thru its capability to dynamically generate device package, this service catalog can be represented in Cisco ACI environment.

The topologies used in this document can be altered to reflect a setup and design that meets the customer's specific needs and environment.

Audience
This document is intended for use by network architects and engineers to aid in developing solutions for Cisco ACI and F5 L4-L7 service insertion and automation.

Scope
This document defines the deployment recommendations for BIG-IP service insertion integration into Cisco ACI architecture with F5 iWorkflow to provide network and application delivery services. Limited background information is included about other related components whose understanding is required for the solution implementation.

More details about the Cisco ACI design can be found in Cisco ACI design guide.

Information about Cisco ACI service insertion can be found in the Cisco ACI white paper.

Details about F5 BIG-IP LTM can be found in BIG-IP LTM documentation.

Cisco APIC Overview
The main characteristics of Cisco ACI include:

- Simplified automation by an application-based policy model
- Centralized management, automation, and orchestration
- Mixed-workload and migration optimization
- Secure and scalable multitenant environment
- Extensibility and openness: open source, open APIs, and open software flexibility for development and operations (DevOps) teams and ecosystem partner integration
- Investment protection (for both staff and infrastructure resources)

The APIC acts as a central point of configuration management and automation for L4-L7 services and tightly coordinates service delivery, serving as the controller for network automation (Figure 1). A service appliance (device) performs a service function defined in the service graph. One or more service appliances may be required to render the services required by a service graph. A single service device can perform one or more service functions.
The APIC enables the user to define a service graph or chain of service functions in the form of an abstract graph: for example, a graph of the web application firewall (WAF) function, the load-balancing function, and the network firewall function. The graph defines these functions based on a user-defined policy. One or more service appliances may be needed to render the services required by the service graph. These service appliances are integrated into the APIC using southbound APIs built into a device package that contains the XML schema of the F5 device model. This schema defines the software version, functions provided by BIG-IP LTM (SSL termination, Layer 4 server load balancing [SLB], etc.), parameters required to configure each function, and network connectivity details. It also includes Python scripts that map APIC events to function calls to BIG-IP.
Hardware and Software Support

Cisco ACI
The joint solution uses the Cisco Nexus® 9000 Series Switches (Figure 2).

Figure 2: Cisco ACI Solution
The solution described in this document requires the following components:

- Spine switches: The spine provides the mapping database function and connectivity among leaf switches.
- Leaf switches: The leaf switches provide physical and server connectivity and policy enforcement.
- APIC: The controller is the point of configuration for policies and the place at which statistics are archived and processed to provide visibility, telemetry, application health information, and overall management for the fabric. The APIC is a physical server appliance like a Cisco UCS® C220 M3 Rack Server.


F5 iWorkflow
F5 iWorkflow version 2.0.0 is being used in this deployment guide. For detail about F5 iWorkflow user documentation, please refer to: [https://support.f5.com/kb/en-us/products/iworkflow/versions.2-0-0.html](https://support.f5.com/kb/en-us/products/iworkflow/versions.2-0-0.html)
F5 BIG-IP

At the time when this document is created, F5 iWorkflow supports F5 VIPRION, BIG-IP, and BIG-IP Virtual Edition (VE) running software Versions 11.5.3 HF2, 11.6.0 HF6 and 12.0 can be integrated with Cisco ACI. For up-to-date F5 iWorkflow, Cisco ACI and F5 BIG-IP software compatibility matrix, please refer to: https://support.f5.com/kb/en-us/solutions/public/k/11/sol11198324.html

If the F5 VE is being used, VMware vSphere integration must be performed with APIC before you use VE. Cisco ACI can be closely integrated with the server virtualization layer. In practice, this integration means that instantiating application policies through Cisco ACI will result in the equivalent constructs at the virtualization layer (that is, port groups) being created automatically and mapped to the Cisco ACI policy.

After the integration with VMware vCenter is completed, the fabric or tenant administrator creates endpoint groups (EPGs), contracts, and application profiles as usual. Upon creation of an EPG, the corresponding port group is created at the virtualization level. The server administrator then connects virtual machines to these port groups.

F5 iApps

App Services iApps "appsvcs_integration_v1.0_001" is being used in this deployment guide. This iApps can be downloaded from: https://github.com/0xHiteshPatel/appsvcs_integration_iapp. The version of the App Services being validated in this deployment guide is MAJOR VERSION 1.0 and MINOR VERSION 008. You can check the App Services iApps version by clicking on iApps -> Templates, click on the iApps and view "Implementation":

---

**Figure 3: F5 BIG-IP HW and VE support in Cisco ACI**

If the F5 VE is being used, VMware vSphere integration must be performed with APIC before you use VE.
This deployment is developed using App Services iApps. Please check with local F5 resources if other F5 iApps are supported.
F5 iWorkflow Dynamic Device Package

F5 iWorkflow + Cisco ACI supported features

- vCMP HA Support with APIC Chassis Manager
  - Virtualized Clustered Multiprocessing (vCMP) is a feature of the BIG-IP® system that allows you to run multiple instances of the BIG-IP software on a single hardware platform
  - Thru APIC Chassis Manager, each F5 BIG-IP vCMP guest that act as concrete device can now be associated with a chassis, in F5 case, vCMP host. This will allow vCMP guests HA across two vCMP hosts
- iWorkflow HA Support with APIC Device Manager
  - Thru Cisco APIC Device Manager, a cluster of iWorkflow instances can be associated with the APIC Logical Device Cluster management, providing HA protection on iWorkflow / cluster level
- Dynamic endpoint attach and detach
  - Endpoints either can be pre specified into corresponding EPGs (statically at any time) or can be added dynamically as they are attached to the Cisco ACI. Endpoints are tracked by a special endpoint registry mechanism of the policy repository. This tracking gives the Cisco APIC visibility into the attached endpoints. APIC passes this information to the BIG-IP. From the BIG-IP’s point of view this end point attached is a member of a pool and hence converts the APIC call that the device package receives into an addition of a member into a particular pool

F5 iWorkflow Dynamic Device Package

F5 iWorkflow dynamic device package is created based on F5 iApps template. The iApps template will determine features supported in the device package.

F5 App Services iApps is designed to be consumed by upper layer orchestration and automation platform. This iApps is available under: https://github.com/0xHiteshPatel/appsvcs_integration_iapp

F5 App Services iApps supports the following features:

  - Deployment Control:
    - Strict Updates setting Control
    - Automated Statistics Handler Creation
    - Deployment mode override
    - Route Domain support
  - L4-7 Functionality: Statistics:
    - TLS/SSL
- HTTP
- Virtual Server/Pool HTTP/HTTPS ADC:
- X-Forwarded-For Header Insertion
- HTTP->HTTPS Redirect creation
- TLS/SSL Easy Cipher String L4 Security:
- L4 Firewall Policy Support
  - Dynamic IP Blacklisting/IP Intelligence (BIG-IP subscription required)
  - Static Blacklist Source Address List
  - Static Allowed Source Address List
- HTTP Strict Transport Security Header Insertion
- Web Application Firewall (ASM) policy bundling/deployment

Custom Extensions:
- Extensibility through custom TCL scripting
  - See include/custom_extensions.tcl for more info

Virtual Server Options:
- Administrative Attributes:
  - Name
  - Description
- L3/4 Functionality:
  - Types:
    - Standard
    - Performance/FastL4
    - Forwarding (L2/IP)
    - Internal - IP
  - Network Mask
  - Port
  - Protocol (tcp/udp)
  - L4 Protocol Profiles (Server/Client-side)
    - Access to any TMSH configurable attribute via 'create' syntax
  - SNAT
    - Automap
    - Pre-existing SNAT Pool
- Dynamic SNAT Pool creation
- Dynamic SNAT Pool referencing (Cisco APIC specific)
  - Connection Limits
  - Dynamic IP Blacklist/IP Intelligence Profiles
  - Source Port Behavior
  - Connection Mirroring
  - Advanced Option Support
    - Access to any TMSH configurable attribute
- L4-7 Functionality:
  - iRules:
    - Reference pre-existing iRules (ordering preserved)
    - Bundled iRules support
  - Advanced Profile Support
    - Reference any pre-existing policy on the device
  - SSL/TLS:
    - Dynamically created Client-SSL profiles
      - Reference pre-existing static Cert/Key
    - ‘auto’ mode to dynamically link pre-existing Cert/Key pair
    - Certificate Chain/Bundle
    - Cipher String
    - Advanced Option Support - Access to any TMSH configurable Client-SSL profile attribute
  - Profiles with create syntax support:
    - L4 Protocol (tcp/udp/fastL4)
    - HTTP
    - OneConnect
    - Compression
    - Request Logging
    - Server-SSL
  - Profiles without create syntax support:
    - Pre-existing Client-SSL
    - Default/fallback Persistence
    - Analytics
- Security Logging
- DoS Protection
- Access Specific (APM):
  - Access Profile
- Connectivity Profile
- Per-Request Profile

Pool Options:

- Administrative Attributes:
  - Name
  - Description
- Pre-existing Health Monitor
- Load Balancing Method
- Dynamic Member Update Defaults (Port)
- Members
  - IP/Pre-existing Node Name
  - Port
  - Connection Limit
  - Ratio
  - Priority Groups
  - Administrative State
- Advanced Option Support
  - Access to any TMSH configurable attribute

For most up-to-date App Services iApps details, please go to:
https://github.com/0xHiteshPatel/appsvcs_integration_iapp
Cisco ACI L4-L7 Service Insertion Prerequisites

Prerequisites
Review the design guide before proceeding to the L4-L7 service insertion configuration. The design guide will help you determine the L2-L3 networking elements and topology required for your use case.

Elements need to be preconfigured before you begin the L4-L7 service insertion.

F5 BIG-IP
Before BIG-IP can be used for L4-L7 service insertion, it needs access to the management network and it needs to be licensed out of band.

Access the Management IP Address
To learn more about how to assign a management IP address to BIG-IP, please go to: https://support.f5.com/kb/en-us/solutions/public/15000/000/sol15040.html

One method for accessing the management IP address, if you have console access to BIG-IP, is to use the `config` command,

1. Log in to the console.
2. Run the command `config` on the command line. A wizard will appear to help you assign the management IP address.

![F5 Management Port Setup](image)

*Figure 4: BIG-IP management IP config*

3. Click <No> and continue with the wizard to enter your own IP address and netmask and default route.

Install the License
You will need a registration key to apply the license.
From the GUI, follow these steps:

1. Log in to the GUI at `https://<mgmt_ip_address>` . The default username is `admin`, and the default password is `admin`.

2. From the Setup Utility menu, choose Network. Then click Finished.

3. After the configuration is saved, choose System from the main menu. Then choose License.

4. Apply the registration key to license the system and follow the wizard.

Click the following links for more information about license installation:

F5 iWorkflow

F5 iWorkflow is a virtual appliance, download iWorkflow 2.0.0 from https://downloads.f5.com/esd/product.jsp?sw=iWorkflow&pro=iWorkflow_v2.x

F5 iWorkflow is control plane only in Cisco ACI integration, please ensure F5 iWorkflow, F5 BIG-IP and Cisco APIC management connectivity (either OOB or inband) is established.

Since F5 iWorkflow is control plane only, it does not need to be integrated with Cisco ACI VMM.

Please follow F5 iWorkflow documentation for initial bring up and licensing: https://support.f5.com/kb/en-us/products/iworkflow/versions.2-0-0.html

F5 iWorkflow supports standalone mode or 3-peers cluster. For production environment, F5 recommends 3-peers cluster iWorkflow configuration in order to provide high availability. Please refer to iWorkflow High Availability guide for detail in configuring iWorkflow cluster: https://support.f5.com/kb/en-us/products/iworkflow/manuals/product/iworkflow-private-cloud-administration-2-0-0/12.html#conceptid

Cisco ACI

Integrating the Virtual Machine Manager When Using Virtual Machines

The APIC is a single-pane manager that automates the entire networking configuration for all virtual and physical workloads, including access policies and L4-L7 services. In the case of vCenter, all the networking functions of the VMware Virtual Distributed Switch (VDS) and port groups are performed using the APIC. The only task that a vCenter administrator needs to perform in vCenter is to place the virtual network interface cards (vNICs) in the appropriate groups that the APIC created.


Defining Fabric Access Policies to Communicate with F5 Hardware

Access policies govern the operation of switch access ports that provide connectivity to resources such as storage, computing, Layer 2 and Layer 3 (bridged and routed) connectivity, virtual machine hypervisors, L4-L7 devices, and so on. If a tenant requires interface configurations other than those provided in the default link, Cisco Discovery Protocol, Link Layer Discovery Protocol (LLDP), Link Aggregation Control Protocol (LACP), or Spanning Tree Protocol, an administrator must configure access policies to enable such configurations on the access ports of the leaf switches.

The following entities need to be configured to add a new device to the fabric:

- Physical and external domains
- VLAN pool
- Attachable access entity profile
- Interface policies
- Switch policies
For a detailed explanation of the steps for configuring these entities (look in the fabric connectivity section):

Creating Tenants

A tenant is a logical container or a folder for application policies. This container can represent an actual tenant, an organization, or a domain, or it can be used simply for convenience in organizing information. A tenant represents a unit of isolation from a policy perspective, but it does not represent a private network.

Create the VRF and Bridge Domain

A VRF (Virtual Routing and Forwarding) is a unique Layer 3 forwarding and application policy domain that provides IP address space isolation for tenants.

A bridge domain represents a Layer 2 forwarding construct within the fabric.

In BIG-IP, a tenant in the APIC maps to a partition in BIG-IP with an unique route domain (RD). A contextual VRF instance is represented in BIG-IP as a route domain.

For a typical deployment for one tenant, define:
- One private network
- One or more bridge domains
  - Two-arm Service Graph: two bridge domains (one representing the client subnet, and one representing the server subnet).
  - One-arm Service Graph: one bridge domain (this bridge domain can either be external, internal or F5 BIG-IP subnet)

Create the Application Profile and EPG

Application profiles contain one or more EPGs. Modern applications contain multiple components. For example, an e-commerce application might require a web server, a database server, data located in a SAN, and access to outside resources that enable financial transactions. The application profile contains as many (or as few) EPGs as necessary that are logically related to the capabilities of an application.

EPGs can be organized according to any of the following:
- The application they provide (such as SAP applications)
- The function they provide (such as infrastructure)
- Where they are in the structure of the data center (such as the DMZ)
- Whatever organizing principle that a fabric or tenant administrator chooses to use

For a detailed explanation of the EPG configuration steps:
F5 BIG-IP Service Insertion with Cisco ACI using iWorkflow

Deployment Workflow

1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)
10) APIC: Create Service Graph Template:
    A. One Arm
    B. Two Arm
    C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach
11) APIC: Deploy Service Graph Template

Cisco ACI, F5 iWorkflow and BIG-IP Terminologies

<table>
<thead>
<tr>
<th>Cisco ACI</th>
<th>F5 iWorkflow</th>
<th>F5 BIG-IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Package</td>
<td>Clouds APIC Connector</td>
<td></td>
</tr>
<tr>
<td>L4-L7 Service Functions</td>
<td>Catalog</td>
<td></td>
</tr>
<tr>
<td>L4-L7 Service Function</td>
<td>Template</td>
<td></td>
</tr>
<tr>
<td>Chassis</td>
<td></td>
<td>vCMP Host</td>
</tr>
<tr>
<td>Device Manager</td>
<td>iWorkflow cluster</td>
<td></td>
</tr>
<tr>
<td>L4-L7 Devices (Logical Device Cluster)</td>
<td>Cluster</td>
<td></td>
</tr>
<tr>
<td>Concrete Device</td>
<td>Devices</td>
<td>BIG-IP (vCMP guest / appliance / VE)</td>
</tr>
<tr>
<td>Tenant + VRF</td>
<td>Tenant</td>
<td>Partition + Route Domain</td>
</tr>
<tr>
<td>Cisco ACI</td>
<td>F5 iWorkflow</td>
<td>F5 BIG-IP</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Service Graph</td>
<td>Services</td>
<td>Application Services Virtual Server</td>
</tr>
<tr>
<td>Endpoint Group (EPG)</td>
<td>Server</td>
<td>Pool</td>
</tr>
<tr>
<td>Endpoint</td>
<td></td>
<td>Member</td>
</tr>
</tbody>
</table>

For Cisco ACI terminology, go to Cisco APIC Tenant space, go to “Quick Start”

There are many resources available. Click on the book icon, APIC terminologies are available:
Tenants
A tenant is a logical container or a folder for application policies. This container can represent an actual tenant, an organization, or a domain or can just be used for the convenience of organizing information. A tenant represents a unit of isolation from a policy perspective, but it does not represent a private network. A context is a representation of a private Layer 3 namespace or Layer 3 network. It is a unit of isolation in the ACI framework. A tenant can rely on several contexts. Contexts can be declared within a tenant (contained by the tenant) or can be in the "common" tenant. This approach enables provisioning both multiple private Layer 3 networks per tenant and shared Layer 3 networks used by multiple tenants.

The primary elements that the tenant contains are: filters, contracts, outside, bridge domains and application profiles that contain endpoint groups (EPGs). These entities and the policy model are described in About the Policy Model. Entities in the tenant inherit its policies. A tenant can contain one or more VRFs or contexts; each context can contain multiple bridge domains (BD).

A user requires read-write privileges for accessing and configuring policies in a domain. A tenant user can have specific privileges into one or more domains. In a multi-tenancy environment, the tenant provides group user access privileges so that resources are isolated from one another (such as for endpoint groups and networking). This isolation also enables different people to manage different tenants.

Three tenants are preconfigured:
- **common:** For defining policies that provide common behavior for all the tenants in the fabric. A policy defined in the common tenant is usable by any tenant.
- **mgmt:** For in-band and out-of-band connectivity configurations of hosts and fabric nodes (leafs, spines, and controllers).
- **infra:** For configuration related to the fabric infrastructure, including the context and bridge domain used for the fabric VXLAN overlay. Only EPGs configured under the infra tenant are allowed to associate with the overlay bridge domain, and these EPGs are implicitly allowed to communicate with each other with no contracts needed or allowed. The infra tenant can also be used to extend the fabric infrastructure to external systems that support overlay protocols such as VXLAN/GRE. For example, the infra tenant’s ‘default’ EPG can be used to configure a fabric infrastructure VLAN on leaf ports that are connected to hypervisors or switches supporting VXLAN encapsulation.

For more information, see About the Policy Model.

About the Policy Model
The ACI fabric policy model enables the specification of application requirements policies. The APIC automatically renders policies in the fabric infrastructure. When a user or process initiates an administrative change to an object in the fabric, the APIC first applies that change to the policy model and then applies the change to the actual managed endpoint. This approach is called a model-driven framework.

Policy Model Key Characteristics
Key characteristics of the APIC policy model include the following:
- As a model-driven architecture, the software maintains a complete representation of the administrative and operational state of the system (the model). The model applies uniformly to fabric, services, system behaviors, and virtual and physical devices attached to the network.
- The logical and concrete domains are separated; the logical configurations are rendered into concrete configurations by applying the policies in relation to the available physical resources. No configuration is carried out against concrete entities. Concrete entities are configured implicitly as a side effect of the changes to the APIC policy model. Concrete entities can be but do not have to be physical (such as a virtual machine or a VLAN).
- The system prohibits communications with newly connected devices until the policy model is updated to include the new device.
- Network administrators do not configure logical and physical system resources directly but rather define logical (hardware independent) configurations and APIC policies that control different aspects of the system behavior.

Managed object manipulation in the model relieves engineers from the task of administering isolated, individual component configurations. These characteristics enable automation and flexible workload provisioning that can locate any workload anywhere in the infrastructure. Network-attached services can be easily deployed, and the APIC provides an automation framework to manage the life cycle of those network-attached services.

Logical Constructs
The policy model manages the entire fabric, including the infrastructure, authentication, security, services, applications, and diagnostics. Logical constructs in the policy model define how the fabric meets the needs of any of the functions of the fabric. The following figure provides an overview of the ACI policy model logical constructs.
**BIG-IP: Import App Services iApps**

Workflow Progress:

1. **BIG-IP: Import App Services iApps**
2. iWorkflow Cloud: Device Discovery
3. iWorkflow Cloud: Create APIC Cloud Connector
4. iWorkflow Cloud: Create Application Template
5. iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6. APIC: Import Device Package
7. APIC: Device Manager configuration
8. (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9. APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)
10. APIC: Create Service Graph Template:
    A. One Arm
    B. Two Arm
    C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach
11. APIC: Deploy Service Graph Template

F5 iApps is a user-customized framework for deploying application, providing a flexible way to automate tasks and templatize F5 virtual server configurations.

The iApps must be exist in F5 BIG-IP in order to allow F5 iWorkflow to create an application template based on this iApps.

Download the App Services iApps from [https://github.com/0xHiteshPatel/appsvcs_integration_iapp](https://github.com/0xHiteshPatel/appsvcs_integration_iapp) to a location that is accessible by the BIG-IP(s) that is going to be used in Cisco ACI.

In the navigation pane on the left, go to iApps -> Templates, click “Import…”

---

**iWorkflow Cloud: Device Discovery**

Workflow Progress:

1. **BIG-IP: Import App Services iApps**
2. **iWorkflow Cloud: Device Discovery**
3. iWorkflow Cloud: Create APIC Cloud Connector
4. iWorkflow Cloud: Create Application Template
DEPLOYMENT GUIDE
F5 BIG-IP Service Insertion with Cisco ACI using iWorkflow

5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)
10) APIC: Create Service Graph Template:
    A. One Arm
    B. Two Arm
    C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach
11) APIC: Deploy Service Graph Template

By registering F5 BIG-IP under iWorkflow, iWorkflow will update the BIG-IP REST framework, ensuring reliable communications between iWorkflow and BIG-IP.

Upon log into iWorkflow, go to iWorkflow Cloud:

Under iWorkflow Cloud, select Devices:

Move the mouse over to Devices menu and click the "+" and select "Discover Device: to register the F5 BIG-IP with F5 iWorkflow:
Enter the BIG-IP management IP and login credentials. For BIG-IP HA setup, make sure discover both BIG-IP:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>BIG-IP mgmt IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>BIG-IP admin</td>
</tr>
<tr>
<td>Password</td>
<td>BIG-IP password</td>
</tr>
</tbody>
</table>

If the REST framework of the BIG-IP is not up-to-date, iWorkflow will push the supported REST framework to BIG-IP. Note: this process could take up to 10-minutes.

Upon successfully discovery, BIG-IP availability become “Available”

iWorkflow Cloud: Create APIC Cloud Connector

Workflow Progress:
1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) **iWorkflow Cloud: Create APIC Cloud Connector**

4) **iWorkflow Cloud: Create Application Template**

5) **iWorkflow Cloud: Dynamic creation of customized F5 Device Package**

6) **APIC: Import Device Package**

7) **APIC: Device Manager configuration**

8) *(OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)*

9) **APIC: Create L4-L7 Device using:**
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)

10) **APIC: Create Service Graph Template:**
    A. One Arm
    B. Two Arm
    C. *(OPTIONAL) Enable Dynamic Endpoints Attach/Detach*

11) **APIC: Deploy Service Graph Template**

Create the iWorkflow Cloud APIC Connectors which will generate a custom device package that contains iWorkflow service catalog. Go to iWorkflow Cloud menu, click "+":

Click the “+” to enter a new cloud. Enter and select the following to complete the creation of the APIC Cloud Connector:

Name: `<user_defined>`, for this example, use “VNG-iW”

Connector Type: “Cisco APIC”

Click “Save” to finish.

**iWorkflow Cloud: Create Application Template**

**Workflow Progress:**

1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)
10) APIC: Create Service Graph Template:
    A. One Arm
    B. Two Arm
    C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach
11) APIC: Deploy Service Graph Template

After BIG-IP is successfully discovered by iWorkflow, the iApps reside on BIG-IP are now exposed to iWorkflow. Create an application template inside iWorkflow Service Catalog. User can specify F5 virtual server requirements and build them into a template. Please note this deployment illustrate a common example, user can customize the template based on F5 virtual server requirements.

Select iWorkflow Catalog. When the Catalog menu appears on the screen, click + to continue:

A New Template screen will appear as the following:
Name: user defined name for the template, recommendation would be type of template for multiple application use, for example: HTTP-NoPersistence-Gold

Input Parameters:
- Accept Defaults: Use default values, no edit
- Common Options: Only provider template parameters available for edit
- All Options: All parameters available for edit

Cloud: Select Cisco APIC Cloud Connector created in previous step

Application Type: Select the App Services iApps
Click “Tenant Preview” will see the default value (provider template) of this iApps, those parameters are considered “Tenant Editable” and will be exposed to Cisco APIC thru device package.

By default, only VIP and Pool Member are tenant editable.

Click to go back for editing

Expand the Virtual Server Listener & Pool Configuration by clicking the >. Scroll down and CHECK the following to make them Tenant Editable. What this does is allow the parameters expose to Cisco APIC thru F5 device package. Administrator has total control over what is exposed via a custom device package (this reduces the complexity). It is highly recommended to expose only what is needed to APIC:

pool__addr: this is the VIP
pool__port: this is the VIP listening port

Notice: by default, this iApps allow VIP as tenant editable field. When you check VIP listening port as tenant editable, iWorkflow will highlight it as it is now different from default value.

- Name: this is the key, it is associated with underlying API to be used to configure BIG-IP
- Description: describe the function of the key
- Default Value: if leaves blank, it will use F5 BIG-IP default value, user can specify custom default value
- Tenant Editable: Only parameters mark “Tenant Editable” will be exposed to Cisco APIC

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
<th>Tenant Editable</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool__AdvOptions</td>
<td>Pool: Advanced Options</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pool__Description</td>
<td>Pool: Description</td>
<td>pool descr</td>
<td></td>
</tr>
<tr>
<td>pool__LbMethod</td>
<td>Pool: Load Balancing Method</td>
<td>round robin</td>
<td></td>
</tr>
<tr>
<td>pool__MemberDefPort</td>
<td>Pool: Member Default Port</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>pool__Monitor</td>
<td>Pool: Health Monitor</td>
<td>/Common/http</td>
<td></td>
</tr>
<tr>
<td>pool__Name</td>
<td>Pool: Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pool__addr</td>
<td>Virtual Server: Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pool__mask</td>
<td>Virtual Server: Mask</td>
<td>255.255.255.255</td>
<td></td>
</tr>
<tr>
<td>pool__port</td>
<td>Virtual Server: Port</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>pool__Members</td>
<td>Pool: Members</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Scroll down and expand the Virtual Server Configuration by clicking > to remove the default settings of the following to EMPTY (Tenant Editable is already UNCHECK):

- vs__ProfileDefaultPersist: this is the default persistence profile
- vs__ProfileFallbackPersist: this is the fallback persistence profile

This will remove the persistence profile from the template and APIC user cannot modify it
Click Save to complete the template:

Notice a new application template now under iWorkflow Cloud Catalog. The "Save" operation will also update the F5 iWorkflow Cloud APIC device package with the updated service catalog.

Double Click on the Template, then click “Tenant Preview”

<table>
<thead>
<tr>
<th>Catalog</th>
<th>HTTP-NoPersistence-Gold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>HTTP-NoPersistence-Gold</td>
</tr>
<tr>
<td>Input Parameters</td>
<td>Common Options</td>
</tr>
<tr>
<td>Cloud</td>
<td>VNG-W</td>
</tr>
<tr>
<td>Application Type</td>
<td>appsvcs_integration_v1.0.001</td>
</tr>
</tbody>
</table>

Tenant users will see a form that looks like this when deploying an application using this Catalog:

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Server: Address</td>
<td></td>
</tr>
<tr>
<td>Virtual Server: Port</td>
<td>80</td>
</tr>
<tr>
<td>Pool: Members</td>
<td></td>
</tr>
</tbody>
</table>
As expected, only “Virtual Server: Port” parameter is added to the list of parameters exposing to APIC. This service catalog is ready to be consumed by Cisco APIC.

**iWorkflow Cloud: Dynamic creation of customized F5 device package**

Workflow Progress:

1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) **iWorkflow Cloud: Dynamic creation of customized F5 Device Package**
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   - A. BIG-IP vCMP guest
   - B. BIG-IP appliance
   - C. BIG-IP Virtual Edition (VE)
10) APIC: Create Service Graph Template:
    - A. One Arm
    - B. Two Arm
    - C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach
11) APIC: Deploy Service Graph Template

Double click on the Clouds Connector “VNG-iW”, notice there is a link to download a customized F5 Device Package that contains this iWorkflow Service Catalog:

Click the Download Device Package “F5DevicePackage.zip” to save the custom device package to a location that is accessible by Cisco APIC.

The configuration steps on iWorkflow necessary prior to F5 ACI integration are completed.
APIC: Import F5 device package

Workflow Progress:
1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)
10) APIC: Create Service Graph Template:
    A. One Arm
    B. Two Arm
    C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach
11) APIC: Deploy Service Graph Template

Thru Cisco APIC, user can perform the workflow in deploying the HTTP application, with the integration of F5 iWorkflow and BIG-IP, user can apply HTTP application L4-L7 requirements within APIC policy model, reducing significant amount of operation complexity.

Import the customized device package generated by F5 iWorkflow into Cisco APIC. This will allow the iWorkflow service catalog available in Cisco APIC. The device package serves as a conduit to facilitate communications between F5 iWorkflow and BIG-IP.

Using APIC GUI and click the following to import the device package:

L4-L7 Services -> Packages

Under Quick Start, click “Import a Device Package”
A new pop-up should appear to allow you to choose the device package to be installed:

Click **BROWSE** and choose the previous downloaded device package - F5DevicePackage.zip and click **SUBMIT** to import the device package.
L4-L7 Service Device Type - F5-iWorkflow-2.0-VNG-iW

Click on Operation, notice only tenant editable parameters of the template is visible in Cisco APIC.

APIC: Device Manager Configuration

Workflow Progress:

1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
C. BIG-IP Virtual Edition (VE)

10) APIC: Create Service Graph Template:
   A. One Arm
   B. Two Arm
   C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach

11) APIC: Deploy Service Graph Template

In order to integrate F5 iWorkflow cluster into Cisco APIC L4-L7 devices, using Cisco APIC device manager feature to define and specify F5 iWorkflow.

From APIC perspective, F5 iWorkflow is a "device manager" managing the F5 BIG-IP ADC (both physical and virtual form factors).

First define the device manager type. In the APIC GUI, click the following to configure the Device Manager Type:

**L4-L7 Services -> Inventory -> Device Manager Type**

Click the **ACTIONS** button at the Work pane and choose **Create Device Manager Type**

A new pop up window will appear

- Vendor: F5 (this is the vendor info of this device manager)
- Model: iWorkflow (product model)
- Version: 2.0-VNG-iW (it is extremely important to state the version value 2.0-<name of the connector specify in iWorkflow>)
- L4-L7 Service Device Type: F5-iWorkflow-2.0-VNG-iW (select the device package)
- Device Manager: Leave this field empty

Click **SUBMIT**. The Device Manager Type is now created and can be associated with a Device Manager. Go to the APIC tenant where the L4-L7 device will be created. In this example, go to Tenant common:

**Tenants common -> L4-L7 Services -> Device Managers**

In the Work pane, click: **ACTIONS -> Create Device Manager**
A new pop up appear:

- **Device Manager Name**: User defined
- **Management EPG**: Leave it blank (only use for inband management)
- **Device Manager Type**: Select the type created
- **Management**: adding each iWorkflow management IP
- **Username**: iWorkflow admin username
- **Password / Confirm Password**: iWorkflow admin password (Notice, all three iWorkflow virtual appliance must have the same admin password)
Click SUBMIT.

This complete the steps to create APIC L4-L7 device manager. This device manager will be used later when creating APIC L4-L7 device.

**(OPTIONAL) APIC: Chassis Manager Configuration**

**Workflow Progress:**

1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) *(OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)*
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
B. BIG-IP appliance
C. BIG-IP Virtual Edition (VE)

10) APIC: Create Service Graph Template:
A. One Arm
B. Two Arm
C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach

11) APIC: Deploy Service Graph Template

If APIC L4-L7 Device using F5 vCMP guest, user will need to configure APIC chassis manager in order to specify the vCMP host information.

From APIC perspective, F5 BIG-IP vCMP host is a "chassis manager" managing the F5 BIG-IP vCMP guest.

First define the chassis manager type. In the APIC GUI, click the following to configure the Chassis Manager Type:

L4-L7 Services -> Inventory -> Chassis Manager Type

Click the ACTIONS button at the Work pane and choose Create Chassis Manager Type

A new pop up window will appear

- Vendor: F5 (this is the vendor info of this device manager)
- Model: iWorkflow (product model)
- Version: 2.0-VNG-iW (it is extremely important to state the version value 2.0-<name of the connector specify in iWorkflow>)
- L4-L7 Service Device Type: F5-iWorkflow-2.0-VNG-iW (select the device package)
- Chassis: Leave this field empty
Click SUBMIT. The Chassis Manager Type is now created and can be associated with a Chassis. Go to the APIC tenant where the L4-L7 device will be created. In this example, go to Tenant common:

Tenants common -> L4-L7 Services -> Chassis

In the Work pane, click: ACTIONS -> Create Chassis

A new pop up window will appear:

- Chassis Name: User defined
- Management EPG: Leave it blank (only use for inband management)
- Chassis Type: Select the type created
- Management: vCMP host management IP
- Username: vCMP host admin username
- Password / Confirm Password: vCMP host admin password

Duplicate this step for 2nd vCMP host in HA environment.
Click **Submit**.

This completes the steps to create APIC L4-L7 chassis manager. This chassis will be used later when creating APIC L4-L7 device that uses F5 vCMP guests as concrete devices.
APIC: Create L4-L7 Device with F5 vCMP guests

Workflow Progress:

1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)
10) APIC: Create Service Graph Template:
    A. One Arm
    B. Two Arm
    C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach
11) APIC: Deploy Service Graph Template

A L4-L7 device (also known as a logical device cluster, LDev) contains one or more devices (also known as concrete devices) that act as a logical entity, it also references F5 iWorkflow information. A L4-L7 device has logical interfaces, which describe the interface information for the logical device cluster. During service graph template rendering, function node connectors are associated with logical interfaces. The APIC allocates the network resources (VLAN or Virtual Extensible LAN [VXLAN]) for a function node connector during service graph template instantiation and rendering and
programs the network resources on the logical interfaces.

An administrator can set up a maximum of two concrete devices for a single logical device clusters in the active-standby mode.

The logical device cluster has information about BIG-IP credentials that the APIC will use to communicate with BIG-IP.

The logical device cluster can be created in tenant common or in your created tenant. The advantage of creating it in tenant common is that this logical device cluster can then be exported to multiple tenants and used by multiple tenants.

In this example, which is multi-tenant scenario, create the L4-L7 device in tenant common and export the L4-L7 device to user-defined tenant. Navigate to Tenant common to create a new L4-L7 Device by clicking the following:

Tenants common -> L4-L7 Services -> L4-L7 Devices

In the Work pane, click:

**ACTIONS -> Create L4-L7 Devices**

A new window should appear to create the L4-L7 Devices.
In the scenario where a pair of vCMP guests are used as concrete devices for APIC L4-L7 Devices:

<table>
<thead>
<tr>
<th>Field Description</th>
<th>What does it mean?</th>
<th>Value use in this example</th>
</tr>
</thead>
</table>
| Managed           | Managed: this L4-L7 device is managed and configured by Cisco APIC  
Unmanaged: L4-L7 device configuration is done by user | CHECK |
| Name              | User defined L4-L7 Device name | F5-vCMP-PodA |
| Service Type      | Firewall or ADC  
F5 BIG-IP is considered an ADC device | ADC |
<p>| Device Type       | Physical or Virtual form factor | Physical |
| Physical Domain   | Physical domain contains dynamic service insertion VLAN pool | ServiceManagedPhy (configured under APIC Fabric) |
| Mode              | Is L4-L7 Device a Single Node or HA Cluster? | HA Cluster |
| Device Package    | Name of the device package associated with this L4-L7 Device, available from pull-down menu | F5-iWorkflow-2.0-VNG-iW |</p>
<table>
<thead>
<tr>
<th>Field Description</th>
<th>What does it mean?</th>
<th>Value use in this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>BIG-IP Generic / BIG-IP VE Generic / Unknown: Pre-defined BIG-IP Interface name or manual input</td>
<td>Choose Unknown(Manual) provide flexibility to enter any F5 BIG-IP interface convention</td>
</tr>
<tr>
<td>Context Aware</td>
<td>Single Context device can be used by only 1 tenant + VRF; where Multi Context device can be shared among multiple tenants + VRFs</td>
<td>Multiple</td>
</tr>
<tr>
<td>APIC to Device Management Connectivity</td>
<td>Out-Of-Band or In-Band management</td>
<td>Out-Of-Band</td>
</tr>
<tr>
<td>Username</td>
<td>BIG-IP admin username</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>BIG-IP admin password</td>
<td>&lt;admin_password&gt;</td>
</tr>
<tr>
<td>Confirmed Password</td>
<td>Confirm BIG-IP admin password</td>
<td>&lt;admin_password&gt;</td>
</tr>
</tbody>
</table>

After completion, it should look like:

```
General

Managed: ☑
Name: F5-vCMP-PodA
Service Type: ADC
Device Type: PHYSICAL VIRTUAL
Physical Domain: ServiceManagedPhy
Mode: Single Node HA Cluster
Device Package: F5-iWorkflow-2.0-VNG-iW
Model: Unknown (Manual)
Context Aware: Multiple Single

Connectivity

APIC to Device Management Connectivity: Out-Of-Band In-Band

Credentials

Username: admin
Password: *****
Confirm Password: *****
```
On the right hand side of the wizard, in the Device 1, enter the following:

<table>
<thead>
<tr>
<th>Field Description</th>
<th>What does it mean?</th>
<th>Value use in this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP Address</td>
<td>Concrete device management IP address</td>
<td><code>&lt;vCMP_guest_management_IP&gt;</code></td>
</tr>
<tr>
<td>Management Port</td>
<td>HTTP or HTTPS</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Chassis</td>
<td>Optional: if chassis manager is used, select chassis. In F5 BIG-IP integration,</td>
<td>vCMPIHost80 for vCMP guest 1</td>
</tr>
<tr>
<td></td>
<td>this field identify the vCMP host of the vCMP guest</td>
<td>vCMPIHost86 for vCMP guest 2</td>
</tr>
<tr>
<td>Device Interfaces Name</td>
<td>Specify the physical interface connect between Cisco ACI and BIG-IP</td>
<td>VPC343 for vCMP guest 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VPC684 for vCMP guest 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This value must match with BIG-IP interface or trunk name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The “Name” is either BIG-IP interface, like 1_1, 1/1_1 or trunk name. Notice that “_” is used instead of “.” to specify BIG-IP interface, this is due to APIC use “.” as object delimiter</td>
</tr>
<tr>
<td>Device Interfaces Path</td>
<td>Specify the Cisco ACI interface (node and interface name) that connect to the device interface</td>
<td>Cisco ACI corresponding VPC</td>
</tr>
</tbody>
</table>

Repeat the same for Device 2, which would be vCMP guest #2

**Device 1**

- Management IP Address: vCMPI guest 1 mgmt IP
- Management Port: **https**
- Chassis: common/vCMPIHost80
- Device Interfaces:

<table>
<thead>
<tr>
<th>Name</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC343</td>
<td>Node-102-103/VPC-F5-Policy-Group</td>
</tr>
</tbody>
</table>

**Device 2**

- Management IP Address: vCMPI guest 2 mgmt IP
- Management Port: **https**
- Chassis: common/vCMPIHost86
- Device Interfaces:

<table>
<thead>
<tr>
<th>Name</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC684</td>
<td>Node-102-103/VPC2-F5-Policy-Group</td>
</tr>
</tbody>
</table>

Under the Cluster, which specify the L4-L7 device info. Notice Device 1 management IP is pre-populated as the cluster
management IP. Change the cluster management IP to one of the iWorkflow management IP. Since Device Manager will be used for this cluster, the cluster management IP will be ignored and “Device Manager” information will be used to establish communication.

<table>
<thead>
<tr>
<th>Field Description</th>
<th>What does it mean?</th>
<th>Value use in this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP Address</td>
<td>Concrete device management IP address</td>
<td>&lt;F5_iWorkflow_management_IP&gt;</td>
</tr>
<tr>
<td>Management Port</td>
<td>HTTP or HTTPS</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Device Manager</td>
<td>In F5 iWorkflow integration, Device Manager is mandatory and it specify iWorkflow cluster info</td>
<td>Select the Device Manager contains the iWorkflow cluster info</td>
</tr>
<tr>
<td>Cluster Interfaces</td>
<td>Map L4-L7 device logical consumer (external) and provider (internal) interfaces with the device(s) Interface(s), ensuring traffic will flow from abstract layer to rendering layer</td>
<td>In this example, since a single VPC is connected between BIG-IP and APIC, this VPC will serve as both consumer and provider interfaces.</td>
</tr>
<tr>
<td>Type</td>
<td>consumer / provider – APIC key to identify the role of the interface</td>
<td>Create one entry for consumer and one entry for provider</td>
</tr>
<tr>
<td>Name</td>
<td>User defined</td>
<td>F5 recommend using external (consumer) and internal (provider) to match F5 terminology</td>
</tr>
<tr>
<td>Concrete Interfaces</td>
<td>The physical interfaces of the concrete device (BIG-IP) that will be used for external or internal or both roles</td>
<td>Pick both device 1 and device 2 VPC. Repeat same for provider interface. Available as drop down menu item</td>
</tr>
</tbody>
</table>

Cluster

Management IP Address: iWorkflow Mgmt IP
Device Manager: common/VNG-iW

Cluster Interfaces:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Concrete Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>consumer</td>
<td>external</td>
<td>Device1/VPC343,Device2/VPC684</td>
</tr>
<tr>
<td>provider</td>
<td>internal</td>
<td>Device1/VPC343,Device2/VPC684</td>
</tr>
</tbody>
</table>

Click “NEXT” to move the Concrete Device configuration
Click “All Parameters” to enter BIG-IP specific information

<table>
<thead>
<tr>
<th>Field Description</th>
<th>What does it mean?</th>
<th>Value use in this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>BIG-IP host name in FQDN format</td>
<td>See below, value is user defined</td>
</tr>
<tr>
<td>NTP Server</td>
<td>NTP server IP, ensuring APIC, BIG-IP and iWorkflow use the same BTP server</td>
<td>&lt;NTP_Server_IP&gt;</td>
</tr>
<tr>
<td>Primary DNS IP Address</td>
<td>Primary DNS</td>
<td>&lt;Primary_DNS_Server_IP&gt;</td>
</tr>
<tr>
<td>Secondary DNS IP Address</td>
<td>Secondary DNS</td>
<td>&lt;Secondary_DNS_Server_IP&gt;</td>
</tr>
<tr>
<td>Syslog Server IP Address</td>
<td>Syslog Server IP</td>
<td>&lt;Syslog_Server_IP&gt;</td>
</tr>
</tbody>
</table>

Enter High Availability information, like HA interfaces, IP, marks, VLAN (locally significant, not manage by APIC)

<table>
<thead>
<tr>
<th>Field Description</th>
<th>What does it mean?</th>
<th>Value use in this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Availability Interface Name</td>
<td>BIG-IP Interface maintain HA heartbeat</td>
<td>1/1_8</td>
</tr>
<tr>
<td>High Availability Self IP Address</td>
<td>Local significant HA interface IP address</td>
<td>&lt;HA_Interface_IP&gt;</td>
</tr>
<tr>
<td>High Availability Self IP Netmask</td>
<td>HA interface netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>High Availability VLAN</td>
<td>HA VLAN (local significant, not visible or managed by APIC)</td>
<td>10</td>
</tr>
</tbody>
</table>

Since APIC “Chassis Manager” and “Device Manager” features are being used, leave VCMP and iWorkflow configuration blank
Click "FINISH" to complete the L4-L7 Device configuration.

A few minutes may be needed for all the configuration to be completed and the high-availability cluster to become stable. After the configuration is completed, navigating to the newly created L4-L7 Device to verify its Configuration State is stable:

Tenants common -> L4-L7 Services -> L4-L7 Devices -> <L4-L7 Device Name>

In the Work pane, ensure the Configuration State is stable, if the device is not stable, click the Faults tab and ensure no faults or all the faults are in clearing state.

Log into BIG-IP and confirm that the device group has been formed (it will contain one or two BIG-IP members depending on whether BIG-IP is deployed in standalone mode or high-availability mode).

The device should be online, active, and synchronized (only if you are deploying BIG-IP in high-availability mode).
Assign APIC “Context Label” to BIG-IP Concrete Device

It is good practice to assign “Context Label” to the concrete device, in this example, BIG-IP vCMP guest. The context label will allow user to specify the placement of the self IP address when deploying service graph. Go to:

Tenants common -> L4-L7 Services -> L4-L7 Devices -> <L4-L7_Device_Name>

Click » to expand
Notice the two vCMP guests, click on one of them (Device_1), on the right hand side work pane, click “Policy”, enter the value for “Context Label” field, make a note of this value.

Duplicate the same steps for Device_2

Export F5 L4-L7 Device

If the L4-L7 device cluster is created in tenant common or tenant mgmt instead of in the user-defined tenant, the logical device cluster will need to be exported from tenant common or tenant mgmt to the user-defined tenant.

The logical device interface, which is a proxy object in the tenant that points to the logical device, is used when the device cluster is defined in a common tenant and other tenants want to use the service provided by this device cluster.
For L4-L7 device cluster using physical BIG-IP (appliance or vCMP guest), this operation allows multiple user-defined tenants to share the same physical resource, tenant separation is done by BIG-IP partition/route-domain. User-defined tenant can only view the name of the L4-L7 device, it does not have the ability to modify the L4-L7 device.

For L4-L7 device cluster using BIG-IP VE, export only to 1 user-defined tenant. This operation allows APIC administrator control over BIG-IP, where user-defined tenant admin does not have BIG-IP or iWorkflow access.

User can export this L4-L7 device to user-defined tenant, go to:

**Tenants common -> L4-L7 Services -> L4-L7 Devices**

Right Click on “L4-L7 Devices” and select “Export L4-L7 Devices”

L4-L7 Devices: drop down menu and select the device to be exported

Tenant: drop down menu and select tenant receiving this device

![Export L4-L7 Devices](image)

Choose L4-L7 devices and a tenant to export

- **L4-L7 Devices:** drop down menu
- **Tenant:** select a tenant

Description:
- BOS
- CDG
- common
- FSEPG
- infra
- L3out
- mgmt
- SEA
- SFO

Click “**SUBMIT**” to complete the task

Upon completion, the user-defined tenant can utilize this L4-L7 device, view under:

**Tenants <user-defined_tenant_name> -> L4-L7 Services -> Imported Devices**
**APIC: Create L4-L7 Device with F5 BIG-IP Appliance**

Workflow Progress:

1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)
10) APIC: Create Service Graph Template:
    A. One Arm
    B. Two Arm
    C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach
11) APIC: Deploy Service Graph Template

Creating APIC L4-L7 Device using F5 BIG-IP appliance as concrete devices, the configuration steps are very similar to vCMP guests, except there is no need to specify a chassis when entering concrete device information.

See below screen shot for reference.
The rest of the configuration is same as BIG-IP physical form factor.

In the case of BIG-IP VE HA cluster, user can use BIG-IP interface 1_3 as HA interfaces.

**APIC: Create L4-L7 Device with F5 BIG-IP Virtual Edition (VE)**

Workflow Progress:

1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
C. BIG-IP Virtual Edition (VE)

10) APIC: Create Service Graph Template:
   A. One Arm
   B. Two Arm
   C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach

11) APIC: Deploy Service Graph Template

Creating APIC L4-L7 Device using F5 BIG-IP Virtual Edition (VE), there are some slight differences in the configuration where the BIG-IP virtual machines and vCenter information must be provided when creating the L4-L7 Devices.

For APIC 1.2(2h) release, an APIC created VMM port-graph can tag 1 VLAN, meaning no multi-context support for APIC L4-L7 devices that use BIG-IP VE as concrete device.

APIC chassis manager feature does not apply to VE.

In this example, creating an APIC L4-L7 Device using a single BIG-IP VE as concrete device. APIC L4-L7 Device Type Virtual:

<table>
<thead>
<tr>
<th>Field Description</th>
<th>What does it mean?</th>
<th>Value use in this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td>Concrete device: Physical or Virtual form</td>
<td>Virtual, BIG-IP VE will be used</td>
</tr>
<tr>
<td>Field Description</td>
<td>What does it mean?</td>
<td>Value use in this example</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>VMM Domain</td>
<td>If Device Type is “Virtual”, enter the VMM domain already integrated with Cisco APIC, available thru drop down menu or user can create thru wizard</td>
<td><code>&lt;VMM_domain_name&gt;</code></td>
</tr>
<tr>
<td>VM</td>
<td>Under Device 1 parameters, select the VM that is “Device 1”</td>
<td><code>&lt;VM_name&gt;</code></td>
</tr>
<tr>
<td>Device Interface</td>
<td>Specify VM interfaces that connect to APIC VMM distributed vSwitch</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of BIG-IP interfaces</td>
<td>1_1 would be BIG-IP 1.1</td>
</tr>
<tr>
<td>VNIC</td>
<td>The VNIC that associated with the BIG-IP interface</td>
<td>Please check with vCenter MAC address for confirmation. Normally, BIG-IP 1.1 is Network Adaptor 2; BIG-IP 1.2 is Network Adaptor 3</td>
</tr>
<tr>
<td>Path</td>
<td>Only for Route Peering</td>
<td>N/A</td>
</tr>
<tr>
<td>Cluster Interfaces</td>
<td>Consumer and Provider of the logical device cluster map to the concrete device interfaces</td>
<td>In physical two-arm setup, mapping BIG-IP interface 1.1 to external and BIG-IP interface 1.2 to internal</td>
</tr>
</tbody>
</table>

**Create L4-L7 Devices**

**STEP 1 > General**

Please select device package and enter connectivity information.

**General**

- **Managed:** F5-VE
- **Name:**
- **Service Type:** ADC
- **Device Type:** PHYSICAL
- **VMM Domain:** vcenter
- **Mode:** Single Node
- **Device Package:** iWorkflow-2.0-VNG-W
- **Model:** Unknown (Manual)
- **Context Aware:** Multiple

**Connectivity**

- **APIC to Device Management Connectivity:** Cut-Of-Band
- **In-Band**

**Credentials**

- **Username:** admin
- **Password:** ****
- **Confirm Password:** ****

**Device 1**

- **Management IP Address:** BIG-IP VE mgmt IP
- **Management Port:** https
- **Device Manager:** common/VNG-W
- **Cluster Interfaces:**
  - **Type:** consumer
  - **Name:** external
  - **Concrete Interfaces:** Device/1_1

**Cluster**

- **Management IP Address:** iWorkflow mgmt IP
- **Management Port:** https
- **Device Manager:** common/VNG-W
- **Cluster Interfaces:**
  - **Type:** consumer
  - **Name:** external
  - **Concrete Interfaces:** Device/1_2
APIC: Create Service Graph Template

Workflow Progress:
1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)
10) APIC: Create Service Graph Template:
    A. One Arm
    B. Two Arm
    C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach
11) APIC: Deploy Service Graph Template

An APIC L4-L7 Service Graph Template is an abstract object allowing L4-L7 configuration build into ACI policy model.

An APIC L4-L7 Service Graph Template that utilize ADC as function node has option to create an one-arm or two-arm graph. APIC ADC one-arm and two-arm graph is a logical construct, user must ensure physical connectivity between Cisco ACI fabric and BIG-IP (physical 1-arm or inline) can support the logical one-arm or two-arm graph.

<table>
<thead>
<tr>
<th>APIC ADC Graph Type (Logical)</th>
<th>Number of VLANs to be configured on BIG-IP</th>
<th>BIG-IP connect to ACI (Physical)</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-Arm</td>
<td>1</td>
<td>1-arm (as a stick)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2-arm (inline)</td>
<td>Yes, use Internal Interface</td>
</tr>
<tr>
<td>Two-Arm</td>
<td>2 (external and internal)</td>
<td>1-arm (as a stick)</td>
<td>Yes, if link can trunk multiple VLANs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2-arm (inline)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Understanding APIC service graph template, consider a 1-node graph in this example:
**APIC ADC Graph Type**

<table>
<thead>
<tr>
<th>Connections</th>
<th>Adjacency Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1=C2</td>
<td>L3 or L2</td>
</tr>
<tr>
<td>C2=C1</td>
<td>L3 or L2</td>
</tr>
</tbody>
</table>

In the case of ACI one-arm graph, C1 and C2 are the same connections. If C1 is L3, then C2 is also L3; if C1 is L2, then C2 must also be L2.

**BD / subnets assignment combinations:**

<table>
<thead>
<tr>
<th>Consumer EPG (BD)</th>
<th>F5 BIG-IP BD</th>
<th>Provider EPG (BD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
<td>C</td>
</tr>
<tr>
<td>A</td>
<td>A</td>
<td>B</td>
</tr>
<tr>
<td>A</td>
<td>B</td>
<td>B</td>
</tr>
<tr>
<td>A</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
</tbody>
</table>

In the case of ACI two-arm graph, C1 and C2 are L2 connections, the consumer EPG and provider EPG must belong to different BD / Subnets:

<table>
<thead>
<tr>
<th>Consumer EPG (BD)</th>
<th>Provider EPG (BD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
</tr>
</tbody>
</table>

After the service graph is deployed in APIC, APIC automatically configures the services according to the service function requirements that are specified in the service graph. APIC also automatically configures the network stitching according to the needs of the service function that is specified in the service graph.

**APIC Function Profiles**

APIC function profile pre-defined service function configurable parameters. Use of the function profile reduces the number of parameters that a user needs to provide when instantiating a service graph template.

By default, each APIC service function has minimum one function profile associated with it. The default function profile capture the service function parameters "as-is" from the device package.

APIC user can create additional function profile(s) that tied to service function. User can pre-define repeatable service function parameters (like self IP and default route) in a function profile.

A service function can have many function profiles. A function profile can only associate with one service function.

A service graph template can tie to only one function profile (default or user-defined), when the service graph is deployed, graph parameters are pre-configured based on the function profiles, this will minimize user input error. APIC
user only responsible in entering graph specific parameters.

Figure 6 below illustrate the relationship between APIC function profiles with related APIC objects.

**Figure 6: APIC Function Profiles**

To create a new Function Profile, click the following in the navigation pane:

Tenants <user-defined_tenant_name> -> L4-L7 Services -> Function Profiles

Right Click on “Function Profile” and select “Create Profile Group”
Enter the name of the function profile group (in this example, F5-Profile-Group), the SUBMIT

Navigate to the “F5-Profile-Group”, then right click, select “Create L4-L7 Services Function Profile”

<table>
<thead>
<tr>
<th>Field Description</th>
<th>What does it mean?</th>
<th>Value use in this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>User defined name of the function profile</td>
<td>HTTP-No-Persistence-2arm</td>
</tr>
</tbody>
</table>
Under “Features and Parameters”, select “All Parameters”

User can now pre-configured parameters for the HTTP-NoPersistence-Gold service function. This is commonly used to pre-configure network parameters.

Here is an example of a function profile with all networking elements configured ahead of time.
This function profile will be used in later step when creating a two-arm service graph template.

**APIC: Create One-Arm Service Graph Template**

**Workflow Progress:**

1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)
10) APIC: Create Service Graph Template:
**DEPLOYMENT GUIDE**
F5 BIG-IP Service Insertion with Cisco ACI using iWorkflow

A. One Arm

B. Two Arm

C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach

11) APIC: Deploy Service Graph Template

Inside the service graph template, user can drag-and-drop the L4-L7 device(s) into the template to provide Firewall or ADC functionality. In this example, the imported L4-L7 device from previous step will be used to provide ADC functionality to a new service graph template. This service graph template is created to provide HTTP-No-Persistence ADC function for the WEB EPG.

To create a new Service Graph Template, click the following in the navigation pane:

**Tenants <user-defined_tenant_name> -> L4-L7 Services -> L4-L7 Service Graph Template**

Right Click on “L4-L7 Service Graph Template” and select “Create L4-L7 Service Graph Template”

New pop up window will appear. In the new window, enter the following:

- Graph Name: <user defined>
- Graph Type: Create a New One (should be the default)

Drag the device cluster from the right side of the window into the graph, place it in between the consumer and provider EPG.

When this graph template is deployed, the traffic will be redirected to the F5 BIG-IP of this device cluster automatically by Cisco ACI.

Double click the word N1 under the Node to change the node name to ADC.

Under `<L4-L7_Device_Name> Information (in this example, F5-vCMP-PodA), click the One-Arm option for this graph.

Select the Profile: F5-iWorkflow-2.0–VNG-iW/HTTP-NoPersistence-Gold

This is the application template created in iWorkflow.
**APIC: Create Two-Arm Service Graph Template**

Workflow Progress:

1. BIG-IP: Import App Services iApps
2. iWorkflow Cloud: Device Discovery
3. iWorkflow Cloud: Create APIC Cloud Connector
4. iWorkflow Cloud: Create Application Template
5. iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6. APIC: Import Device Package
7. APIC: Device Manager configuration
8. (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9. APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)
10. **APIC: Create Service Graph Template:**
    A. One Arm
    B. **Two Arm**
    C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach
11. APIC: Deploy Service Graph Template

The steps are identical as the one-arm graph creation, except in the ADC box, select “two-arm”. In this example, when selecting profile of the service graph template, select the function profile created in the earlier step from the drop down menu.
DEPLOYMENT GUIDE
F5 BIG-IP Service Insertion with Cisco ACI using iWorkflow

APIC: Enable Dynamic Endpoints Attach/Detach

Workflow Progress:
1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)
10) APIC: Create Service Graph Template:
   A. One Arm
   B. Two Arm
   C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach
11) APIC: Deploy Service Graph Template

Cisco APIC supports dynamic endpoints attach/detach. By enabling “attach notification” feature on the service graph provider connector, after the graph is deployed between two EPGs, when a new endpoint is added to the provider EPG, APIC sends the endpoint attach notification (IP address) to iWorkflow/BIG-IP thru device package. As a result, a new member will be added to the BIG-IP virtual server Pool. User need to specify a single port value to be used for the pool, this can be accomplished when creating the template.
When an endpoint is removed from the provider EPG, same logic applies where APIC will send endpoint detach notification to iWorkflow/BIG-IP thru device package. As a result, the member (endpoint) will be removed from the BIG-IP virtual server Pool.

This feature is useful if the workload to be load balanced is elastic. It is also useful if there are large number of servers because dynamic endpoints only require one operation task in assigning an endpoint to an APIC EPG, compared to two operation tasks of adding endpoint to EPG and adding member to BIG-IP pool.

**Please note:** F5 operation model supports either dynamic endpoints (pool member information from APIC) or static endpoints (user enter pool member information manually), but not both. If there is requirement where each pool member need to listening to different port, static pool model must be used.

Terminology comparison:

<table>
<thead>
<tr>
<th>Cisco ACI</th>
<th>F5 BIG-IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider EPG</td>
<td>Pool</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Member</td>
</tr>
</tbody>
</table>

To enable graph template with attachment notification, go to:

Tenant <user-defined_tenant_name> -> L4-L7 Services -> L4-L7 Service Graph Template
Expand on the graph template -> Function Node – ADC -> provider

Check the box “Attachment Notification”
APIC: Deploy One-Arm Service Graph Template

Workflow Progress:

1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)
10) APIC: Create Service Graph Template:
    A. One Arm
    B. Two Arm
    C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach
11) APIC: Deploy Service Graph Template

APIC Service Graph Template is considered abstract object, it is not yet deployed between a pair of EPG and no configuration has yet to apply on F5 BIG-IP.

In this example, the service graph template “HTTP-NoPersistence-Gold” created in the previous step will be deployed between APIC L3out EPG (clients coming from outside) to the Web EPG (Web tier) with no persistence requirement. Notice the EPG function, in this example Web tier (HTTP), match with the L4-L7 service function “HTTP-NoPersistence-Gold” inside the service graph.

To deploy the service graph, click the following in the Navigation pane of the tenant:

   Tenants <user-defined_tenant_name> -> L4-L7 Services -> L4-L7 Service Graph Template

Select the Service Graph Template “HTTP-No-Persistence-Graph” from the Left-hand-side work pane. Right click and choose the option to: Apply L4-L7 Service Graph Template
In the new window, select the EPGs the Service Graph will be inserted in between.

Select the following for the EPG information:

<table>
<thead>
<tr>
<th>Field Description</th>
<th>What does it mean?</th>
<th>Value use in this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer EPG / External Network</td>
<td>this EPG consume service</td>
<td>L3out (Outside-ALL)</td>
</tr>
<tr>
<td>Provider EPG / External Network</td>
<td>this EPG provide service</td>
<td>Web (epg-web)</td>
</tr>
</tbody>
</table>

Under Contract Information, use the option to create a new Contract:

<table>
<thead>
<tr>
<th>Field Description</th>
<th>What does it mean?</th>
<th>Value use in this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract</td>
<td>Using a new contract or existing contract</td>
<td>CHECK &quot;Create A New Contract&quot;</td>
</tr>
<tr>
<td>Contract Name</td>
<td>User defined contract Name</td>
<td>HTTP-No-Persistence-Contract</td>
</tr>
<tr>
<td>No Filter (Allow All Traffic)</td>
<td>Does this contract allow all traffic?</td>
<td>CHECK</td>
</tr>
</tbody>
</table>
Click “NEXT” to go to STEP 2

STEP 2, user can apply Service Graph specific parameters. For One-Arm graph, there is 1 connector, user needs to map the connector with the L4-L7 Device cluster interface, this is particularly important, as the graph connector is associated with a APIC bridge domain (BD), which contains subnet information. This mapping will provide connectivity between the BIG-IP and backend servers, ensuring BIG-IP monitor to work as expected.

Under Connector

<table>
<thead>
<tr>
<th>Field Description</th>
<th>What does it mean?</th>
<th>Value use in this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>General / Route Peering – select “General” for BD, “Route Peering” for L3 Ext Net</td>
<td>General</td>
</tr>
<tr>
<td>BD (if Type is General)</td>
<td>the bridge domain that connects the two devices</td>
<td>SFOwebBD</td>
</tr>
<tr>
<td>L3 Ext Network (if Type is Route Peering)</td>
<td>select L3 network for dynamic routing</td>
<td>N/A</td>
</tr>
<tr>
<td>Cluster Interface</td>
<td>map L4-L7 Device cluster interface (external or internal) to the connector</td>
<td>Internal</td>
</tr>
</tbody>
</table>

Click “NEXT” to go to STEP 3
STEP 3, graph specific parameters for the L4-L7 Device. In this step, user can enter F5 virtual server specific parameters based on the template of the iWorkflow service catalog.

Click “All Parameters”

In “All Parameters” tab, the folder and parameters will appear. To edit, expand the parameter by clicking the and double click the field to change the parameter’s name and value.

There are two major folder, Device Config and Function Config.

Device Config is BIG-IP device level network configuration, like self IP, Route and SNAT Pool

Function Config is BIG-IP Virtual Server level configuration, in this case, will be the service catalog template parameters that associated with a BIG-IP iApps. Function Config will reference Device Config as a way to utilize resources of the BIG-IP.

Under Device Config

Press to expand the Network configuration folder

Double click “InternalSelfIP”, under “Apply to Specific Device”, enter the Context Label value previously defined when creating the L4-L7 device (notice the drop down menu does not work), then click “UPDATE”

Press to expand the folder InternalSelfIP

Double click each of the following parameters, and enter its value, then click “UPDATE”
**Enable Floating?**

Is this a floating IP? Select (Yes/No) from drop down menu

- 2 non floating and 1 floating

**Internal Self IP Address**

BIG-IP self IP address value, facing server side

- Floating self IP and internal self IP for each BIG-IP

**Internal Self IP Netmask**

Netmask value of the Internal self IP

- 255.255.255.0

**Port Lockdown**

BIG-IP self IP port lockdown values (Default / All / None)

- Default

---

**Apply L4-L7 Service Graph Template To EPGs**

**STEP 3 > F5-VCMP-PodA Parameters**

Click to enter additional Internal self IP, one internal self IP for vCMP guest #2 and one floating internal self IP

**Notice below, floating self IP does not need to assign to a specific device, as floating self IP will be configured in both BIG-IP**
If network environment requires, user can enter default GW information for the BIG-IP

<table>
<thead>
<tr>
<th>Folder/Param</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Config</td>
<td>Device</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Network</td>
<td></td>
</tr>
<tr>
<td>InternalSelfIP1</td>
<td>InternalSelfIP</td>
<td>vCMP81</td>
</tr>
<tr>
<td>Enable Floating</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>Internal Self IP Address</td>
<td>SelfIPAddress</td>
<td>vCMP #1 Internal self IP</td>
</tr>
<tr>
<td>Internal Self IP Netmask</td>
<td>SelfIPNetmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Port Lockdown</td>
<td>PortLockdown</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>InternalSelfIP2</td>
<td>InternalSelfIP</td>
<td>vCMP82</td>
</tr>
<tr>
<td>Enable Floating</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>Internal Self IP Address</td>
<td>SelfIPAddress</td>
<td>vCMP #2 Internal self IP</td>
</tr>
<tr>
<td>Internal Self IP Netmask</td>
<td>SelfIPNetmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Port Lockdown</td>
<td>PortLockdown</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>InternalSelfIP3</td>
<td>InternalSelfIP</td>
<td></td>
</tr>
<tr>
<td>Enable Floating</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Internal Self IP Address</td>
<td>SelfIPAddress</td>
<td>Internal Floating self IP</td>
</tr>
<tr>
<td>Internal Self IP Netmask</td>
<td>SelfIPNetmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Port Lockdown</td>
<td>PortLockdown</td>
<td>NONE</td>
</tr>
</tbody>
</table>

**Under Function Config**

The Network information configured under Device Config must be referenced under Function Config in order for the virtual server to utilize this network resource.

Go to "Network Relation", click ➔, and double click on "Select Network", the network created under Device Config can be selected under the drop down menu, then click "UPDATE”

To configure template (HTTP-NoPersistence-Gold) specific parameters, click ➔ beside the name of the template. Double click the name, and remove "-Default”, then click "UPDATE”

69
The parameter will change from **RED** to **GREEN**

<table>
<thead>
<tr>
<th>Function Config</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP-NoPersistence-Gold</td>
<td>HTTP-NoPersistence-Gold</td>
</tr>
</tbody>
</table>

In this example, based on the HTTP-NoPersistence-Gold template, the following parameters are exposed to APIC:

- Pool Members: add BIG-IP virtual server pool member(s) IP
- Address: VIP address
- Port: VIP listening port

You can add multiple pool member(s) by using the +, similar operation as adding internal self IP address

<table>
<thead>
<tr>
<th>Function Config</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP-NoPersistence-Gold</td>
<td>HTTP-NoPersistence-Gold</td>
</tr>
<tr>
<td>Pool Members</td>
<td>pool__Members</td>
</tr>
<tr>
<td>Member</td>
<td>member</td>
</tr>
<tr>
<td>IPAddress</td>
<td>pool member #1 IP</td>
</tr>
<tr>
<td>Member</td>
<td>member2</td>
</tr>
<tr>
<td>IPAddress</td>
<td>pool member #2 IP</td>
</tr>
<tr>
<td>Address</td>
<td>VIP address</td>
</tr>
<tr>
<td>Port</td>
<td>80</td>
</tr>
<tr>
<td>NetworkRelation</td>
<td>NetworkRel</td>
</tr>
</tbody>
</table>

Click “FINISH” to deploy the graph.

The graph template now going from abstract layer to rendering layer, it is now deployed between a pair of EPG. Thru F5 device package, APIC instantiate configuration on F5 BIG-IP:

- Create partition and assign unique RD to this partition, to associate with APIC tenant and VRF
- Assign VLAN
- Create self IP and associate the self IP to corresponding VLAN
- Create default GW (if configure)

Thru F5 device package, APIC sends template specific parameters to F5 iWorkflow cluster. F5 iWorkflow, upon receiving APIC dictionary, then deploys the service catalog template using APIC provided parameters on F5 BIG-IP as a format of iApps deployment.

Upon successful deployment, on APIC, user should see no faults in both “Deployed Graph Instances” and “Deployed Devices” under “L4-L7 Services”
On F5 iWorkflow, APIC tenant information is available under “Tenants”, notice the tenant name and VRF name.

Under F5 iWorkflow Cloud -> Services, the application services (deployed template / iApps) information is available.

Application Type is the name of the template within Service Catalog.

Notice the table of “Customize Application Template”, those are the parameters exposed to and completed by APIC.
Under F5 iWorkflow Cloud -> Catalog, all parameters are now locked as the template is deployed. This will prevent accidental changes to the template and result in outage to virtual servers already in service.
On the F5 BIG-IP, notice APIC created a partition that is based on APIC tenant and VRF name:

Notice the virtual server is deployed based on iApps. Unique route domain number, in this example 1154, is assigned by device package to associate this partition with APIC tenant + VRF.

Under BIG-IP -> iApps -> Application Services, notice a full feature virtual server is deployed by entering just a few parameters thru Cisco APIC:
Cisco APIC is handling network stitching, on Cisco APIC -> L4-L7 Services -> Deployed Device, VLAN dynamically assigned by APIC:

Same VLAN tag is configured on BIG-IP by APIC thru device package, Under Network – VLANs:

On BIG-IP, vCMP guest 1 self IP configuration:
APIC: Deploy Two-Arm Service Graph Template with Function Profile and Dynamic Endpoints

Workflow Progress:

1) BIG-IP: Import App Services iApps
2) iWorkflow Cloud: Device Discovery
3) iWorkflow Cloud: Create APIC Cloud Connector
4) iWorkflow Cloud: Create Application Template
5) iWorkflow Cloud: Dynamic creation of customized F5 Device Package
6) APIC: Import Device Package
7) APIC: Device Manager configuration
8) (OPTIONAL) APIC: Chassis Manager configuration (F5 vCMP guest only)
9) APIC: Create L4-L7 Device using:
   A. BIG-IP vCMP guest
   B. BIG-IP appliance
   C. BIG-IP Virtual Edition (VE)
10) APIC: Create Service Graph Template:
    A. One Arm
    B. Two Arm
    C. (OPTIONAL) Enable Dynamic Endpoints Attach/Detach
11) APIC: Deploy Service Graph Template

The steps to deploy a two-arm service graph template is very similar to the one-arm service graph deployment. In this example, notice the advantage of using user-defined function profile and dynamic endpoints.

Go to:

Tenants <user-defined_tenant_name> -> L4-L7 Services -> L4-L7 Service Graph Template

Select the Service Graph Template “HTTP-No-Persistence-2arm” from the Left-hand-side work pane. Right click and choose the option to: Apply L4-L7 Service Graph Template
Select the same pair of EPG as one-arm graph, consumer is Outside-ALL and provider is epg-web.

Create a new contract, HTTP-No-Persistence-2arm-Contract

Click NEXT

Notice in two-arm graph template deployment, there are two connectors (consumer and provider), map the bridge domain (BD) with the cluster interfaces (External and Internal). In this example, the BD for consumer connector is the BD contains public VIP subnet.
Click NEXT to STEP 3

By using the function profile, majority of the graph parameters are completed. User only need to enter the VIP address.

Using App Services iApps, in order to enable dynamic endpoints, enter 1 single member IP address of 0.0.0.0, this will act as a trigger to accept endpoints dynamically.

Click FINISH to deploy the graph.

Cisco APIC assign 2 VLAN for 2-arm graph deployment
F5 BIG-IP VLAN matches with Cisco APIC

When virtual server is initially deployed in BIG-IP, it is unavailable due to the Pool is empty:
Once endpoints information is received from Cisco APIC, Pool members are populated. This is based on there are two endpoints in the WEB EPG.

BIG-IP self IP information is configured based on the function profile

BIG-IP virtual server configuration is based on App Services iApps
Full feature BIG-IP virtual server is deployed to serve HTTP application thru API. By templatizing the application requirements in iWorkflow Catalog, and have this catalog exposed to Cisco API thru device package, user only needs to enter a few parameters in API level, significant operational cost saving and minimize operator error.
F5 BIG-IP as Unmanaged Device in Cisco ACI

In the Unmanaged Mode deployment model, F5 BIG-IP is not managed by Cisco APIC. All F5 BIG-IP configurations must be completed by the user, including network and virtual server configurations.

In unmanaged mode, there is no device package requirement, as a result, no service insertion.

F5 iWorkflow can still play a role in this deployment model, continue as service catalog life cycle management and deploy templates directly on BIG-IP.

Regardless service insertion or unmanaged mode, physical connectivity between F5 BIG-IP and Cisco ACI of using single port, trunk or VPC is supported.

Prior to APIC release 1.2(1*), EPG mode is used to attach F5 BIG-IP to ACI fabric without service insertion. There are subtle differences between EPG mode and Unmanaged mode, Figure 7 below illustrate the differences between the two models.

<table>
<thead>
<tr>
<th>EPG Mode (Option A1)</th>
<th>Unmanaged Mode (Option A2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No service graph representation</td>
<td>Service graph representation</td>
</tr>
<tr>
<td>• Manual binding of VLAN’s, binding contracts to EPG’s</td>
<td>• Automatic binding of VLAN’s and contracts</td>
</tr>
<tr>
<td>Manual configuration to steer traffic</td>
<td>Automatically steer traffic</td>
</tr>
<tr>
<td>• One Application tier -&gt; Chain of L4-L7 service devices -&gt; To another application tier</td>
<td>• One application tier -&gt; Chain of L4-L7 service devices -&gt; To another application tier</td>
</tr>
</tbody>
</table>

![Figure 7: APIC EPG mode vs. Unmanaged Mode](image)

**Deployment Workflow**

1) APIC: Create Unmanaged L4-L7 Device
2) APIC: Create Service Graph Template:
3) APIC: Deploy Service Graph Template
4) BIG-IP: Configure Network parameters
5) BIG-IP: Configure Virtual Servers
6) iWorkflow: Discover Device
7) iWorkflow: Create BIG-IP Cloud Connector
8) iWorkflow: Create Template for “All Clouds”
9) iWorkflow: Create application user / tenant / role
10) iWorkflow: Login as application user
11) iWorkflow: Deploy Services based on template

**APIC: Create Unmanaged L4-L7 Device**

Deployment Workflow Progress:

1) APIC: Create Unmanaged L4-L7 Device
2) APIC: Create Service Graph Template
3) APIC: Deploy Service Graph Template
4) BIG-IP: Configure Network parameters
5) BIG-IP: Configure Virtual Servers
6) iWorkflow: Discover Device
7) iWorkflow: Create BIG-IP Cloud Connector
8) iWorkflow: Create Template for “All Clouds”
9) iWorkflow: Create application user / tenant / role
10) iWorkflow: Login as application user
11) iWorkflow: Deploy Services based on template

Due to the nature that unmanaged device, VLANs are statically bind, therefore, unmanaged L4-L7 device should be created under user-defined tenant.

As each customer L2-L3 network requirements are different, please consult Cisco ACI team on network design and the necessary network configuration for network stitching between Cisco ACI to F5 BIG-IP to server farm.

Similar to non-ACI environment, in unmanaged mode, F5 BIG-IP administrator would expect VLAN tag and subnet / IP addresses information from the network administrator.

Create Unmanaged L4-L7 device under user-defined (SFO) tenant, go to:

**Tenants common -> L4-L7 Services -> L4-L7 Devices**

A new wizard pop up:

<table>
<thead>
<tr>
<th>Field Description</th>
<th>What does it mean?</th>
<th>Value use in this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed</td>
<td>Managed: this L4-L7 device is managed and configured by Cisco APIC Unmanaged: L4-L7 device configuration is done by user</td>
<td>UNCHECK</td>
</tr>
<tr>
<td>Name</td>
<td>User defined L4-L7 Device name</td>
<td>vCMP-Unmanaged-L3Out</td>
</tr>
<tr>
<td>Service Type</td>
<td>Firewall or ADC F5 BIG-IP is considered an ADC device</td>
<td>ADC</td>
</tr>
<tr>
<td>Device Type</td>
<td>Physical or Virtual form factor</td>
<td>Physical</td>
</tr>
<tr>
<td>Physical Domain</td>
<td>Physical domain contains static VLAN</td>
<td>ServiceUnmanagedPhy (configured</td>
</tr>
<tr>
<td>Field Description</td>
<td>What does it mean?</td>
<td>Value use in this example</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Is L4-L7 Device a Single Node or HA Cluster?</td>
<td>HA Cluster</td>
</tr>
<tr>
<td><strong>Function Type</strong></td>
<td>GoTo or GoThrough</td>
<td>GoTo</td>
</tr>
<tr>
<td></td>
<td>GoTo: L4-L7 device as next-hop</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GoThrough: L4-L7 device act like bump-in-the-wire</td>
<td></td>
</tr>
<tr>
<td><strong>Device Interfaces Name</strong></td>
<td>F5 BIG-IP Interface connect to ACI</td>
<td>1/1_3 == VIPRION 1/1.3</td>
</tr>
<tr>
<td><strong>Device Interface Path</strong></td>
<td>ACI fabric interface connecting to the corresponding BIG-IP interface</td>
<td>Node-102/eth1/39 (Device 1) Node-103/eth1/39 (Device 2)</td>
</tr>
<tr>
<td><strong>Cluster Interface Name</strong></td>
<td>User-defined</td>
<td>External and Internal</td>
</tr>
<tr>
<td><strong>Concrete Interfaces</strong></td>
<td>Which device interface will be used for external and interface traffic?</td>
<td>Select both Device 1 and Device 2 interface – since only 1 link between ACI and BIG-IP, this link serve both external and internal traffic</td>
</tr>
<tr>
<td><strong>Encap</strong></td>
<td>Static binding VLAN information</td>
<td>vlan-2603 – internal VLAN value APIC send to BIG-IP vlan-2103 – external VLAN value APIC send to BIG-IP</td>
</tr>
</tbody>
</table>
Click **FINISH**.

Notice that no BIG-IP information (management IP, login, password, etc.) is provided. Only connectivity is defined in unmanaged L4-L7 Device.

**APIC: Create Service Graph template using Unmanaged Device**

Deployment Workflow Progress:

1) APIC: Create Unmanaged L4-L7 Device
2) **APIC: Create Service Graph Template**
3) APIC: Deploy Service Graph Template
4) BIG-IP: Configure Network parameters
5) BIG-IP: Configure Virtual Servers
6) iWorkflow: Discover Device
7) iWorkflow: Create BIG-IP Cloud Connector
8) iWorkflow: Create Template for “All Clouds”
9) iWorkflow: Create application user / tenant / role
10) iWorkflow: Login as application user
11) iWorkflow: Deploy Services based on template

Create an unmanaged two-arm service graph

APIC: Deploy Service Graph Template using Unmanaged Device

Deployment Workflow Progress:
1) APIC: Create Unmanaged L4-L7 Device
2) APIC: Create Service Graph Template
3) APIC: Deploy Service Graph Template
4) BIG-IP: Configure Network parameters
5) BIG-IP: Configure Virtual Servers
6) iWorkflow: Discover Device
7) iWorkflow: Create BIG-IP Cloud Connector
8) iWorkflow: Create Template for “All Clouds”
9) iWorkflow: Create application user / tenant / role
10) iWorkflow: Login as application user
11) iWorkflow: Deploy Services based on template

Deploy the graph template between two EPG

Consumer: Outside-ALL
Provider: epg-web
New Contract: Unmanaged-L3out-2arm-contract
Map cluster interface with the BD. In the case of using L3out as consumer EPG, mapping LDev external interface to the L3 external network. A router ID is also created for the BIG-IP. **Note: different network topologies and requirements will result in different network settings, please consult Cisco ACI team.**

Click **FINISH**

Notice, there is no F5 BIG-IP related configuration.

The above steps will complete the network stitching on the ACI side, where VLAN tags, in this example 2103 and 2603, will be used in the external and internal paths that connect to the BiG-IP.

**BIG-IP: Configure Network parameters**

Deployment Workflow Progress:

1) APIC: Create Unmanaged L4-L7 Device
2) APIC: Create Service Graph Template
3) APIC: Deploy Service Graph Template
4) **BIG-IP: Configure Network parameters**
5) BIG-IP: Configure Virtual Servers
6) iWorkflow: Discover Device
7) iWorkflow: Create BIG-IP Cloud Connector
8) iWorkflow: Create Template for “All Clouds”
9) iWorkflow: Create application user / tenant / role
10) iWorkflow: Login as application user
11) iWorkflow: Deploy Services based on template

F5 BIG-IP administrator need to configure both network and virtual server elements on BIG-IP.

In this example, vCMP is used, create VLAN on vCMP host. Notice the tag matches with APIC VLAN encap value, also tagging on the uplink that connect BIG-IP to ACI

Add this VLAN to the vCMP guest
vCMP guest VLAN list will have VLAN information from vCMP host.
Repeat the same for standby BIG-IP

Configure external and internal self IPs and floating self IPs based on network requirements and subnet information from network administrator.

Upon completion, the network traffic re-direction that stitches consumer EPG <-> Cisco ACI <-> F5 BIG-IP <-> provider EPG is established.

**BIG-IP: Configure Virtual Servers**

Deployment Workflow Progress:

1) APIC: Create Unmanaged L4-L7 Device
2) APIC: Create Service Graph Template
3) APIC: Deploy Service Graph Template
4) BIG-IP: Configure Network parameters
5) **BIG-IP: Configure Virtual Servers**
6) iWorkflow: Discover Device
7) iWorkflow: Create BIG-IP Cloud Connector
8) iWorkflow: Create Template for “All Clouds”
9) iWorkflow: Create application user / tenant / role
10) iWorkflow: Login as application user
11) iWorkflow: Deploy Services based on template

F5 BIG-IP administrator can configure virtual server on BIG-IP based on application requirements. Please refer to F5 BIG-IP configuration guide on virtual server configurations.


**iWorkflow: Discover Device**

Deployment Workflow Progress:

1) APIC: Create Unmanaged L4-L7 Device
2) APIC: Create Service Graph Template
3) APIC: Deploy Service Graph Template
4) BIG-IP: Configure Network parameters
5) BIG-IP: Configure Virtual Servers
6) **iWorkflow: Discover Device**
7) iWorkflow: Create BIG-IP Cloud Connector
8) iWorkflow: Create Template for “All Clouds”
9) iWorkflow: Create application user / tenant / role
10) iWorkflow: Login as application user
11) iWorkflow: Deploy Services based on template

Alternatively, F5 administrator can use F5 iWorkflow to deploy iApps based virtual server in BIG-IP.
F5 iWorkflow can be used as service catalog lifecycle management platform in Cisco ACI unmanaged environment as well.

Make sure the unmanaged BIG-IP has the App Services iApps.

Go to F5 iWorkflow Cloud -> Devices, click +

Enter BIG-IP management IP and admin credentials

Make sure BIG-IP availability is “Available”

vCMP84 is shown in the example below. 2nd vCMP guest (vCMP90) will need to be discovered as well.
**DEPLOYMENT GUIDE**  
F5 BIG-IP Service Insertion with Cisco ACI using iWorkflow

## iWorkflow: Create BIG-IP Cloud Connector

Deployment Workflow Progress:
1) APIC: Create Unmanaged L4-L7 Device
2) APIC: Create Service Graph Template
3) APIC: Deploy Service Graph Template
4) BIG-IP: Configure Network parameters
5) BIG-IP: Configure Virtual Servers
6) iWorkflow: Discover Device
7) **iWorkflow: Create BIG-IP Cloud Connector**
8) iWorkflow: Create Template for “All Clouds”
9) iWorkflow: Create application user / tenant / role
10) iWorkflow: Login as application user
11) iWorkflow: Deploy Services based on template

Create a BIG-IP Cloud Connector – this is the local connector that enable iWorkflow to deploy Application Services (iApps based virtual server) on BIG-IP using a service catalog model.

<table>
<thead>
<tr>
<th>Field Description</th>
<th>What does it mean?</th>
<th>Value use in this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>User-defined</td>
<td>VNG-84-90</td>
</tr>
<tr>
<td>Connector Type</td>
<td>Available iWorkflow Cloud Connector: (ACI, NSX, BIG-IP, vCMP)</td>
<td>BIG-IP – this is the local connector enabling iWorkflow to deploy iApps on BIG-IP</td>
</tr>
<tr>
<td>Devices</td>
<td>BIG-IP associated with this connector</td>
<td>Select the unmanaged BIG-IP pair from drop down menu</td>
</tr>
</tbody>
</table>

Click **Save**

## iWorkflow: Create Template for “All Clouds”

Deployment Workflow Progress:
1) APIC: Create Unmanaged L4-L7 Device
2) APIC: Create Service Graph Template
3) APIC: Deploy Service Graph Template
DEPLOYMENT GUIDE
F5 BIG-IP Service Insertion with Cisco ACI using iWorkflow

4) BIG-IP: Configure Network parameters
5) BIG-IP: Configure Virtual Servers
6) iWorkflow: Discover Device
7) iWorkflow: Create BIG-IP Cloud Connector
8) iWorkflow: Create Template for “All Clouds”
9) iWorkflow: Create application user / tenant / role
10) iWorkflow: Login as application user
11) iWorkflow: Deploy Services based on template

Create a template under iWorkflow Cloud Catalog

Select “All Clouds” under Cloud option, making this template available to all cloud connectors (including APIC) of this iWorkflow. Having the template available to all cloud connectors is especially useful when migrating from ACI unmanaged mode to ACI service insertion mode, as same template being used, deployment and migration consistency is possible.

Tenant Preview

Tenant users will see a form that looks like this when deploying an application using this Catalog.

iWorkflow: Create application user / tenant / role

Deployment Workflow Progress:
1) APIC: Create Unmanaged L4-L7 Device
2) APIC: Create Service Graph Template
3) APIC: Deploy Service Graph Template
4) BIG-IP: Configure Network parameters
5) BIG-IP: Configure Virtual Servers
6) iWorkflow: Discover Device
7) iWorkflow: Create BIG-IP Cloud Connector
8) iWorkflow: Create Template for “All Clouds”
9) iWorkflow: Create application user / tenant / role
10) iWorkflow: Login as application user
11) iWorkflow: Deploy Services based on template

An application user, tenant and roles must be configured for template deployment.

Under iWorkflow Cloud -> Users, create a new user (demo) for template deployment

<table>
<thead>
<tr>
<th>Users</th>
<th>New User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin User</td>
<td>demo</td>
</tr>
<tr>
<td>Tenant</td>
<td>demo</td>
</tr>
</tbody>
</table>

Under iWorkflow Cloud -> Tenants, create a local tenant (DemoTenant) for iApps deployment

Select the BIG-IP cloud connector consists of the unmanaged BIG-IP
DEPLOYMENT GUIDE
F5 BIG-IP Service Insertion with Cisco ACI using iWorkflow

Under iWorkflow Cloud -> Roles, add the user (demo) to **Active Users and Groups** of DemoTenant

![iWorkflow Cloud](image_url)

**iWorkflow: Login as application user**

**Deployment Workflow Progress:**

1. APIC: Create Unmanaged L4-L7 Device
2. APIC: Create Service Graph Template
3. APIC: Deploy Service Graph Template
4. BIG-IP: Configure Network parameters
5. BIG-IP: Configure Virtual Servers
6. iWorkflow: Discover Device
7) iWorkflow: Create BIG-IP Cloud Connector
8) iWorkflow: Create Template for “All Clouds”
9) iWorkflow: Create application user / tenant / role
10) iWorkflow: Login as application user
11) iWorkflow: Deploy Services based on template

Open a new iWorkflow window and login as the tenant user

Go to iWorkflow Cloud

Demo tenant has limited view compare to admin tenant, only capable in deploying Services
**iWorkflow: Deploy Services based on Catalog Template**

Deployment Workflow Progress:

1. APIC: Create Unmanaged L4-L7 Device
2. APIC: Create Service Graph Template
3. APIC: Deploy Service Graph Template
4. BIG-IP: Configure Network parameters
5. BIG-IP: Configure Virtual Servers
6. iWorkflow: Discover Device
7. iWorkflow: Create BIG-IP Cloud Connector
8. iWorkflow: Create Template for “All Clouds”
9. iWorkflow: Create application user / tenant / role
10. iWorkflow: Login as application user
11. **iWorkflow: Deploy Services based on template**

When a new service is deployed, iWorkflow will instantiate an Application Services (iApps based virtual server) in BIG-IP. The iWorkflow catalog templates configured with specific cloud connector or “All Clouds” are visible in application tenant space.

Add a new Services
Notice service template that use “All Clouds” connectors now available

Click Save to deploy the template on BIG-IP

Upon completion, on iWorkflow – Services, Virtual Servers and Servers information is visible

On BIG-IP: application service is configured based on the iApps

Thru iWorkflow service catalog model, deployment of virtual servers is templatized based on application requirements in iWorkflow Catalog.
Upon deployment, iWorkflow Cloud -> Services has visibility of the BIG-IP deployed application services:

![HTTP-Fast-VS](image)

F5 iWorkflow also has visibility to the virtual servers and pool members:

![Virtual Servers](image)

On F5 BIG-IP vCMP guest, virtual servers is deployed thru F5 iWorkflow as an application services based on the App Services iApps
Thru F5 iWorkflow, from application user perspective, only tenant editable parameters are available. A view on F5 BIG-IP application services display a full function iApps based virtual server is deployed that satisfy application requirements. By enabling "All Clouds" connector when creating the template, this very same template can be used in both BIG-IP (local) and Cisco APIC cloud connectors.
Troubleshooting

APIC

For ACI specific troubleshooting, please refer ACI troubleshooting guide:

For service insertion–specific troubleshooting, refer to the debug.log and apic.log file on the APIC.

1. SSH into the APIC that owns the shard of the F5 config
2. Enter bash
3. Enter cd /data/devicescript/<device_package_name>/logs/
4. View these three files for problems related to F5 service insertion:
   - debug.log
   - periodic.log
   - apic.log

iWorkflow

Examine iWorkflow restjavad.0.log

1. SSH into iWorkflow using root login and password
2. Enter cd /var/log
3. Examine restjavad.*.log

For API calls, /var/log/audit (SOAP commands) and /var/log/restjavad-audit.*.log are also useful

If increasing restjavad log verbosity to FINE may help, please refer to:

For GET / POST commands, please refer to /var/log/webd/access.log

BIG-IP

Troubleshooting API calls received from iWorkflow on iApps deployment:

1. SSH into BIG-IP using root login and password
2. Enter cd /var/tmp
3. Examine scriptd.out

Troubleshooting information for BIG-IP LTM–related problems can be found in the /var/log directory.

1. SSH into BIG-IP using root login and password
2. Enter cd /var/log
3. View the files in Ltm

For more information about BIG-IP troubleshooting: https://f5.com/education/training/courses/troubleshooting-big-ip-local-traffic-manager-ltm-v