



F5 Super-NetOps Program

F5 Programmability Training

<https://f5.com/supernetops>

Contents:

1	Welcome	5
2	Class 1: Introduction to Automation & Orchestration	7
2.1	Lab Topology & Environments	7
2.2	BIG-IP Basics (optional)	20
2.3	Module 1: Imperative Automation with the BIG-IP iControl REST API	22
2.4	Module 2: Abstracting Services using iApp Templates	78
2.5	Module 3: Creating Declarative Service Interfaces with iWorkflow	102
2.6	Conclusion	130
3	Class 2: Building Continuous Delivery Pipelines	131
3.1	Module 1: f5-super-netops-container Toolkit	131
3.2	Module 2: F5 f5-postman-workflows & f5-newman-wrapper	140
3.3	Module 3: Stitching Workflows from Class 1 into new Orchestratable Collections	166
3.4	Module 4: Continuous Integration / Continuous Delivery	182
4	Class 3: Introduction to SecDevOps	201
4.1	Lab Topology	202
4.2	Module 1: iControl REST API Refresher	202
4.3	Module 2: Programmatic Control of Firewall Services	216
4.4	Module 3: Programmatic Control of Web Application Firewall Services	231
5	HOWTOs: Index	259
5.1	HOWTO - Update Existing iApp templates to Work with iWorkflow v2.1	259

Welcome

Welcome to F5's Automation, Orchestration and Programmability Training series. The intended audience for these labs are Super NetOps and DevOps engineers that would like to leverage the various programmability tools offered by the F5 platform. If you require a pre-built lab environment please contact your F5 account team and they can provide access to environments on an as-needed basis.

The content contained here adheres to a DevOps methodology and automation pipeline. All content contained here is sourced from the following GitHub repository:

<https://github.com/f5devcentral/f5-automation-labs/>

Bugs and Requests for enhancements are handled in two ways:

- Fork the Github Repo, fix or enhance as required and submit a Pull Request
 - <https://help.github.com/articles/creating-a-pull-request-from-a-fork/>
- Open an [Issue](#) within the repository.

Class 1: Introduction to Automation & Orchestration

This introductory class covers the following topics:

- Imperative Automation using the F5 BIG-IP iControl REST API
- Service Abstraction and Automation using F5 iApp templates
- Building Declarative Interfaces with the F5 iWorkflow product

Expected time to complete: **4 hours**

To continue please review the information about the Lab Environment. Additionally, if you are new to the F5 BIG-IP Platform we've created an overview in the BIG-IP Basics section.

2.1 Lab Topology & Environments

Warning: All work for this lab will be performed exclusively from the Linux Jump host. No installation or interaction with your local system is required.

All pre-built environments implement the Lab Topology shown below. Please review the topology first, then find the section matching the lab environment you are using for connection instructions.

2.1.1 Lab Topology

The network topology implemented for this lab is very simple. Since the focus of the lab is Control Plane programmability rather than Data Plane traffic flow we can keep the data plane fairly simple. The following components have been included in your lab environment:

- 2 x F5 BIG-IP VE (v12.1.x)
- 1 x F5 iWorkflow VE (v2.3)
- 1 x Linux Server
- 1 x Linux Jump host

The following table lists VLANs, IP Addresses and Credentials for all components:

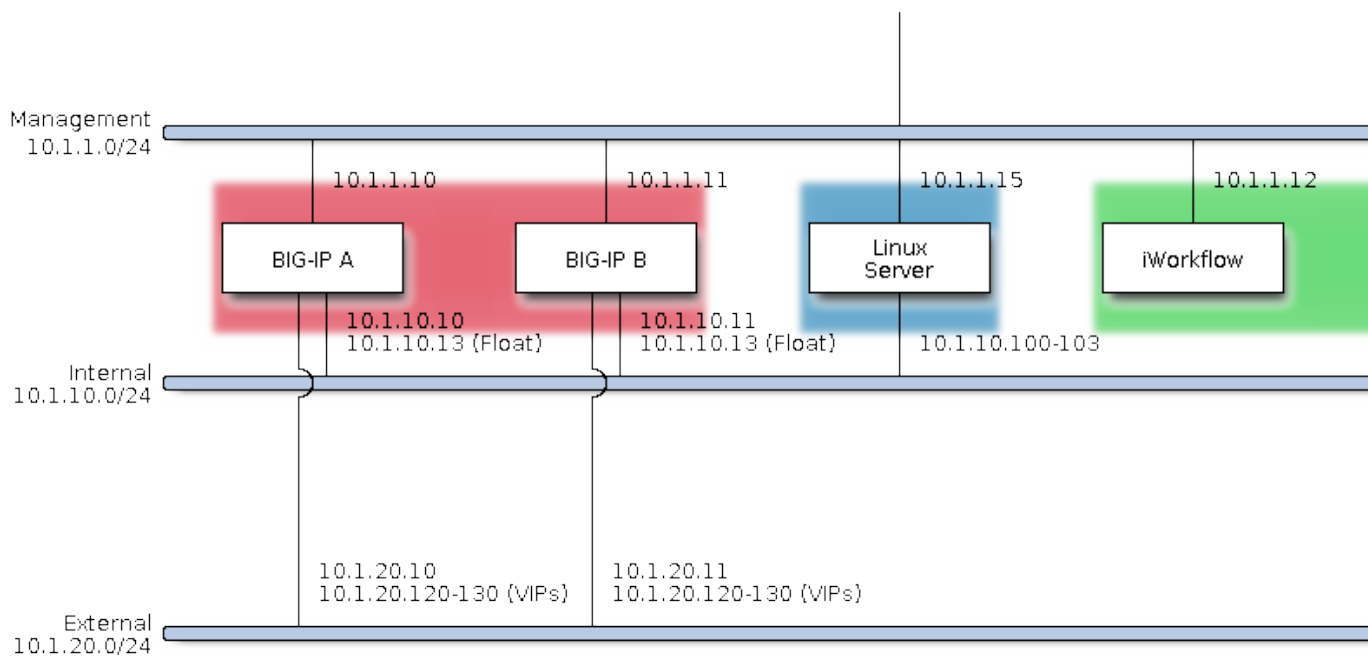


Fig. 2.1: Lab Topology

Component	Management IP	VLAN/IP Address(es)	Credentials
Linux Jumphost	10.1.1.20	Internal: 10.1.10.20 External: 10.1.20.20	ubuntu/supernetops
BIG-IP A	10.1.1.10	Internal: 10.1.10.10 Internal (Float): 10.1.10.13 External: 10.1.20.10 External (VIPs): 10.1.20.120-130	admin/admin root/default
BIG-IP B	10.1.1.11	Internal: 10.1.10.11 Internal (Float): 10.1.10.13 External: 10.1.20.11 External (VIPs): 10.1.20.120-130	admin/admin root/default
iWorkflow	10.1.1.12	N/A	admin/admin root/default
Linux Server	10.1.1.15	Internal: 10.1.10.100-103	root/default

2.1.2 Lab Environments

In order to complete this class you will need to utilize a specific **Lab Environment**. You can consume this training in a couple of ways:

- Pre-built Environment using a Ravello Blueprint
 - Used at official F5 events such as F5 Agility, F5 Agility Roadshows, User Groups, MeetUps, etc.
 - Access can be provided by your F5 Account Team
- Pre-built Environment using an Amazon AWS CloudFormation Template (CFT)
 - Access is on-demand and uses *your* AWS account
- Pre-built Environment using the F5 Unified Demo Framework (UDF)
 - This environment is currently available for F5 employees only
- Self-built Environment on your own infrastructure
 - Review the Topology and Guide below for prerequisites

Select the Environment from the list below to get started:

Amazon AWS Lab Environment Guide

Error: The AWS CFT is currently in testing and not complete. This notice will be updated as progress is made. This functionality should be available by Dec 1st 2017.

Warning: The AWS CFT will run in your account. The template includes components and instances that will incur a charge. This charge will be billed to your account.

You can use an Amazon CloudFormation Template (CFT) to launch your own lab environment in AWS. This guide assumes the following:

- Pre-existing Amazon AWS account
- Access to create AWS Instances and Resources
- You have created an AWS Key Pair:
 - <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>
- *You will be responsible for all charges incurred*

More information about AWS can be found here:

<https://aws.amazon.com/>

Task 1 - Determine your Source IP Address

The AWS lab environment restricts access based on your Source IP Address. We will use a website to determine your Source IP for use in the next Task.

Note: If your Source IP address changes you will lose access to your environment.

Perform the following steps to complete this task:

1. Open a web browser window or tab and navigate to <https://www.whatismyip.com/>

2. Copy the IP Address shown in the *Your IP Address is:* box into your clipboard

Task 2 - Launch the CloudFormation Template

Perform the following steps to complete this task:

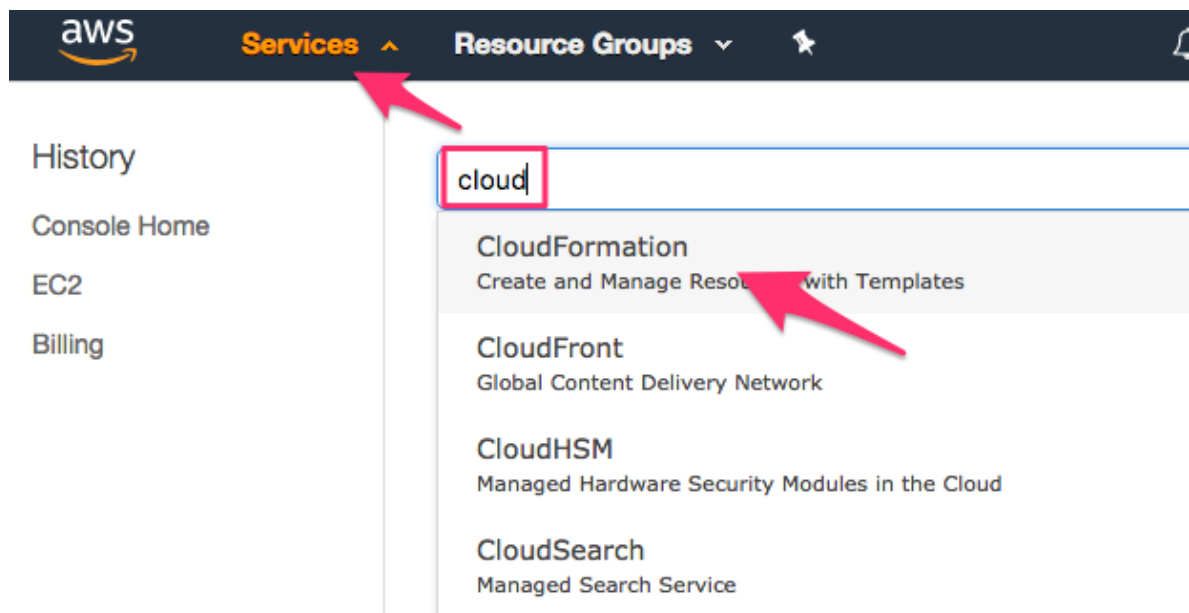
1. Login to your AWS Management Console

Note: Access to the console is determined by your individual account setup.

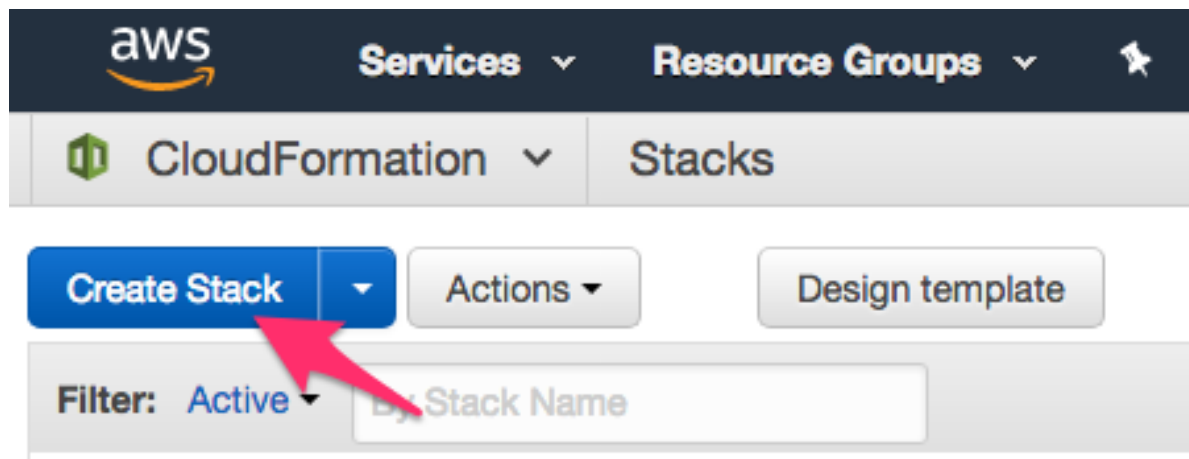
If you are using a personal account you should be able to login using <https://console.aws.amazon.com/console/home>

If you are using a corporate account please contact your IT Help Desk.

2. Click *Services* at the top of the window. Then type `cloud` into the search box and look for the *CloudFormation* item. Click on the *CloudFormation* item:



3. Click the *Create Stack* button:



4. On the *Select Template* screen, select the *Specify an Amazon S3 template URL* option. Copy and paste the URL below into the box:

```
https://s3.us-east-2.amazonaws.com/supernetops-cf-templates/class1.  
template
```

Click on the *Next* button

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. [Learn more.](#)
[Design template](#)

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. [Learn more.](#)

☐ Select a sample template

☐ Upload a template to Amazon S3
[Choose File](#) No file chosen

☒ Specify an Amazon S3 template URL
 [View/Edit template in Designer](#)

[Cancel](#) [Next](#)

5. Complete the form in the *Specify Details* screen:

- **Stack Name:** Super-NetOps-Lab or a name of your choice
- **Branch:** master
- **InstanceType:** t2.medium
- **KeyName:** Select your AWS Key Pair
- **UserIP:** Paste the IP Address from Task 1 and add /32 to the end.

Note: You can also specify a CIDR formatted Subnet in this field

6. Click the *Next* button
7. On the *Options* screen click the *Next* button at the bottom of the screen
8. On the *Review* screen check the *I acknowledge that AWS CloudFormation might create IAM resources with custom names* field and click the *Create* button at the bottom of the screen

Capabilities

i The following resource(s) require capabilities: [AWS::CloudFormation::Stack]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more.](#)

☒ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Cancel Previous Create

9. Click the Super-NetOps-Lab stack to view details of the deployment

Filter: Active ▾ By Stack Name Showing 1 stack

	Stack Name	Created Time	Status	Description
<input checked="" type="checkbox"/>	Super-NetOps-Lab	2017-10-25 17:04:27 UTC-0500	CREATE_IN_PROGRESS	This will deploy the Ubu...

10. Monitor the *Events* section of the page as the Stack deploys:

Super-NetOps-Lab

Other Actions ▾ Update Stack

Stack name: Super-NetOps-Lab

Stack ID:

Status: CREATE_IN_PROGRESS

Status reason:

Termination protection: Disabled

IAM Role:

Description This will deploy the Ubuntu instance to access and use the f5-automation lab. The instance deployed is a Ubuntu 16.04 LTS - Xenial HVM; please MAKE SURE YOU ACCEPTED THE TERMS FOR THIS INSTANCE BEFORE LAUNCHING THIS STACK

► Outputs

► Resources

▼ Events

2017-10-25	Status	Type	Logical ID	Status reason
► 17:07:23 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	TopologyStack	Resource creation Initiated
► 17:07:22 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	TopologyStack	
► 17:07:17 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	Super-NetOps-Lab	User Initiated

11. The CFT used performs a nested deployment, leveraging other CFT's. The *Events* will notify you when new status messages are available. Total deployment time varies. As the Stack is being deployed you will see periodic `CREATE_COMPLETE` messages:

▼ Events				
2017-10-25	Status	Type	Logical ID	Status reason
▶ 17:10:08 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	ServerStack	Resource creation Initiated
▶ 17:10:08 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	JumpHostStack	Resource creation Initiated
▶ 17:10:07 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	ServerStack	
▶ 17:10:06 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	JumpHostStack	
▶ 17:10:04 UTC-0500	CREATE_COMPLETE	AWS::CloudFormation::Stack	TopologyStack	
▶ 17:07:23 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	TopologyStack	Resource creation Initiated
▶ 17:07:22 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	TopologyStack	
▶ 17:07:17 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	Super-NetOps-Lab	User Initiated

12. You can also go back to the page listing 'Stacks' and monitor the progress of the nested templates from there:

The screenshot shows the AWS CloudFormation console. At the top, the navigation bar includes 'Services' and 'Resource Groups'. Below this, the 'CloudFormation' service is selected, and the 'Stacks' page is active. A red arrow points to the 'Stacks' breadcrumb. The main content area shows a list of stacks. The 'Super-NetOps-Lab-JumpHos...' stack is selected. Below the stack list, there are tabs for 'Overview', 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', 'Stack Policy', and 'Change Sets'. The 'Events' tab is selected, and a red arrow points to it. The 'Events' tab displays a table of events for the selected stack, including 'CREATE_COMPLETE' and 'CREATE_IN_PROGRESS' status changes for various resources.

Stack Name	Created Time	Status	Description
Super-NetOps-Lab-ServerSta... NESTED	2017-10-25 17:10:08 UTC-0500	CREATE_IN_PROGRESS	This will deploy the Ubuntu HTTP server instance t...
Super-NetOps-Lab-JumpHos... NESTED	2017-10-25 17:10:07 UTC-0500	CREATE_IN_PROGRESS	This will deploy the Ubuntu instance to access an...
Super-NetOps-Lab-Topology... NESTED	2017-10-25 17:07:23 UTC-0500	CREATE_COMPLETE	This Cloud Formation Template creates the network...
Super-NetOps-Lab	2017-10-25 17:07:17 UTC-0500	CREATE_IN_PROGRESS	This will deploy the Ubuntu instance to access an...

2017-10-25	Status	Type	Logical ID	Status reason
▶ 17:10:34 UTC-0500	CREATE_COMPLETE	AWS::EC2::NetworkInterface	ENIManagement	
▶ 17:10:34 UTC-0500	CREATE_COMPLETE	AWS::EC2::NetworkInterface	ENIExternal	
▶ 17:10:19 UTC-0500	CREATE_IN_PROGRESS	AWS::EC2::Instance	F5SNOpsRDP	Resource creation Initiated
▶ 17:10:18 UTC-0500	CREATE_IN_PROGRESS	AWS::EC2::NetworkInterface	ENIManagement	Resource creation Initiated
▶ 17:10:18 UTC-0500	CREATE_IN_PROGRESS	AWS::EC2::Instance	F5SNOpsRDP	
▶ 17:10:17 UTC-0500	CREATE_IN_PROGRESS	AWS::EC2::NetworkInterface	ENIManagement	
▶ 17:10:17 UTC-0500	CREATE_IN_PROGRESS	AWS::EC2::NetworkInterface	ENIExternal	Resource creation Initiated

13. Once the *Status* of the Super-NetOps-Lab **root** stack shows `CREATE_COMPLETE` click the *Outputs* tab. You will see a *Key* named `JumpHostPublicIP`. The *Value* is the IP Address you can use to connect to the Lab JumpHost using RDP, HTTPS or SSH (diagnostics only).

Filter: Active

Super-NetOps

Showing 4 stacks

Stack Name	Created Time	Status	Description
<input type="checkbox"/> Super-NetOps-Lab-Topology... <div>NESTED</div>	2017-10-25 17:32:53 UTC-0500	CREATE_COMPLETE	This Cloud Formation Template creates the network...
<input checked="" type="checkbox"/> Super-NetOps-Lab	2017-10-25 17:32:46 UTC-0500	CREATE_COMPLETE	This will deploy the Ubuntu instance to access and...

Overview

Outputs

Resources

Events

Template

Parameters

Tags

Stack Policy

Change Sets

Key	Value	Description	Export Name
InternalSubnetId		Internal Subnet ID	
ExternalSubnetId		External Subnet ID	
VpcId		VPC ID	
ManagementSubnetId		Management Subnet ID	
Region		AWS Region	
JumpHostPublicIP	34.213.	Jump Host Public IP (SSH & RDP)	

14. You can now connect to the JumpHost using RDP or HTTPS:

- RDP: Configure your RDP client to connect to the `JumpHostPublicIP`
- HTTPS: Use a HTML5 browser to connect to `https://<JumpHostPublicIP>`

15. Select how you would like to continue:

- Review: *BIG-IP Basics (optional)*
- Start: *Module 1: Imperative Automation with the BIG-IP iControl REST API*

Ravello

If you are taking this class at a Meetup, User Group, F5 Agility or another official event, access details will be provided by your instructor.

If you would like to take this class using our lab environment please contact your F5 Account Team for access. You can also send an email to **supernetopshelp (at) f5.com**.

Once you have connected to your environment you can select how you would like to continue:

- Review: *BIG-IP Basics (optional)*
- Start: *Module 1: Imperative Automation with the BIG-IP iControl REST API*

F5 Unified Demo Framework (UDF)

Note: This environment is currently available for F5 employees only

Determine how to start your deployment:

- **Official Events (ISC, SSE Summits):** Please follow the instructions given by your instructor to join the UDF Course.
- **Self-Paced/On Your Own:** Login to UDF, *Deploy* the Programmability Class 1: Introduction to Automation & Orchestration Blueprint and *Start* it.



Connecting to the Environment

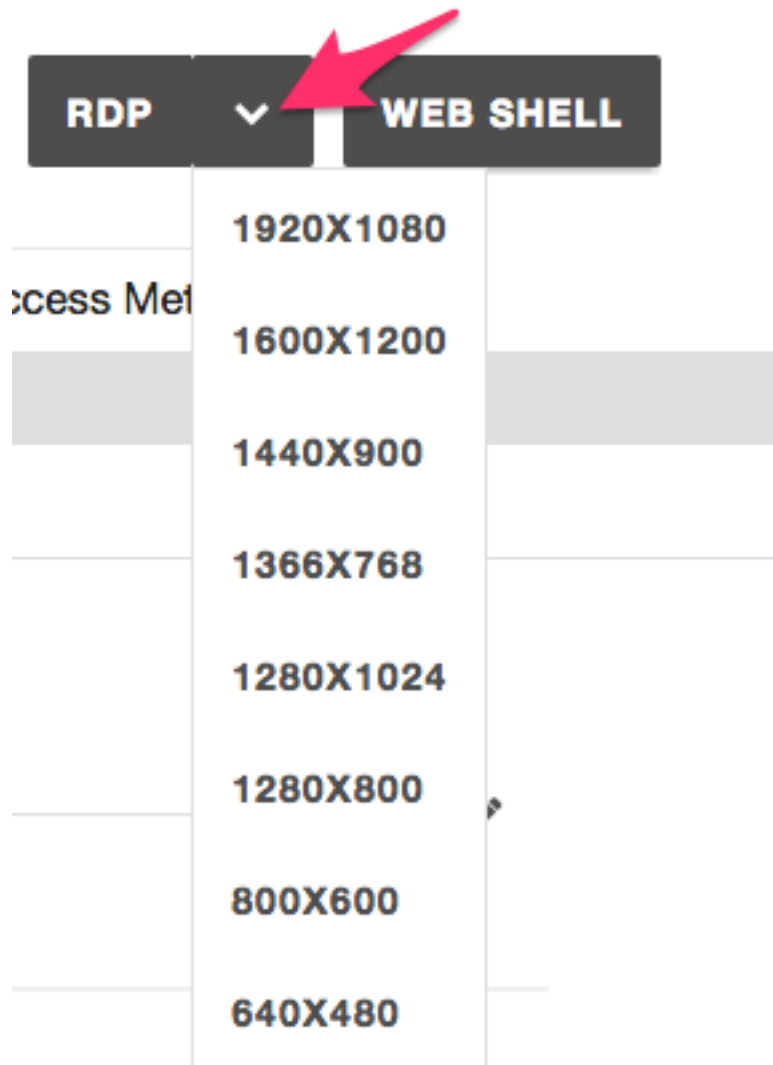
To connect to the lab environment we will use a Remote Desktop Protocol client to connect to the JumpHost.

Note: We recommend that students open this lab guide on their Jumphost using the Chrome web browser. The browser is configured to open the lab guide as it's start page.

Connect using RDP

1. In the UDF navigate to your *Deployments*
2. Click the *Details* button for your Deployment
3. Click the *Components* tab
4. Find the `Linux Jumphost` Component and click the *Details* button.
5. Download the RDP file by completed *one* of the following:

- **Full Screen:** Click the  button to download an RDP file that will start the RDP session in full screen mode
- **Specify Resolution:** Click the  button and select a screen resolution to use for the connection:



6. If you do not have the official Microsoft Remote Desktop Client, please install it using the instructions at <https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-clients>
7.

Warning: If you have a HiDPI display please refer to the [Using HiDPI Displays \(RDP & Windows\)](#) instructions below
8. Open the RDP file in the Remote Desktop Client and connect. If you have any problems please ask your instructor for help
9. Select how you would like to continue:
 - Review: [BIG-IP Basics \(optional\)](#)
 - Start: [Module 1: Imperative Automation with the BIG-IP iControl REST API](#)

Using HiDPI Displays (RDP & Windows)

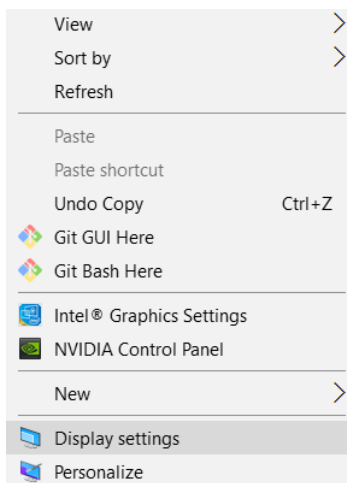
Warning: Do these steps BEFORE you connect via RDP. Choose ONE only. Do not do both.

If you are using Hi Resolution Display on Windows, we recommend that you either:

- **RECOMMENDED:** Resize your display to 1080p (1920 x 1080) or
- Use your RDP clients “Zoom” functionality to increase the size

Resize your display (Windows 10) - RECOMMENDED

1. Right click on your Desktop and select Display Settings.

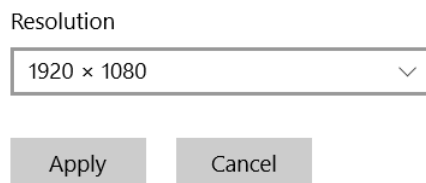


2. Click on *Advanced Display Settings*



[Advanced display settings](#)

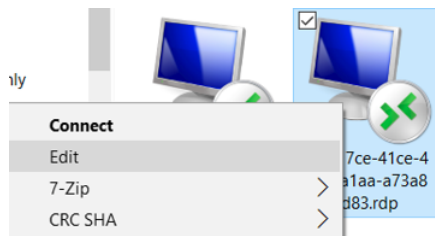
3. Change the Resolution to 1920 × 1080 and click the *Apply* button



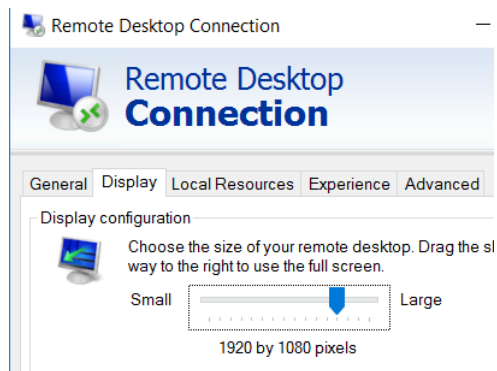
4. Connect to the RDP session
5. Select how you would like to continue:
 - Review: [BIG-IP Basics \(optional\)](#)
 - Start: [Module 1: Imperative Automation with the BIG-IP iControl REST API](#)

Use RDP Zoom

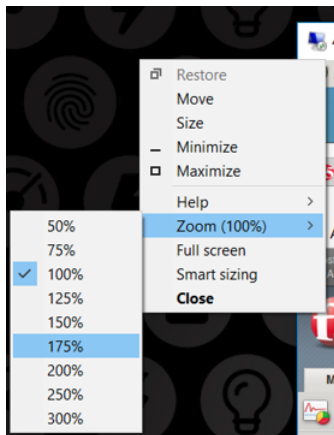
1. Right click on the RDP file and click on *Edit*



2. Under the *Display* tab change the resolution to 1920x1080, then click *Connect*



3. After you connect, access the menu at the top left of your RDP Window and change the Zoom level (i.e. 175%).



4. Select how you would like to continue:
 - Review: *BIG-IP Basics (optional)*
 - Start: *Module 1: Imperative Automation with the BIG-IP iControl REST API*

Self-Built Environment

Note: Due to the variability of self-built environments we cannot guarantee that you will be able to complete the class successfully.

If you are building your own lab environment please complete the following steps and pre-requisites first:

1. Your network configuration matches the topology in the [Lab Topology](#)
2. Ensure your BIG-IP devices are licensed and have the following modules provisioned:
 - LTM
 - ASM
3. Your server instance can be built two ways:
 - (a) Build or reuse your own instance. It should have the following services installed and running:
 - HTTP Server - TCP/80
 - DNS Server - UDP/53
 - (b) Use our server image build script located at the url below to configure an Ubuntu 16.04 base installation automatically.

Note: Please ensure that HTTP & DNS services are not installed on the base image

https://raw.githubusercontent.com/f5devcentral/f5-automation-labs/sp/lab_environments/AWS/snops_server_setup.sh

4. Your host should have the following applications installed:
 - Postman v5.3.0 - <https://getpostman.com>
 - Google Chrome - <https://google.com/chrome>
5. You will need to install the `f5-postman-workflows` framework into Postman:
 - (a) Open Postman
 - (b) Click the 'Import' button
 - (c) Select 'Import from Link'
 - (d) Enter `https://raw.githubusercontent.com/0xHiteshPatel/f5-postman-workflows/master/F5_Postman_Workflows.postman_collection.json` in the field
 - (e) Click the 'Import' button
 - (f) Navigate to your Postman Collections
 - (g) Expand the 'F5_Postman_Workflows' collection
 - (h) Expand the 'Install' folder
 - (i) Click the 'Install/Upgrade f5-postman-workflows' items
 - (j) Click the 'Send' button
 - (k) Verify the installation was successful by:
 - i. Examine the response tests and ensure the 'Install Successful' test passed
 - ii. Examine your Postman Global Environment and look for a `_f5_workflow_functions` item populated with JavaScript code
6. Select how you would like to continue:
 - Review: [BIG-IP Basics \(optional\)](#)

- Start: *Module 1: Imperative Automation with the BIG-IP iControl REST API*

2.2 BIG-IP Basics (optional)

Just in case you're new to the F5 BIG-IP platform (or need a refresher) we've included some links and videos below that will help get you started.

2.2.1 What is BIG-IP

Source: <https://devcentral.f5.com/articles/lightboard-lessons-what-is-big-ip-26793>

2.2.2 BIG-IP Basic Nomenclature

Source: <https://devcentral.f5.com/articles/lightboard-lessons-big-ip-basic-nomenclature-26144>

2.2.3 F5 DevCentral BIG-IP Basics Articles

BIG-IP Basics Articles: <https://devcentral.f5.com/articles?tag=devcentral+basics>

2.2.4 Using F5 in Various Environments

- Public Cloud:
 - **AWS/Azure/GCP/etc.:** <http://clouddocs.f5.com/cloud/public/v1/>
- Private Cloud:
 - **OpenStack:** <http://clouddocs.f5.com/cloud/openstack/>
 - **VMware:** <https://f5.com/solutions/technology-alliances/vmware>
- Container Ecosystems:
 - **Cloud Foundry:** <http://clouddocs.f5.com/containers/latest/cloudfoundry/>
 - **Kubernetes:** <http://clouddocs.f5.com/containers/latest/kubernetes>
 - **Mesos Marathon:** <http://clouddocs.f5.com/containers/latest/marathon>
 - **RedHat OpenShift:** <http://clouddocs.f5.com/containers/latest/openshift/>

2.2.5 HA Proxy to BIG-IP Quick Start

If you're already familiar with HA Proxy, learning F5 BIG-IP is straightforward once you learn the associated F5 terminology.

Here is a list of common HA Proxy configuration terminology and its F5 equivalent:

HA Proxy	F5 BIG-IP
Frontend	Virtual Server (VIP)
Backend	Pool
Server	Member
mode http	HTTP Profile
default_backend	Default pool
use_backend	LTM policy
check port	Health monitor

2.2.6 NGINX to BIG-IP Quick Start

If you are already familiar with NGINX, learning F5 BIG-IP will be straightforward once you learn the F5 terminology.

NGINX administrators usually use multiple files and leverage the include command in their config to break down the config and make it easier to manage. F5 leverages *Profiles* which can be applied to a *Virtual Server*.

NGINX uses in-band (passive) health monitors which can be enabled on F5 through the creation of an *inband monitor*. BIG-IP also supports the use of active health monitors, which will poll the pool member periodically. Both can be used together for better monitoring of your services.

F5 BIG-IP supports control-plane and data-plane programmability with:

- Node.js through the use of iRulesLX, iControlLX and iAppsLX
- TCL through the use of iRules and iApp Templates

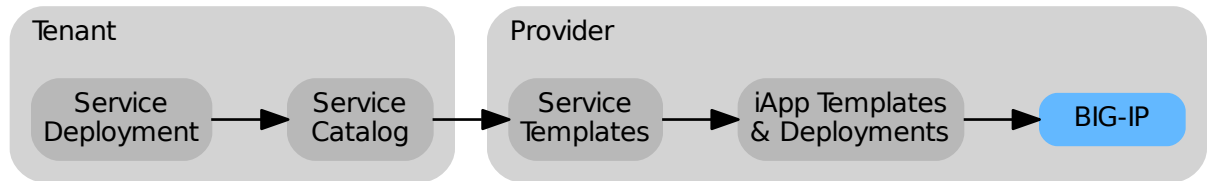
A lot of the manual configuration and scripting steps that are required with NGINX are supported more easily through various config parameters and profiles in BIG-IP. By leveraging the control-plane programmability features this class covers you can achieve full automation of your services with the BIG-IP platform.

F5 BIG-IP is designed to be a full proxy by default. In most cases there is no need to tune TCP & HTTP buffering like you would on NGINX (i.e. using `proxy_buffering`). This is because the default settings have been optimized and can adapt to most situations.

Here is a list of common NGINX configuration terminology and its F5 equivalent:

NGINX	F5 BIG-IP
listen	Virtual Server Port (VIP)
upstream	Pool
proxy_pass	Default Pool
server	Member
ssl_certificate	SSL Profile Option
return	LTM HTTP Policy Option
proxy_set_header X Forwarded For	HTTP Profile Option Insert X-Forwarded-For
proxy_set_header	LTM HTTP Policy Option
add_header	LTM HTTP Policy Option
location & proxy_pass	LTM HTTP Policy Option
Proxy Cache	Web Acceleration Policy

2.3 Module 1: Imperative Automation with the BIG-IP iControl REST API



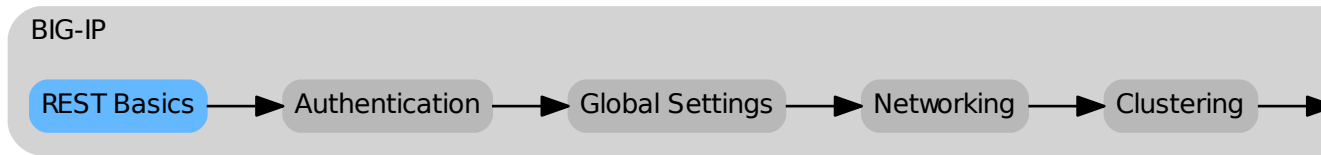
In this module you will learn the basic concepts required to interact with the BIG-IP iControl REST API. Additionally, you will walk through a typical Device Onboarding workflow to deploy a fully functional BIG-IP Active/Standby pair. It's important to note that this module will focus on demonstrating an **Imperative** approach to automation.

Note: The Lab Deployment for this lab includes two BIG-IP devices. For most of the labs, we will only be configuring the BIG-IP A device (management IP configuration and licensing has been completed). BIG-IP B will have some minimal configuration pre-loaded. In real-world scenario, it would be necessary to perform Device Onboarding functions on ALL BIG-IP devices. In this lab exercise, we chose to perform it only on a single device due to lab time allocation constraints.

Note: In order to confirm the results of REST API calls made in this lab, it's recommended to keep GUI/SSH sessions to BIG-IP and iWorkflow devices open. By default, BIG-IP and iWorkflow will log all the REST API related events locally to **restjavad.0.log**. These logs can also be directed to a remote syslog server (see <https://support.f5.com/csp/article/K13080>). On a side note, the **ltm** log files listed below contains log messages specific to BIG-IP local traffic management events.

- BIG-IP:
 - /var/log/ltm
 - /var/log/restjavad.0.log
 - iWorkflow:
 - /var/log/restjavad.0.log
-

2.3.1 Lab 1.1: Exploring the iControl REST API



Task 1 - Explore the API using the TMOS Web Interface

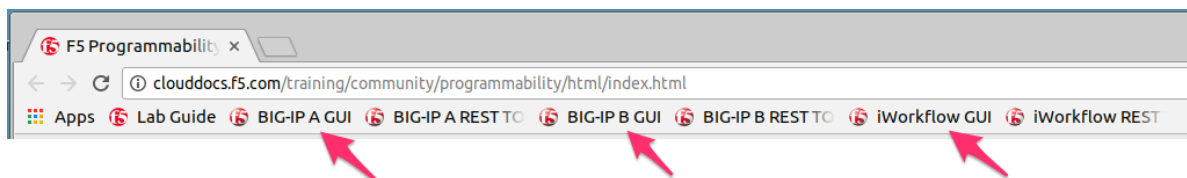
In this lab, we will explore the API using an interface that is built into TMOS. This utility is useful for understanding how TMOS objects map to the REST API. The interfaces implement full Create, Read, Update and Delete (CRUD) functionality, however, in most practical use cases it's far easier to use this interface as a 'Read' tool rather than trying to Create objects directly from it. You can use TMUI or TMSH to create the object as needed and then use this tool to view the created object with all the correct attributes already populated.

Note: This guide may require you to Copy/Paste information from the guide to your jumphost. To make this easier you can open a copy of the guide by using the **Lab Guide** bookmark in Chrome.

1. Open Google Chrome and navigate to the following bookmarks: **BIG-IP A GUI**, **BIG-IP B GUI** and **iWorkflow GUI**. Bypass any SSL errors that appear and ensure you see the login screen for each bookmark.

Warning: Skipping this step will result in errors in subsequent steps

Warning: We are using a self-signed certificate in this lab. In your environment you must make sure that you use certificates issued by your certificate authority for both production and lab equipments. Not doing so would make it possible for an attacker to do a man-in-the-middle attack and allow him the ability to steal passwords and tokens.



2. Navigate to the URL `https://10.1.1.10/mgmt/toc` (or click the BIG-IP A REST TOC bookmark). The `/mgmt/toc` path in the URL is available on all TMOS versions 11.6 or newer.
3. Authenticate to the interface using the default credentials (`admin/admin`)

4. You will now be presented with a top-level list of various REST resources. At the top of the page there

filter worker...

is a search box that can be used to find items on the page. Type `net` in the search box and then click on the 'net' link under iControl REST Resources:





Table of Contents

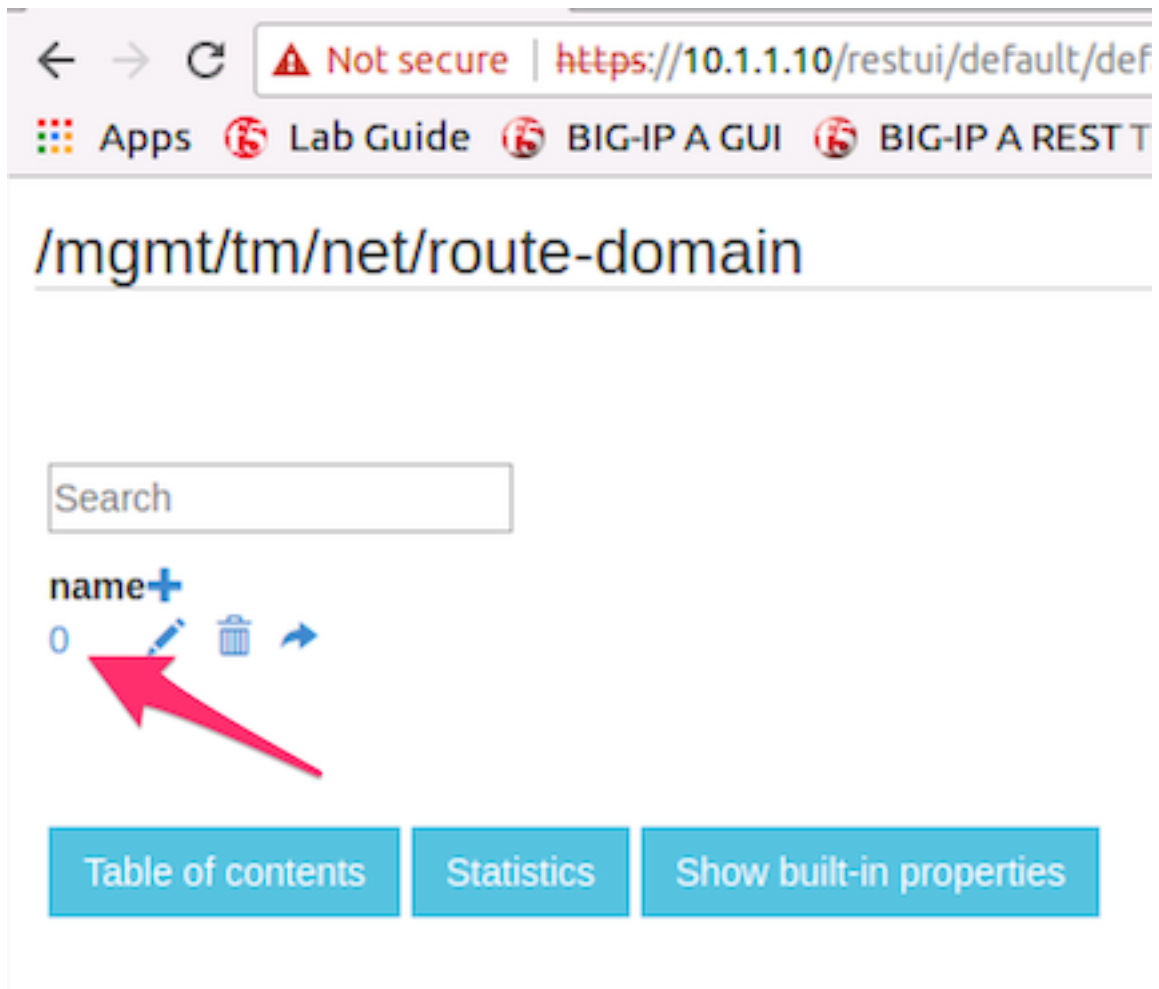
net

iControl REST Resources

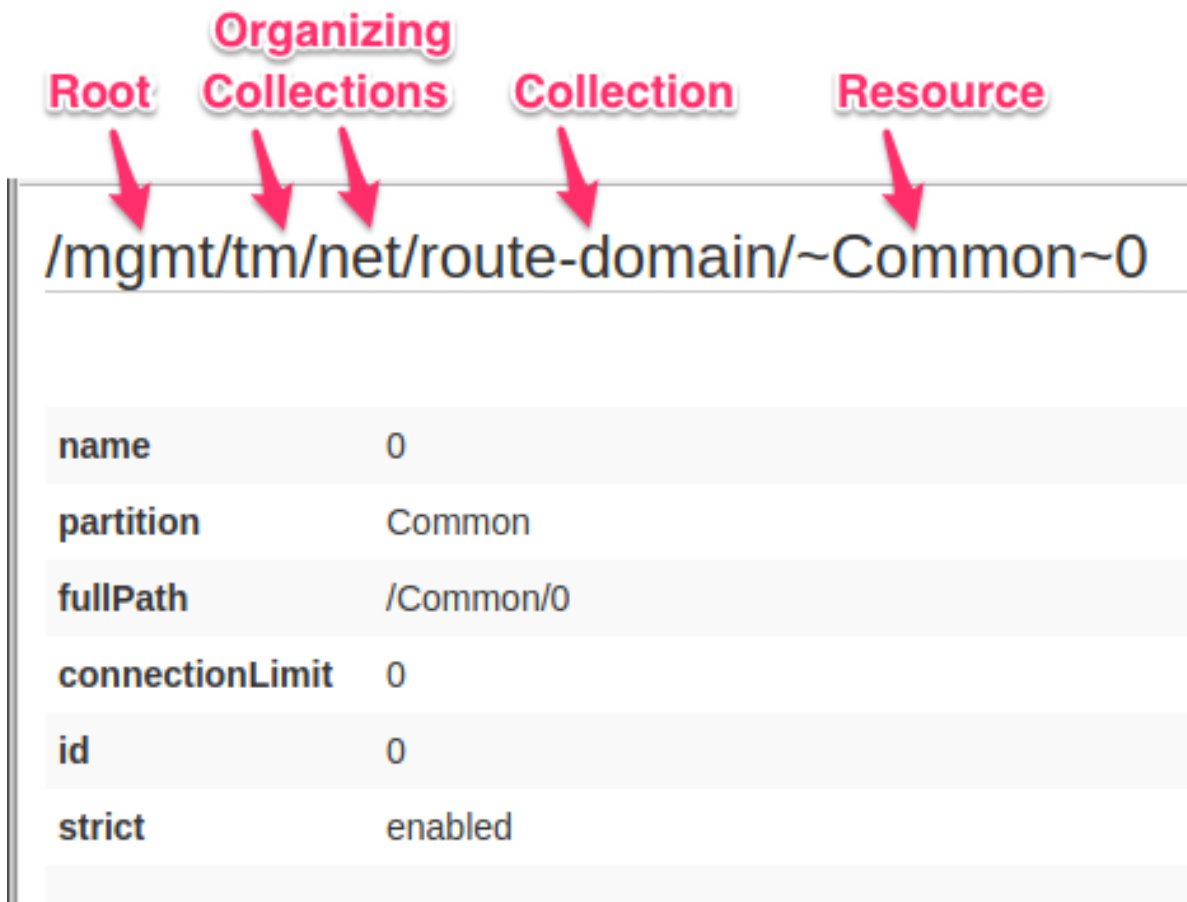
net

Traffic Management

5. Find the `/mgmt/tm/net/route-domain` **Collection** and click it.
6. You will now see a listing of the **Resources** that are part of the route-domain(s) collection. As you can see the default route domain of 0 is listed. You can also create new objects by clicking the  button. Additionally, resources can be deleted using the  button or edited using the  button. The  is used to copy JSON formatted resource with Ctrl+C. This can be useful when you want to slightly change an existing resource.
7. Click the 0 resource to view the attributes of route-domain 0 on the device:

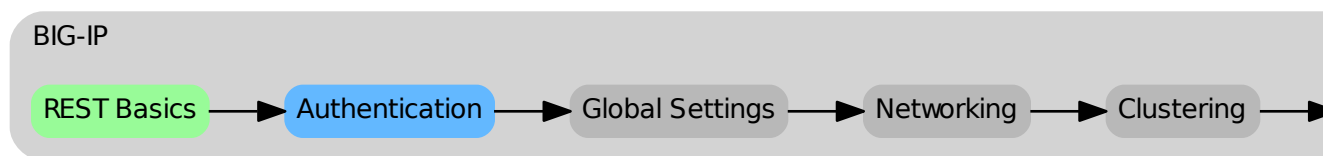


8. You can now see the properties of the route-domain 0 Resource. The components of the URI have been labeled in the screenshot below:



Note: If you would like to learn more about the iControl REST API be sure to read the **Demystifying iControl REST** article series at <https://devcentral.f5.com/wiki/icontrolrest.homepage.ashx>

2.3.2 Lab 1.2: REST API Authentication & 'example' Templates



One of the many basic concepts related to interaction with REST API's is how a particular consumer is authenticated to the system. BIG-IP and iWorkflow support two types of authentication: **HTTP BASIC** and **Token-Based (TBA)**. It's important to understand both of these authentication mechanisms, as consumers


of the API will often make use of both types depending on the use case. This lab will demonstrate how to interact with both types of authentication.

Throughout this and other classes in the series we will make use of the Postman REST API Client. You can find more information about Postman at <https://getpostman.com>

Task 1 - Import the Postman Collection & Environment

In this task you will Import a Postman Collection & Environment for this lab. Perform the following steps to complete this task:

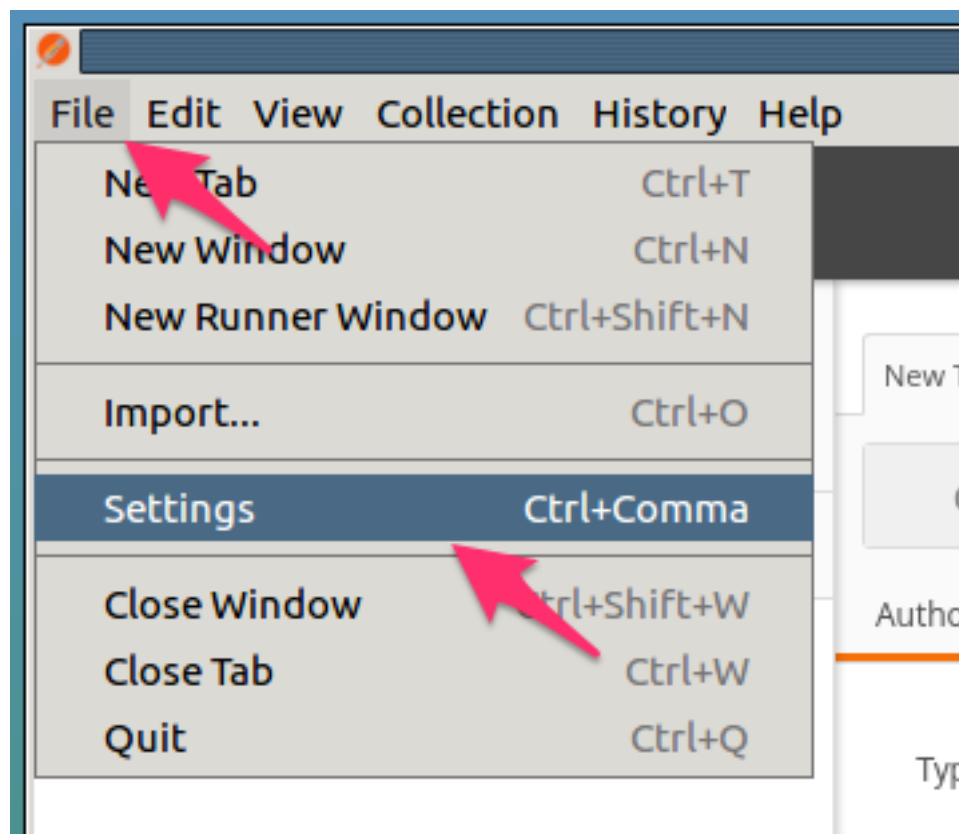


1. Open the Postman tool by clicking the  icon of the desktop of your Linux Jumpshot. **The initial window may take a few moments to appear.**

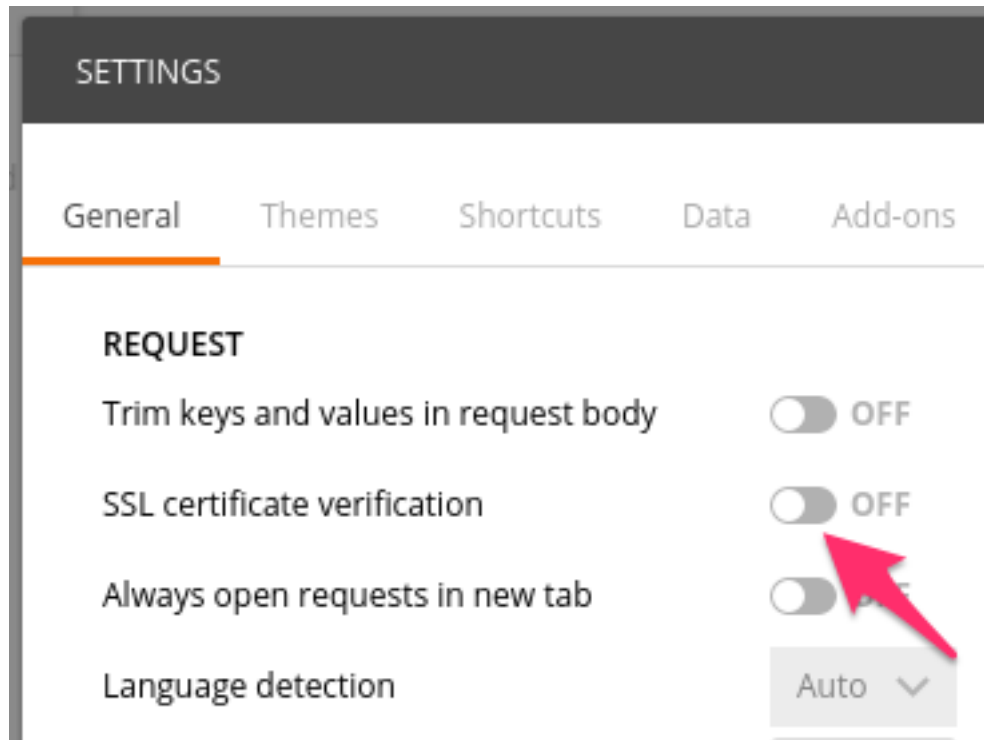
Note: The Postman client receives very frequent updates. If you are prompted to update the client please click the *Remind me later* button to skip updating the version installed in your lab environment

2. By default, the Postman client requires verification of SSL/TLS Certificates to a public Root Certificate Authority. However, by default, BIG-IP and many other devices use a self-signed certificate for SSL/TLS connections. To allow connections with self-signed certificates we need to modify the default settings of Postman.

- Open the Postman Settings windows by clicking *File* → *Settings*:

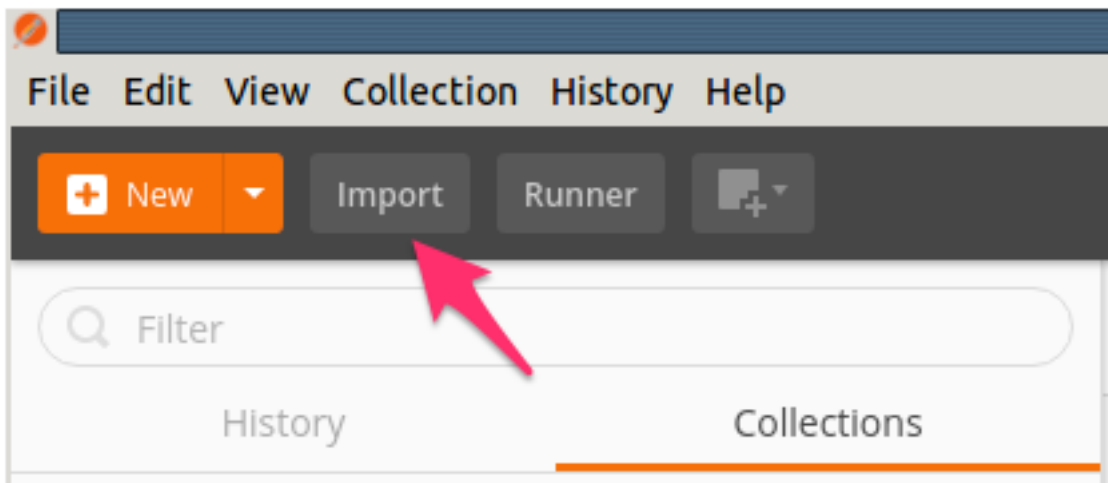


- Verify your client is configured to allow self-signed certificates by setting SSL certificate verification to OFF



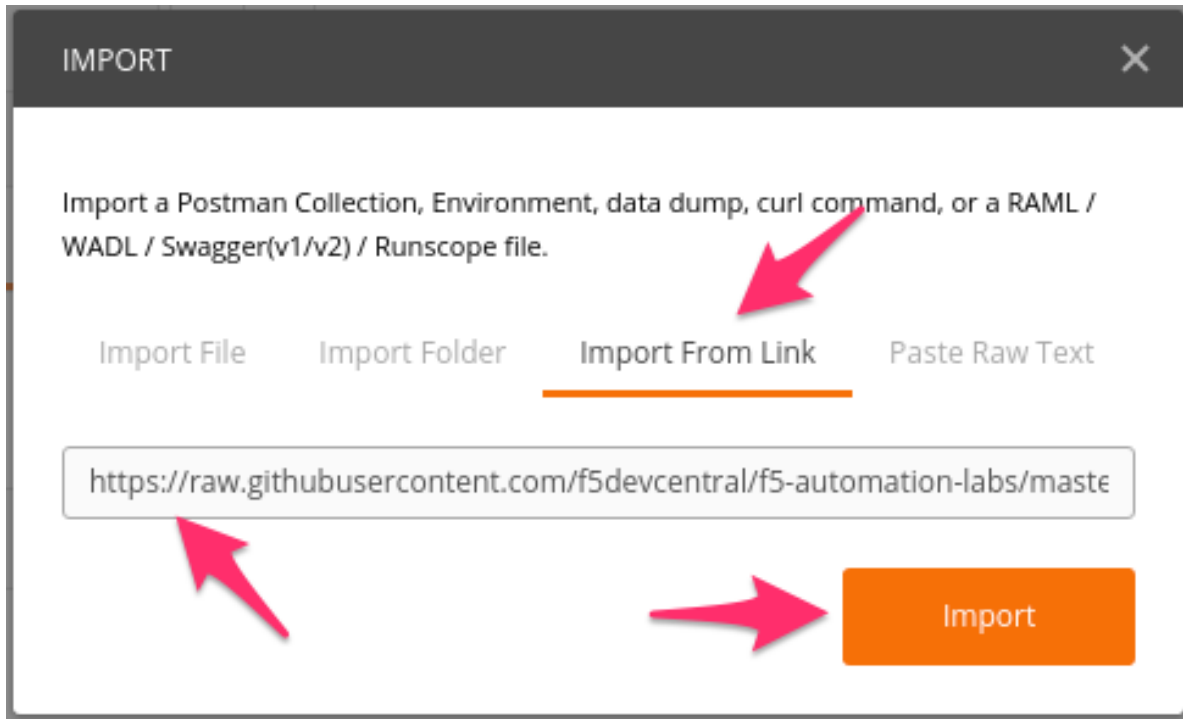
- Click the **X** in the top right of the Settings window

3. A Postman Collection lets you group individual REST requests together. This Postman collection can then be shared and imported. To import a Postman Collection, click the *Import* button in the top left of the Postman window

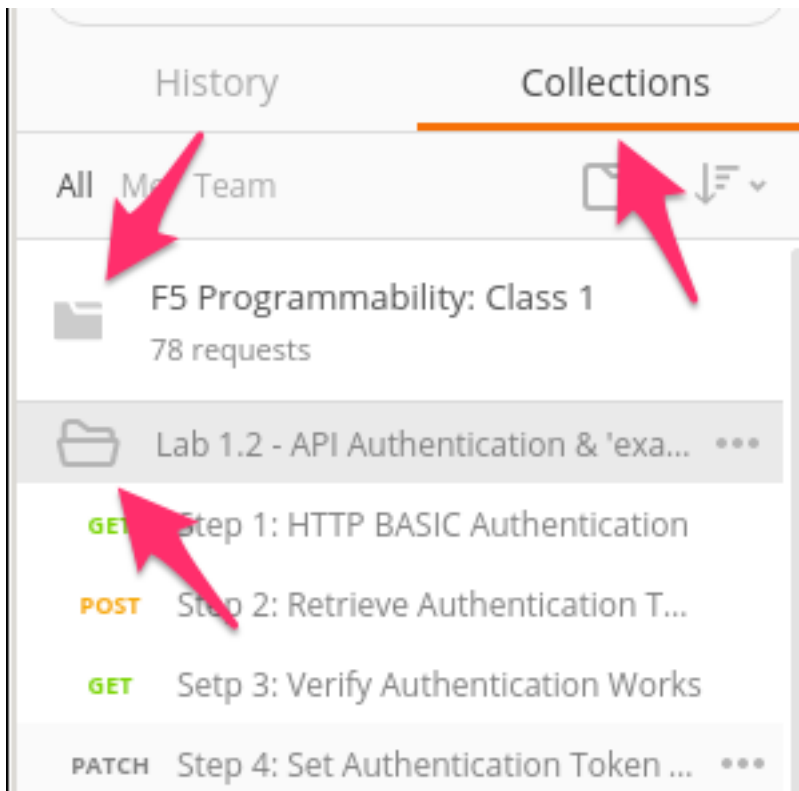


4. Click the *Import from Link* tab. Paste the following URL into the text box and click *Import*

`https://raw.githubusercontent.com/f5devcentral/f5-automation-labs/sp/postman_collections/Class_1_Service_Provider.postman_collection.json`



5. You should now see a collection named **F5 Programmability: Class 1** in your Postman Collections sidebar. Postman automatically resizes its GUI depending on its window size. It might be necessary to use the short `Ctrl + \` (on Windows) or click the show sidebar icon at the bottom left corner of postman if you do not see the sidebar.

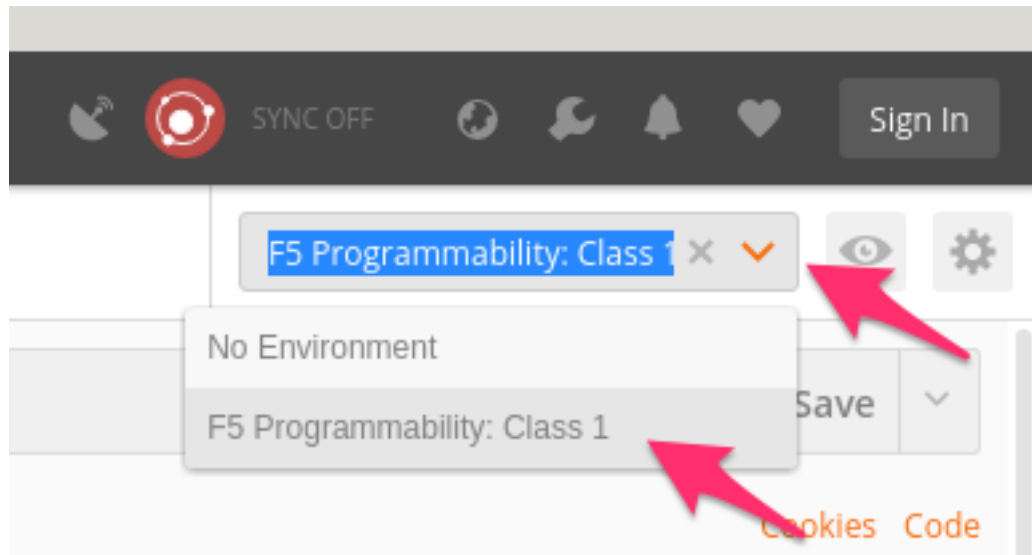


6. To assist in multi-step procedures we make heavy use of the **Environments** capability in Postman.

This capability allows us to set various global variables that are then substituted into a request before it's sent. Import the Environment file by clicking *Import* → *Import from Link* and pasting the following URL and clicking *Import*:

```
https://raw.githubusercontent.com/f5devcentral/f5-automation-labs/sp/postman_collections/Class_1.postman_environment.json
```

7. Set your environment to F5 Programmability: Class 1 by using the menu at the top right of your Postman window:



Important: In the pre-built lab environment a framework named `f5-postman-workflows` has been pre-installed in the environment. The Collection we installed above **REQUIRES** this framework for testing and polling functionality. If you are using a Self-Built Environment **you must install this framework into Postman by importing another collection**. Instructions to do this can be found [here](#)

Task 2 - HTTP BASIC Authentication

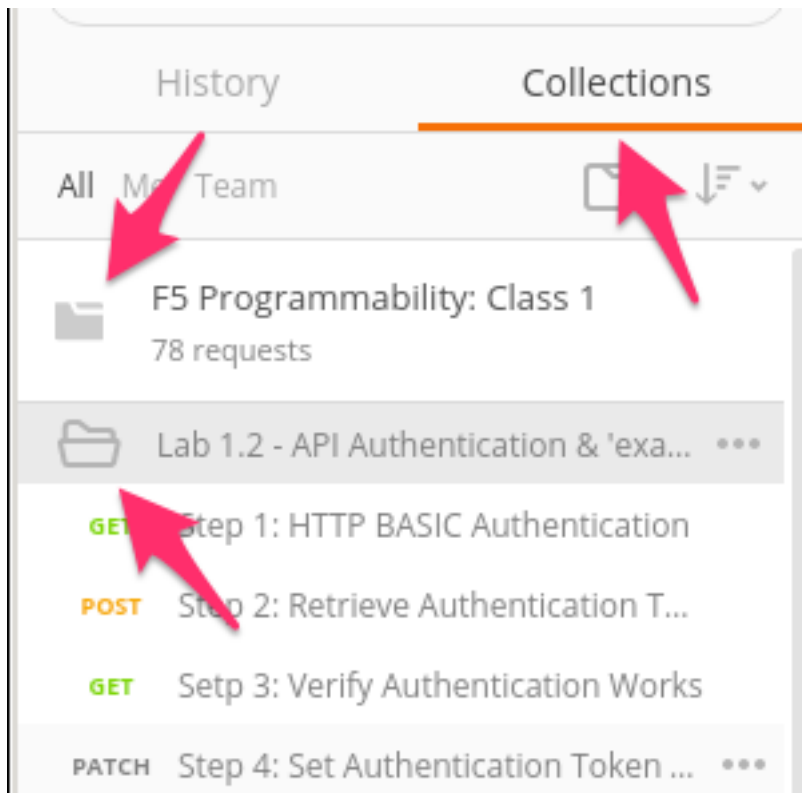
In this task, we will use the Postman client to send API requests using HTTP BASIC authentication. As its name implies this method of authentication encodes the user credentials via the existing BASIC authentication method provided by the HTTP protocol. The mechanism this method uses is to insert an HTTP header named 'Authorization' with a value that is built by Base 64 encoding the string `<username>:<password>`. The resulting header takes this form:

```
Authorization: Basic YWRtaW46YWRtaW4=
```

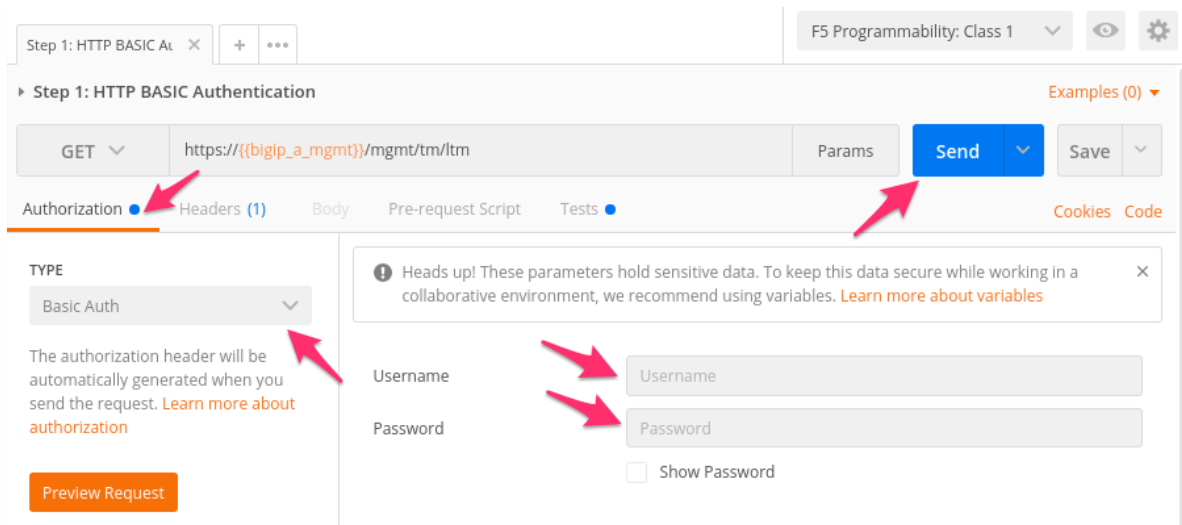
It should be noted that cracking this method of authentication is TRIVIAL; as a result API calls should always be performed using HTTPS encryption (F5 default) with a certificate signed by an authority rather than HTTP.

Perform the following steps to complete this task:

1. Click the *Collections* tab on the left side of the screen, expand the `F5 Programmability: Class 1` collection on the left side of the screen, expand the `Lab 1.2 - API Authentication & 'example' Templates` folder:



2. Click the Step 1: HTTP BASIC Authentication item. Click the *Authorization* tab and select Basic Auth as the Type. Fill in the username and password (admin/admin) and click the *Send* button:



3. Click the *Headers* tab and examine the HTTP header. Notice that the number of Headers in the Headers tab changed from 1 to 2. This is because Postman automatically created the HTTP header and updated your request to include it.

Authorization ● Headers (2) Pre-request Script Tests ●	
Key	Value
Authorization	Basic YWRtaW46YWRtaW4=
<input checked="" type="checkbox"/> Content-Type	application/json
<input type="text" value="New key"/>	<input type="text" value="Value"/>

- Click the *Body* tab, if the request succeeded you should be presented with a listing of the `/mgmt/tm/ltn` Organizing Collection:

Body Cookies (2) Headers (25) Test Results (3/3)

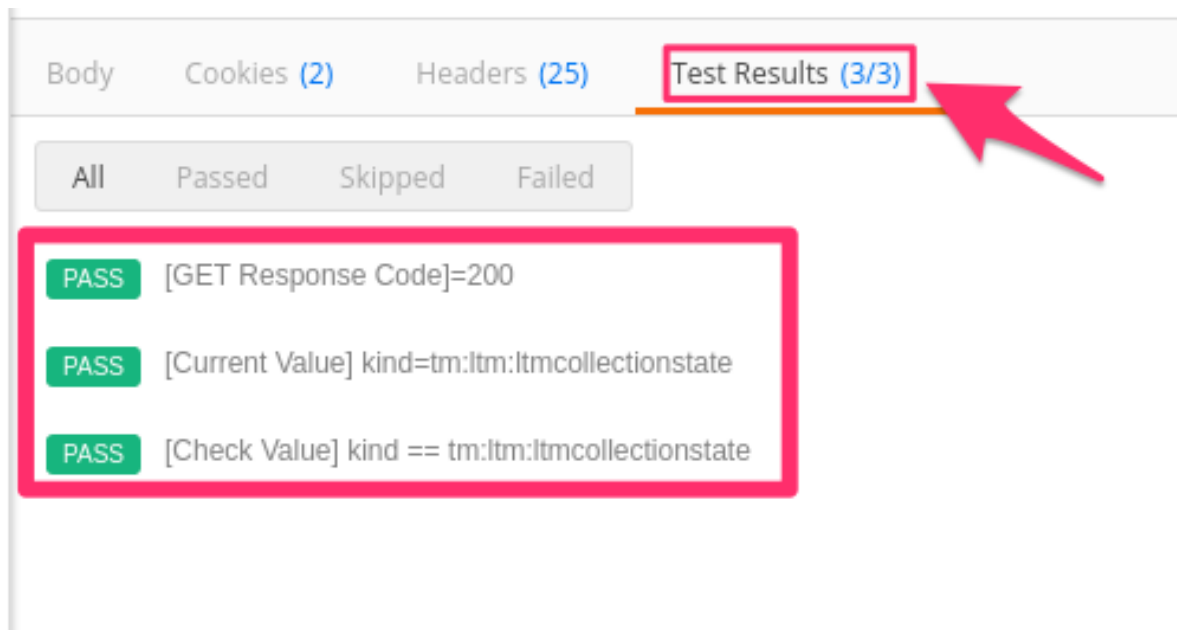
Pretty New Preview JSON 

```

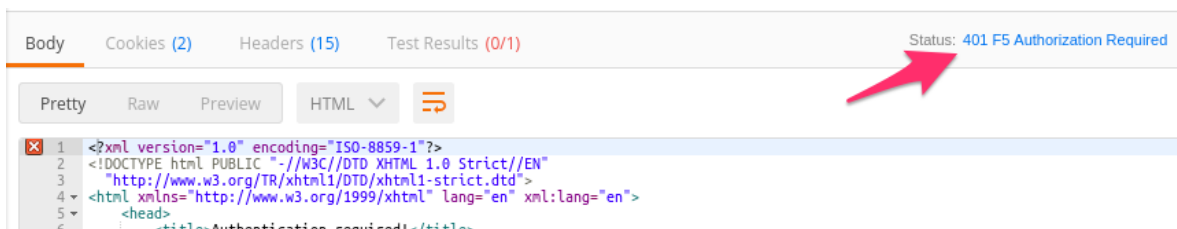
1 {
2   "kind": "tm:ltn:ltncollectionstate",
3   "selfLink": "https://localhost/mgmt/tm/ltn?ver=12.1.1",
4   "items": [
5     {
6       "reference": {
7         "link": "https://localhost/mgmt/tm/ltn/auth?ver=12.1.1"
8       }
9     },
10    {
11      "reference": {
12        "link": "https://localhost/mgmt/tm/ltn/data-group?ver=12.1.1"
13      }
14    },
15    {
16      "reference": {
17        "link": "https://localhost/mgmt/tm/ltn/dns?ver=12.1.1"
18      }
19    }
20  ]
21 }

```

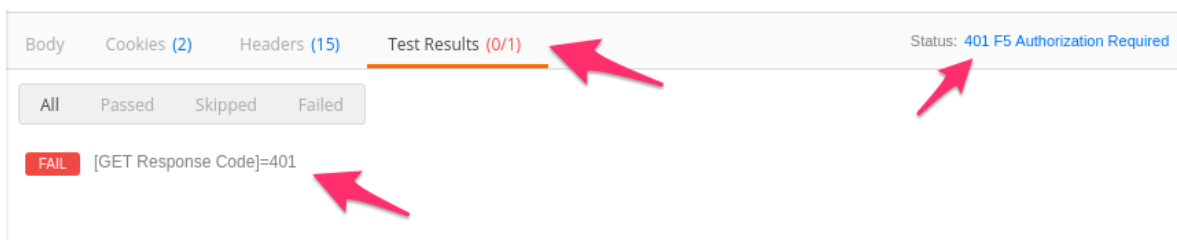
- Click the *Test Results* tab and ensure all the tests for this request have passed:



6. Update the credentials and specify an INCORRECT password. Send the request again and examine the response:



7. Check the *Test Results* tab and notice that our *Unit Tests* for this request are now failing (as expected):



Important: As you progress through this lab be sure to check the *Test Results* tab. We have included *Unit Tests* where applicable to help you verify the requests being sent are succeeding. If you notice a test has failed please double check your input or ask for help.

Task 3 - Token Based Authentication

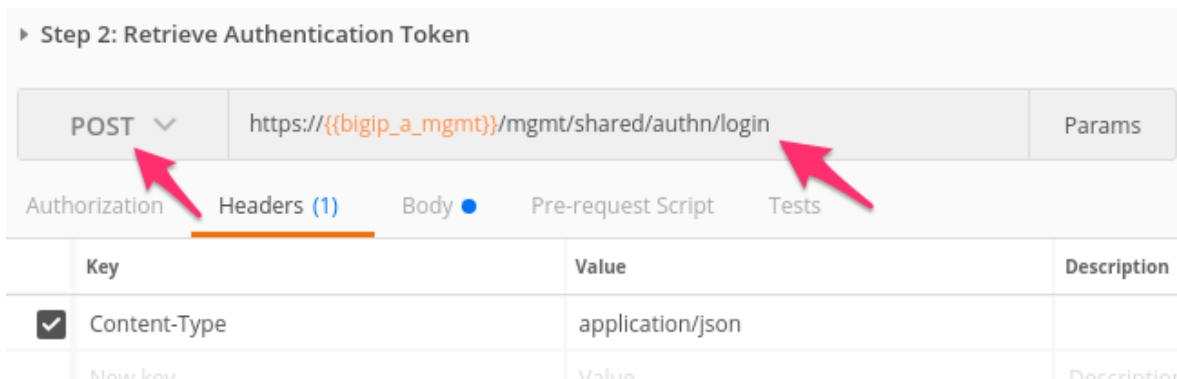
One of the disadvantages of BASIC Authentication is that credentials are sent with each and every request. This can result in a much greater attack surface being exposed unnecessarily. As a result, **Token Based Authentication (TBA)** is preferred in many cases. TBA only sends the credentials once, on the first request. The system then responds with a unique token for that session and the consumer then uses that token for all subsequent requests. BIG-IP and iWorkflow support token-based authentication that drops

down to the underlying authentication subsystems available in TMOS. As a result, the system can be configured to support external authentication providers (Active Directory, RADIUS, TACACS, etc) and those authentication methods can flow through to the REST API. In this task we will demonstrate TBA using the local authentication database, however, authentication to external providers is fully supported.

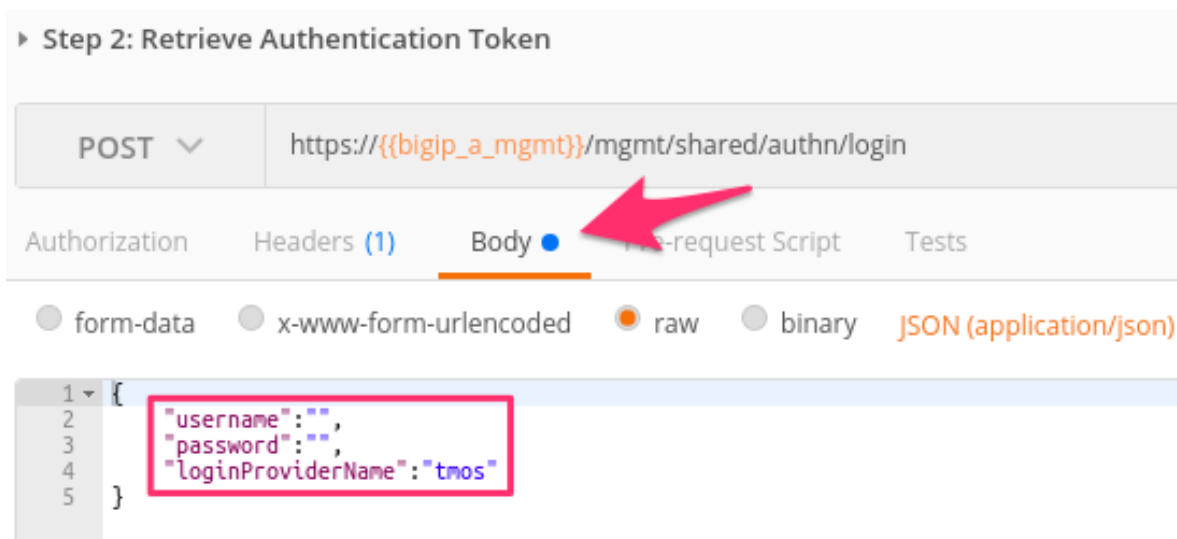
Note: For more information about external authentication providers see the section titled **About external authentication providers with iControl REST** in the iControl REST API User Guide available at <https://devcentral.f5.com/d/icontrolr-rest-api-user-guide-version-1300-241> (v13)

Perform the following steps to complete this task:

1. Click the **Step 2: Retrieve Authentication Token** item in the Lab 1.2 Folder.
2. Notice that we send a **POST** request to the `/mgmt/shared/authn/login` endpoint.



3. Click the **Body** tab and examine the JSON that we will send to BIG-IP to provide credentials and the authentication provider:

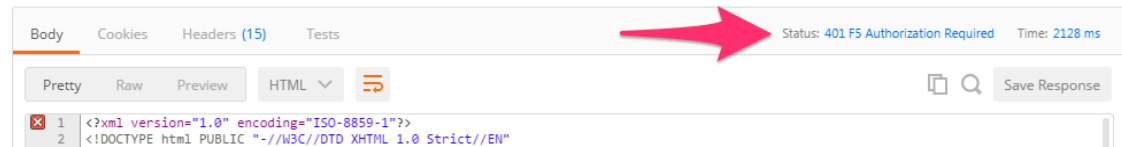


4. Modify the JSON **Body** and add the required credentials (`admin/admin`). Then click the **Send** button.
5. Examine the response status code. If authentication succeeded and a token was generated the response will have a `200 OK` status code. If the status code is `401` then check your credentials:

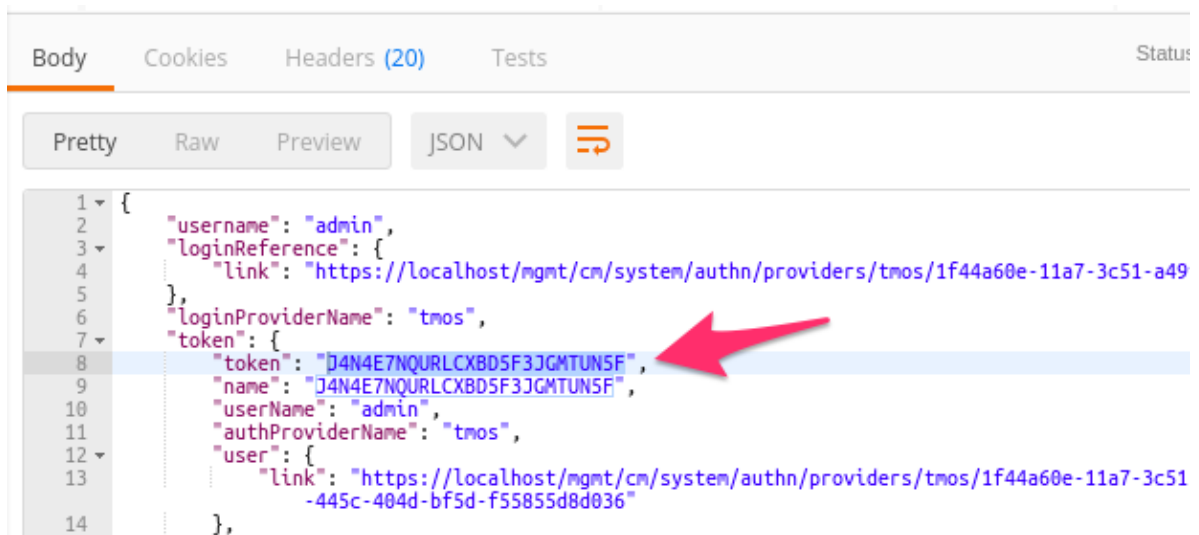
- **Successful:**



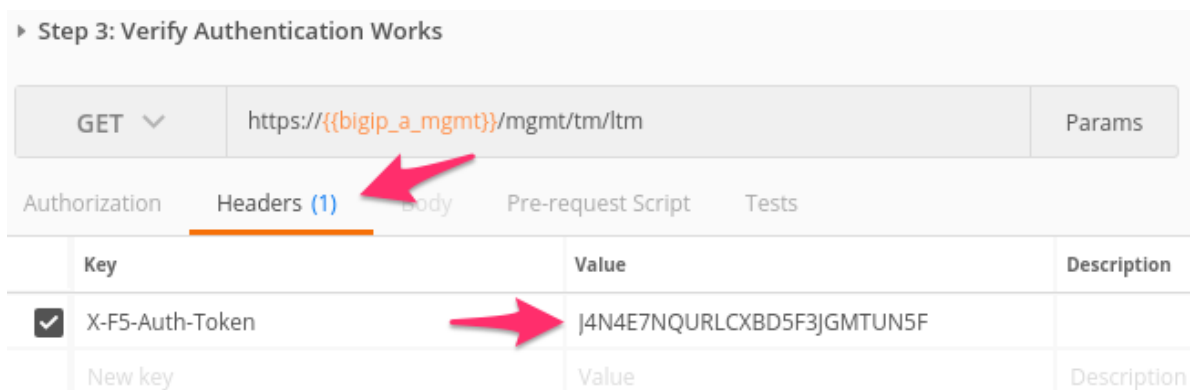
• **Unsuccessful:**



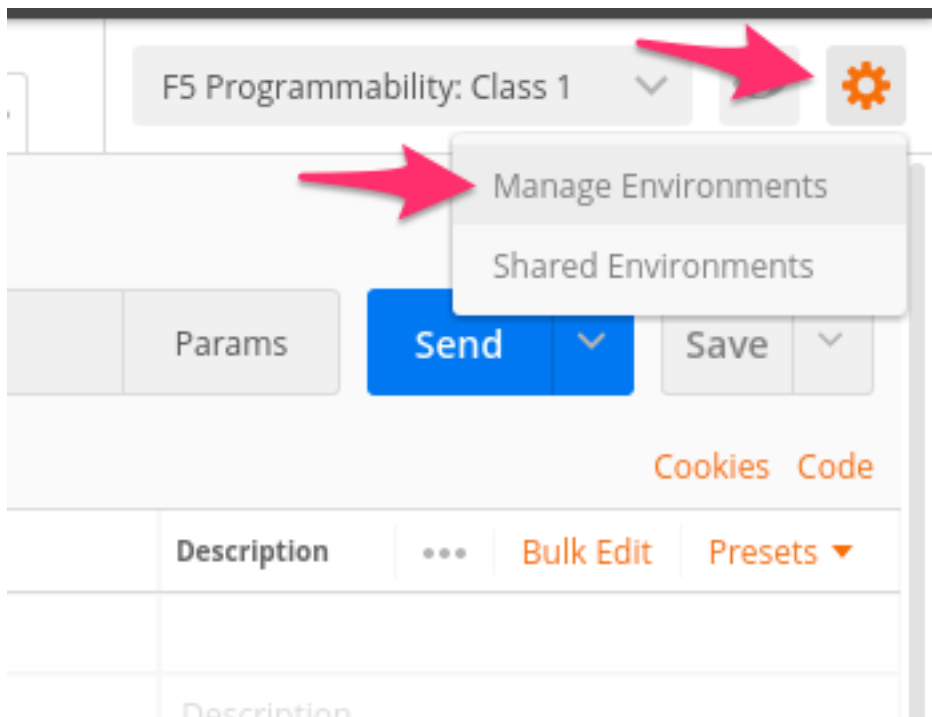
6. Once you receive a 200 OK status code examine the Response *Body*. The various attributes show the parameters assigned to the particular token. Find the `token` attribute and copy it into your clipboard (Ctrl+c) for use in the next step.



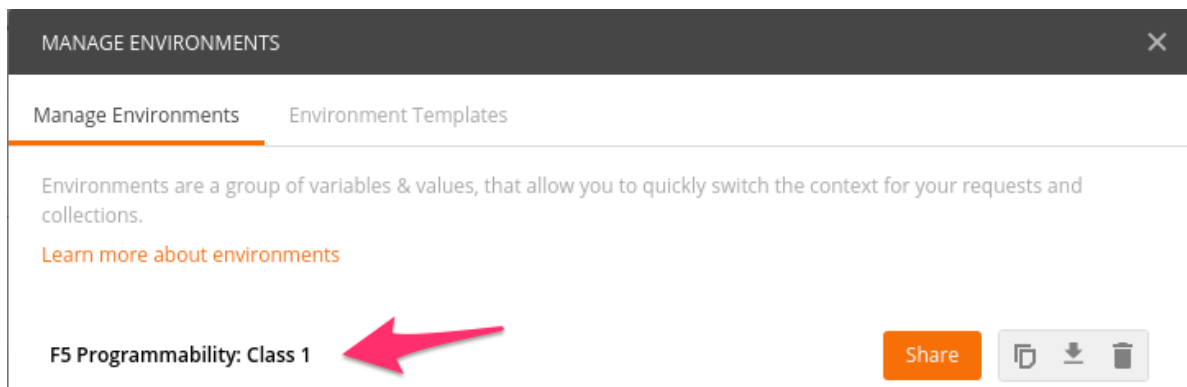
7. Click the **Step 3: Verify Authentication Works** item in the Lab 1.2 Postman collection. Click the *Headers* tab and paste the token value copied above as the VALUE for the X-F5-Auth-Token header. This header is required to be sent on all requests when using token-based authentication.



8. Click the *Send* button. If your request is successful you should see a 200 OK status and a listing of the `ltn` Organizing Collection.
9. We will now update your Postman environment to use this auth token for the remainder of the lab. Click the Environment menu in the top right of the Postman window and click *Manage Environments*:



10. Click the F5 Programmability: Class 1 item:



11. Update the value for `bigip_a_auth_token` by Pasting (Ctrl+v) in your auth token:

MANAGE ENVIRONMENTS ×

Manage Environments Environment Templates

Edit Environment

F5 Programmability: Class 1

	Key	Value	Bulk Edit
<input checked="" type="checkbox"/>	bigip_a_mgmt	10.1.1.10	
<input checked="" type="checkbox"/>	bigip_b_mgmt	10.1.1.11	×
<input checked="" type="checkbox"/>	iwf_mgmt	10.1.1.12	
<input checked="" type="checkbox"/>	bigip_a_auth_token	J4N4E7NQURLCXB5F3JGMTUN5F	×
<input checked="" type="checkbox"/>	bigip_b_auth_token		

- Click the **Update** button and then close the *Manage Environments* window. Because the subsequent requests refer to the `{{bigip_a_auth_token}}` variable, you will not have to set the token in the header of the following requests.
- Click the **Step 4: Set Authentication Token Timeout** item in the Lab 1.2 Postman folder. This request will **PATCH** your token Resource (notice the URI) and update the timeout attribute so we can complete the lab easily. Examine the request type and **JSON Body** and then click the **Send** button. Verify that the timeout has been changed to **36000** in the response:

▶ Step 4: Set Authentication Token Timeout

PATCH ▼

https://{{bigip_a_mgmt}}/mgmt/shared/authz/tokens/{{bigip_a_auth_token}}

Authorization

Headers (2)

Body ●

Pre-request Script

Tests

☐ form-data

☐ x-www-form-urlencoded

☒ raw

☐ binary

JSON (application/json) ▼

1 {

2 "timeout": "36000"

3 }

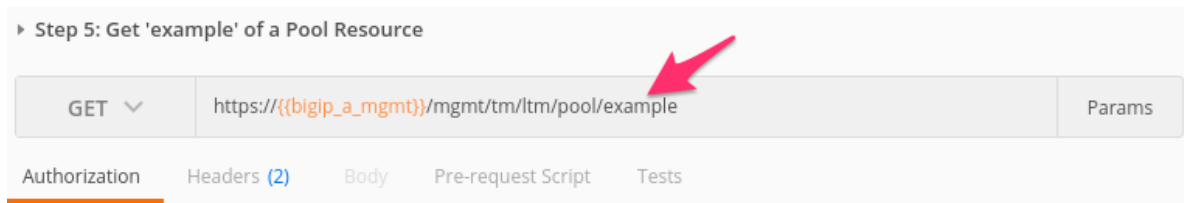
Task 4 - Get a pool 'example' Template

In order to assist with REST API interactions, you can request a template of the various attributes of a Resource type in a Collection. This template can then be used as the body of a **POST**, **PUT** or **PATCH** request as needed.

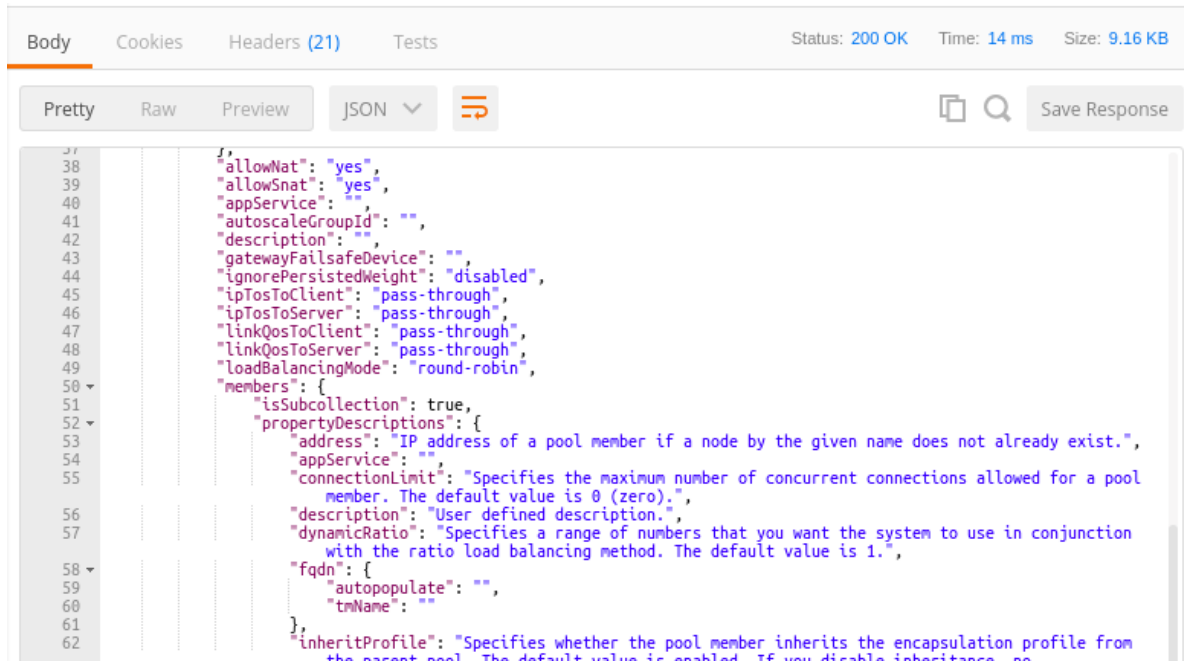
Perform the following steps:

- Click the **Step 5: Get 'example' of a Pool Resource** item in the Lab 1.2 Postman collection.

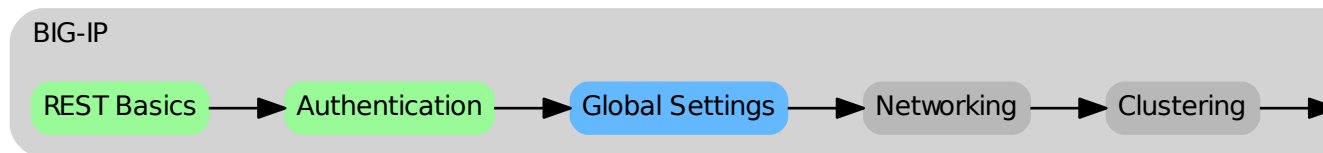
2. Examine the URI. Notice the addition of `example` at the end of the collection name:



3. Click *Send* and examine the FULL response. You will see descriptions and then all the attributes for the *Pool* resource type. The response also shows the default values for the attributes if applicable:



2.3.3 Lab 1.3: Review/Set Device Settings



All devices are already licensed so we can focus on configuring the basic infrastructure related settings to complete the Device Onboarding process. The remaining items include (list not exhaustive):

- Device Settings

- **NTP/DNS Settings**
- Remote Authentication
- **Hostname**
- **Admin Credentials**
- L1-3 Networking
 - Physical Interface Settings
 - L2 Connectivity (**VLAN**, VXLAN, etc.)
 - L3 Connectivity (**Self IPs**, **Routing**, etc.)
- HA Settings
 - **Global Settings**
 - * **Config Sync IP**
 - * **Mirroring IP**
 - * **Failover Addresses**
 - **CMI Device Trusts**
 - **Device Groups**
 - **Traffic Groups**
 - **Floating Self IPs**

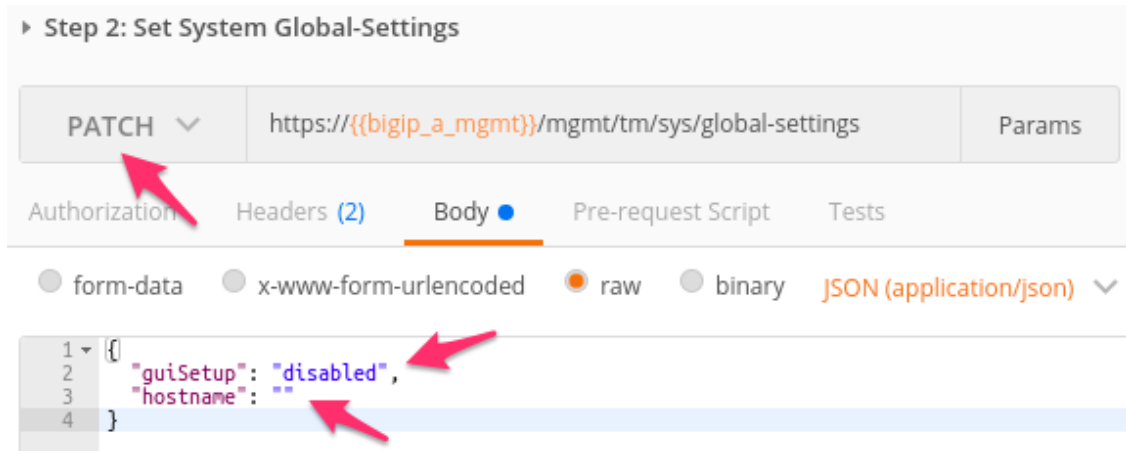
We will specifically cover the items in **BOLD** above in the following labs. It should be noted that many permutations of the Device Onboarding process exist due to the nature of real-world environments. This class is designed to teach enough information so that you can then apply the knowledge learned and help articulate and/or deliver a specific solution for your environment.

Task 1 - Set Device Hostname & Disable GUI Setup Wizard

In this task we will modify the device hostname and disable the GUI Setup Wizard. The Resource that contains these settings is `/mgmt/tm/sys/global-settings`.

Perform the following steps to complete this task:

1. Expand the `Lab 1.3 - Review/Set Device Settings` folder in the Postman collection.
2. Click the `Step 1: Get System Global-Settings` request. Click the *Send* button and review the response *Body* to see what the current settings on the device are. Examine the resulting response to understand what settings are currently applied.
3. Click the `Step 2: Set System Global-Settings` request. This item uses a `PATCH` request to the `global-settings` resource to modify the attributes contained within it. We will update the `guiSetup` and `hostname` attribute.
 - Click on *Body*. Review the JSON body and modify the `hostname` attribute to set the hostname to `bigip-a.f5.local`
 - Also notice that we are disabling the GUI Setup Wizard as part of the same request:



4. Click the *Send* button and review the response *Body*. You should see that the attributes modified above have been updated by looking at the response. You can also GET the `global-settings` by sending the Step 1: `Get System Global-Settings` request again to verify they have been updated.

Task 2 - Modify DNS/NTP Settings

Note: This task will make use of JSON arrays. The syntax for defining a JSON array is:

```
myArray: [ Object0, Object1 ... ObjectX ]
```

To define an array consisting of Strings the syntax is:

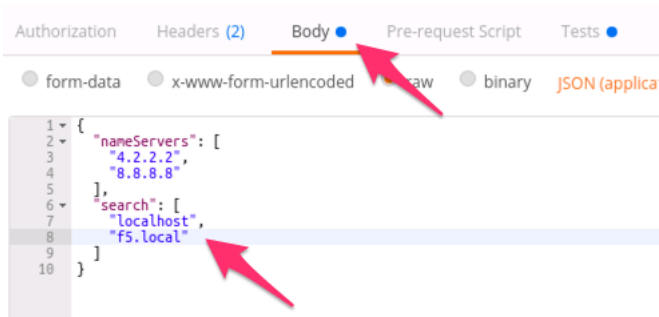
```
myStringArray: [ "string0", "string1" ... "stringX" ]
```

Much like the previous task we can update system DNS and NTP settings by sending a PATCH request to the correct resource in the `sys` Organizing Collection. The relevant Resources for this task are:

URL	Type
/mgmt/tm/sys/dns	DNS Settings
/mgmt/tm/sys/ntp	NTP Settings

Perform the following steps to complete this task:

1. Click the Step 3: `Get System DNS Settings` item in the folder. Click *Send* and review the current settings.
2. Click the Step 4: `Set System DNS Settings` item in the folder. Click *Body*. Review the JSON body to verify the name server IPs `4.2.2.2` and `8.8.8.8` are listed. Additionally, add a search domain of `f5.local`. You will modify a JSON array to add a search domain:



3. Click the *Send* button and verify the requested changes were successfully implemented by looking at the response or by sending the Step 3: Get System DNS Settings request again.
4. Click the Step 5: Get System NTP Settings item in the folder. Click *Send* and review the current settings.
5. Click the Step 6: Set System NTP Settings item in the folder. Click *Body*. Review the JSON body to verify the NTP servers with hostnames 0.pool.ntp.org and 1.pool.ntp.org are contained in the `servers` attribute (another JSON array!).
6. Click the *Send* button and verify the requested changes were successfully implemented by looking at the response or sending the Step 5: Get System NTP Settings again.

Task 3 - Update default user account passwords

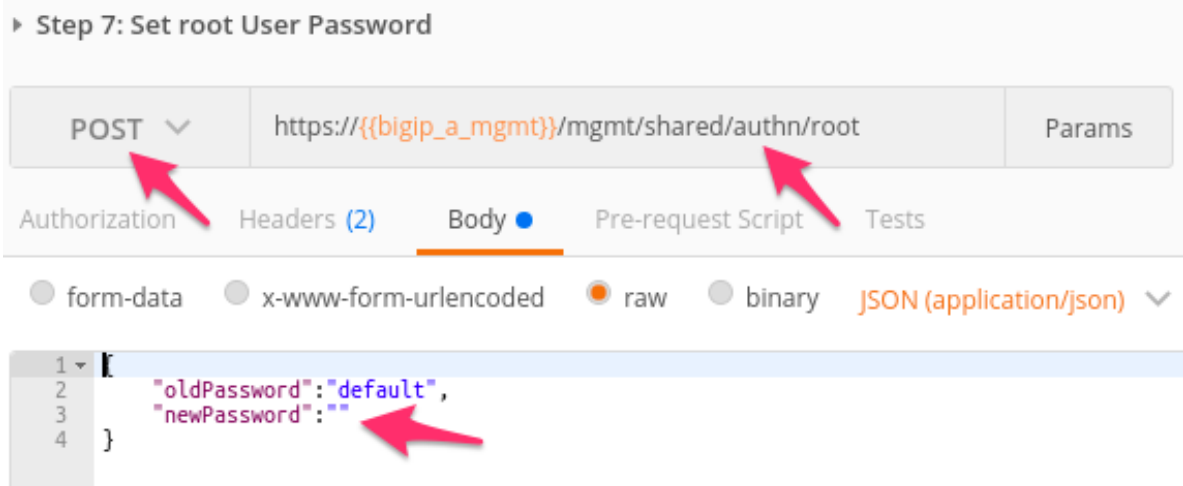
In this task we will update the passwords for the `root` and `admin` accounts. The process for updating the root account is different than other system accounts because it is used by underlying Linux OS.

To update the root account password we will use a `POST` to the `/mgmt/shared/authn/root` REST endpoint.

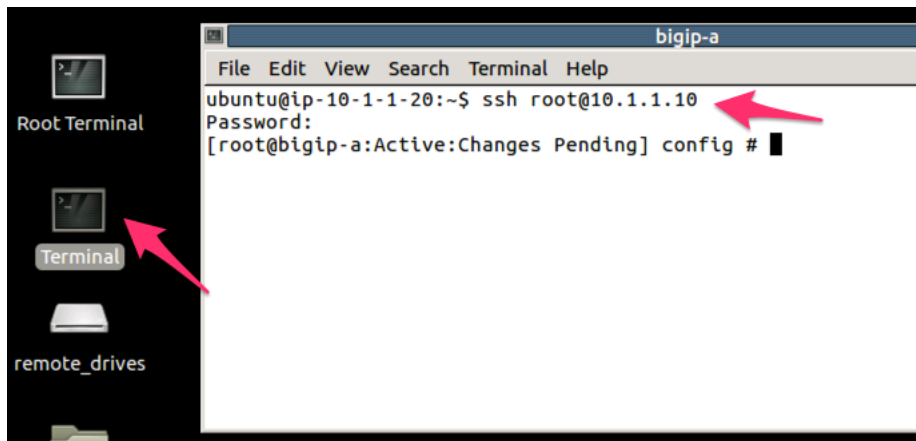
To update all other system accounts we will `PATCH` the `/mgmt/tm/auth/user/<username>` Resource.

Perform the following steps to change the `root` user password:

1. Click the Step 7: Set root User Password item in the folder.
2. We are performing a `POST` operation to change the root user password and have to specify the `oldPassword` because the REST implementation on the BIG-IP uses the underlying Linux mechanism. Click *Body*. Modify the JSON body to update the password to the value `newdefault` and click the *Send* button.



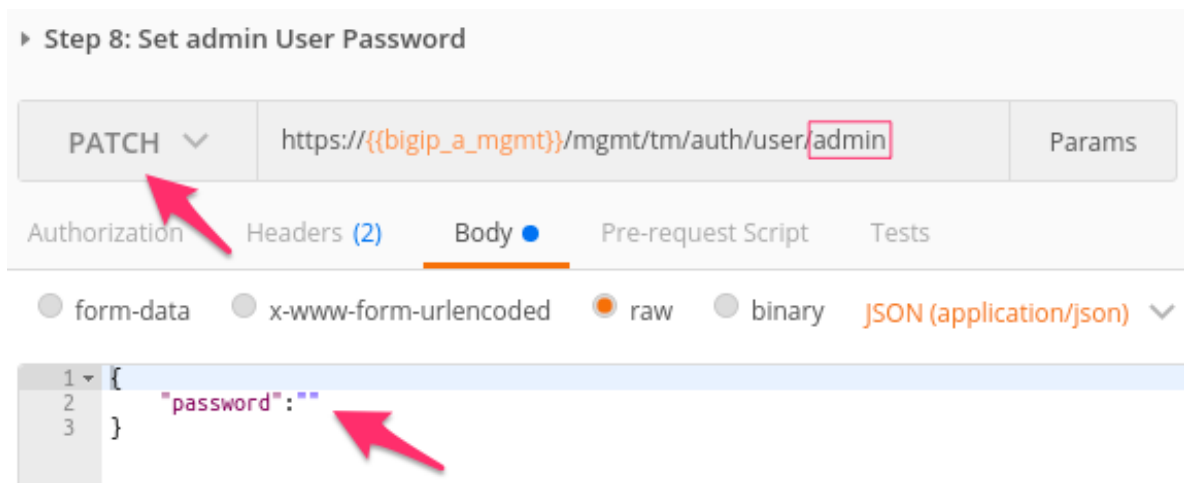
3. You can verify the password has been changed by opening an SSH session to BIG-IP A. A shortcut to a terminal is included on the desktop of the Linux jump host. Open a Terminal window and then open an SSH connection to BIG-IP A using the command `ssh root@10.1.1.10`:



4. Repeat the procedure above to change the password back to `default`

Perform the following steps to change the **admin** user password:

1. Click the Step 8: Set admin User Password item in the collection.
2. We are performing a `PATCH` operation to admin user Resource. Click *Body* and modify the JSON body to update the password to the value `newadmin` and click the *Send* button.



3. You can verify the password has been changed by opening an SSH session OR by logging into TMUI (HTTP GUI) to BIG-IP A in a Chrome browser tab.
4. Repeat the procedure above to change the password back to `admin`

Task 4 – [Service Provider] SNMP & Syslog

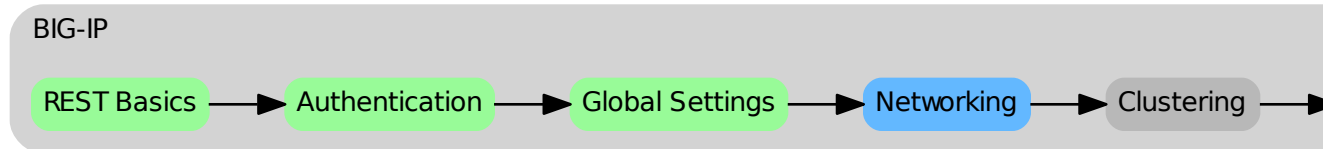
In this task we will do basic SNMP and syslog configuration using POST, PUT, DELETE commands.

Perform following steps to complete this task:

1. Expand the Lab 1.3A – SNMP & Syslog folder in the Postman Collection

2. Send the requests in Steps 1-14 and verify the expected result occurred on BIG-IP A. For requests using the `GET` method you can review the response JSON body rather than using the BIG-IP GUI.

2.3.4 Lab 1.4: Basic Network Connectivity



This lab will focus on configuration of the following items:

- L1-3 Networking
 - Physical Interface Settings
 - L2 Connectivity (**VLAN**, VXLAN, etc.)
 - L3 Connectivity (**Self IPs**, **Routing**, etc.)

We will specifically cover the items in **BOLD** above in the following labs. It should be noted that many permutations of the Device Onboarding process exist due to the nature of different organizations. This class is designed to teach enough information so that you can then apply the knowledge learned and help articulate and/or deliver a specific solution for your environment.

The following table and diagram lists the L2-3 network information used to configure connectivity for BIG-IP A:

Type	Name	Details
VLAN	Internal	Interface: 1.1 Tag: 10
VLAN	External	Interface: 1.2 Tag: 20
Self IP	Self-Internal	Address: 10.1.10.10/24 VLAN: Internal
Self IP	Self-External	Address: 10.1.20.10/24 VLAN: External
Route	Default	Network: 0.0.0.0/0 GW: 10.1.20.1

Task 1 - Create VLANs

Note: This lab shows how to configure VLAN tags, but does not deploy tagged interfaces. To use tagged interfaces the `tagged` attribute needs to have the value `true`

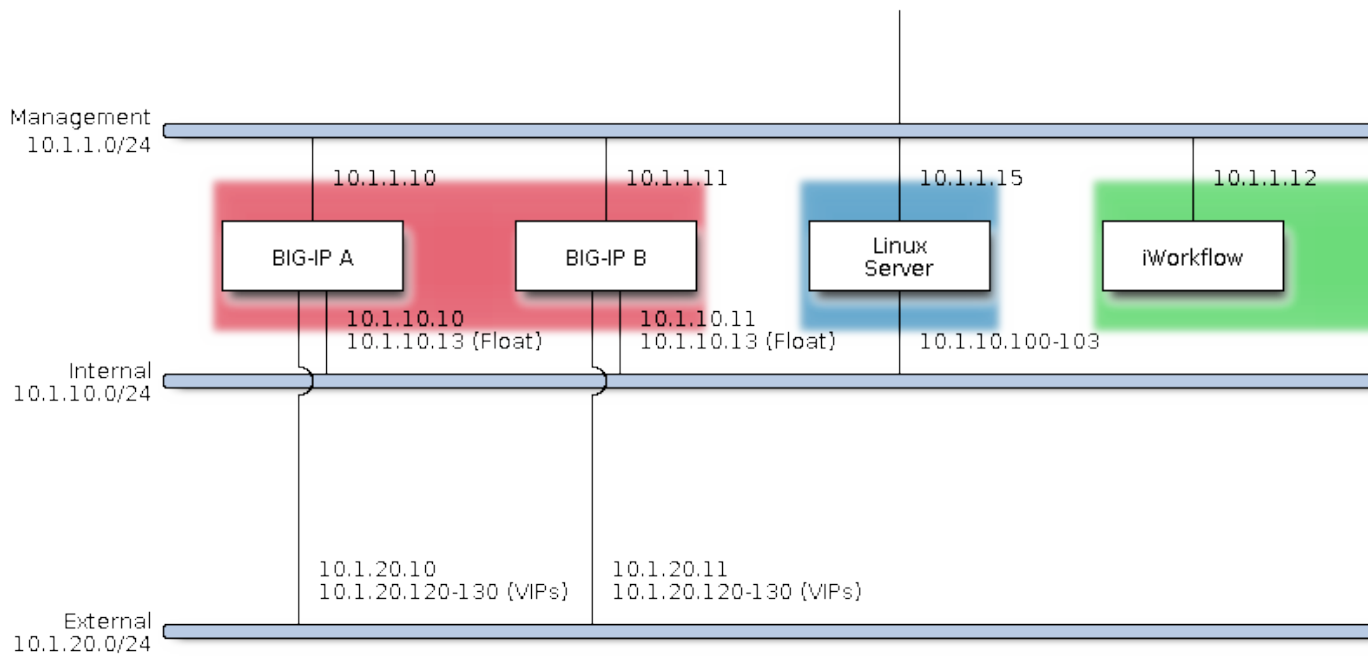


Fig. 2.2: Lab Topology

Perform the following steps to configure the VLAN objects/resources:

1. Expand the Lab 1.4 - Basic Network Connectivity folder in the Postman collection.
2. Click the Step 1: Create a VLAN request in the folder. Click *Body* and examine the JSON request body; the values for creating the Internal VLAN have already been populated.
3. Click the *Send* button to create the VLAN
4. **Repeat Step 1**, however, this time modify the JSON body to create the External VLAN using the parameters shown in the table above. In order to do so you can replace the following:
 - name: Internal -> External
 - tag: 10 -> 20
 - interfaces[] --> name: 1.1 -> 1.2

```

1 {
2   "name": "External",
3   "partition": "Common",
4   "autoLasthop": "default",
5   "cmpHash": "default",
6   "mtu": "1500",
7   "tag": "20",
8   "interfaces":
9   [
10    {
11      "name": "1.2",
12      "tagged": false
13    }
14  ]
15 }

```

5. Click the Step 2: Get VLANs request in the folder. Click the *Send* button to GET the VLAN collection. Examine the response to make sure both VLANs have been created.

Task 2 - Create Self IPs

Perform the following steps to configure the Self IP objects/resources:

1. Click the **Step 3: Create Internal Self IP** request in the folder. Click *Body* and examine the JSON body; the values for creating the Self-Internal Self IP have already been populated.

Note: The JSON body sets the VLAN to `/Common/External` on purpose. You will modify this value in the steps below. Please do not change the value.

2. Click the *Send* button to create the Self IP.
3. Click the **Step 4: Create External Self IP** request in the folder and click *Send*
4. Click the **Step 5: Get Self-Internal Self IP Attributes** request in the folder and click the *Send* button. Examine the VLAN settings of the Resource. As noted above the Self IP has been assigned to the **wrong** VLAN (intentionally).

Note: Postman has the ability to check the responses for specific values to verify if the result of a request is what it is expected to be. The *Test Results* for this request will show a failure for the `[Check Value] vlan == /Common/Internal` value. This is intentional and you should continue to the next section.

► Step 5: Get Self-Internal Self IP Attributes

GET https://{{bigip_a_mgmt}}/mgmt/tm/net/self/~Common~Self-Internal

Authorization Headers (2) Body Pre-request Script Tests

Type No Auth

Body Cookies Headers (21) Tests

Pretty Raw Preview JSON

```

1 {
2   "kind": "tm:net:self:selfstate",
3   "name": "Self-Internal",
4   "partition": "Common",
5   "fullPath": "/Common/Self-Internal",
6   "generation": 74,
7   "selfLink": "https://localhost/mgmt/tm/net/self/~Common~Self-Internal?ver=12.1.1",
8   "address": "10.1.10.10/24",
9   "addressSource": "from-user",
10  "floating": "disabled",
11  "inheritedTrafficGroup": "false",
12  "trafficGroup": "/Common/traffic-group-local-only",
13  "trafficGroupReference": {
14    "link": "https://localhost/mgmt/tm/cm/traffic-group/~Common~traffic-group-local-only?ver=12.1.1"
15  },
16  "unit": 0,
17  "vlan": "/Common/External",
18  "vlanReference": {
19    "link": "https://localhost/mgmt/tm/net/vlan/~Common~External?ver=12.1.1"
20  },
21  "allowService": [
22    "default"
23  ]
24 }

```

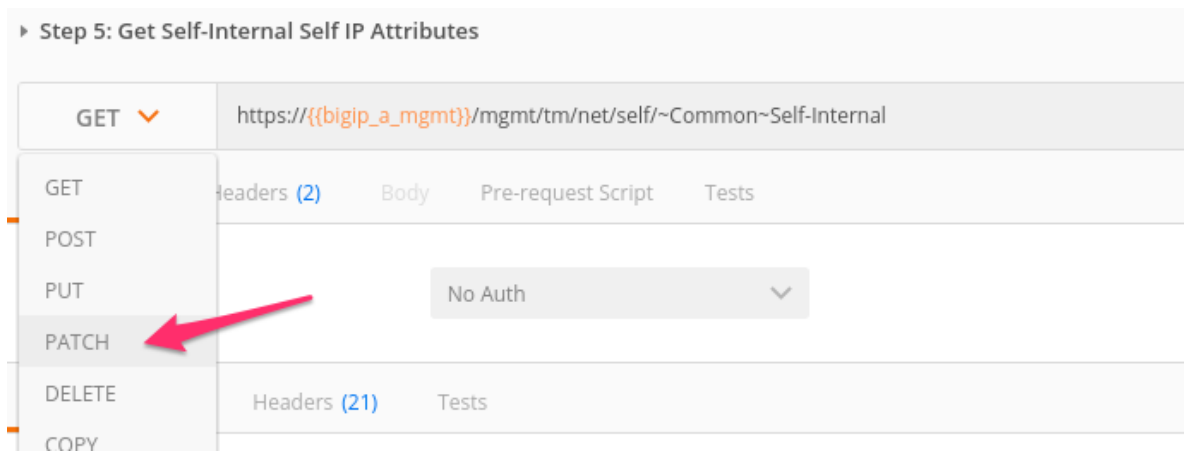
Task 3 - Modify Existing Self IP Resource

In order to modify an existing object via the REST API, the URI path has to be changed. In the previous examples we used a `POST` to create Resources under a Collection, therefore, the URI used was that of the Collection itself. If you wish to update/modify a Resource you must refer to the Resource directly.

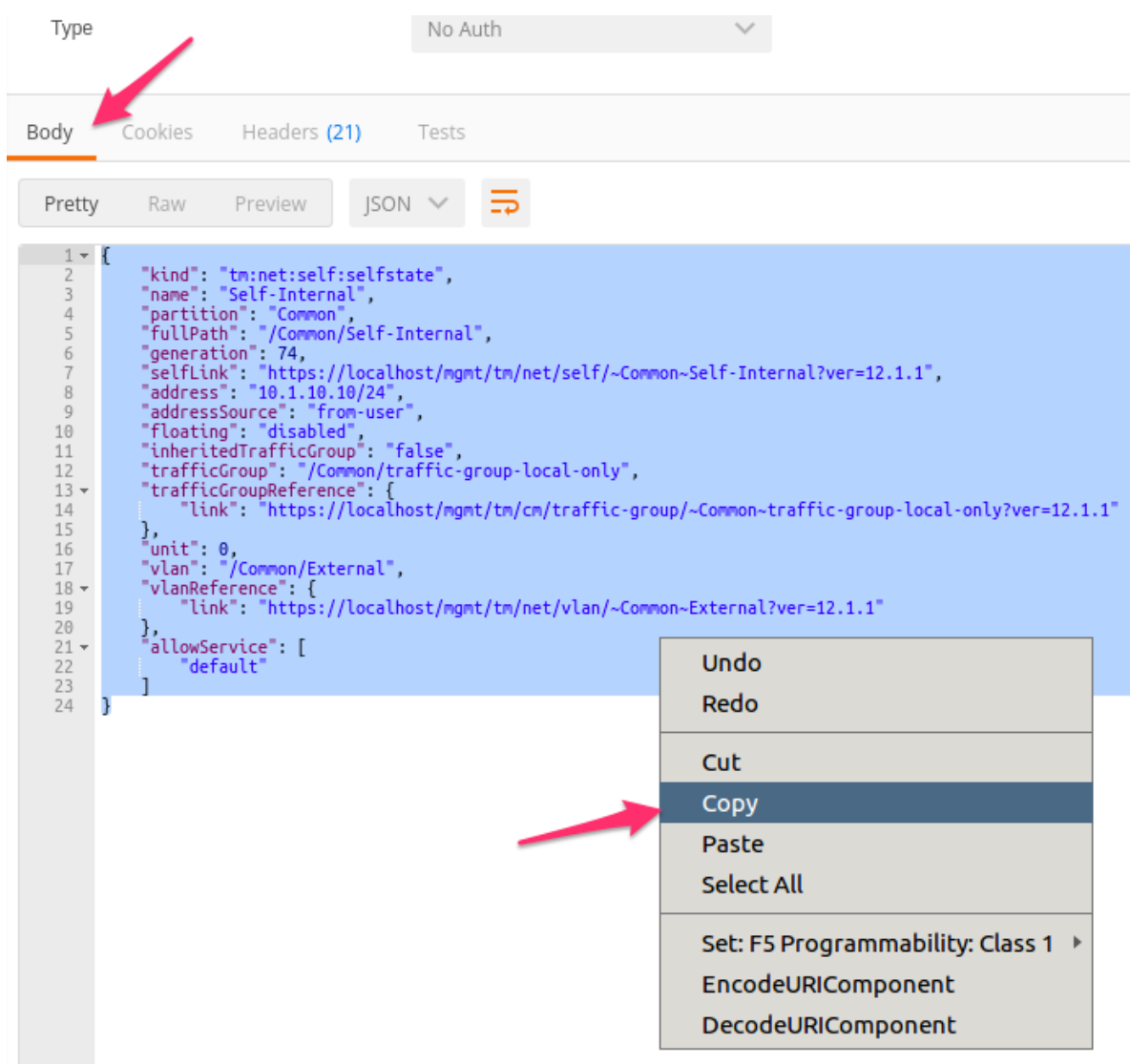
For example, the Collection URI for Self IPs is `/mgmt/tm/net/self`.

The Resource URI for the Self-Internal Self IP is `/mgmt/tm/net/self/~Common~Self-Internal`. Notice that the BIG-IP partition and object name has been added to the Collection URI to for the Resource URI.

1. On the open Step 5: Get Self-Internal Self IP Attributes request change the request method from `GET` to `PATCH`. The `PATCH` method is used to modify the attributes of an existing Resource.



2. Copy (Ctrl+c) the entire JSON **RESPONSE** from the previous GET request.



3. Paste (Ctrl+v) the text into JSON Request body:

Note: Be sure to highlight any existing text and replace it while pasting.

Step 5: Get Self-Internal Self IP Attributes Examples (0)

PATCH `https://{{bigip_a_mgmt}}/mgmt/tm/net/self/~Common-Self-Internal` Params Send Save

Authorization Headers (2) Body Pre-request Script Tests Cookies Code

form-data x-www-form-urlencoded raw binary JSON (application/json)

1 {
2
3 }
4
5
6
7
8
9
10

Undo
Redo
Cut
Copy
Paste
Select All
Set: F5 Programmability: Class 1
EncodeURIComponent
DecodeURIComponent

Body Cookies Headers (21) Tests Status: 200 OK Time: 22 ms Size: 1.4 KB

Pretty Raw Preview JSON Save Response

```
1 {  
2   "kind": "tm:net:self:selfstate",  
3   "name": "Self-Internal",  
4   "partition": "Common",  
5   "fullPath": "/Common/Self-Internal",  
6   "generation": 74,  
7   "selfLink": "https://localhost/mgmt/tm/net/self/~Common-Self-Internal?ver=12.1.1",  
8   "address": "10.1.10.10/24",  
9   "addressSource": "from-user",  
10  "floating": "disabled",  
11 }
```

4. In the JSON body change the `vlan` attribute to `/Common/Internal` and click Send:

► Step 5: Get Self-Internal Self IP Attributes

PATCH ▼ https://{bigip_a_mgmt}/mgmt/tm/net/self/~Common~Self-Internal

Authorization Headers (2) Body ● Pre-request Script Tests

form-data x-www-form-urlencoded raw binary JSON (application/json) ▼

```

1 {
2   "kind": "tm:net:self:selfstate",
3   "name": "Self-Internal",
4   "partition": "Common",
5   "fullPath": "/Common/Self-Internal",
6   "generation": 74,
7   "selfLink": "https://localhost/mgmt/tm/net/self/~Common~Self-Internal?ver=12.1.1",
8   "address": "10.1.10.10/24",
9   "addressSource": "from-user",
10  "floating": "disabled",
11  "inheritedTrafficGroup": "false",
12  "trafficGroup": "/Common/traffic-group-local-only",
13  "trafficGroupReference": {
14    "link": "https://localhost/mgmt/tm/cm/traffic-group/~Common~traffic-group-local-only?ver=12.1.1"
15  },
16  "unit": 0,
17  "vlan": "/Common/Internet",
18  "vlanReference": {
19    "link": "https://localhost/mgmt/tm/net/vlan/~Common~External?ver=12.1.1"
20  },
21  "allowService": [
22    "default"
23  ]
24 }

```

5. Click the Step 6: Get Self IPs item in the collection. Click the Send button to GET the Self IP collection. Examine the response to make sure both Self IPs have been created and associated with the appropriate vlan.

Task 4 - Create Routes

Perform the following steps to configure the Route object/resource:

1. Before creating the route, we double check the content of the routing table. Click the Step 7: Get Routes item in the collection. Click the Send button to GET the routes collection. Examine the response to make sure there is no route.
2. Click the Step 8: Create a Route item in the collection. Click *Body* and examine the JSON body; the values for creating the default route have already been populated.
3. Click the Send button to create the route.
4. Click the Step 9: Get Routes item in the collection again. Click the Send button to GET the routes collection. Examine the response to make sure the route has been created.

Task 5 – [Service Provider] Route Domain and Partition

In this task we will perform basic Route Domain and Partition configuration.

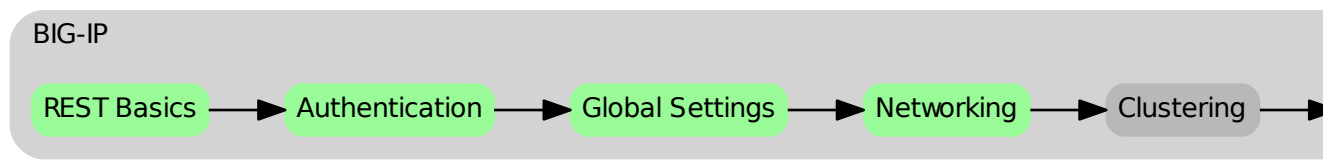
Perform following steps to complete this task:

1. Expand the Lab 1.4A – Route Domain & Partition in the Postman Collection
2. Send the requests in Steps 1-10 and verify the expected result occurred on BIG-IP A. For requests using the GET method you can review the response JSON body rather than using the BIG-IP GUI.

3. Send the requests in Steps 11-18 to clean up the previously created Route Domain, VLANs and Partitions

All route domain and partitions should now be deleted. Please confirm this on BIG-IP A. Any configuration that remains from this task will interfere with cluster setup in the subsequent labs.

2.3.5 Lab 1.5: Building Imperative Workflows with Postman Collections



As you have seen in the previous labs, we can use the Collections and Folders features of the Postman client to group REST requests logically. Additionally, as you've seen most of the examples so far have consisted of executing a sequence of REST request to achieve some outcome.

In this lab, we will use a feature in Postman called the **Collection Runner (Runner)** to execute a sequence of REST requests. Using the Runner we can rapidly prototype REST requests into an **Imperative Workflow** that can be executed without user intervention.

The purpose of this exercise is to provide an example of how new workflows can be built from scratch or existing workflows can be modified.

Additionally, we will use some Postman Javascript Tests to programmatically populate environment variables with the output of our workflow.

Task 1 - Open and Run a Collection

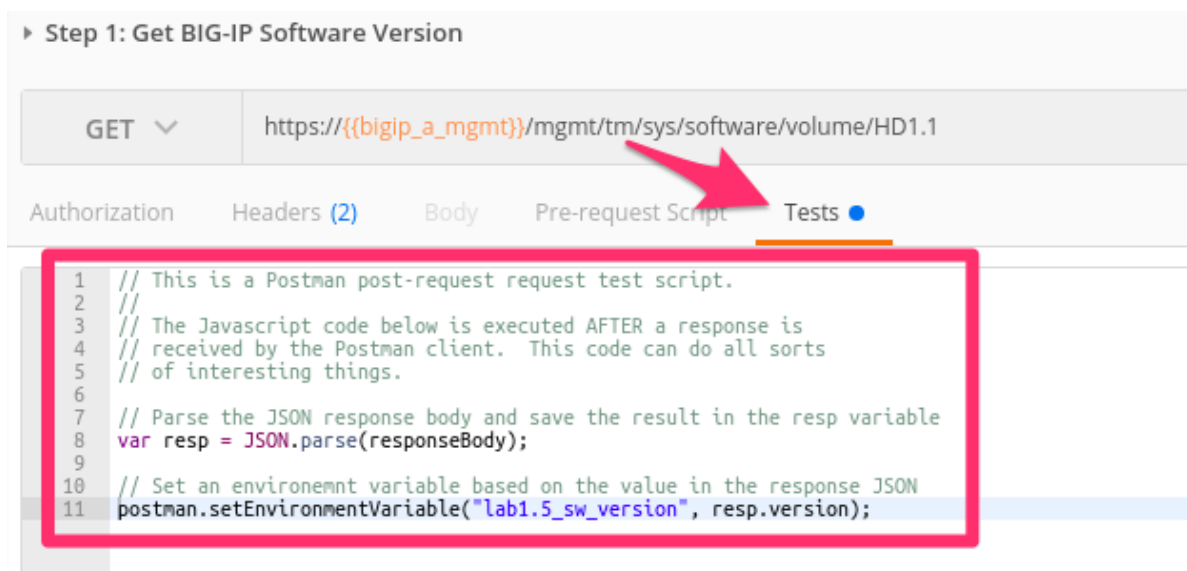
1. The collection we will run in this task will populate some environment variables with various data about the BIG-IP system. First, let's examine the Environment Variables that are currently set. Click



the icon in the top right of the Postman window. Notice that there are no variables starting with the name `lab1.5_`:

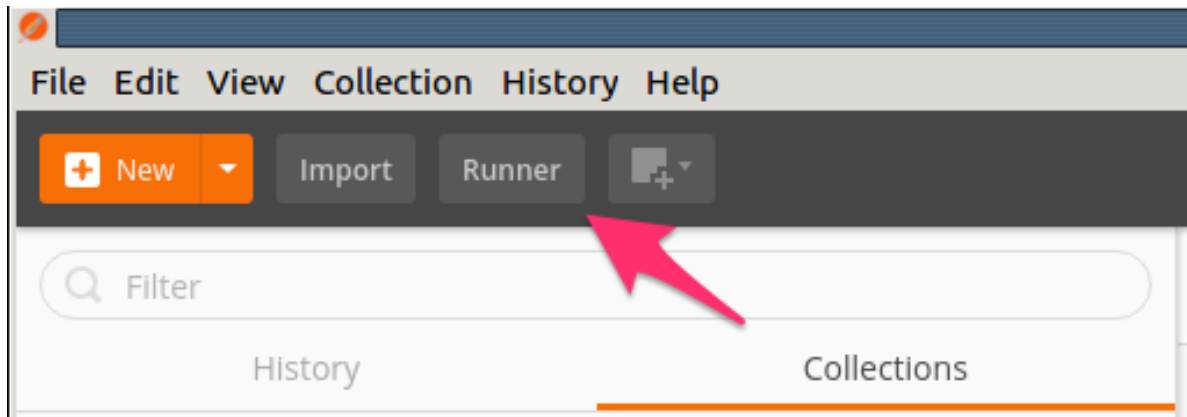


2. Click the Lab 1.5 - Building Imperative Workflows folder to expand it
3. Click the Step 1: Get BIG-IP Software Version request. Click the Tests tab and examine the Javascript code and comments:

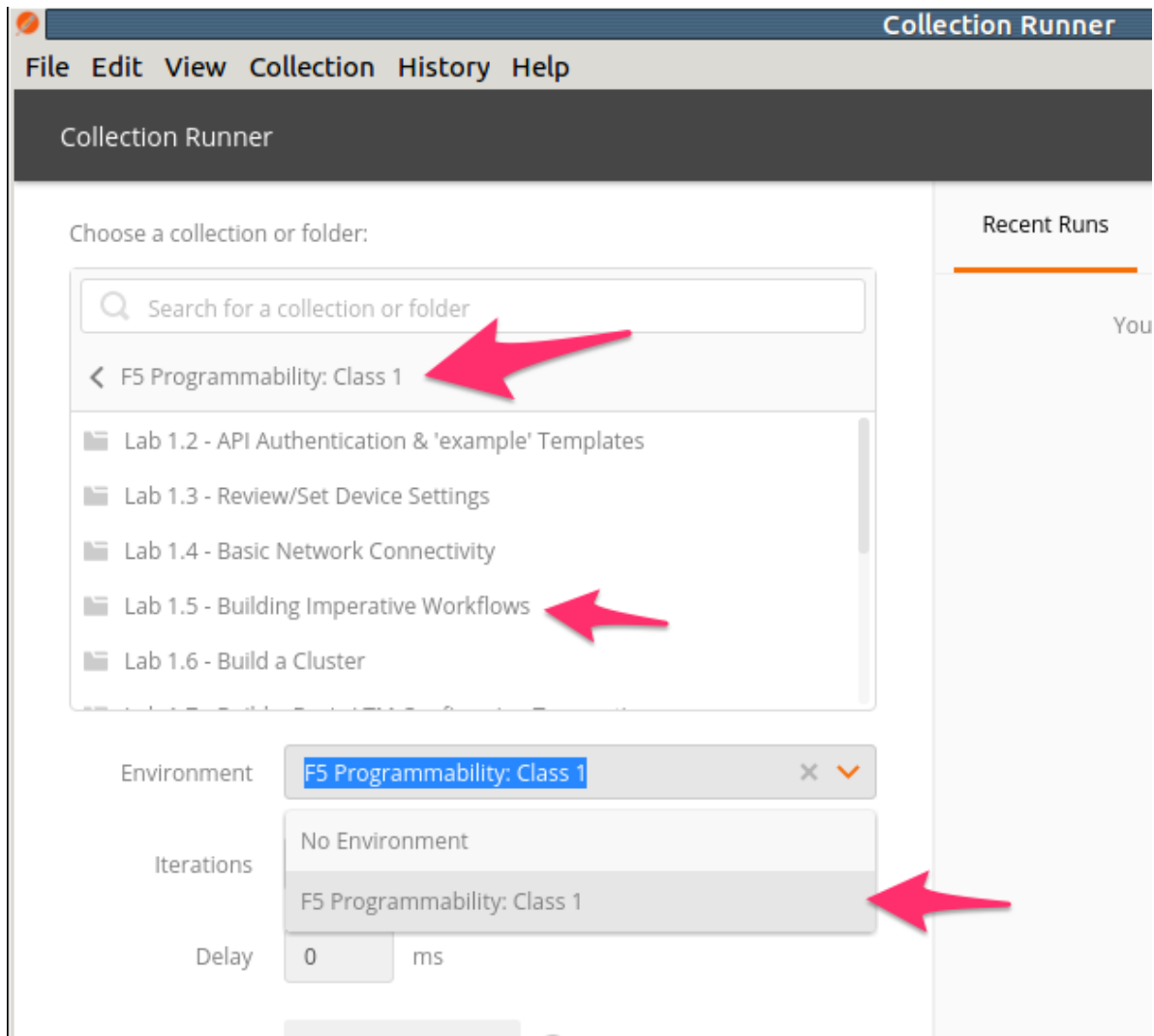


The Javascript code in the Test script will populate an environment variable based on the response from the BIG-IP system.

4. Click the *Runner* button at the top left of your Postman window:



5. Select the F5 Programmability: Class 1 Collection then the Lab 1.5 - Building Imperative Workflows folder. Next, be sure the environment is set to F5 Programmability: Class 1:



Your Runner window should look like:

Collection Runner

Choose a collection or folder:

< Lab 1.5 - Building Imperative Workflows

GET Step 1: Get BIG-IP Software Version

GET Step 2: Get BIG-IP CPU Count

GET Step 3: Get BIG-IP Base MAC Address

Environment

F5 Programmability: Class 1

Iterations

1

Delay

0

ms

Log Responses

For all requests



Data

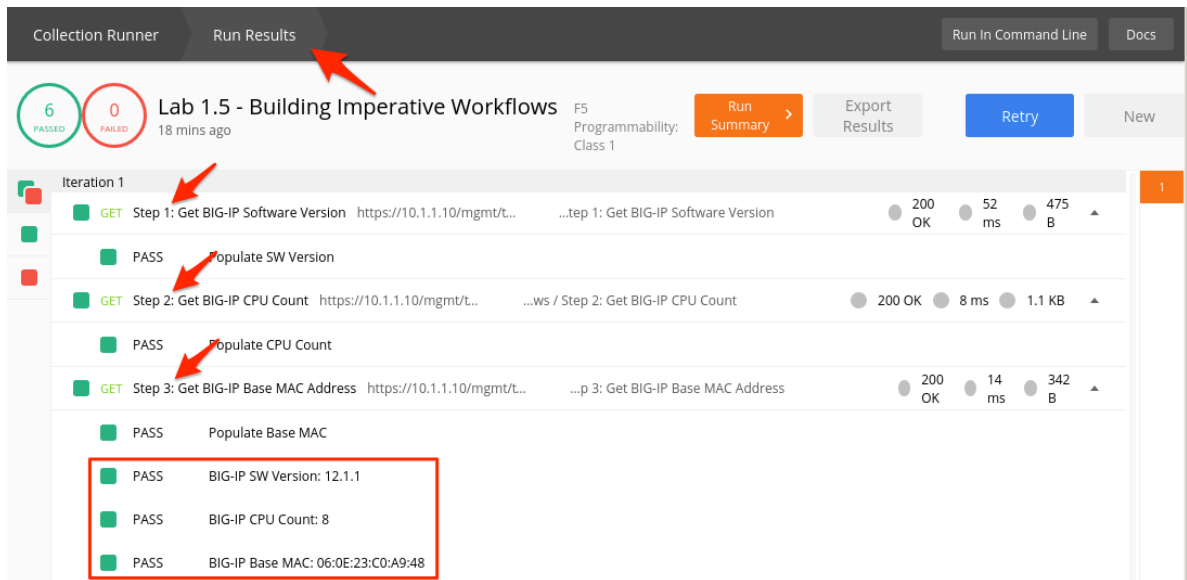
Select File




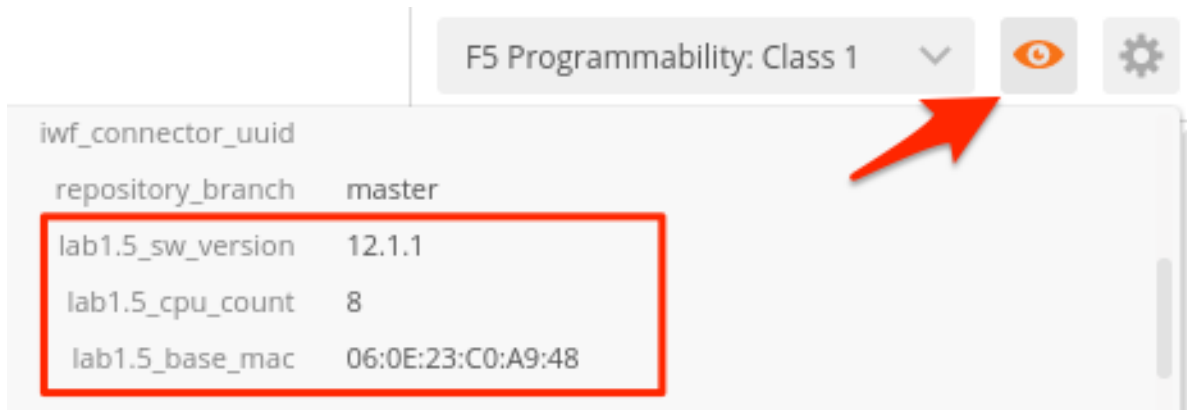
Persist Variables

As you can see from the screenshot or your own Collection Runner screen, we will be sending 3 requests (Steps 1-3 in Lab 1.5). Each request has a *unit test* implemented in JavaScript to ensure it's ok to continue to the next request when using the Collection Runner. The Runner will step through each request unless one of the tests fails.

6. Click the *Run Lab 1.5 - Buil...* button
7. The results window will now populate. You will see each request in the folder is sent and its associated test results are displayed on the screen. The last request in the folder includes some Javascript code to dump the results to the screen:



8. Next, switch back to the main Postman window. Click the  button again and examine the environment variables. Notice that three new variables starting with the name `lab1.5_` have been populated. You may need to scroll down to see these variables:



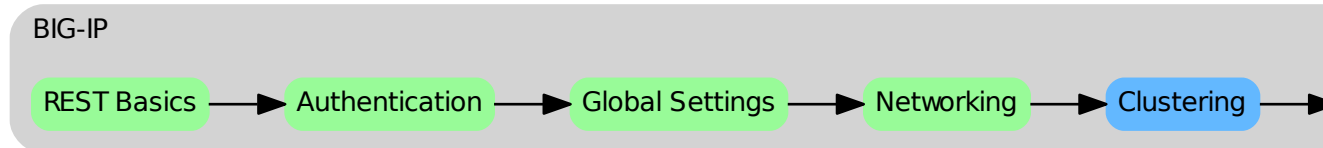
Note: It is normal for the values of Software Version, CPU Count and Base MAC Address to be different from the screenshot(s).

In this lab, we demonstrated running a simple Imperative Workflow using the Postman Collection Runner. In subsequent labs, we will expand on this simple use case to perform more complex functions. As you continue through the labs, be sure to take time to explore the details of the requests being sent. The Postman Collection used in this class can also serve as a starting point for building your own collections or modifying existing ones.

As we move through the rest of this module you will see the complexity involved in building Imperative Work-

flows. While these types of workflows are incredibly powerful, they are also time-consuming to build from scratch. As we move into Module 2 you will see the importance of leveraging **Abstraction** and **Declarative Interfaces** to minimize the amount of time spent on building Imperative Workflows.

2.3.6 Lab 1.6: Build a BIG-IP Cluster using a Collection



In this lab, we will build an active-standby cluster between BIG-IP A and BIG-IP B using the REST API. As mentioned previously, to save time, BIG-IP B is already licensed and has its device-level settings configured. This lab will use the Postman Runner functionality introduced in the previous lab. We will run the requests in a Collection Folder to build the cluster. If you examine the `Lab 1.6 - Build a Cluster` folder in the Collection you can see how complex **Imperative** processes can become. Clustering is one of the *transition* points for most customers to move into the **Declarative** model (if not already done) due to the need to abstract device/vendor level specifics from automation consumers.

The high-level procedure required to create the cluster is:

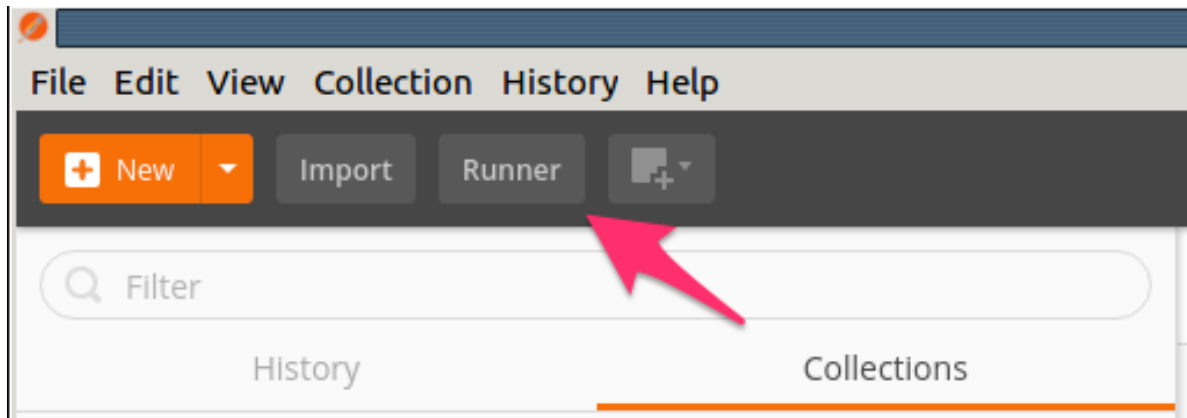
1. Obtain Authentication Tokens for BIG-IP A & B
2. Check that both devices are licensed and ready to configure
3. Configure Device Level settings on both devices
4. Configure Networking on BIG-IP B (remember this was already done in Lab 1.4 for BIG-IP A)
5. Set BIG-IP A & BIG-IP B CMI Parameters (Config Sync IP, Failover IPs, Mirroring IP)
6. Add BIG-IP B as a trusted peer on BIG-IP A
7. Check the status of the Sync Groups
8. Create a sync-failover Device Group
9. Check the status of the created Device Group
10. Perform initial sync of the Device Group
11. Check status (again)
12. Change the Traffic Group to use HA Order failover
13. Create Floating Self IPs
14. Failover the Traffic Group to make BIG-IP A the Active device

Task 1 - Build a Cluster using Runner

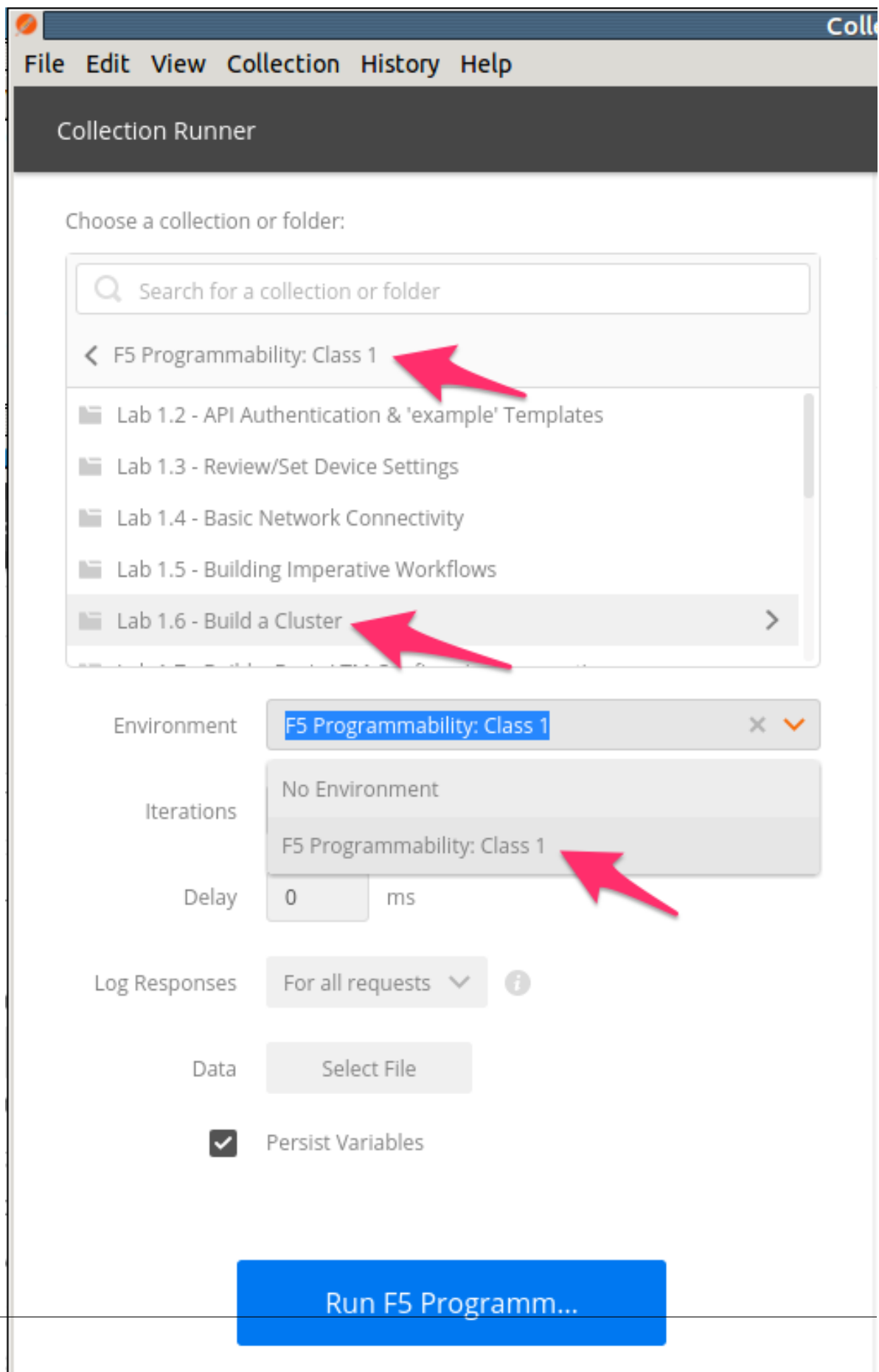
In this task we will use the *Runner* to execute a series of requests contained in the `Lab 1.6 - Build a Cluster` folder. As mentioned previously this folder contains a large number of REST requests required to build an Active/Standby cluster. Additionally, we will make use of a JavaScript framework called `f5-postman-workflows` that extends the Postman client to include common test and polling functions.

Perform the following steps to build the cluster:

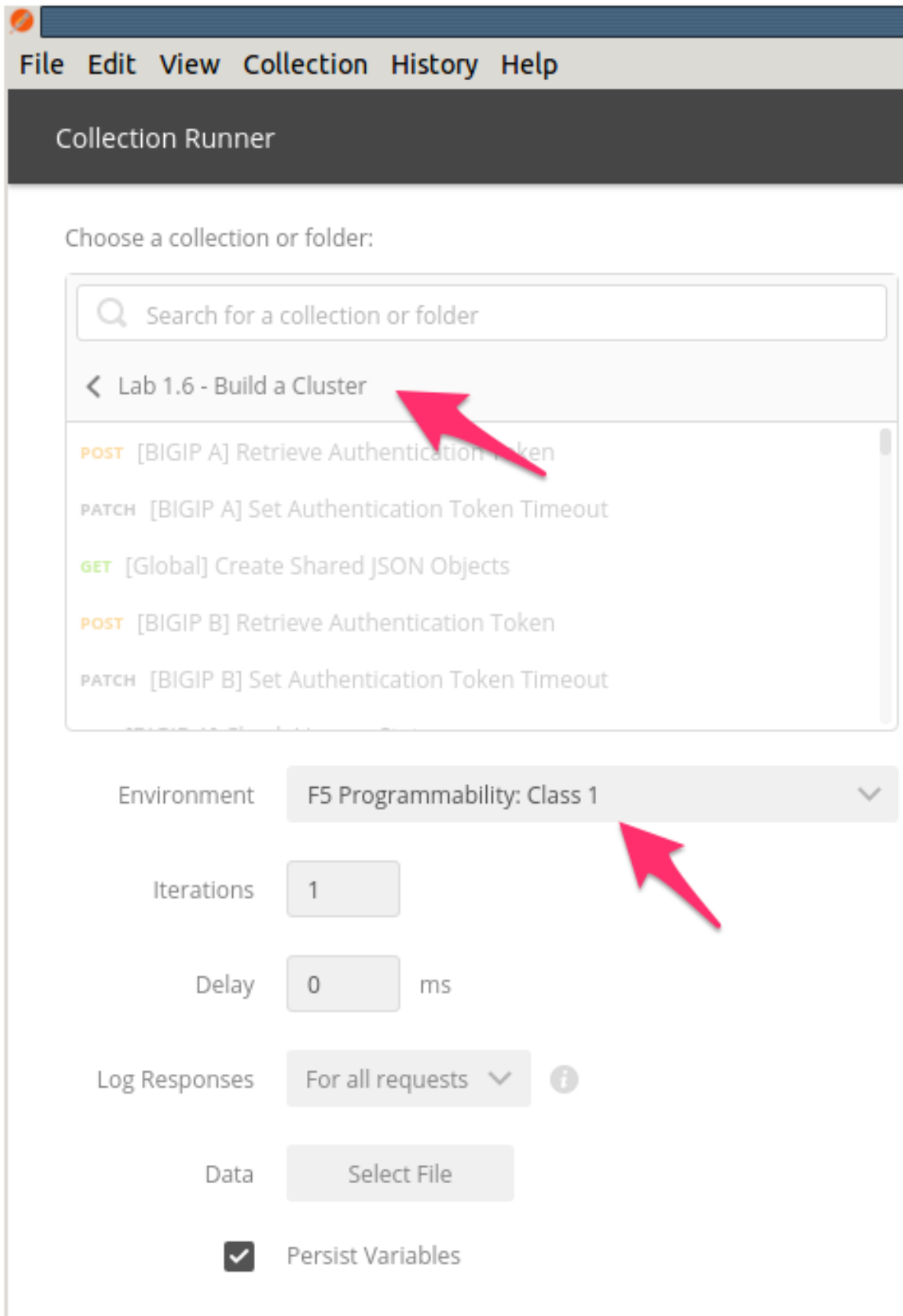
1. Click the *Runner* button at the top left of your Postman window:



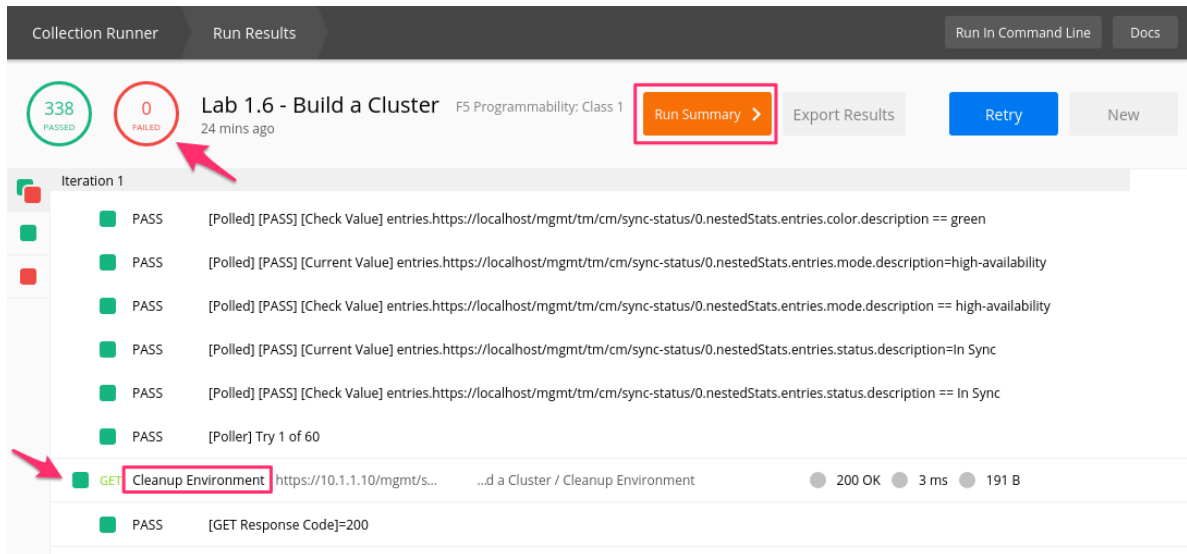
2. Select the `F5 Programmability: Class 1` Collection then the `Lab 1.6 - Build a Cluster` folder. Next, be sure the environment is set to `F5 Programmability: Class 1`:



Your Runner window should look like:



3. Click the *Run Lab 1.6 - Buil...* button
4. The results window will now populate. You will see each request in the folder is sent and its associated test results are displayed on the screen. Building the cluster can take a few minutes. You can follow the progress by scrolling down the results window.
5. Once the *Run Summary* button appears, the folder has completed running. You should have 0 failures and the last item in the request list should be named `Cleanup Environment`



Note: If you have an issue with your authentication token issue please return to Lab 1.3, Step 8 in Postman to set your admin password to `admin`.

Task 2 - Verify the Built Cluster in BIG-IP GUI

1. At this point you can log into BIG-IP A using Chrome at <https://10.1.1.10>. Verify that the cluster was built by navigating to *Device Management* → *Overview* using the menu in the BIG-IP TMUI GUI. Verify that the cluster and failover status indicators are all green.

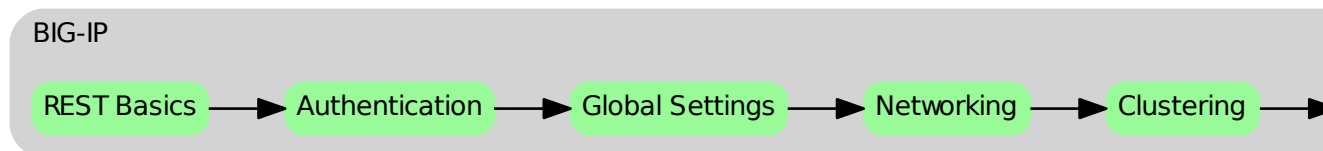
The screenshot shows the BIG-IP GUI with the following details:

- Browser Address Bar:** `https://10.1.1.10/xui/`
- Navigation Bar:** Apps, Lab Guide, BIG-IP A GUI, BIG-IP A REST TO, BIG-IP B GUI, BIG-IP B REST TO, iWorkflow GUI, iWorkflow REST
- System Info:** Hostname: bigip-a.f5.local, Date: Oct 18, 2017, Time: 7:37 PM (PDT), User: admin, Role: Administrator, Partition: Common
- Device Management Overview:**
 - Device Groups Table:**

Name	Sync Status	Number of Devices	Device Group Type	Sync Type
DeviceGroup1	In Sync	2	Sync-Failover	Auto
datasync-global-dg	In Sync	2	Sync-Only	Manual
device_trust_group	In Sync	2	Sync-Only	Auto
 - Sync Summary:** Status: In Sync, Summary: All devices in the device group are in sync
 - Devices Table:**

HA Status	Name	Sync Status	Configuration Time
Online	bigip-a.f5.local (Self)	In Sync	10/18/2017 15:18:03
Online	bigip-b.f5.local	In Sync	10/18/2017 15:18:03

2.3.7 Lab 1.7: Build a Basic LTM Config using REST Transactions



In this lab we will build a basic LTM Config using iControl REST API Transactions.

Task 1 - Create a Transaction

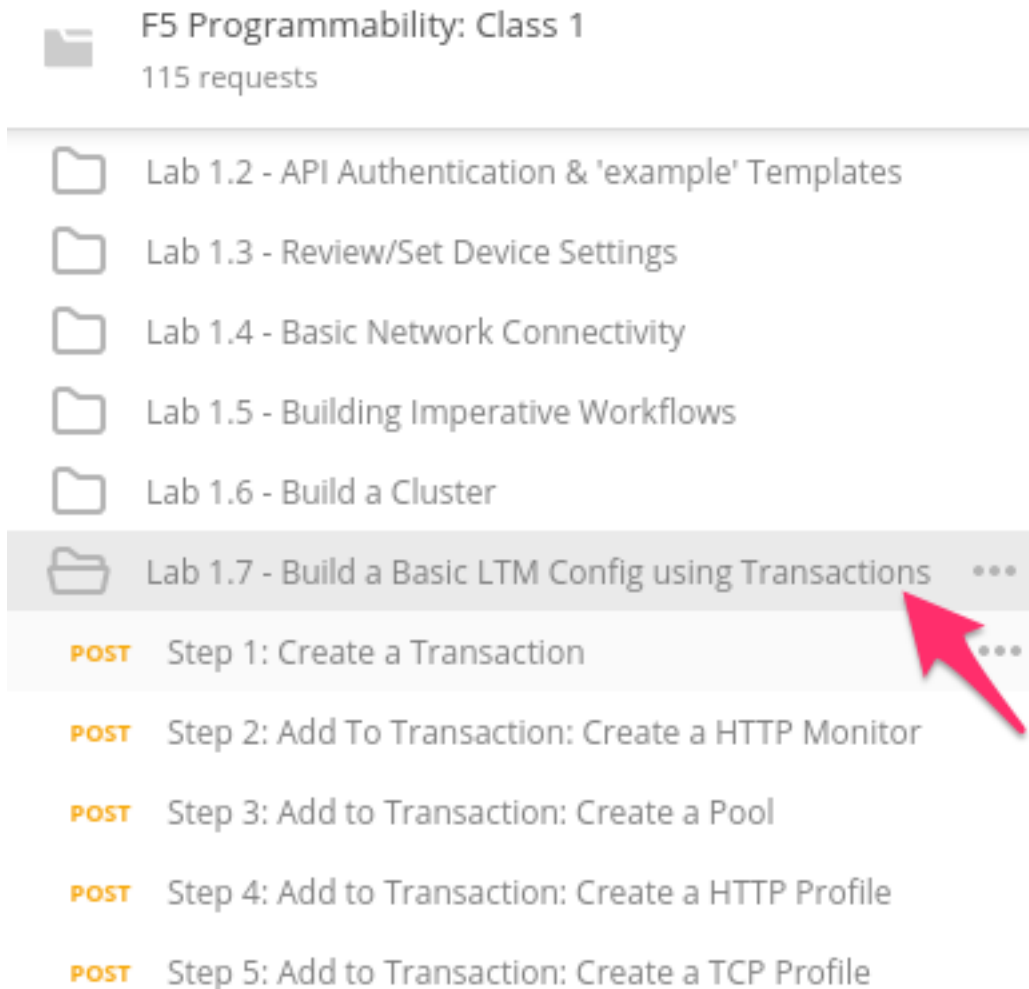
Transactions are very useful in cases where you would like to have discrete REST operations to act as a batch operation. As a result, the nature of a transaction is that either all the operations succeed or none of them do (all-or-nothing). This is very useful when we are creating a configuration that is linked together because it allows roll back of operations in case one fails. All the commands issued are queued one after the other in the transaction. We will also review how to change the order of a queued command or remove a single command from the queued list before committing.

Note: Transactions are essential to ensure that an Imperative process is **Atomic** in nature.

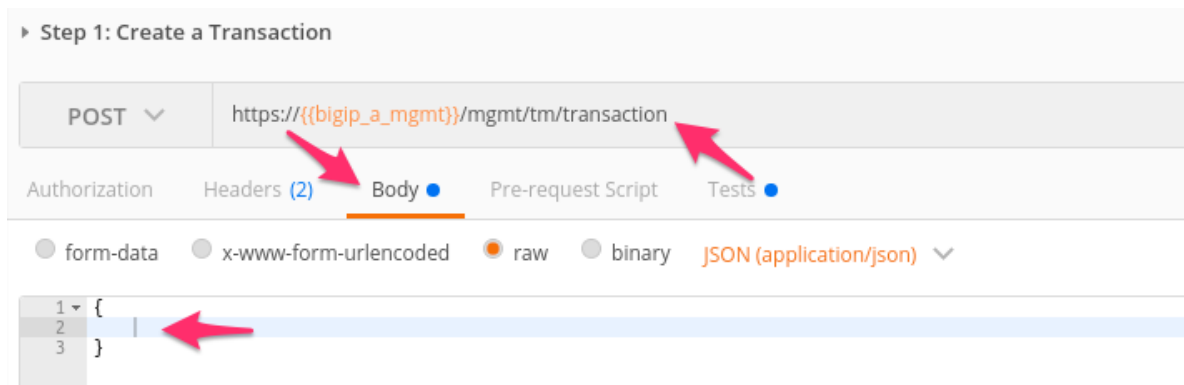
Warning: Transactions have a default timeout of 120 seconds. Taking longer than the timeout period to execute a transaction will result in automatic deletion of the transaction. **To avoid having to redo the steps in this task, please first read through the steps below and execute each of them in a timely manner.**

Perform the following steps to complete this task:

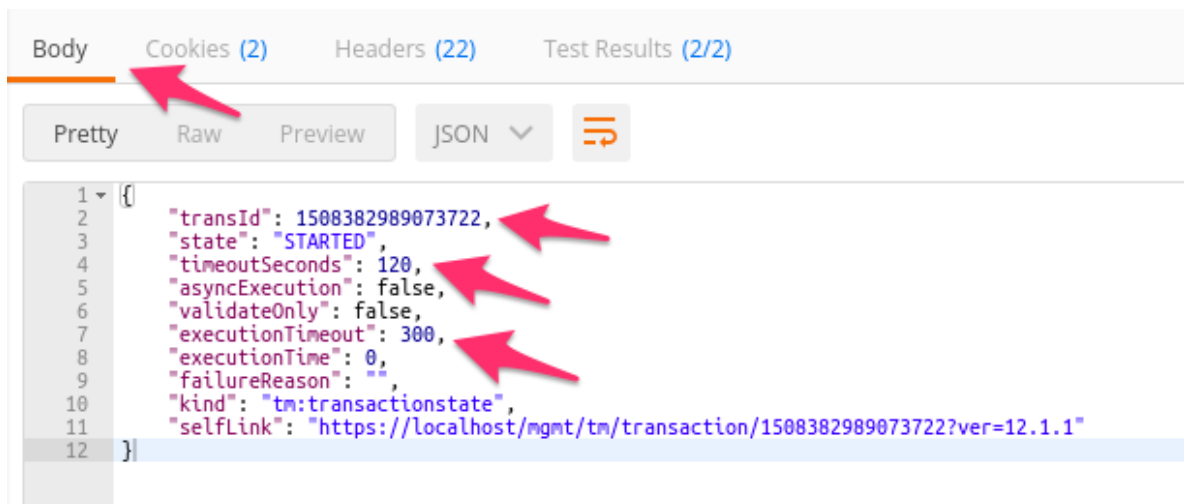
1. Expand the Lab 1.7 - Build a Basic LTM Config using Transactions folder in the Postman collection:



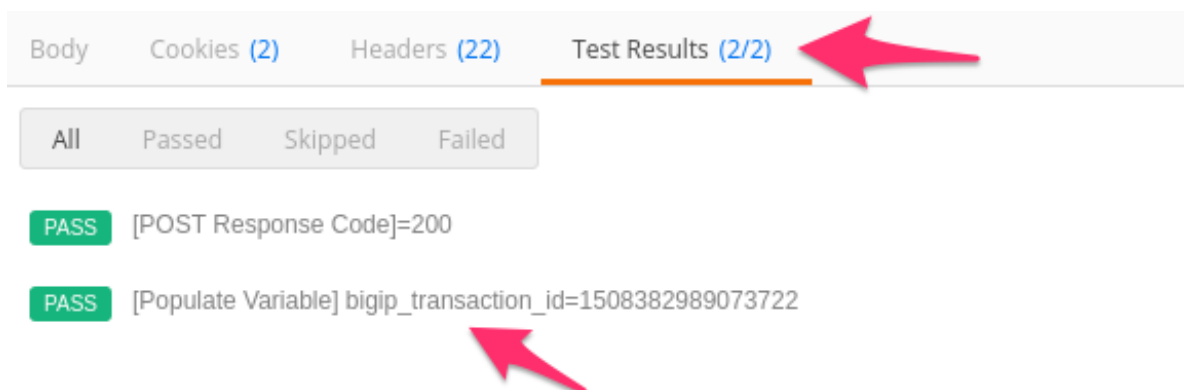
2. Click the Step 1: Create a Transaction request. Examine the URL and JSON Body. We will send a POST to the /mgmt/tm/transaction endpoint with an empty JSON body to create a new transaction.



- Click the *Send* button to send the request. Examine the response and find the `transId` attribute. Additionally, notice that there are timeouts for both the submission of the transaction and how long it would take to execute. Please be aware that upon exceeding the `timeoutSeconds` period, the `transId` will be silently removed:



The `transId` value has been automatically populated for you in the `bigip_transaction_id` environment variable:



- Click the *Step 2: Add to Transaction: Create a HTTP Monitor* request in the folder. This request is similar to a non-transaction enabled request in terms of the `POST` request method, `URI` and `JSON` body. The difference is that, a header named `X-F5-REST-Coordination-Id` with the value of the `transId` attribute is added to the transaction:

Step 2: Add To Transaction: Create a HTTP Monitor

POST ▾	https://{{bigip_a_mgmt}}/mgmt/tm/ltn/monitor/http	Params
Authorization	Headers (3)	Body ● Pre-request Script Tests
Key	Value	
<input checked="" type="checkbox"/> Content-Type	application/json	
<input checked="" type="checkbox"/> X-F5-REST-Coordination-Id	{{bigip_transaction_id}}	
<input checked="" type="checkbox"/> X-F5-Auth-Token	{{bigip_a_auth_token}}	
New key	value	

- Click the *Send* button and examine the response.
- Examine and click *Send* on **Steps 3-6** in the folder.
- Click Step 7: View the Transaction Queue. Examine the request type and URI and click *Send*. This request allows you to see the current list of ordered commands in the transaction.

Task 2 - Modify a Transaction

- Click the Step 8: View Queued Command 4 from Transaction request in the folder. Examine the request method and URI. We will GET command number 4 from the transaction queue.

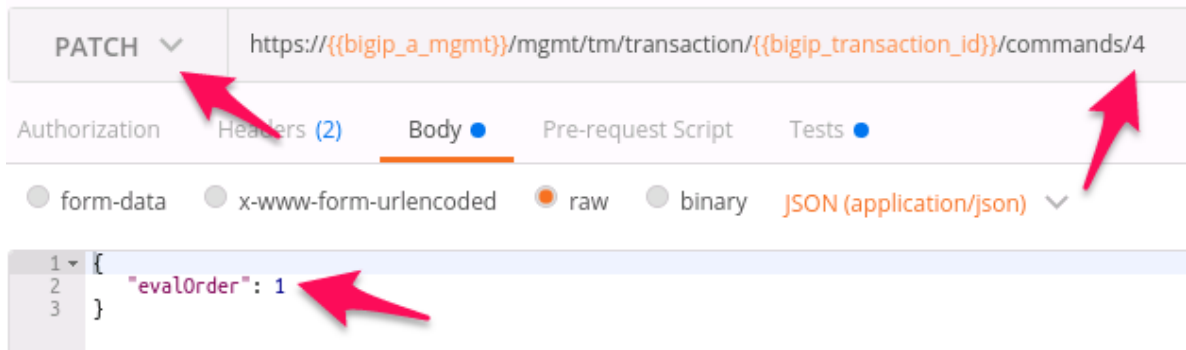
Step 8: View queued command 4 from Transaction

GET ▾	https://{{bigip_a_mgmt}}/mgmt/tm/transaction/{{bigip_transaction_id}}/commands/4	Params
Authorization	Headers (2)	Body Pre-request Script Tests
Type	No Auth ▾	
Body	Cookies	Headers (21) Tests Status: 200 OK
Pretty	Raw	Preview JSON ▾
<pre> 1 { 2 "method": "POST", 3 "uri": "https://localhost/mgmt/tm/ltn/profile/tcp", 4 "body": { 5 "name": "Lab1.7_tcp_clientside", 6 "nagle": "disabled", 7 "sendBufferSize": "16000" 8 }, 9 "evalOrder": 4, 10 "commandId": 4, 11 "kind": "tm:transaction:commandsstate", 12 "selfLink": "https://localhost/mgmt/tm/transaction/1494358032450450/commands/4?ver=12.1.1" 13 }</pre>		

- Click the Step 9: Change Eval Order 4 -> 1 request in the folder. Examine the request method, URI, JSON body, then click *Send*. We will PATCH our transaction resource and change the

value of the `evalOrder` attribute from 4 to 1 to move to the first position of the transaction queue:

► Step 9: Change Eval Order 4 -> 1



Note: Requests in the ordered transaction queue must obey the order of operations present in the underlying BIG-IP system.

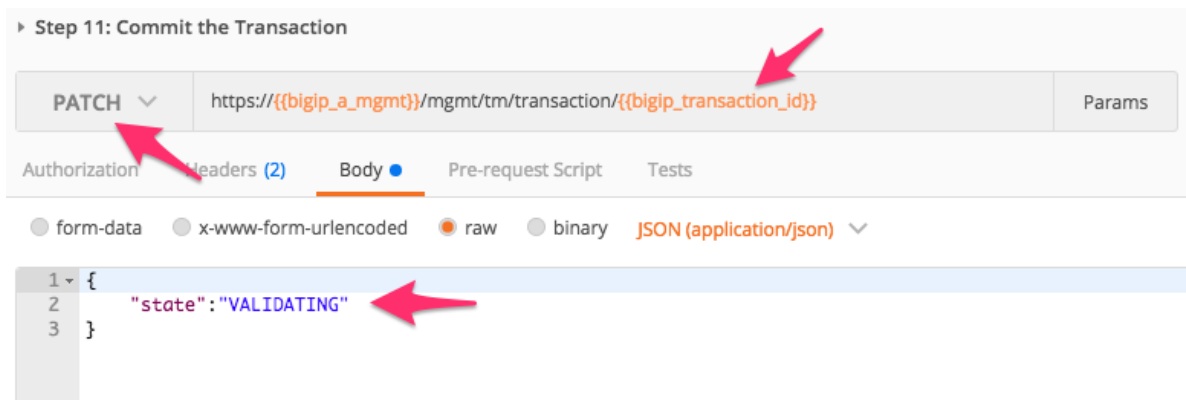
Warning: When sending the Header `X-F5-REST-Coordination-Id`, the system assumes that you want to **ADD** an entry in the transaction queue. You **MUST** remove this header if you want to issue any other transaction queue changes (such as deleting an entry from the queue, changing the order, or committing a transaction). If you fail to remove the header, the system will respond with a 400 HTTP error code with the following error text:

`"message": "Transaction XXXXX operation is not allowed to be added to transaction."`

3. Click the Step 10: View the Transaction Queue Changes request in the folder. Verify that command number 4 has moved into position 1 and the order of all other commands has been updated accordingly.

Task 3 - Commit a Transaction

1. Click the Step 11: Commit the Transaction request in the folder. Examine the request type, URI and JSON body. We will PATCH our transaction resource and change the value of the `state` attribute to submit the transaction:



2. Click the *Send* button and examine the response. The `state` may already be `COMPLETED`, however, it's a good practice to explicitly check for this.
3. Click the `Step 12: View the Transaction Status` request in the folder and click the *Send* button. Verify that the `state` of the transaction is `COMPLETED`
4. You can verify the configuration was created on the BIG-IP device via the BIG-IP A GUI at `https://10.1.1.10`
5. Verify that the virtual server works by opening `http://10.1.20.120` in Chrome web browser

Task 4 - [Service Provider] AFM and CGNAT

In this task we will do basic AFM logging setup, CGNAT LSN Pool setup, AFM basic policy and setup of VS and associated AFM policies.

Perform following steps to complete this task:

1. Step 1: Verify AFM Security report settings using GET. Validate response in postman.

Note: The response shows the the default settings for AFM. Notice that there are some settings that are disabled, some are enabled.

2. Step 2: Update AFM Security report settings using PATCH. We are setting all settings to disabled.

Step 1b: Update AFM Security Reporting Settings disabled All

PATCH ▼ https://{{bigip_a_mgmt}}/mgmt/tm/security/analytics/settings

Authorization Headers (2) Body ● Pre-request Script Tests


TYPE

Inherit auth from parent ▼

The authorization header will be automatically generated when you send the request. [Learn more about authorization](#)

This request is using an authori

Body Cookies (2) Headers (26) Test Results

Pretty Raw Preview JSON ▼ 

```
1 {
2   "kind": "tm:security:analytics:settings:settingsstate",
3   "selfLink": "https://localhost/mgmt/tm/security/analytics/settings?ver=12.1.3",
4   "aclRules": {
5     "collectClientIp": "disabled",
6     "collectClientPort": "disabled",
7     "collectDestIp": "disabled",
8     "collectDestPort": "disabled",
9     "collectServerSideStats": "disabled"
10  },
11   "collectedStatsExternalLogging": "disabled",
12   "collectedStatsInternalLogging": "disabled",
13   "dns": {
14     "collectClientIp": "disabled"
15  },
16   "dosL2L4": {
17     "collectClientIp": "disabled"
18  },
19   "l3L4Errors": {
20     "collectClientIp": "disabled",
21     "collectDestIp": "disabled"
22  },
23   "staleRules": {
24     "collect": "disabled"
25  }
26 }
```

All settings disabled

Verify in the BIG-IP A GUI

Security » Reporting : Settings : Reporting Settings

⚙️
Reporting Settings
Real-Time Sessions

Reporting Settings

Local Storage	<input type="checkbox"/> Enabled
Remote Storage	<input type="checkbox"/> Enabled
Protocol DNS	<input type="checkbox"/> Collect Source IP Address
DoS Network	<input type="checkbox"/> Collect Source IP Address
Network Firewall Rules	<input type="checkbox"/> Collect Source IP Address <input type="checkbox"/> Collect Destination IP Address <input type="checkbox"/> Collect Source IP Port <input type="checkbox"/> Collect Destination IP Port <input type="checkbox"/> Collect Server Side Statistics <input type="checkbox"/> Collect Stale Rules Statistics
TCP/IP Errors	<input type="checkbox"/> Collect Source IP Address and Port <input type="checkbox"/> Collect Destination IP Address and Port
SMTP Configuration for Reports Export	no configuration found Create...

Save

- Step 3: Update AFM Security report settings using PATCH. We are setting all settings to enabled.

Security » Reporting : Settings : Reporting Settings

⚙️
Reporting Settings
Real-Time Sessions

Reporting Settings

Local Storage	<input checked="" type="checkbox"/> Enabled
Remote Storage	<input checked="" type="checkbox"/> Enabled
Publisher	none
Protocol DNS	<input checked="" type="checkbox"/> Collect Source IP Address
DoS Network	<input checked="" type="checkbox"/> Collect Source IP Address
Network Firewall Rules	<input checked="" type="checkbox"/> Collect Source IP Address <input checked="" type="checkbox"/> Collect Destination IP Address <input checked="" type="checkbox"/> Collect Source IP Port <input checked="" type="checkbox"/> Collect Destination IP Port <input checked="" type="checkbox"/> Collect Server Side Statistics <input checked="" type="checkbox"/> Collect Stale Rules Statistics
TCP/IP Errors	<input checked="" type="checkbox"/> Collect Source IP Address and Port <input checked="" type="checkbox"/> Collect Destination IP Address and Port
SMTP Configuration for Reports Export	no configuration found Create...

Save

- Step 4: Verify AFM Event Logging settings using GET. Validate response in postman.
- Step 5: Create AFM Event Logging settings using POST. Validate response in postman, and F5.

Security » Event Logs : Logging Profiles

Protocol Network Network Address Translation DoS **Logging Profiles**

Search

<input type="checkbox"/> ▲ Profile Name	Protocol Security	Network Firewall
<input type="checkbox"/> Log all requests	Disabled	Disabled
<input type="checkbox"/> Log illegal requests	Disabled	Disabled
<input type="checkbox"/> SP_AFM_Logger	Disabled	Enabled
<input type="checkbox"/> global-network	Disabled	Enabled
<input type="checkbox"/> local-dos	Disabled	Disabled

Delete

6. Step 6: Verify AFM Source address translation using GET. There should be no Pools configured.

Note: Source Address translation in AFM is used for LSN pools in old CGNAT configuration.

7. Step 7: Create AFM Source address translation using POST. Validate successful creation in F5.

Security » Network Address Translation : Source Translation » Lab_1.7a_LSN

Active Rules
Policies
Source Translation
Destination Translation

Name
Lab_1.7a_LSN

Description

Type
Dynamic PAT

Addresses
10.128.10.20/32

add an address/address-range

Add

Ports
1024-65365

add a port number/port-range

Add

ICMP Echo
Disabled

PAT Mode
NAPT

InBound Mode
None

Mapping
Mode: Address Pooling Paired
Timeout: 300

Client Connection Limit
0

Hairpin Mode
Disabled

Egress Interfaces
Enabled on...

☐ External
☐ Internal
☐ http-tunnel
☐ socks-tunnel

Update

Delete

8. Step 8: Create AFM CGNAT Policy using POST. Validate successful creation in F5.

Security » Network Address Translation : Policies

Filter Policy List

▲ Name	◆ Description
<input type="checkbox"/> Lab1.7a_LSN_Policy	

Note: There are no Rules in this Policy (these will be created in the next step).

Security » Network Address Translation : Policies » Lab1.7a_LSN_Policy

Properties

Name	Lab1.7a_LSN_Policy
Description	

Filter Policy List

ID	Name	State	Protocol	Source	Destination
No records to display					

9. Step 9: Create AFM CGNAT NAT within the above created Policy using POST. Validate successful creation in F5.

Security » Network Address Translation : Policies » Lab1.7a_LSN_Policy

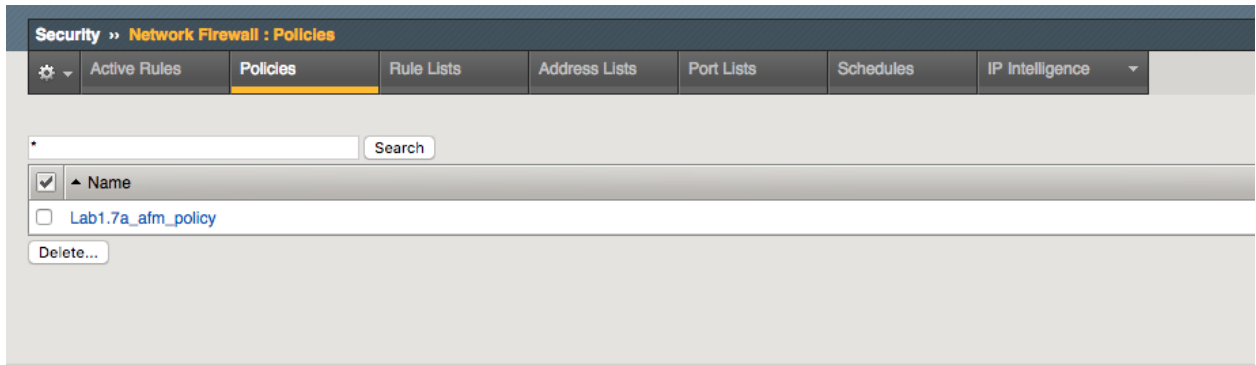
Properties

Name	Lab1.7a_LSN_Policy
Description	

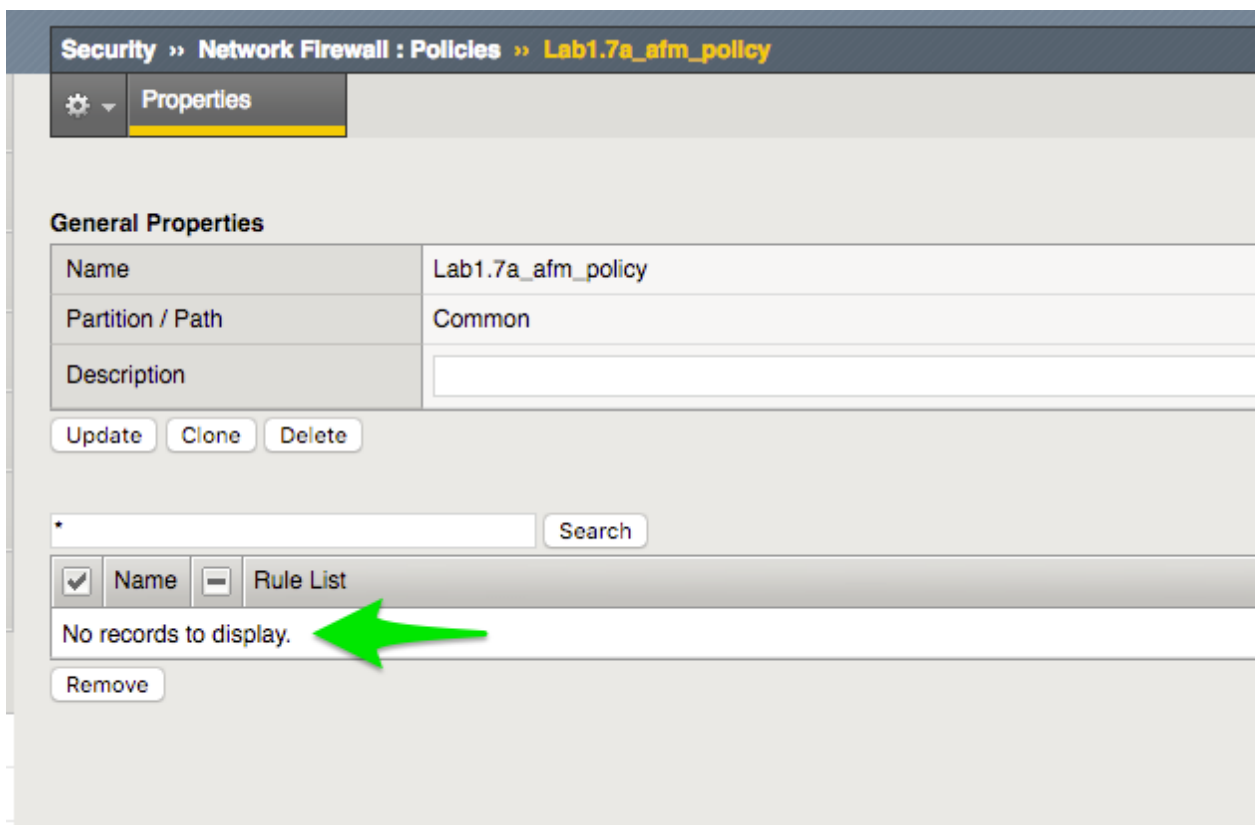
Filter Policy List

ID	Name	State	Protocol	Source	Destination	Translated Source	Translated Destination	Log Profile
<input type="checkbox"/> 1	source_LSN	enabled	any	Addresses 10.128.50.0/24	Any	Lab 1.7a_LSN Type: Dynamic PAT Addresses 10.128.10.20/32 Ports 1024-65365	None	SP_AFM_Logger

10. Step 10: Create AFM Firewall Policy using POST. Validate successful creation in F5.

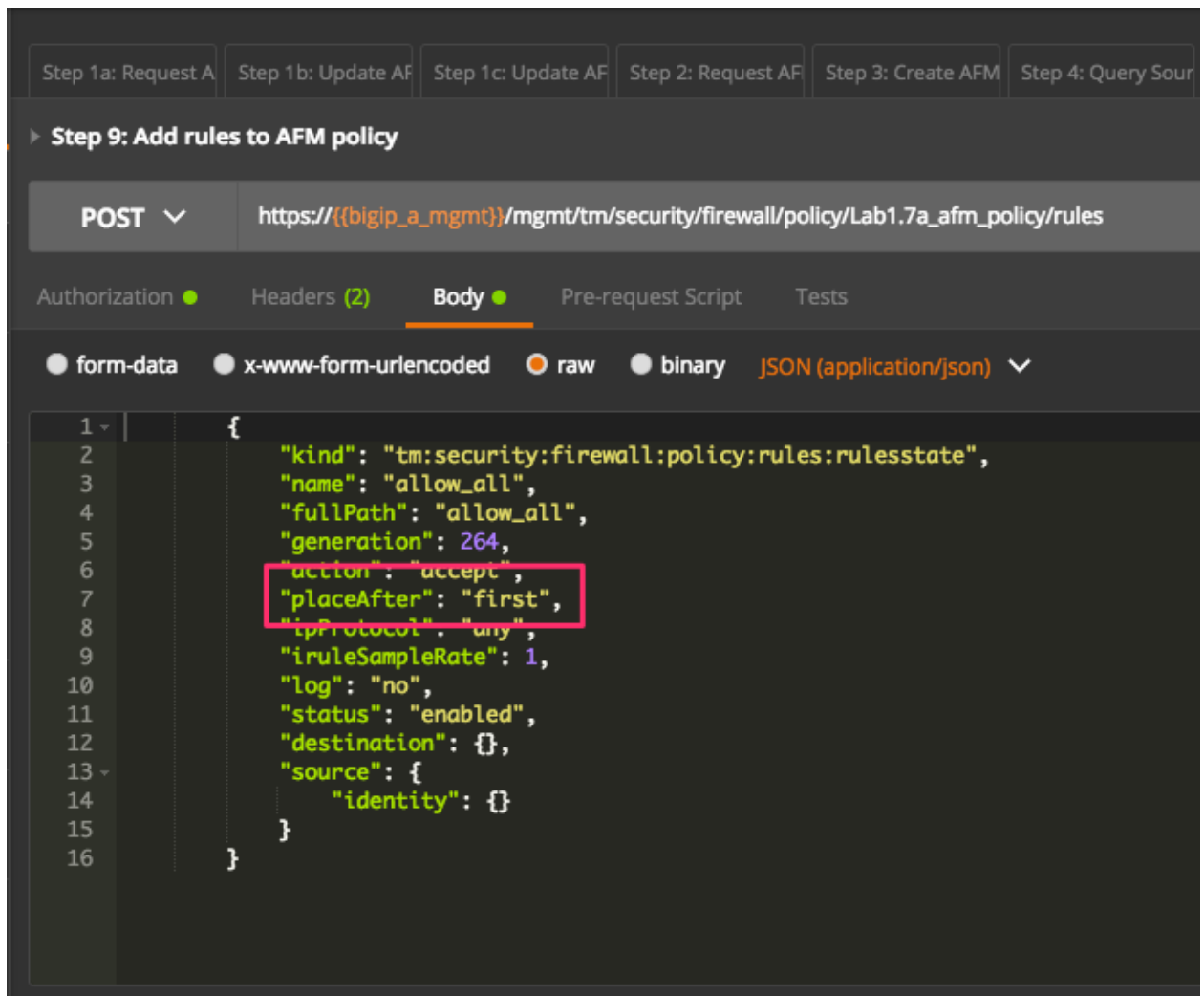


Note: There are no rules in this policy (these will be created in the next step).

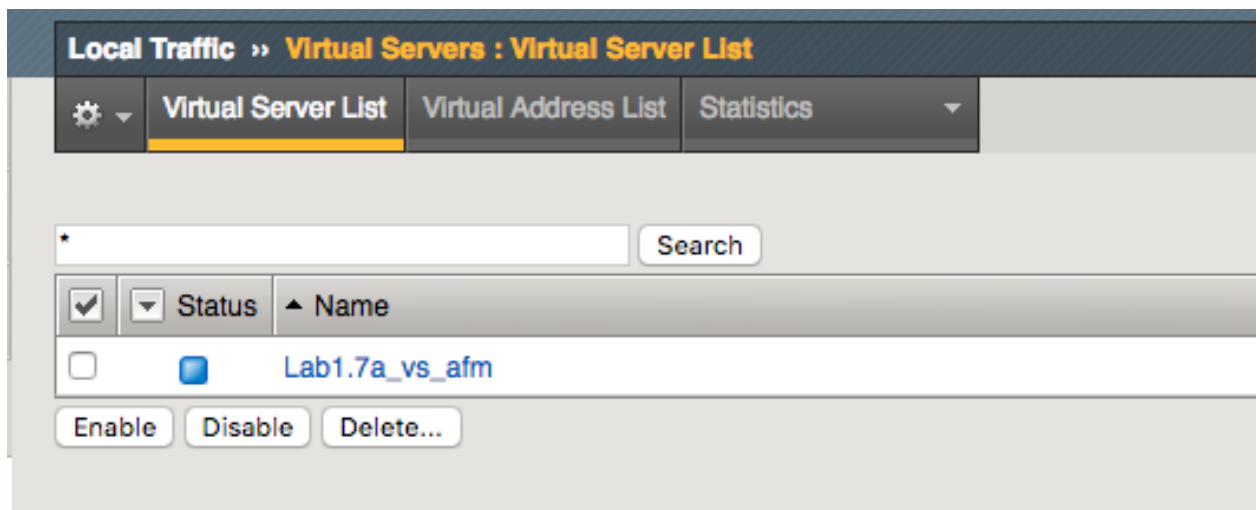


11. Step 11: Create AFM rules and add to Policy using POST. Validate successful creation in F5.

Note: The use of the `placeAfter` attribute in rules is required otherwise rule placement will not occur.



12. Step 12: Create FastL4 forwarding Virtual Server using a POST. Validate successful creation in the BIG-IP A GUI.



Note: There are no security policies, network translation, or firewall rules present in the Virtual

Server. These items will be associated using a `PATCH` the next step.

Local Traffic » Virtual Servers : Virtual Server List » Lab1.7a_vs_afm

Settings Properties Resources **Security** Statistics

Policy Settings: Advanced

Destination	0.0.0.0:0
Service	*
Network Firewall	Enforcement: Disabled Staging: Disabled
Network Address Translation	<input type="checkbox"/> Use Device Policy <input type="checkbox"/> Use Route Domain Policy Policy: None
Service Policy	None
IP Intelligence	Disabled
DoS Protection Profile	Disabled
Log Profile	Disabled
Activation Time	
Compilation Duration	
Compiled Size	
Maximum Transient Memory	

Update

* Search Policy Type Enforced

<input checked="" type="checkbox"/>	Name	Rule List	Description
	(Default)		

Delete... Search Logs... Reset Count

13. Step 13: Add Network Firewall, NAT and Rules to the Virtual Server using a `PATCH`. Validate successful creation in using the BIG-IP A GUI

Local Traffic » Virtual Servers : Virtual Server List » Lab1.7a_vs_afm

Properties Resources Security Statistics

Policy Settings: Advanced

Destination	0.0.0.0:0
Service	*
Network Firewall	Enforcement: Enabled... Policy: Lab1.7a_afm_policy
	Staging: Disabled
Network Address Translation	<input type="checkbox"/> Use Device Policy <input type="checkbox"/> Use Route Domain Policy Policy Lab1.7a_LSN_Policy
Service Policy	None
IP Intelligence	Disabled
DoS Protection Profile	Disabled
Log Profile	Disabled
Activation Time	2018-02-11 10:16:21 PST
Compilation Duration	0:0:0
Compiled Size	12.2K
Maximum Transient Memory	20.5M

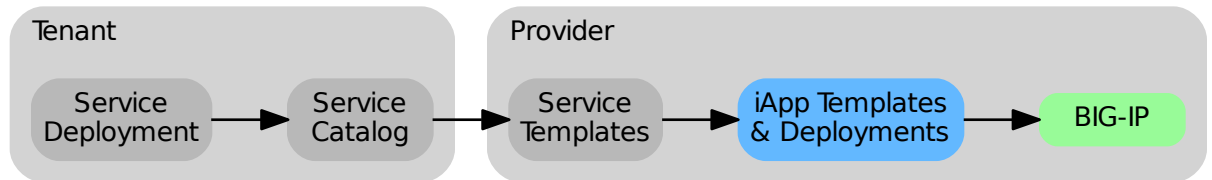
Update

Search Policy Type Enforced

<input checked="" type="checkbox"/>	Name	Rule List
<input type="checkbox"/>	allow_all	
	(Default)	

Delete... Search Logs... Reset Count

2.4 Module 2: Abstracting Services using iApp Templates



In this Module, we will continue working with the BIG-IP REST interface. However, we will now introduce F5 Declarative Interfaces built with F5 iApp Templates.

iApps is a user-customizable framework for deploying applications that enables you to templatize sets of functionality on your F5 devices. For example, you can automate the process of adding Virtual Servers or manage your iRules inventory through the use of a custom iApp Template.

iApps are commonly thought of as a Wizard style deployment helper, but they are actually a Declarative Interface. When iApp Templates are created they can be written to accomodate API centric use cases.

When an iApp deploys, a **single** call - declaring the desired deployment - is processed on the BIG-IP with the correct order of operations. If the deployment were to fail the iApp would *automatically* rollback the transaction and leave the configuration unchanged. All created objects are associated with an Application Service Object (ASO). The ASO model identifies which objects belong to the iApp service deployment. Upon service deletion, all service related objects are recursively deleted.

We will be using the **F5 App Services Integration iApp** (App Services iApp for short).

For further information about the App Services iApp see:

- **GitHub Repository:** <https://github.com/F5Networks/f5-application-services-integration-iApp>
- **User Guide:** https://devcentral.f5.com/wiki/iApp.AppSvcsiApp_userguide_userguide.ashx

An overview of iApps and different iApp templates that available can be found at:

- <https://devcentral.f5.com/iapps>

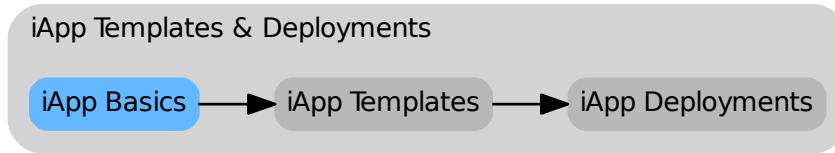
Note: This module requires the underlying network configuration that was completed in Module 1. Additionally, **BIG-IP A** must be the **Active** node in the cluster. When viewing the BIG-IP A GUI it should say **ONLINE (ACTIVE)** in the upper left corner of the interface.

Note: This module deploys the configuration to BIG-IP A. iApp deployments leverage the underlying config-sync mechanisms in the cluster. Once deployed on BIG-IP A, the configuration will be automatically synced to BIG-IP B.

You can learn more about clustering features in this video:

Source: <https://devcentral.f5.com/articles/lightboard-lessons-device-services-clustering-25575>

2.4.1 Lab 2.1: Exploring iApps



iApp Templates & Deployments

There are multiple ways to install an iApp on BIG-IP. These includes using TMOS Shell (TMSH through SSH), the GUI (TMUI), and the REST Interface. All of these mechanisms are supported and, if required, can be used in conjunction with each other.

For instance, you can install an iApp template from BIG-IP GUI and then deploy a new service via iControl REST using tools such as cURL, Postman and Ansible.

Note: Redeployment of iApp templates is facilitated/protected by a mechanism in BIG-IP platform to ensure safe changes to the configurations without disrupting existing user traffic.

F5 iApps was introduced in TMOS (BIG-IP operating system) Version 11. They can interact within and across different F5 modules to provide full Layer 4-7 Application Services capabilities. The **iApp Template** is used to execute an **iApp Deployment** that generates a series of configuration object grouped under an **Application Service Object (ASO)**. The ASO model houses objects belonging to the iApp service deployment. Upon deletion of a specific iApp service deployment, all the associated objects will be recursively deleted.

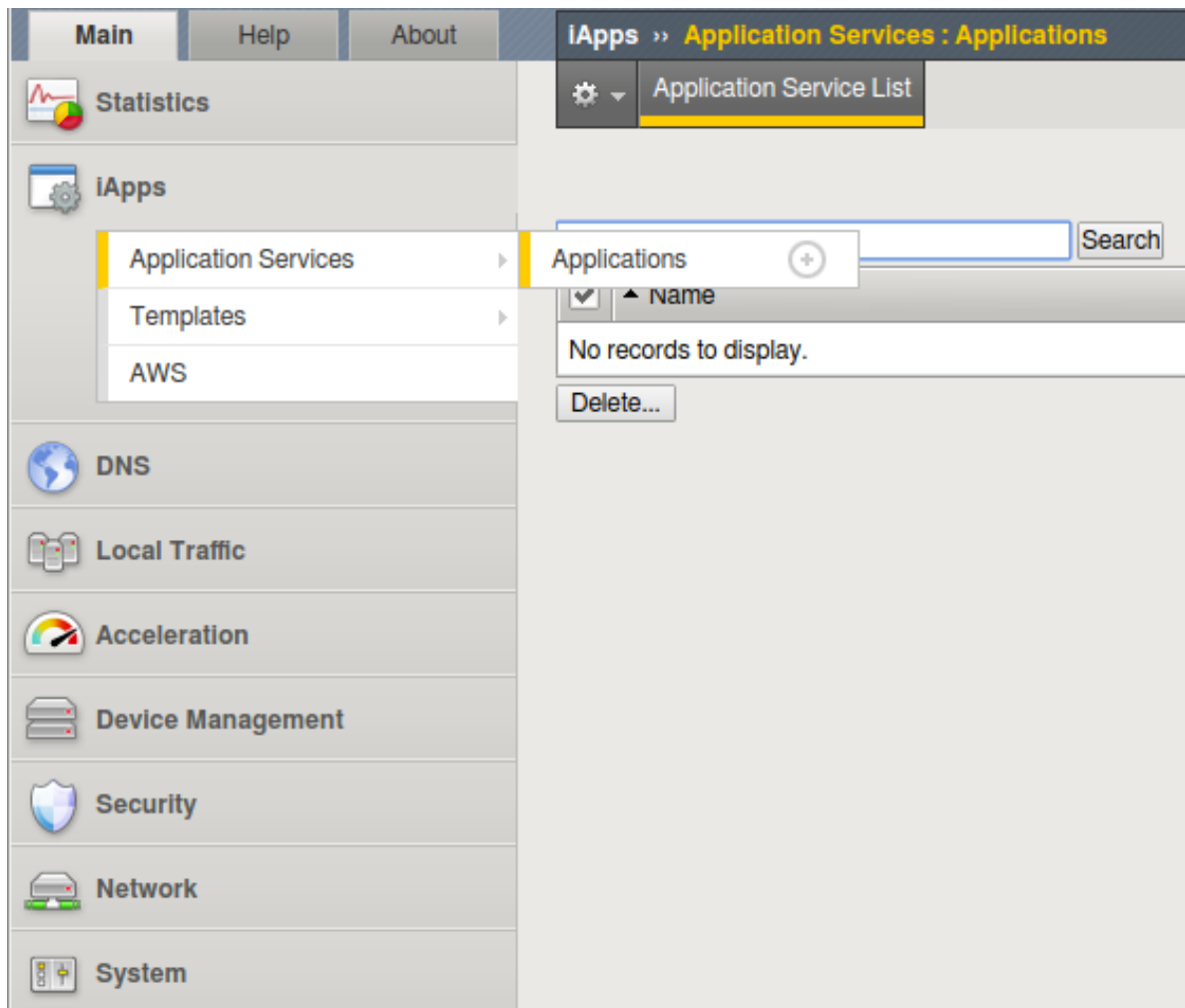
Below are some of the modules that can be configured using iApp templates:

- Local Traffic Manager
- Advanced Firewall Manager
- Application Security Manager
- Access Policy Manager

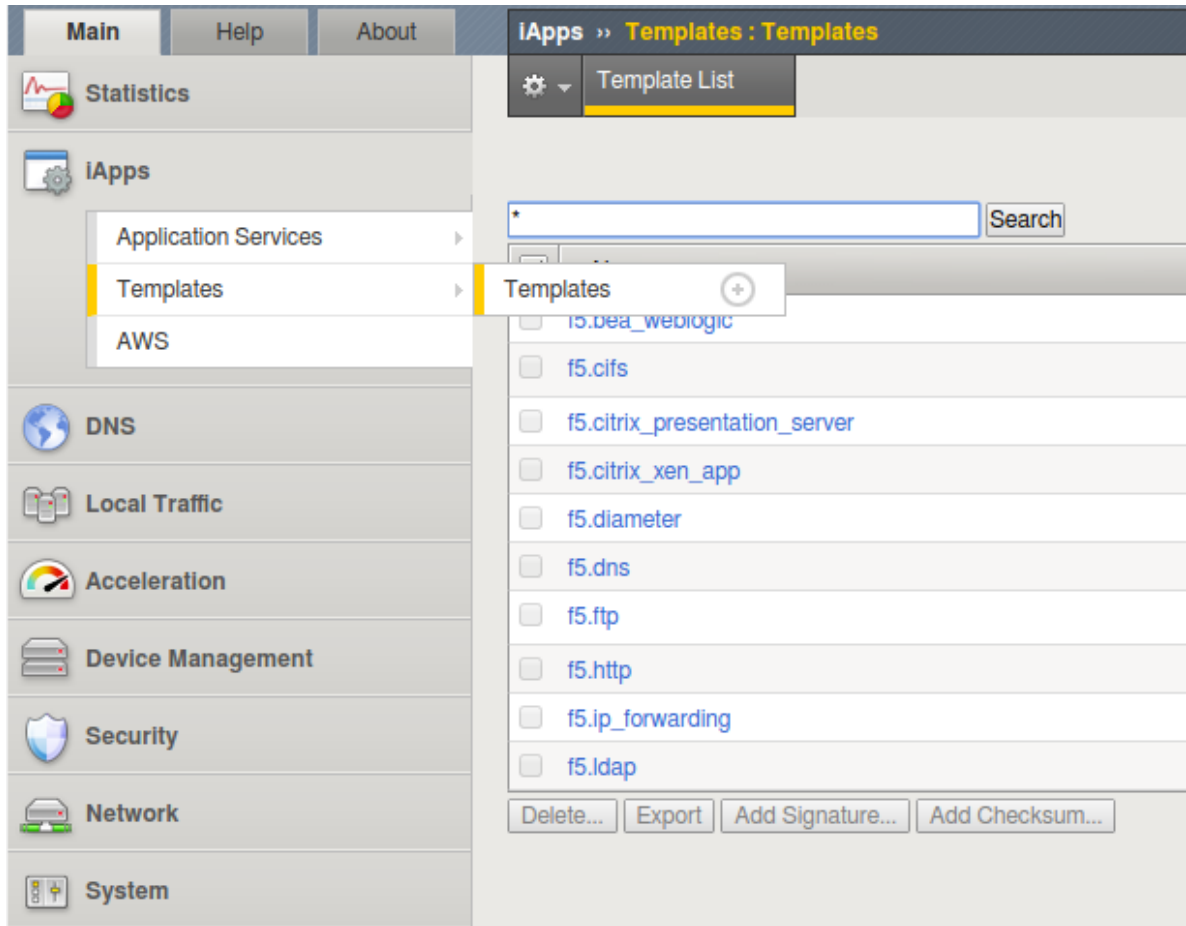
Note: The term `Application Service` in the GUI and `service` in the REST API are the same objects. The name is abbreviated in the API.

You can find the GUI representation of iApps on the left-hand side of the UI under *iApps*. iApp deployments are located under *Application Services*, while iApp templates are located under *Templates* on the system.

- *Application Services* (iApp deployments)



- *Templates* (iApp templates)



The associated REST API endpoints are:

- **iApp Deployments:** `/mgmt/tm/cloud/services/iapp`
- **iApp Templates:** `/mgmt/tm/sys/application/template`

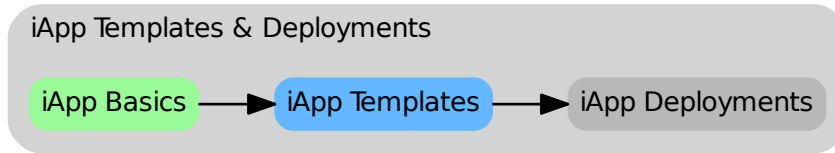
iApp Deployments and Source-of-Truth

By default, iApp implements a strict source-of-truth preservation mechanism called **Strict Updates**. The App Services iApp does allow granular configuration of underlying TMOS objects **without** disabling the Strict Updates mechanism. However, not all iApp templates supports this functionality.

In an automated environment, we **must** always ensure that the **iApp template inputs** are being used as the Source-of-Truth for an underlying deployment. Therefore, **Strict Updates should not be disabled** in order to preserve the integrity of service deployments using iApp templates.

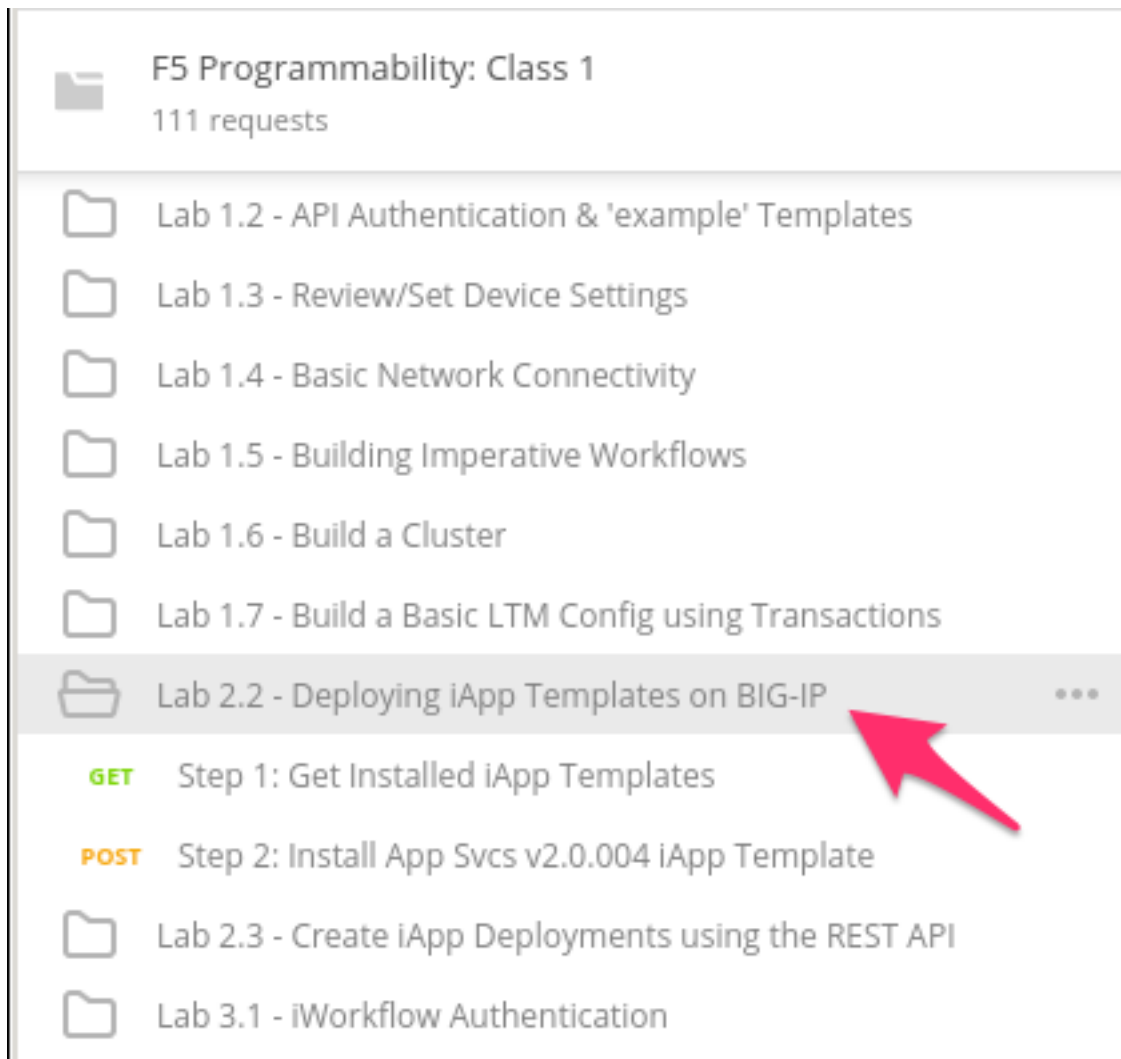
For instance, after an iApp service is deployed, modifying the underlying configuration **with Strict Updates disabled** will result in Source-of-Truth violation. Changes made directly to the configuration will cause iApp configuration objects to be overwritten. The direct modification of objects configured on BIG-IP will alter the integrity of iApp deployment input values that automation tools are interacting with, causing failures. It is therefore important to keep **Strict Updates** enabled at all times for automated deployments.

2.4.2 Lab 2.2: Deploying iApp Templates on BIG-IP



iApps typically come in the form of a `.tmpl` file, which contains the content needed for the BIG-IP to utilize it as a Service framework. Different toolkits will install iApps in different ways. We'll be using the REST API in a raw form, so the content of the file is what we need. As a result, we need to ensure that the content of the iApp is URL encoded to make sure the BIG-IP reads the payload correctly. This is specific for the iApp deployment over REST API. When using other tools like Ansible, the whole `.tmpl` file can be uploaded, removing the need for encoding.

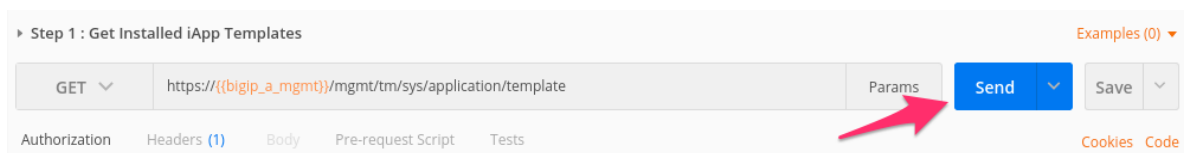
Note: This lab work will be performed from `Lab 2.2 - Deploying iApp Templates on BIG-IP` folder in the Postman Collection



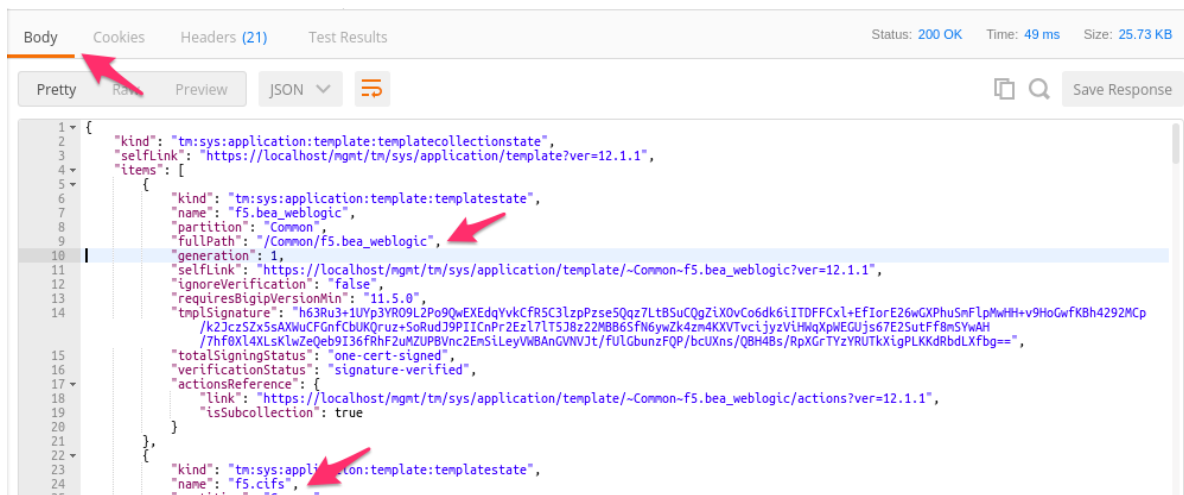
Task 1 - View Installed iApp Templates

Perform the following steps to complete this task:

1. **Send** the Step 1: Get Installed iApp Templates request to view iApp templates installed on the BIG-IP device:



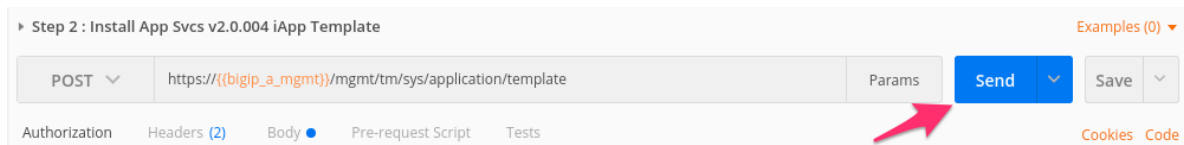
2. Review the JSON response *Body*. The JSON payload shows iApp templates that are installed on the BIG-IP device:



Task 2 - Install the App Services iApp Template

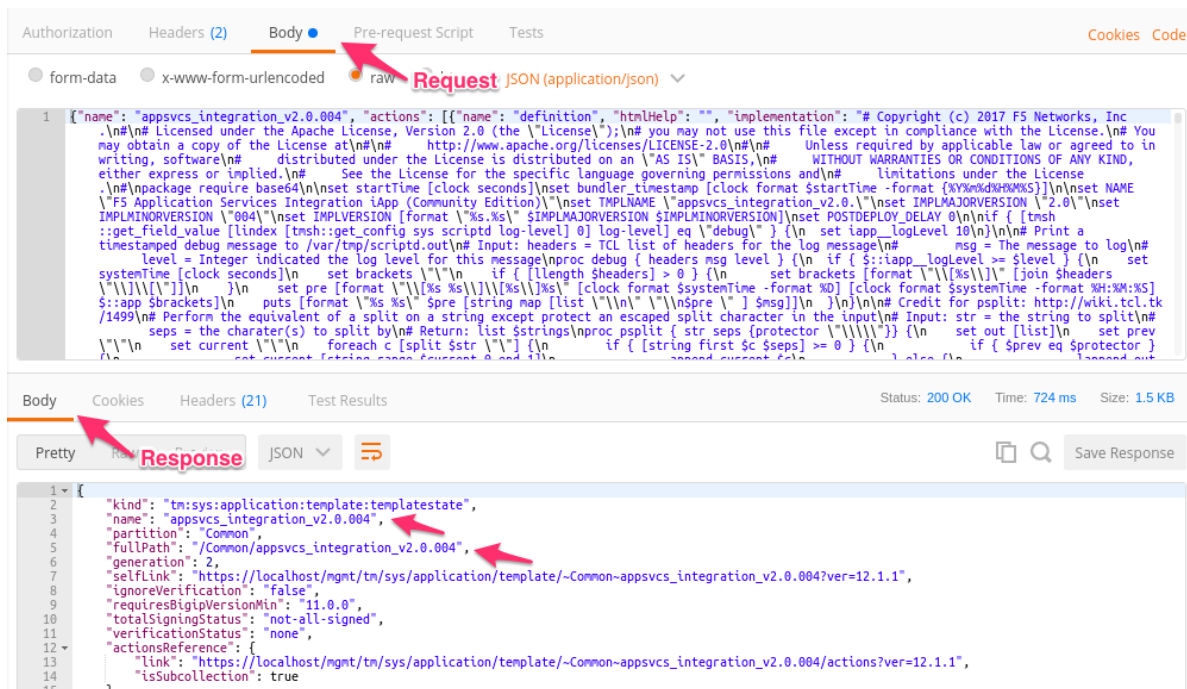
Perform the following steps to complete this task:

1. **Send** the Step 2: Install App Svcs v2.0.004 iApp Template request to install the App Services iApp template:

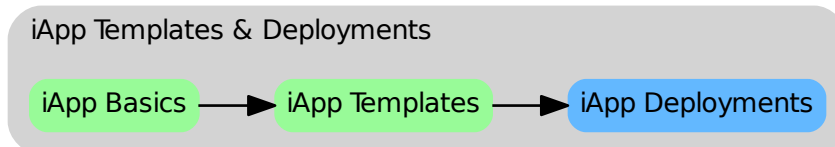


2. Review the **Request JSON Body**, and the **Response JSON Body**. In this task we installed the App Services iApp Template and the BIG-IP sent back a response that the iApp was installed with its object name.

Note: The JSON body in the **Request** portion is automatically generated as part of the build process for the App Services iApp and the request in the Postman Collection was copied from a pre-built collection that ships with releases of the App Services iApp template.

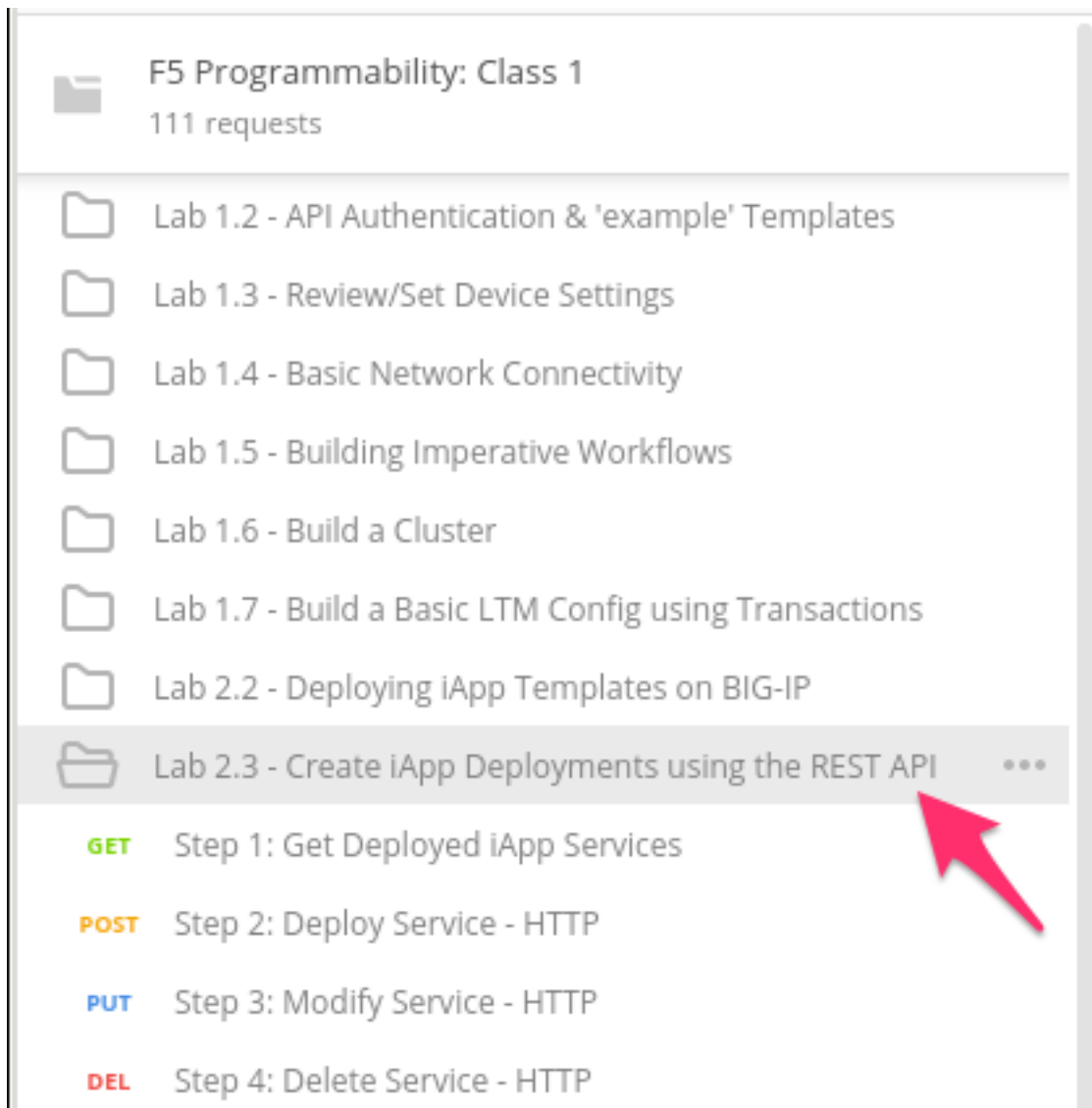


2.4.3 Lab 2.3: Create iApp Deployments using the REST API



Now that the App Services iApp template is installed, we can deploy a new Layer 4 to 7 Service. We will start with **Creating** a Basic HTTP Service, demonstrate **Modifying/Mutate** the service by changing the node state, and finally **Delete** the whole service. Once we've demonstrated with these tasks, we'll introduce more complex deployments options with iRules, Custom Profiles, Certificates, and an ASM Policy.

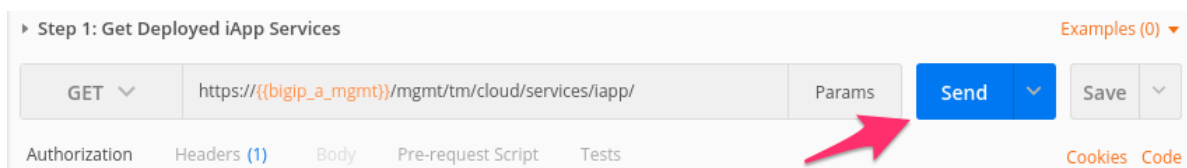
Note: This lab work will be performed from Lab 2.3 - Create iApp Deployments using the REST API folder in the Postman Collection



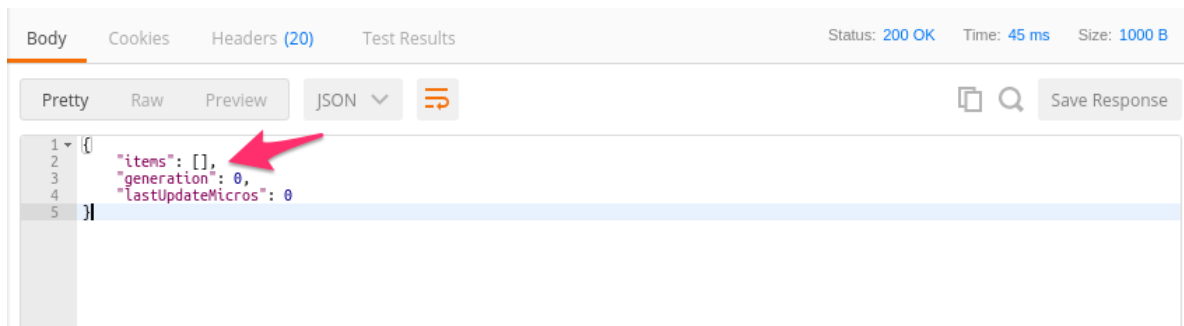
Task 1 - View Deployed Services

Perform the following steps to complete this task:

1. **Send** the Step 1: Get Deployed iApp Services request to view current iApp deployments on the BIG-IP device:



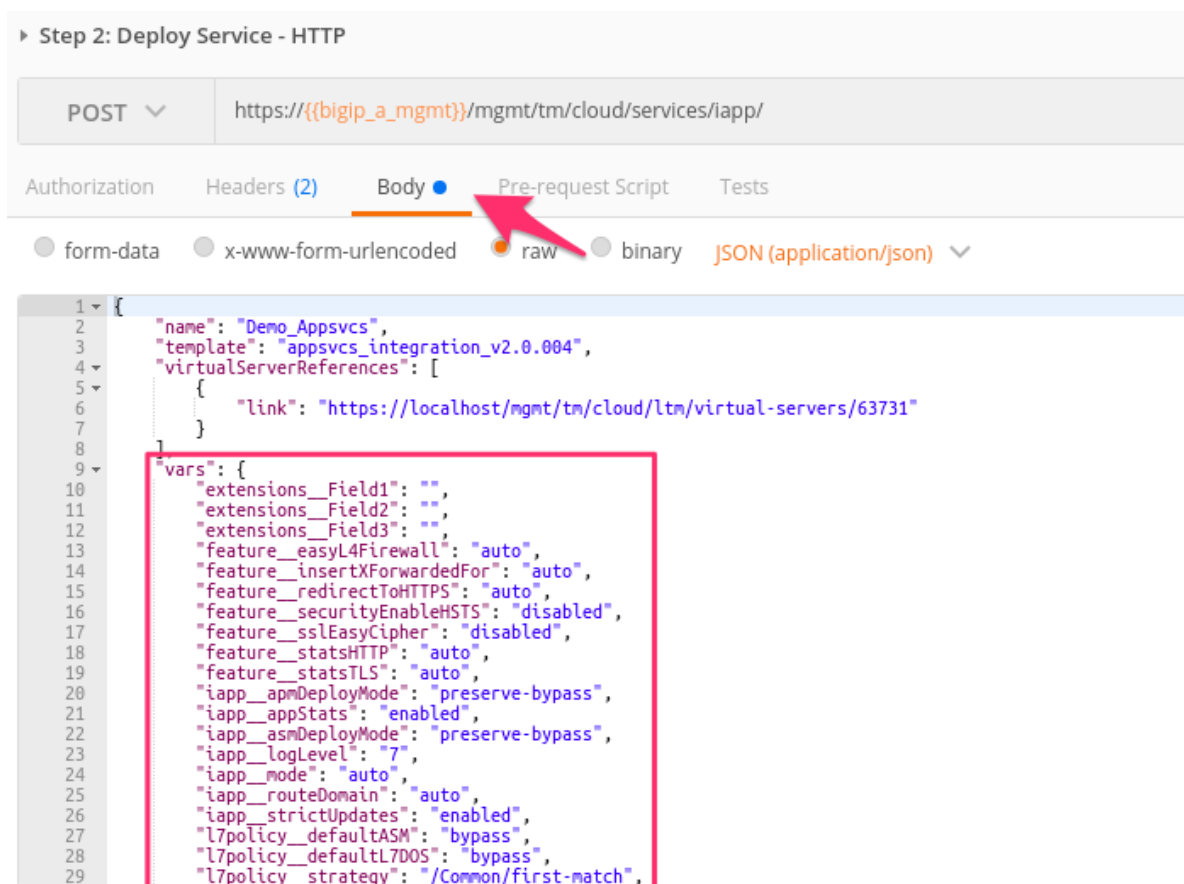
2. Review the JSON Response *Body*. The BIG-IP device does not have any iApp deployments. As a result the `items` array is empty (`[]`):



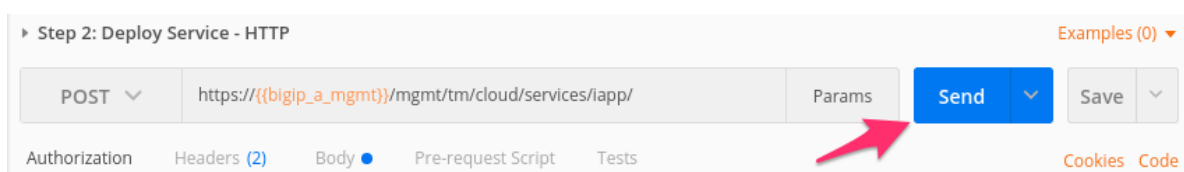
Task 2 - Deploy Basic HTTP Service

Perform the following steps to complete this task:

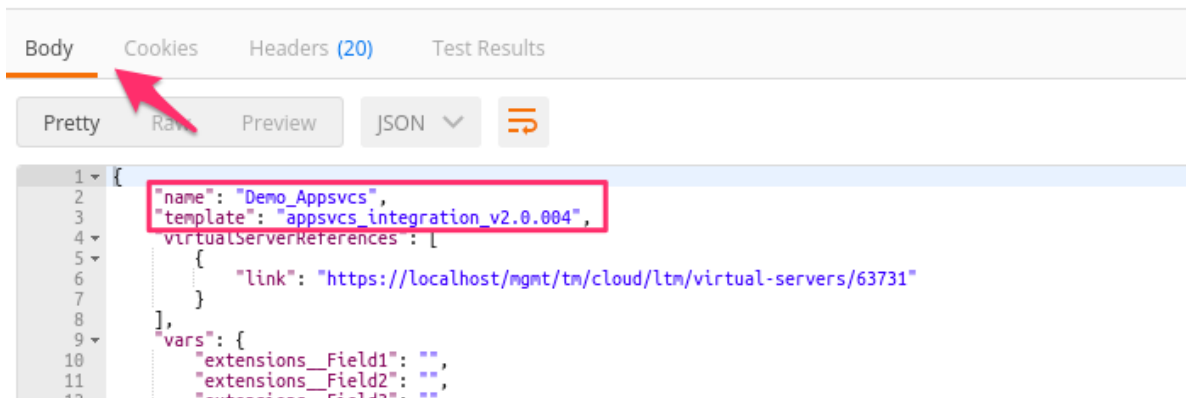
1. Click Step 2: Deploy Service - HTTP. Review the **Request JSON Body**. The JSON body of the POST contains the input for the iApp template to execute the deployment of the service.



2. Click the **Send** button to **Create** a Basic HTTP Service:



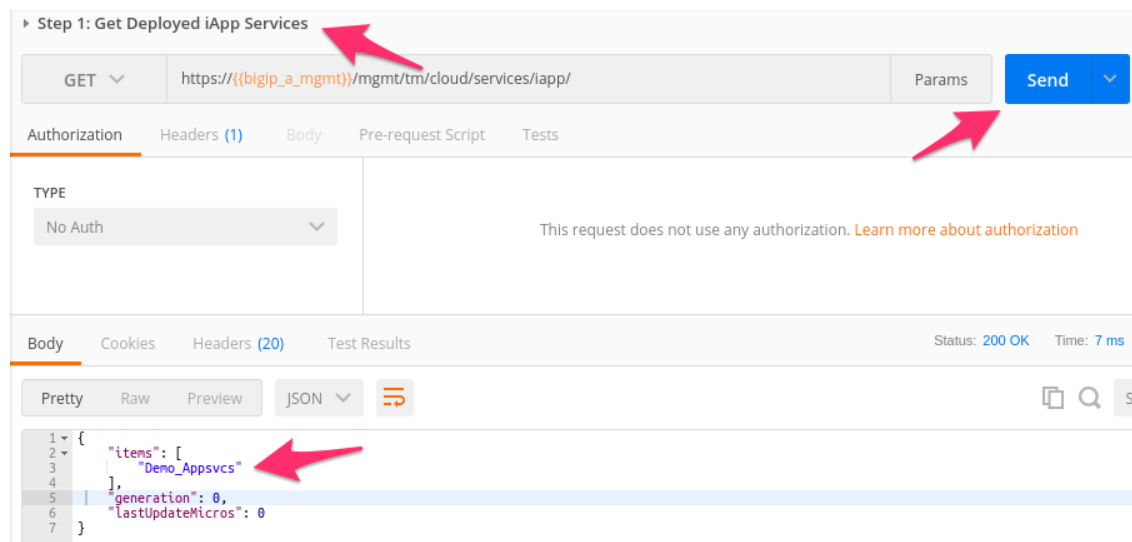
In this task, we will deploy our first service. Review the **Response JSON Body** to verify if the Service has been deployed.



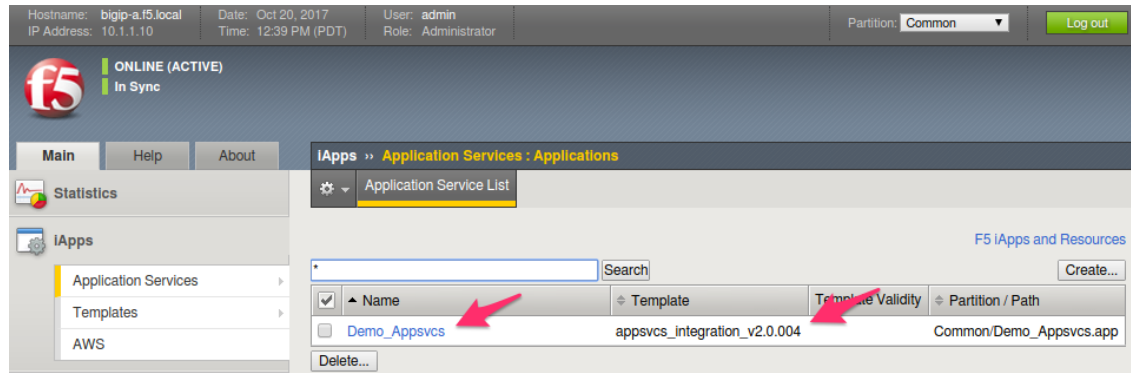
Note: We've just progressed into a **Declarative** instantiation, by defining the end state and relying on the iApp templates to handle the order of operations and configuration of specific objects. By doing this, we have drastically reduced the amount of **Domain Specific Knowledge** required to interact with the device. In the next module, we will combine this concept with **Abstraction** to further simplify the interface the service consumer has to interact with.

- Now that the service has been deployed, let's review the BIG-IP configuration. You can validate by sending the Step 1: Get Deployed iApp Services request again. Alternatively, you can login to BIG-IP A GUI to observe the service deployment via TMUI:

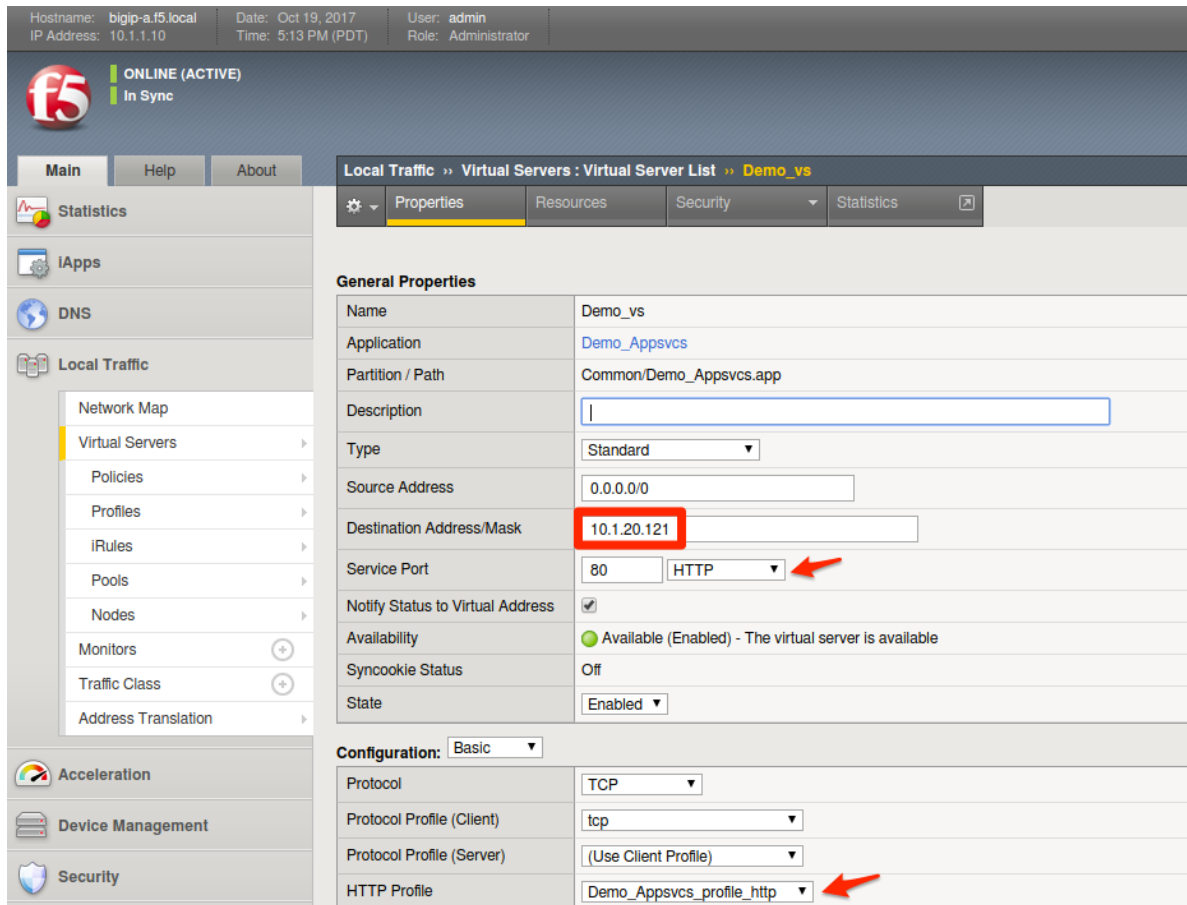
- **REST:** Send Step 1: Get Deployed iApp Services request:



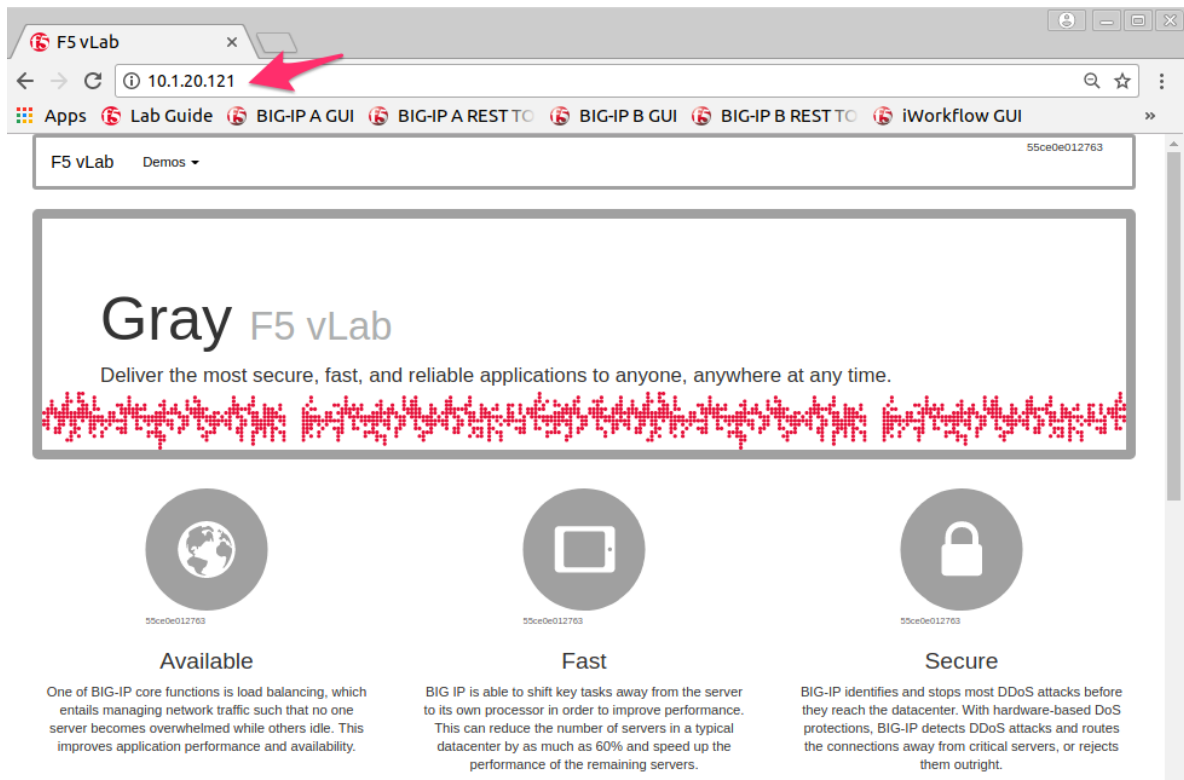
- **TMUI GUI:** *iApps* → *Application Services* → *Applications*



- From the TMUI GUI, examine the Virtual Server that was created from this deployment by clicking *Local Traffic* → *Virtual Servers* → *Virtual Server List* → *Demo_vs*. The configuration is simple, but it does contain the key components for an HTTP service (Listener, HTTP Profile, Monitor, Pool, and Pool Members):



- The service is available and active, you can connect to the Virtual Server using Chrome web browser at `http://10.1.20.121` and examine its responses:



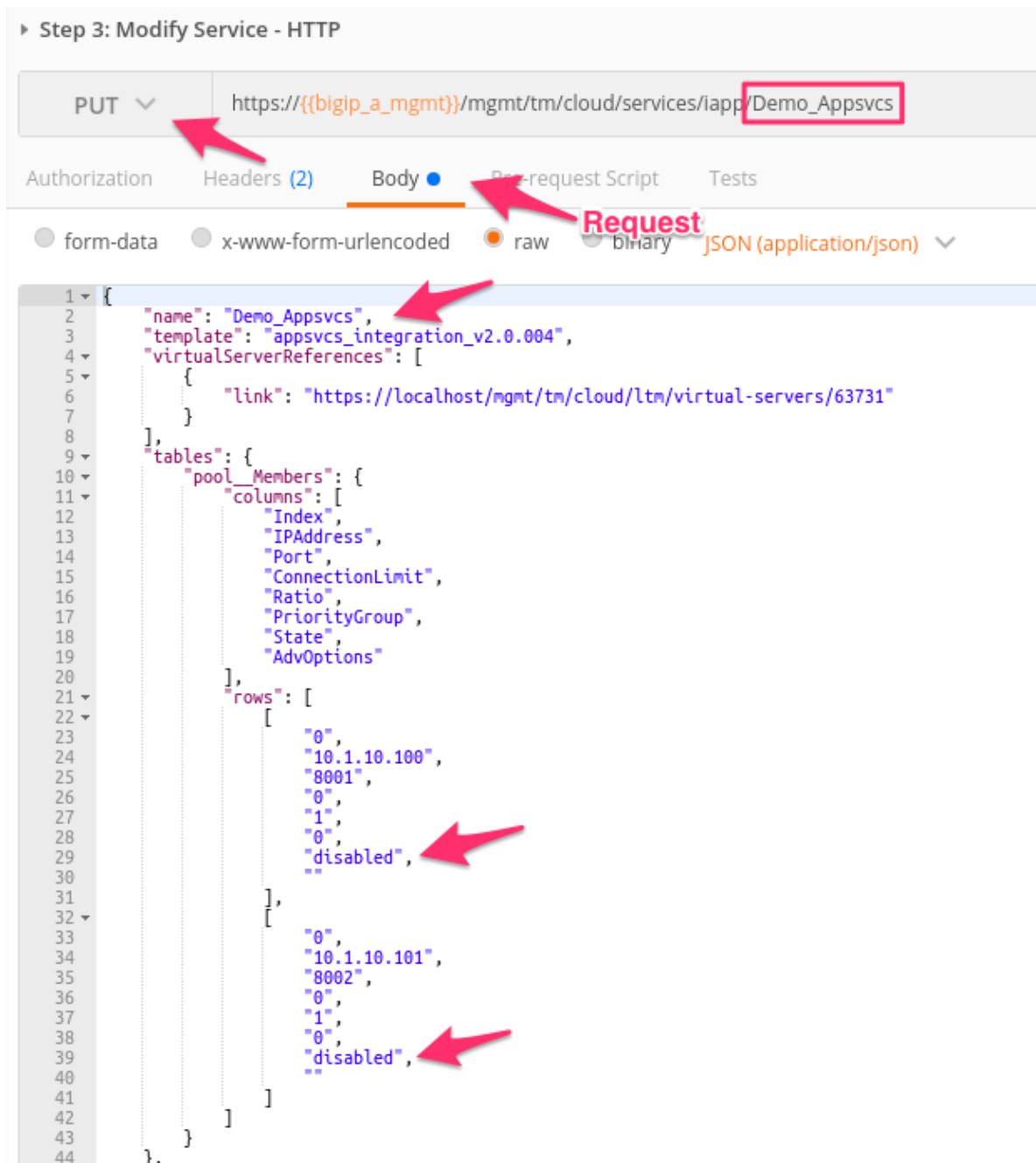
Note: The colors of the text, images, and borders may vary depending on the back-end server selected during the load balancing process.

Task 3 - Modify our Deployed Service

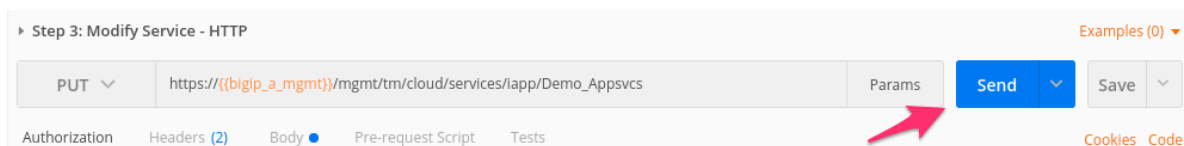
In this task, we will modify the existing service. We will disable all pool members and bring the service down.

Perform the following steps to complete this task:

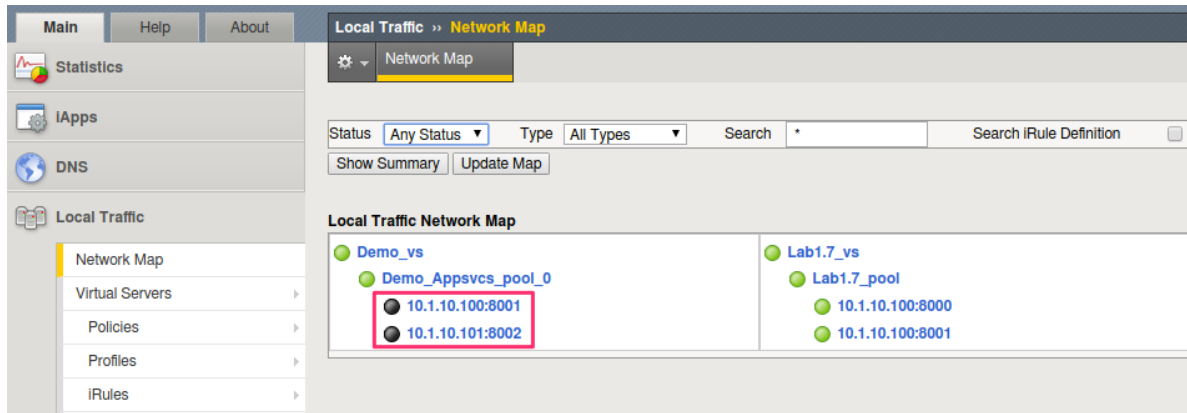
1. Click on **Step 3: Modify Service – HTTP**. Review the **Request URL** and **JSON Body**. Notice that we specified the **Resource** URL for our deployment. Modifying or *Redeploying* a service is handled by sending **only** the updated JSON to the specific Resource (our service) using a **PUT** request method. We set the state of the pool members to `disabled` which forces the service to go offline.



2. Click the **Send** button to **Modify** the previously deployed Basic HTTP Service:



3. In the BIG-IP GUI click **Local Traffic** → **Network Map** to view the new state of the Pool Members (Black indicators reflect the disabled state). The state has been updated to reflect the state we declared in our call. The Virtual Server is no longer passing traffic at `http://10.1.20.121` because all the Members in the Pool have been disabled:

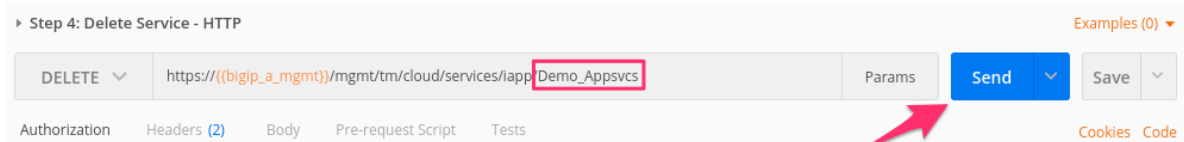


Task 4 - Delete our Deployed Service

The lifecycle of a service also includes the service removal. We will now delete an existing service.

Perform the following steps to complete this task:

1. **Send** the Step 4: Delete Service - HTTP request to **Delete** the previously deployed Basic HTTP Service:

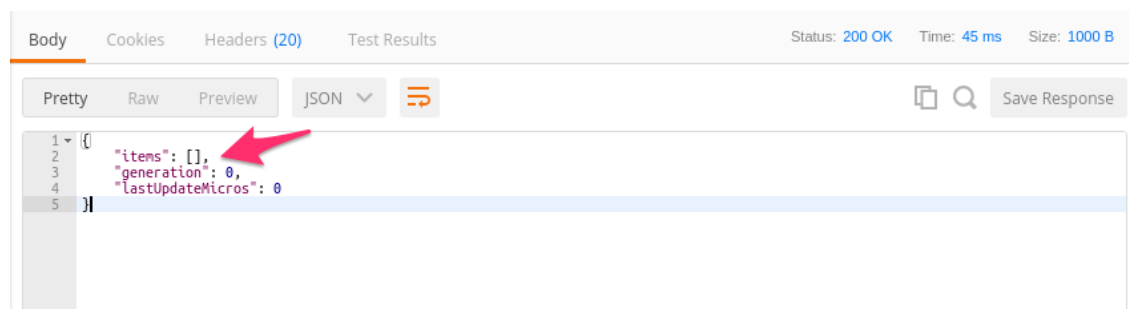


2. Similar to modification process, the deletion of a service is performed on the **Resource** URL. When we created the service, we defined a Declarative state to the iApp template which subsequently created the configuration and all of its associated objects. With a **DELETE** request, BIG-IP will process the removal of all objects linked to the ASO in a recursive manner. This is crucial to Application Lifecycle Management as it provides a mechanism to make sure all parts of the service are removed successfully.

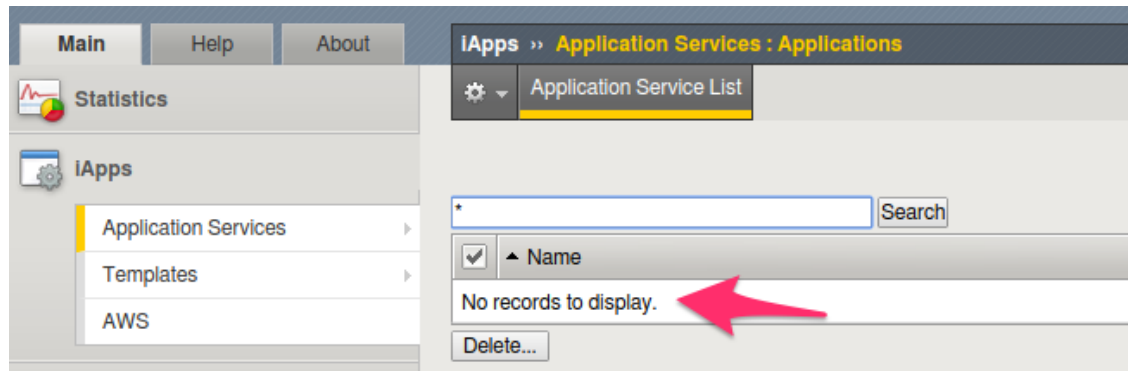
Note: There is no JSON body to a **DELETE** call, as the HTTP Method is defining the action.

Now that the service has been deleted, let's review the BIG-IP configuration. You can review via REST by sending the Step 1: Get Deployed iApp Services request again, or you can login to the BIG-IP A GUI to observe the service deployment via TMUI:

- **REST:** *Send* Step 1: Get Deployed iApp Services request:



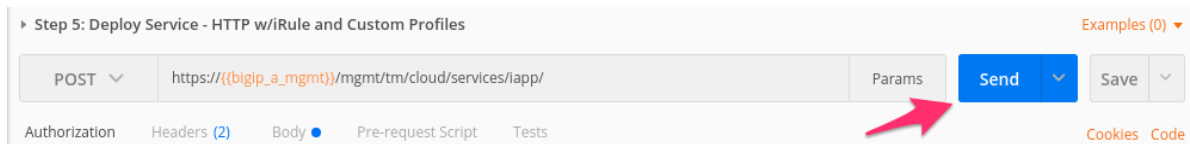
- **TMUI GUI:** *iApps* → *Application Services* → *Applications*



Task 5 - Deploy an HTTP Service with Custom created Profile and a referenced iRule

Perform the following steps to complete this task:

1. **Send** the Step 5: Deploy Service - HTTP w/ iRule and Custom Profiles request to deploy an HTTP Service with Custom Profiles and an iRule:

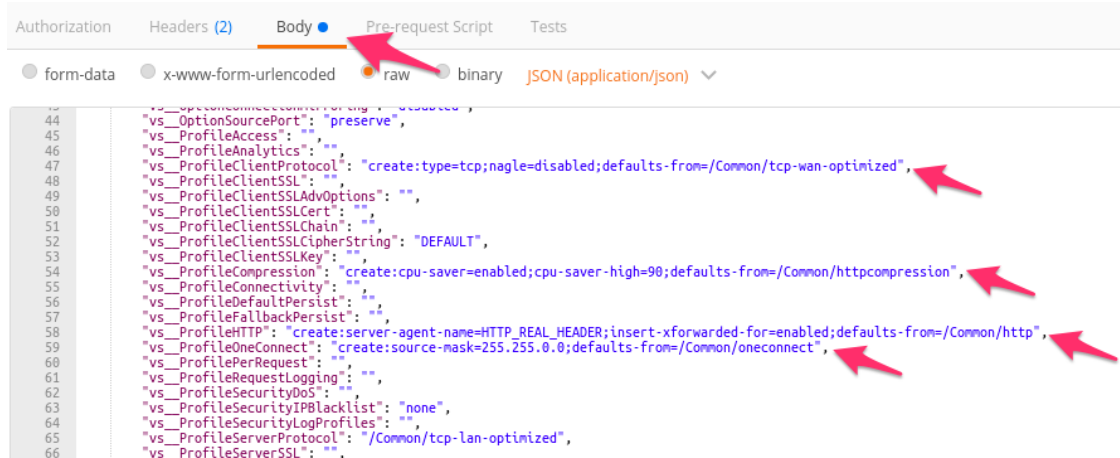


2. The App Services iApp can *Create* or *Reference* various objects. In this deployment we perform two actions:
 - (a) Create custom profiles on the BIG-IP device with various options specified. These profiles do not exist on the BIG-IP but are created dynamically during the deployment.
 - (b) Create an iRule on the BIG-IP device by using a **URL Reference**. The App Services iApp downloads the iRule resource from the URL and then creates a new iRule object on the system. The iRule object is then automatically linked to the Virtual Server

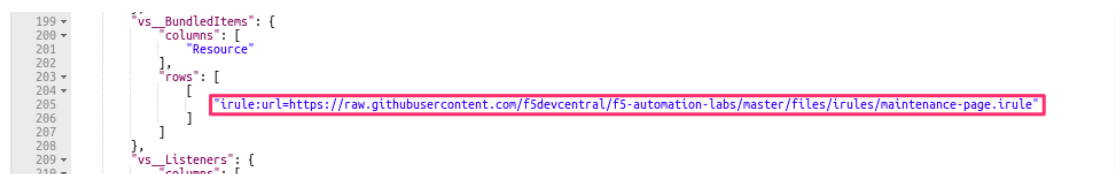
Warning: When using URL references, it is important to properly secure the repository which hosts the resource(s). The example in this lab uses a publicly readable repository, however, most environments should use a private repository with appropriate access control.

3. Review the **Request JSON Body** to see how the desired outcomes above were declared:

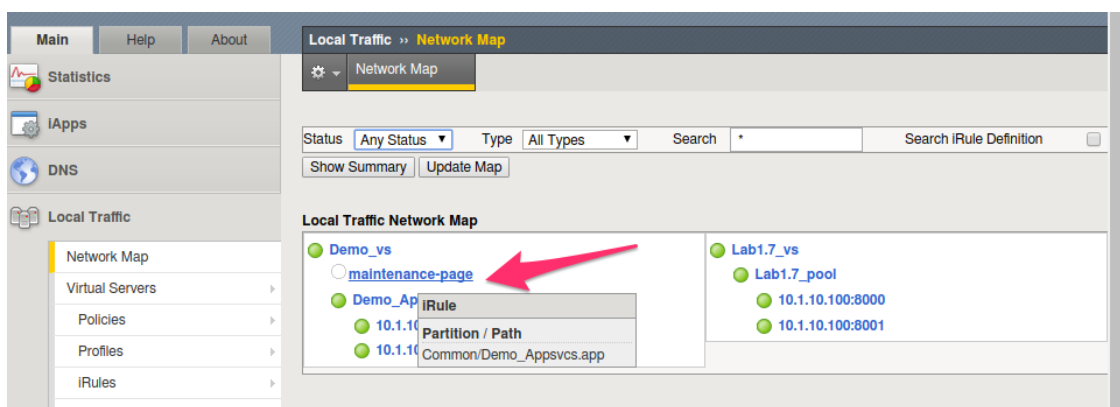
- **Custom Profiles:**



• URL Referenced iRule:



• iRule linked to Virtual Server: (Local Traffic → Network Map)



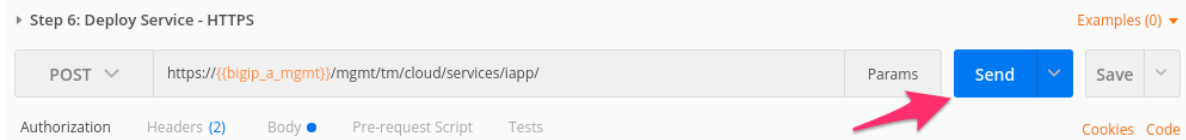
4. Open Chrome and connect to the Virtual Server at <http://10.1.20.121>. The iRule that was attached to the service contains an HTTP_RESPONSE event, which responds with a simple Maintenance Page.



Task 6 - Deploy an HTTPS Service

Perform the following steps to complete this task:

1. **Send** the Step 6: Deploy Service - HTTPS request to deploy an HTTPS Service using **URL Resources** for the SSL/TLS Key, Certificate and Certificate Bundle.



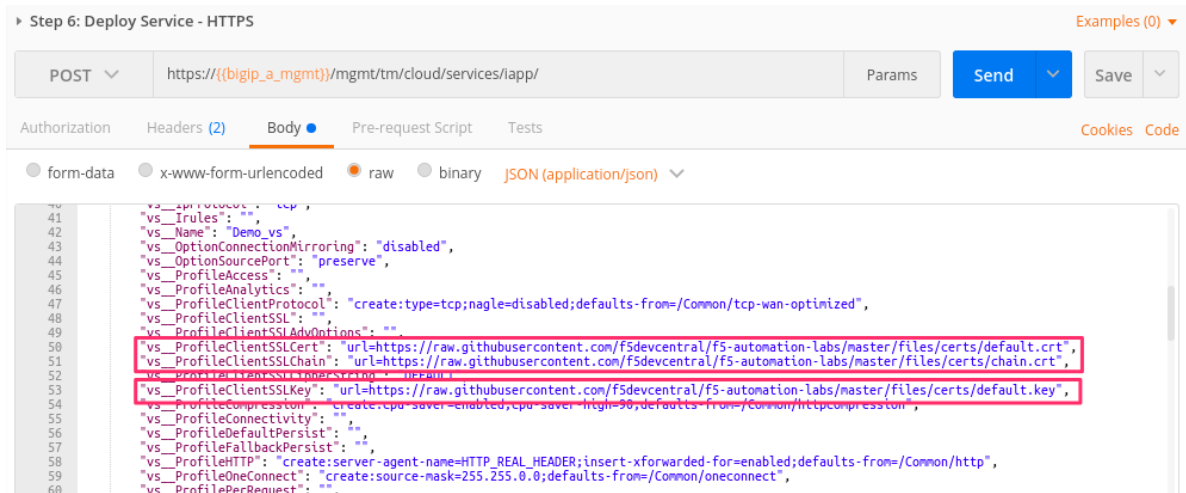
2. iApps are a Declarative interface, allowing us to modify deployment without the need to delete it (this also means we can re-name objects **if** we needed too). For this service we will:

- Use the same custom profiles
- Remove the iRule
- Change the Listener port to 443 (HTTPS)
- Use URL Resources to obtain the SSL/TLS Key, Certificate and Certificate Bundle

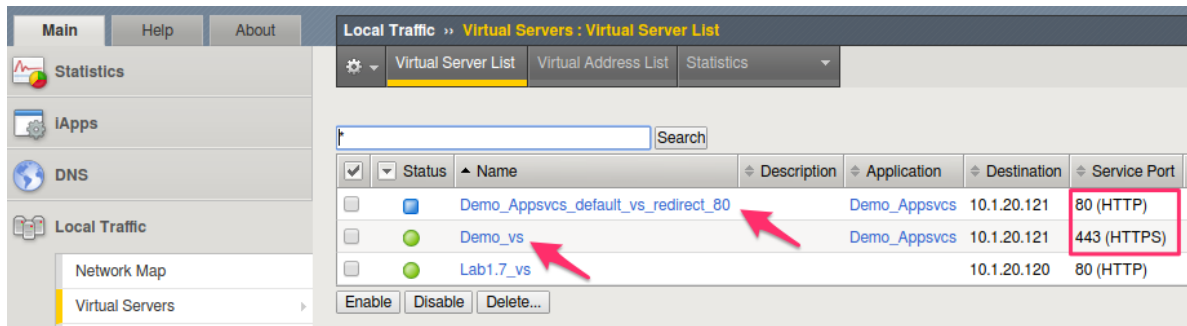
Warning: When using URL references, it is important to properly secure the repository which hosts the resource(s). The example in this lab uses a publicly readable repository. However, most environments should use a private repository with appropriate access control.

- Create and apply a Client SSL Profile

3. Review the **Request JSON Body** to see how the desired outcomes above were declared:



4. Review the configured Virtual Servers in the TMUI GUI. The App Services iApp created a new Virtual Server to redirect TCP / 80 traffic to TCP / 443 and reconfigured the Virtual Server to listen on TCP / 443



5. The configuration of the Virtual Server now uses an SSL Client profile containing our imported SSL Resources. The deployment is now providing SSL Offload for the backend compute nodes.

Local Traffic » Virtual Servers : Virtual Server List » Demo_vs

Properties Resources Security Statistics

General Properties

Name	Demo_vs
Application	Demo_Appsvcs
Partition / Path	Common/Demo_Appsvcs.app
Description	
Type	Standard
Source Address	0.0.0.0/0
Destination Address/Mask	10.1.20.121
Service Port	443 HTTPS
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
Availability	Available (Enabled) - The virtual server is available
Synccookie Status	Off
State	Enabled

Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	Demo_Appsvcs_profile_tcp_clientside
Protocol Profile (Server)	tcp-lan-optimized
HTTP Profile	Demo_Appsvcs_profile_http
FTP Profile	None
RTSP Profile	None
SSH Proxy Profile	None
SSL Profile (Client)	<div> <div>Selected</div> <div> / Common / Demo_Appsvcs.app Demo_Appsvcs_clientssl </div> </div> <div> <div>Available</div> <div> / Common clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl </div> </div>

- Open Chrome and access the service with `http://10.1.20.121`. It should redirect you to `https://10.1.20.121`.

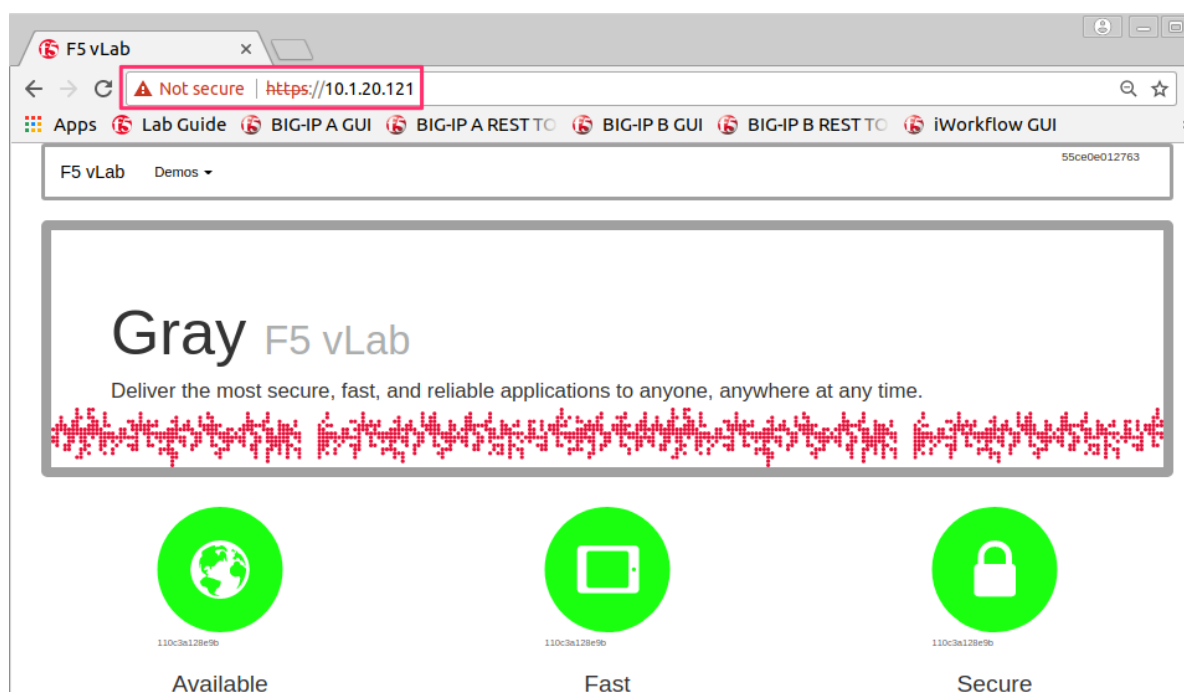
Note: We are using self signed certificates in the lab so an SSL warning will be shown.

Important: RFC2616 (HTTP/1.1) allows for a TCP session to stay open. Had we not included “noserver Cache-Control no-cache *Connection Close*” in the iRule the following would have happened:

When you would have refreshed the page, the maintenance page would still appear because of two reasons:

- (a) Chrome keeps HTTP connections open in the background to improve network performance
- (b) BIG-IP maintains a fully versioned configuration internally. Stateful connections, like HTTP, are then pinned to a specific version of the configuration for the lifetime of the connection.

As a result, because Chrome has not closed the actual TCP connection, BIG-IP still processes traffic with the configuration that was present when the connection was originally created. That *stale* connection was still using the version of the configuration with the iRule attached to the Virtual Service resulting in the maintenance page being shown.

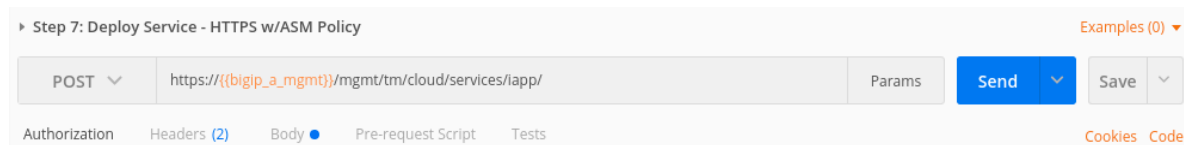


Task 7 - Deploy an HTTPS Service with an Web Application Firewall Policy

Another advantage of Service Deployment using iApp Templates is that they can deploy advanced Layer 4-7 services from various F5 modules. In this task we will deploy a service that includes a Web Application Firewall policy with the base HTTPS offload and load balancing features.

Perform the following steps to complete this task:

1. **Send the Step 7: Deploy Service - HTTPS w/ WAF Policy** request to deploy an HTTPS Service using **URL Resources** for a Web Application Firewall policy that will be used with the Application Security Manager (ASM) module.

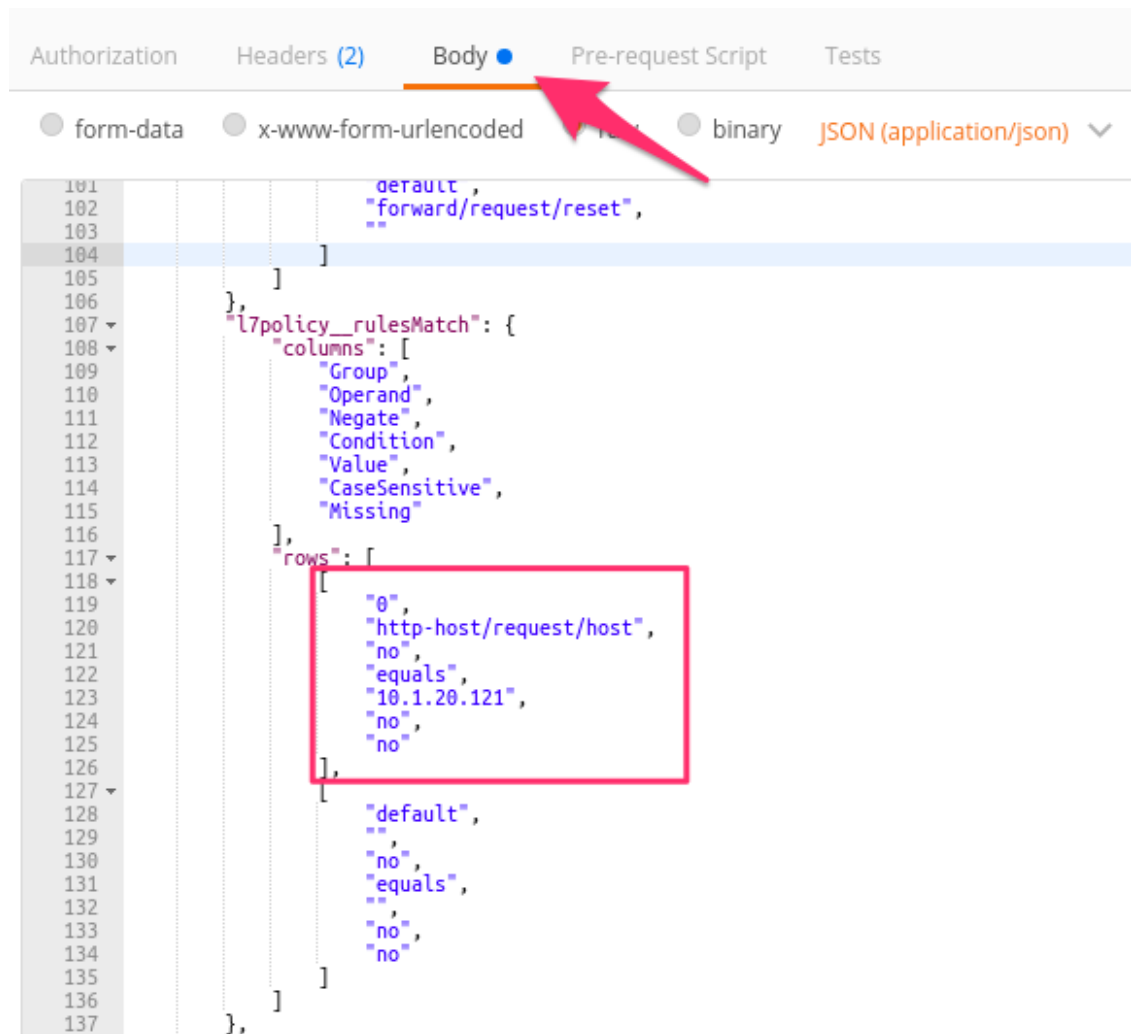


2. This final iApp deployment will build upon our service by having the iApp load a WAF policy Resource from our repository. The App Services iApp will then create a Layer 7 Traffic Policy and apply it to the Virtual Server.

This deployment recognizes the need for Security from the beginning of the application lifecycle. It lays the groundwork for **Continuous Improvement** by having the policy reside in a repository. It allows us to treat resources as code leading to an Infrastructure as Code (IaC) methodology. As the policy is updated in the repository, additional automation and orchestration can be enabled to deploy the policy into the environment. The result is an ability to rapidly build, test and iterate Layer 7 security policies and guarantee deployment into the environment.

3. Review the **Request** JSON *Body* to see how the desired outcomes above were declared:

- **Layer 7 Policy Rules:**



- **Layer 7 Policy Actions:**

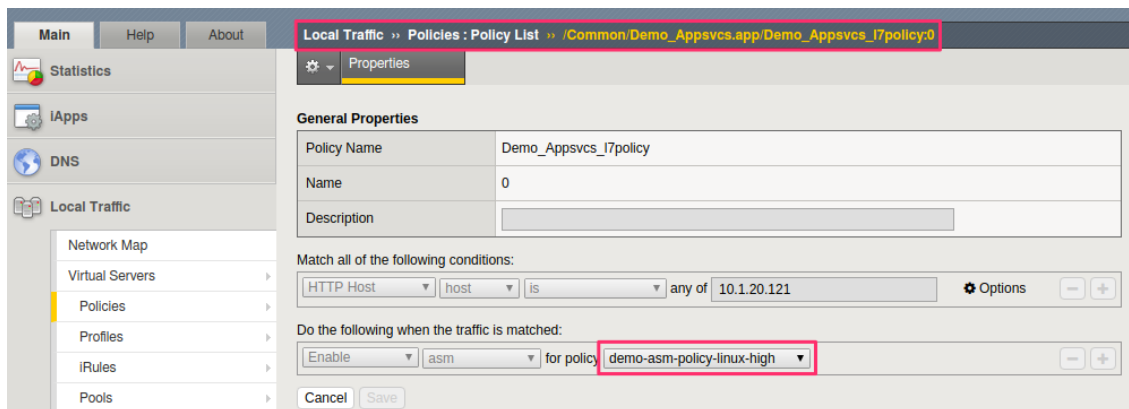


- **ASM Policy URL:**

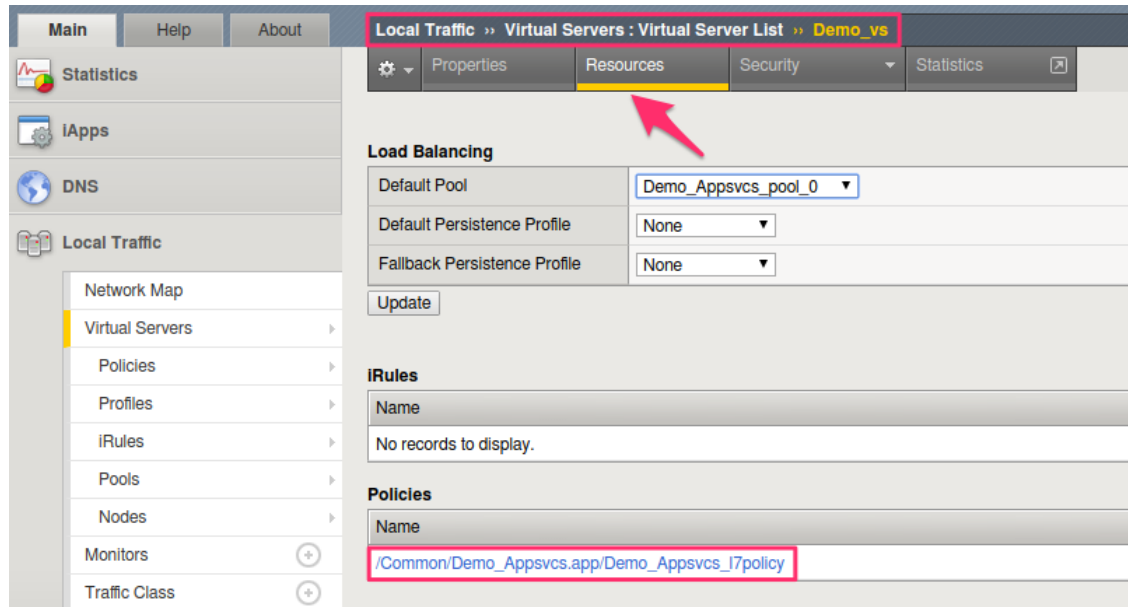


4. In the TMUI GUI, you will notice a Layer 7 policy has been applied to the Virtual Server. In *Application Security*, we will be able to observe that the policy is being dynamically fetched, applied, and set to Blocking mode.

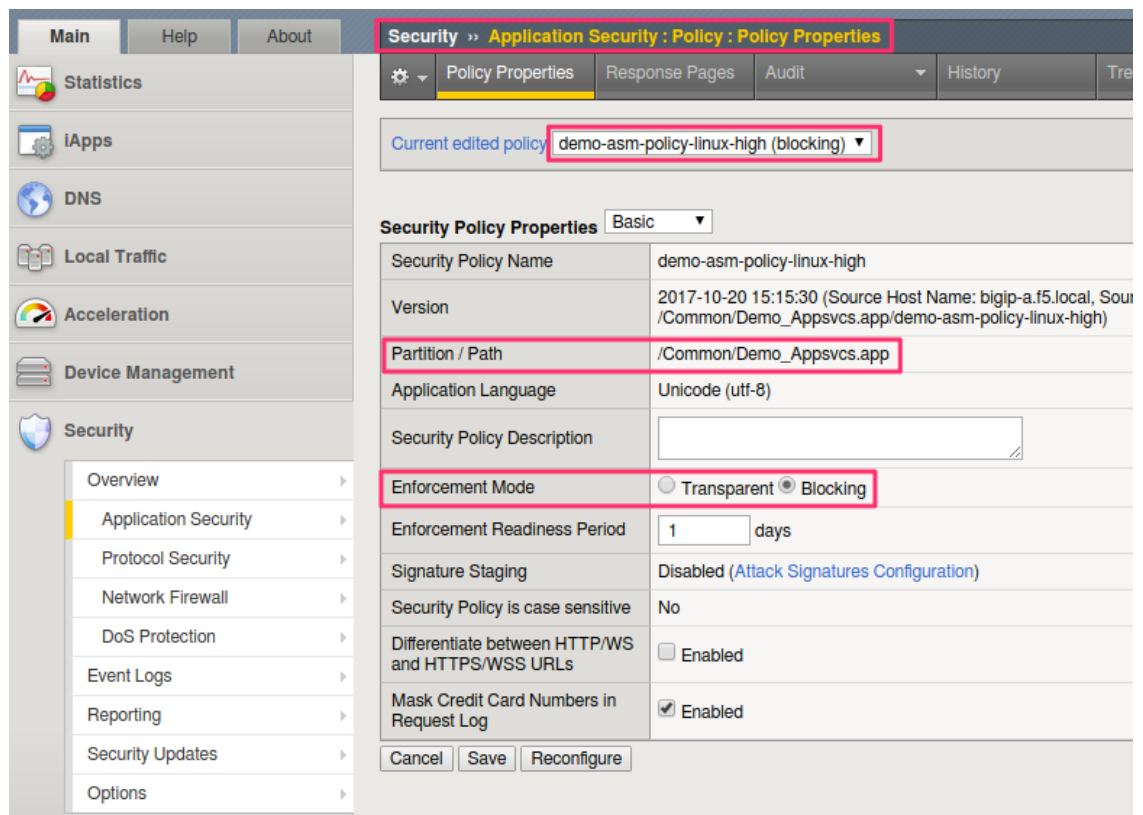
- **Layer 7 Policy:**



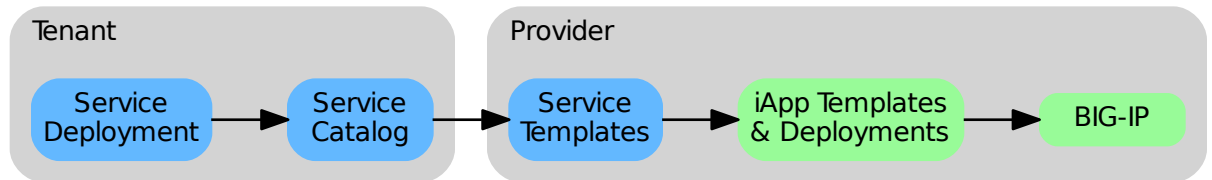
- **Layer 7 Policy attached to Virtual Server:**



- **ASM WAF Policy:**



2.5 Module 3: Creating Declarative Service Interfaces with iWorkflow



2.5.1 Overview

In this module we will explore how to use F5's iWorkflow platform to further abstract Application Services and deliver those services, with a **Declarative** interface to Consumers.

When moving to an iWorkflow based toolchain it's important to understand that automation in L1-3 (Device Onboarding, Networking, etc) and L4-7 (Deployment of Virtual Servers, Pools, etc) is separated and delivered by different features.

Layer 1-3 Networking and Device Onboarding

L1-3 Networking and Device Onboarding are highly specific to the particular environment the BIG-IP instances are deployed on. The onboarding process for various platforms and ecosystems is very different due to differences in the L1-3 capabilities and APIs of each platform. As a result F5 publishes specific documentation and guidance for each of these environments:

- Public Cloud:
 - **AWS/Azure/GCP/etc.:** <http://clouddocs.f5.com/cloud/public/v1/>
- Private Cloud:
 - **OpenStack:** <http://clouddocs.f5.com/cloud/openstack/>
 - **VMware:** <https://f5.com/solutions/technology-alliances/vmware>

iWorkflow enables generic functionality in all of these environments by using a **BIG-IP Cloud Connector**. This connector allows iWorkflow to utilize BIG-IP devices running on any of these environments.

Note: F5 BIG-IP also supports integration with Container Ecosystems. However, in these environments iWorkflow may not be required. For more information you can refer to:

- Container Ecosystems:
 - **Cloud Foundry:** <http://clouddocs.f5.com/containers/latest/cloudfoundry/>
 - **Kubernetes:** <http://clouddocs.f5.com/containers/latest/kubernetes>
 - **Mesos Marathon:** <http://clouddocs.f5.com/containers/latest/marathon>

Layer 4-7 Application Service Delivery

L4-7 Application Service Delivery is accomplished by:

- Consuming F5 iApp templates on BIG-IP devices and creating a Service Catalog (**Declarative**).
- Consuming the iWorkflow REST Proxy to drive API calls to BIG-IP devices (**Imperative**).

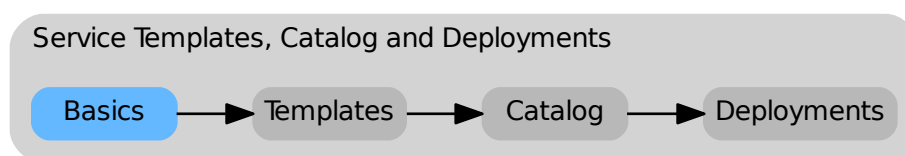
The labs in the module will focus on the high level features in place to achieve full L4-7 automation. As mentioned above, iApp Templates are a key component of the chain of linked tools (toolchain) we are building.

In this Module we will focus on building a **Service Catalog** using the App Services iApp template you learned about in Module 2. The focus in Module 2 was to show how to deploy advanced configurations. However, a large amount of F5 **Domain Specific Knowledge** was still required to build each deployment. From a conceptual point of view, iApp templates alone do not fully satisfy the requirement for a fully **Declarative** interface because while the iApp template simplifies the underlying **Imperative** actions, it does not allow the administrator to build an **Interface** that minimizes or eliminates the need for **Domain Specific Knowledge**.

For example, we deployed a service that enabled HTTP Traffic Management with an iRule attached and Profile Customizations. To the F5 administrator these are all very familiar terms, however, to a consumer, such as an Application Owner, the terms *Virtual Server*, *iRule*, *Profile*, etc. are foreign concepts.

To solve this problem iWorkflow allows the administrator to create a **Service Template** that is an **Abstraction** of the iApp templates input fields. By doing this the F5 administrator can **create an interface tailored to the use case and knowledge level of the CONSUMER rather than the ADMINSTRATOR**, enabling full featured and complex Layer 4-7 Application and Security services that are tailored to business need and use case rather than the technical implementation. Additionally, the **Service Abstraction** achieved when creating the **Service Catalog** enables the easy integration of F5 services with third-party tools and methodologies such as DevOps.

Lab 3.1: iWorkflow Onboarding



In this lab we will use the *Runner*, introduced in previous labs to complete the onboarding of the F5 iWorkflow device. The onboarding process creates the initial configuration required to start creation of Service Catalog Templates.

iWorkflow Overview

Before looking at the details of the onboarding process, let's discuss the new components iWorkflow introduces to our toolchain.

Device Discovery

In order for iWorkflow to interact with a BIG-IP device it must be discovered by iWorkflow. The device discovery process leverages the existing CMI Device Trust infrastructure on BIG-IP. Currently there is a limitation that a single BIG-IP device can only be 'discovered' by ONE of iWorkflow or BIG-IQ CM at a time. In this lab we will discover the existing BIG-IP devices from your lab environment.

Tenants & Connectors

iWorkflow implements a Tenant/Provider interface to enable abstracted deployments of L4-7 Services into various environments. In conjunction, iWorkflow Connectors serve as the L1-3 Network and Device Onboarding automation component in the automation toolchain. In this lab we will create a 'BIG-IP Connector' for the BIG-IP devices in the lab environment. This connector will then allow you to drive a fully automated deployment from the iWorkflow Service Catalog.

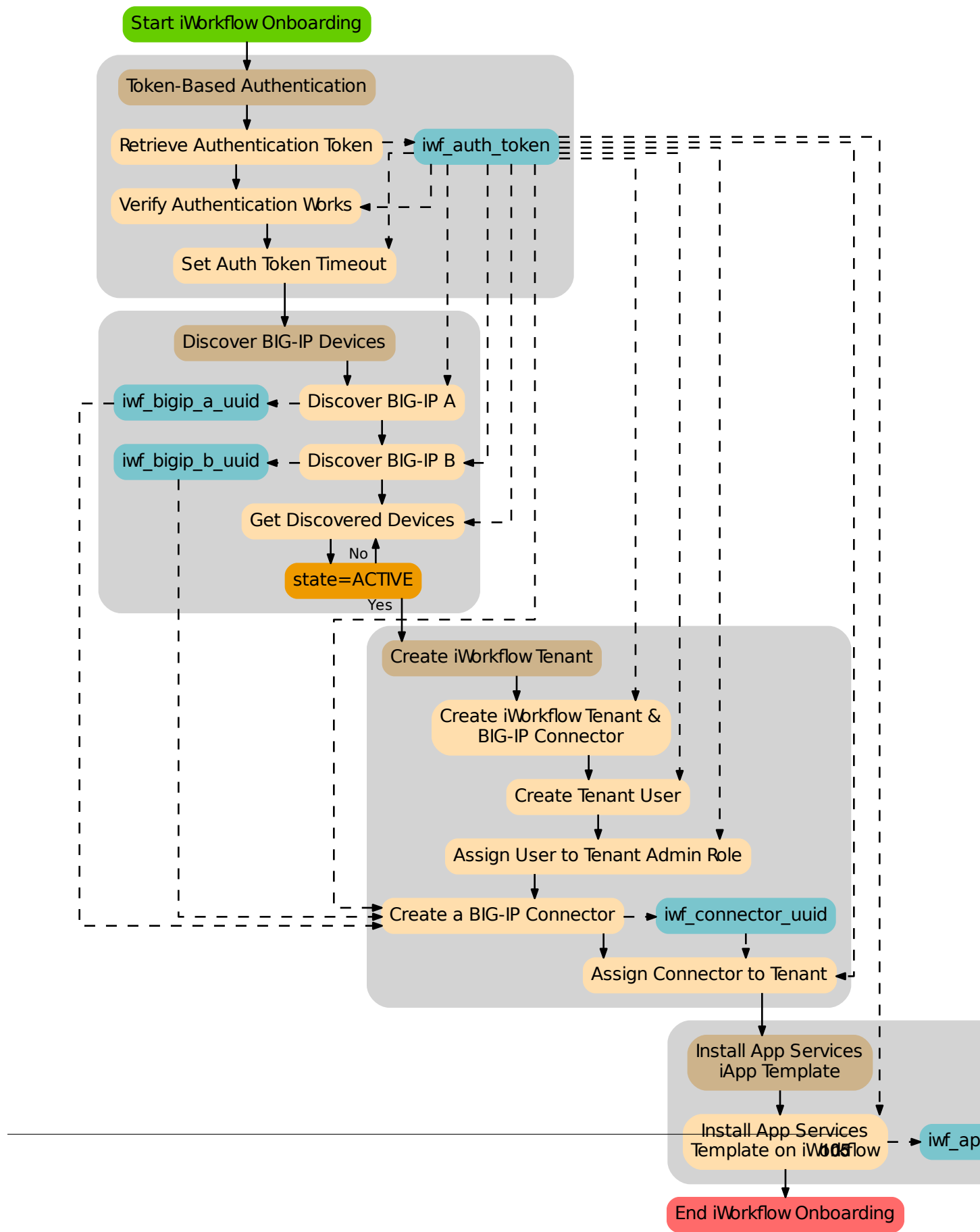
iApp Templates

iWorkflow serves as an iApp Template Source-of-Truth for discovered BIG-IP devices. This allows an F5 administrator to manage iApp templates in a single place with iWorkflow installing required templates on BIG-IP devices as required **during** service deployment.

Onboarding Process Overview

The process implemented in the `Lab 3.1 - iWorkflow Onboarding` folder of the Postman collection is diagrammed below.

Note: The diagram below represents environment variables in blue. You can follow the lines on each variable to understand which request populates the variable and how they are subsequently used.

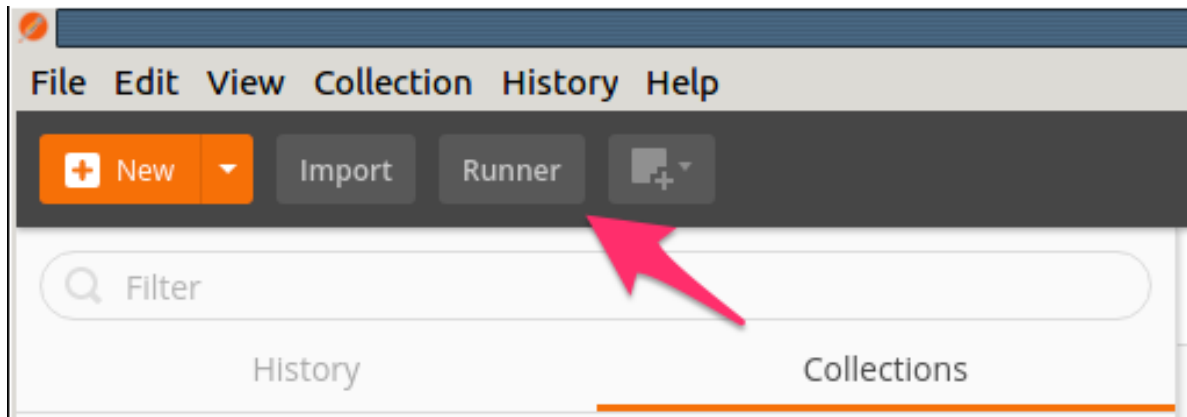


Task 1 - Onboard iWorkflow using Runner

In this task we will use the *Runner* to execute a series of requests contained in the Lab 3.1 - iWorkflow Onboarding folder.

Perform the following steps to build the cluster:

1. Click the *Runner* button at the top left of your Postman window:



2. Select the F5 Programmability: Class 1 Collection then the Lab 3.1 - iWorkflow Onboarding folder. Next, be sure the environment is set to F5 Programmability: Class 1:

Collection Runner

Choose a collection or folder:

< Lab 3.1 - iWorkflow Onboarding

Token-Based Authentication

Discover BIG-IP Devices

Create Tenant & BIG-IP Connector

Install App Services iApp Template

Environment

F5 Programmability: Class 1

Iterations

1

Delay

0

ms

Log Responses

For all requests



Data

Select File



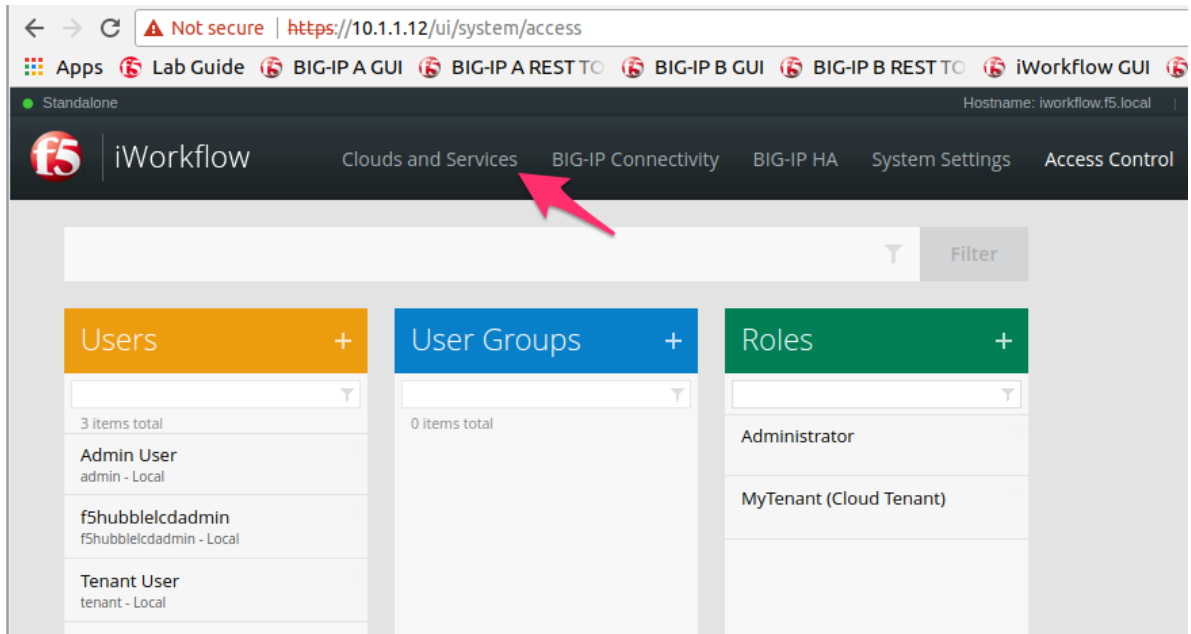
Persist Variables

Run Lab 3.1 - iWor...

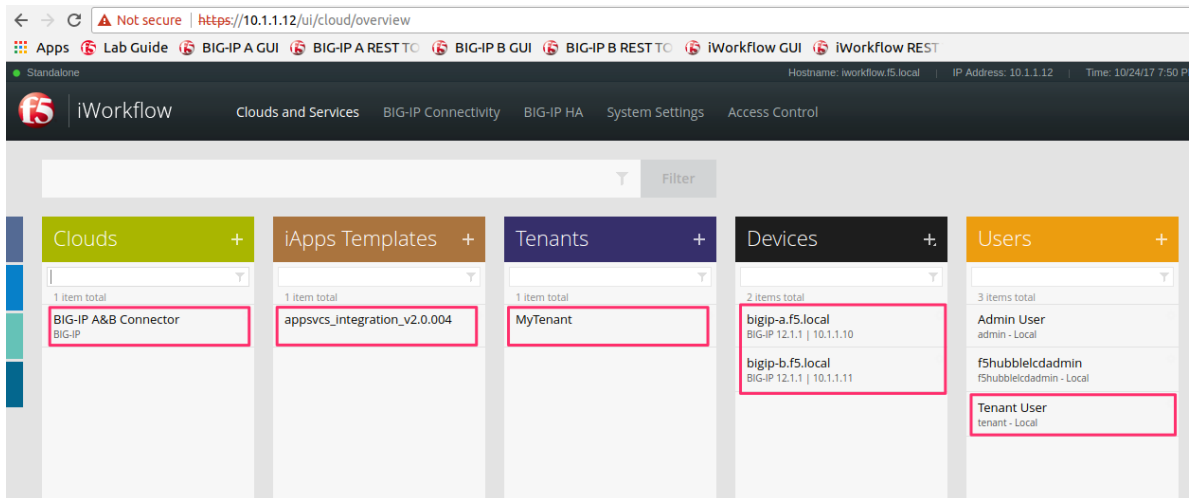
3. Click the *Run Lab 3.1 - iWor...* button
4. The results window will now populate. You will see each request in the folder is sent and it's associated test results are displayed on the screen. Onboarding iWorkflow can take a few minutes. You can follow the progress by scrolling down the results window.
5. Once the *Run Summary* button appears the folder has finished running. You should have 0 failures and the last item in the request list should be named *Install App Services Template on iWorkflow*

The screenshot displays the 'Run Results' interface for a lab titled 'Lab 3.1 - iWorkflow Onboarding'. At the top, there are tabs for 'Collection Runner' and 'Run Results', along with buttons for 'Run In Command Line' and 'Docs'. The summary bar indicates 210 passed tests and 0 failed tests, with a 'Run Summary' button highlighted in orange. Below the summary, the results for 'Iteration 1' are listed. The list includes several 'PASS' status items for various test steps, followed by a 'PATCH' step 'Step 5: Assign Connector to Tenant'. The final item in the list is a 'POST' request 'Install App Services Template on iWorkflow', which is highlighted with a red box and a red arrow. The 'Run Summary' button is also highlighted with a red box and a red arrow.

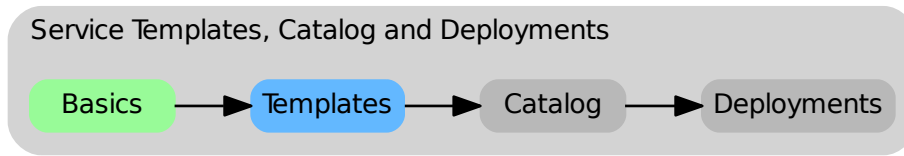
6. At this point you can log into iWorkflow using Chrome at <https://10.1.1.12> and `admin/admin` credentials. Click *Clouds and Services* at the top of the window:



7. Browse the various panes to see what was created:



Lab 3.2: Create a Declarative Service Catalog



In the introduction to this module we discussed the importance of using **Service Templates** to build a **Declarative Service Catalog**. This lab will show to create a few examples of **Service Templates** (Templates). It's important to understand that while the packaged examples used in this lab are great starting points, you should use them as a starting point for creating your own **Service Catalog** that meets the requirements of your environment.

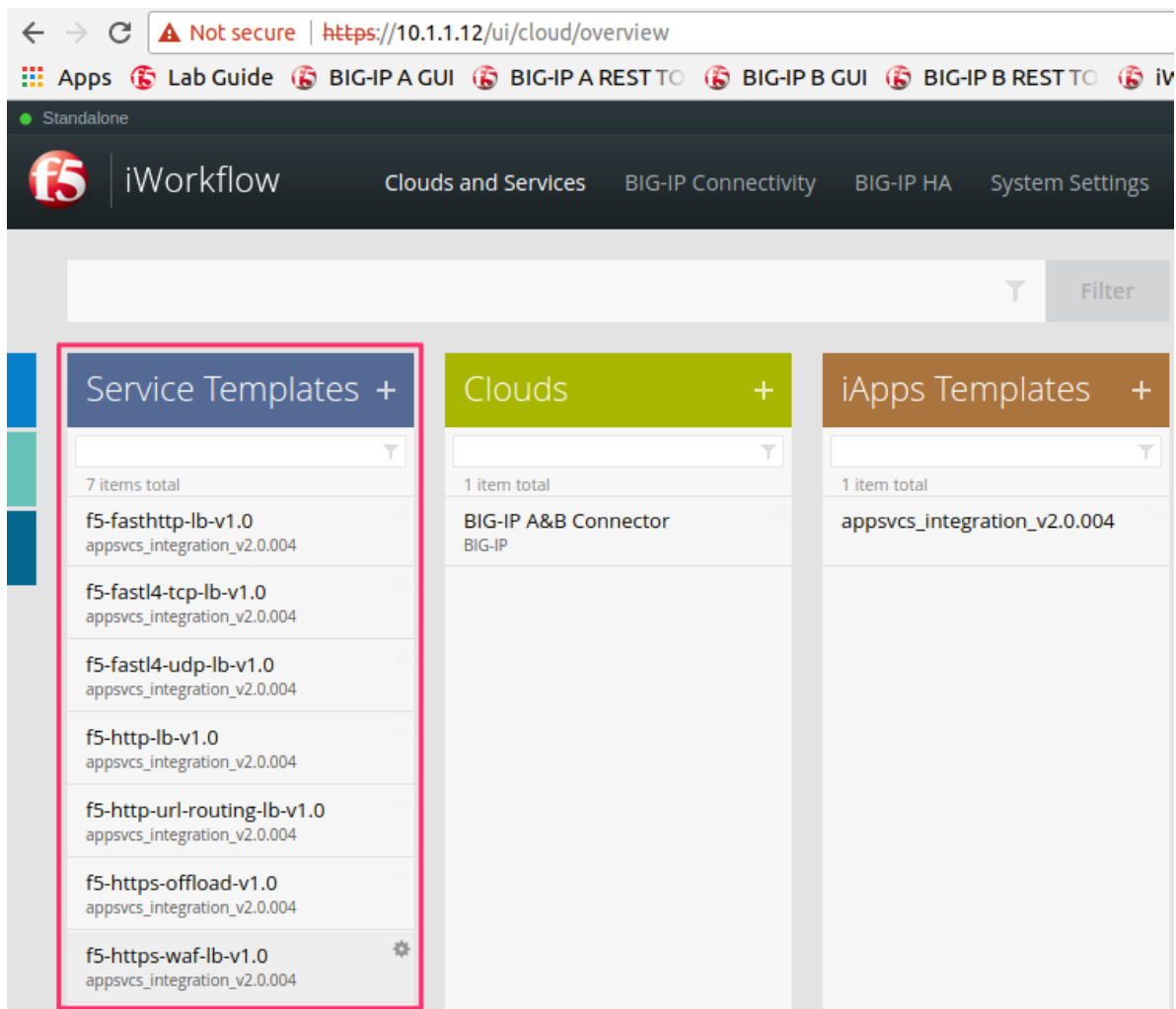
We will explore the first example in depth so you can gain an understanding of how the templates are structured. For the remaining templates you can just repeat the steps used with the first example.

The templates used in this lab all have a version number appended to the name (Example: `f5-http-lb-v1.0`). It's important that this pattern is followed in your environment. Explicitly versioning the templates allows for migration between template versions in a stable manner. Without versioning any changes to the template could result in *every* deployment associated with the template being modified at the same time. With versioning, the application owner or F5 administrator can choose to either migrate all deployments at the same time OR perform the migration on a per deployment manner.

Task 1 - Create the Service Templates

In this task we will use the Runner to quickly create our sample Service Templates. Perform the following steps to complete this task:

1. Click the *Runner* button at the top left of your Postman window.
2. Select *F5 Programmability: Class 1* → *Lab 3.2 - Create a Declarative Service Catalog* folder.
3. Select the *F5 Programmability: Class 1* environment
4. Click the *Run Lab 3.2 - Crea...* button and wait for the run to complete. Verify no errors were encountered.
5. Open the iWorkflow GUI in Chrome by navigating to `https://10.1.1.12`
6. Expand the *Service Templates* panel and verify all the templates have been created:



Task 2 - Explore the f5-http-lb-v1.0 Template

Now that we've created our Templates let's review one of them in depth.

Perform the following steps to complete this task:

1. Open the `f5-http-lb-v1.0` Template by double clicking it:

Service Templates + f5-http-lb-v1.0 Delete Tenant Preview Save Cancel

7 items total

- f5-fasthttp-lb-v1.0
appsvcs_integration_v2.0.004
- f5-fastl4-tcp-lb-v1.0
appsvcs_integration_v2.0.004
- f5-fastl4-udp-lb-v1.0
appsvcs_integration_v2.0.004
- f5-http-lb-v1.0**
appsvcs_integration_v2.0.004
- f5-http-url-routing-lb-v1.0
appsvcs_integration_v2.0.004
- f5-https-offload-v1.0
appsvcs_integration_v2.0.004
- f5-https-waf-lb-v1.0
appsvcs_integration_v2.0.004

Properties

iApps Template - Name & Version	appsvcs_integration_v2.0.004
Name	f5-http-lb-v1.0
Cloud Availability	All Clouds
Displayed Parameters	<input checked="" type="radio"/> Tenant Editable and Service Tier <input type="radio"/> All

Sections

Virtual Server Listener & Pool Configuration

Name	Description	Default Value	<input type="checkbox"/> Tenant Editable
------	-------------	---------------	--

- Let's examine the *Properties* pane.
- Select *All* in the *Displayed Parameters* section:

f5-http-lb-v1.0 Delete

Properties

iApps Template - Name & Version	appsvcs_integration_v2.0.004
Name	f5-http-lb-v1.0
Cloud Availability	All Clouds
Displayed Parameters	<input type="radio"/> Tenant Editable and Service Tier <input checked="" type="radio"/> All

- This pane shows detailed information about the Template such as:
 - iApp Template Name & Version the Service Template is using
 - The Connectors/Clouds that may use this template
 - A control that toggles which Parameters are displayed in the pane
 - The input Sections and Fields (collapsed in screenshot) for the iApp Template

f5-http-lb-v1.0

Delete
Tenant Preview
Save
Cancel

Properties

iApps Template - Name & Version	appsvcs_integration_v2.0.004
Name	f5-http-lb-v1.0
Cloud Availability	All Clouds ▼
Displayed Parameters	<input type="radio"/> Tenant Editable and Service Tier <input checked="" type="radio"/> All

▶ Service Tier Information

Sections Expand All

▶ Custom Extensions Section	3/3
▶ L4-7 Helpers	7/9
▶ iApp Options	7/7
▶ L7 Traffic Policy	3/13
▶ Virtual Server Listener & Pool Configuration	5/19
▶ Virtual Server Configuration	36/39
▶ Pool Monitor(s) Configuration	0/4

5. In the *Sections* portion of the pane, find the *Virtual Server Listener & Pool Configuration* section. Click the triangle to expand the section:

▶ L7 Traffic Policy 3/13

▼ Virtual Server Listener & Pool Configuration 5/19

Name	Description	Default Value	<input type="checkbox"/> Tenant Editable
------	-------------	---------------	--

6. You can now see all the input fields associated with this section of the iApp template. These fields are defined by the iApp Template itself. In the previous lab, when we installed the App Services iApp Template, iWorkflow created an internal representation of the input fields used in the iApp template. iWorkflow then allows you to create a template that:

- Define which fields are `Tenant Editable`, therefore exposed to the Tenant interface
- Setting a default value for the field

- If the field is NOT `Tenant Editable` the default value is sent during a Service Deployment, however, the Tenant cannot see or modify the value
- If the field is `Tenant Editable` the default value is populated for the Tenant and the Tenant may edit it during a Service Deployment

Name	Description	Default Value	<input type="checkbox"/> Tenant Editable
pool__DefaultPoolIndex	Virtual Server: Default Pool Index	0	<input type="checkbox"/>
pool__MemberDefaultPort	Pool: Member Default Port		<input type="checkbox"/>
pool__addr	Virtual Server: Address		<input checked="" type="checkbox"/>
pool__mask	Virtual Server: Mask	255.255.255.255	<input type="checkbox"/>
pool__port	Virtual Server: Port	80	<input checked="" type="checkbox"/>

In the case of the fields shown in the above example:

- `pool__DefaultPoolIndex`: A value of 0 will be sent during a deployment
- `pool__MemberDefaultPort`: Nothing will be sent
- `pool__addr`: Tenant will be allowed to populate the field with a value
- `pool__mask`: A value of 255.255.255.255 will be sent
- `pool__port`: Tenant will see 80 and can change the field

By combining different combinations of **Default Values** and `Tenant Editable` fields you can create many different types of templates to match your requirements.

Note: The App Services iApp Template has been specifically designed to integrate with iWorkflow and Automation use cases. While any iApp template that is properly versioned can be used with iWorkflow, you should consider whether the template was designed for Automation use cases or not. Many iApp templates were designed for a GUI or Wizard based interaction through the BIG-IP TMUI GUI. As a result those templates may not present a good API interface.

7. In addition to simple text fields, iApp templates also support table based input. The App Services iApp uses this capability to allow input of more complex data such as Pools, Pool Members and Layer 7 Routing Policies. iWorkflow allows you to have granular control over how the Tenant can interact with a table. Let's find the `pool__Pools` table and click the triangle to expand it:

Note: To accomodate screen size this screenshot does not show all the columns in the table.

The screenshot shows the 'Pool: Pool Table' configuration window. A red arrow points to the 'pool_pools' tab. Four numbered callouts highlight specific features:

- 1**: Points to the 'Min Rows' and 'Max Rows' fields, which are set to '0' and 'No Maximum' respectively.
- 2**: Points to the 'Column Default Value' field, which is set to '0'.
- 3**: Points to the 'Column Tenant Editable' checkbox, which is checked.
- 4**: Points to the 'Table Default Rows' field, which is set to '2'.

The highlighted sections in the image above correspond to the capabilities in the list below:

- [1] Definition of the *Min* and *Max* number of rows in a table
 - Example: Define a fixed number or limit for the number of Pools a Tenant can deploy
- [2] *Default Values* for each column in a table
 - Example: Define a default Load Balancing Method for deployed Pools
- [3] *Tenant Editable* flag for each column in the table
 - Example: Only allow the Tenant to control the Load Balancing Method and Name of a Pool, while defaulting all other values.
- [4] *Default Rows* that auto-populate a desired input for the Tenant. Each row can have a No Access, Read-Only or Write ACL applied.
 - Example: Define a Service that allows URL Based Content Routing to only two pools.
 - * Define 2 *Default Rows* in the Pools table
 - * Set the *Min* & *Max* value to 2

8. Finally, to assist in designing a Tenant interface, iWorkflow allows you to preview what the Tenant UI would look like for a Service Template. To view the preview, click the *Tenant Preview* button:

The screenshot shows the 'f5-http-lb-v...' service template interface. A red arrow points to the 'Tenant Preview' button. Below the button, the 'Properties' table is displayed:

iApps Template - Name & Version	appsvcs_integration_v2.0.004
Name	f5-http-lb-v1.0
Cloud Availability	All Clouds ▼
Displayed Parameters	<input type="radio"/> Tenant Editable and Service Tier <input checked="" type="radio"/> All

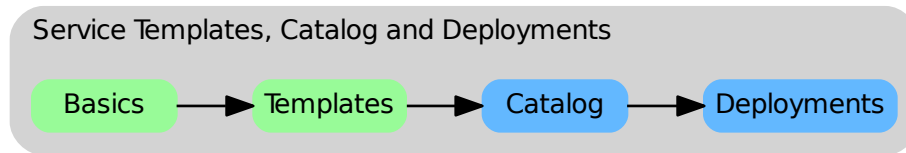
9. The preview window shows how the Tenant UI would present the Service Template. As you can see the interface is vastly simplified and only *Tenant Editable* fields are shown. Because the true deployment details are filtered from the Tenant, the Service Deployment requires much less **Domain Specific Knowledge**. Keep in mind that while the Tenant interface may be simple, you can still leverage advanced functionality in the Service Template.

Task 3 - Explore the Remaining Service Templates

Using the pattern in the last task explore the other Service Templates that were created earlier. A description of each Service Template is included in the table below. In all cases the Template has been configured with the appropriate Monitors, Profiles and Options for the use case.

Service Template	Description
f5-http-lb-v1.0	HTTP Load Balancing to a Single Pool
f5-https-offload-v1.0	HTTPS Offload and Load Balancing to a Single Pool
f5-fasthttp-lb-v1.0	Performance-enhanced HTTP Load Balancing to a Single Pool
f5-fastl4-tcp-lb-v1.0	Generic L4 TCP Load Balancing to a Single Pool
f5-fastl4-udp-lb-v1.0	Generic L4 UDP Load Balancing to a Single Pool
f5-http-url-routing-lb-v1.0	HTTP Load Balancing with URL Based Content Routing to Multiple Pools
f5-https-waf-lb-v1.0	HTTPS Offload, Web Application Firewall Protection and Load Balancing to a Single Pool

Lab 3.3: Deploy L4-7 Services



Up to this point we have spent a lot of time building our toolchain to create a Declarative Service Catalog. We are now at the point where we can perform a Declarative, Abstracted Service Deployment using the iWorkflow Tenant Service Catalog, Tenant API and optionally the built-in Tenant GUI.

As we did in the previous lab we will explore the first deployment in depth so you can implement a full Service Lifecycle: Create, Read, Update and Delete (CRUD) operations. For the remaining deployments you can just repeat the steps used with the first example.

Tenant Overview

iWorkflow Tenants allow Consumers to perform Service Lifecycle operations in an isolated environment. All actions performed prior to this lab have been in what's called the `Provider` space and, by nature, are masked from Tenants unless specifically exposed. As a result of the Tenant isolation, each Tenant maintains its own set of Users and Roles associated with those users, allowing each Tenant full control of the actions Tenant Users can perform.

During our iWorkflow Onboarding process in Lab 3.1 we created a *Tenant* named `MyTenant` and an associated *Tenant User* with a username of `tenant`. Additionally we gave `MyTenant` access to the *BIG-IP Connector* named `BIG-IP A&B Connector`:

The screenshot shows the 'Tenant Properties' form. On the left, a list of tenants is shown with 'MyTenant' selected. A red arrow points to this selection. The main form area displays the details for 'MyTenant'. It includes fields for Name (MyTenant), Description (My Tenant), and Access (Available Clouds: BIG-IP A&B Connector). A second red arrow points to the 'Available Clouds' dropdown menu. Below the Access section is the Contact Info section, which includes fields for Address, Phone, and Email.

This gives the `tenant` user the ability to perform CRUD operations on Service Deployments.

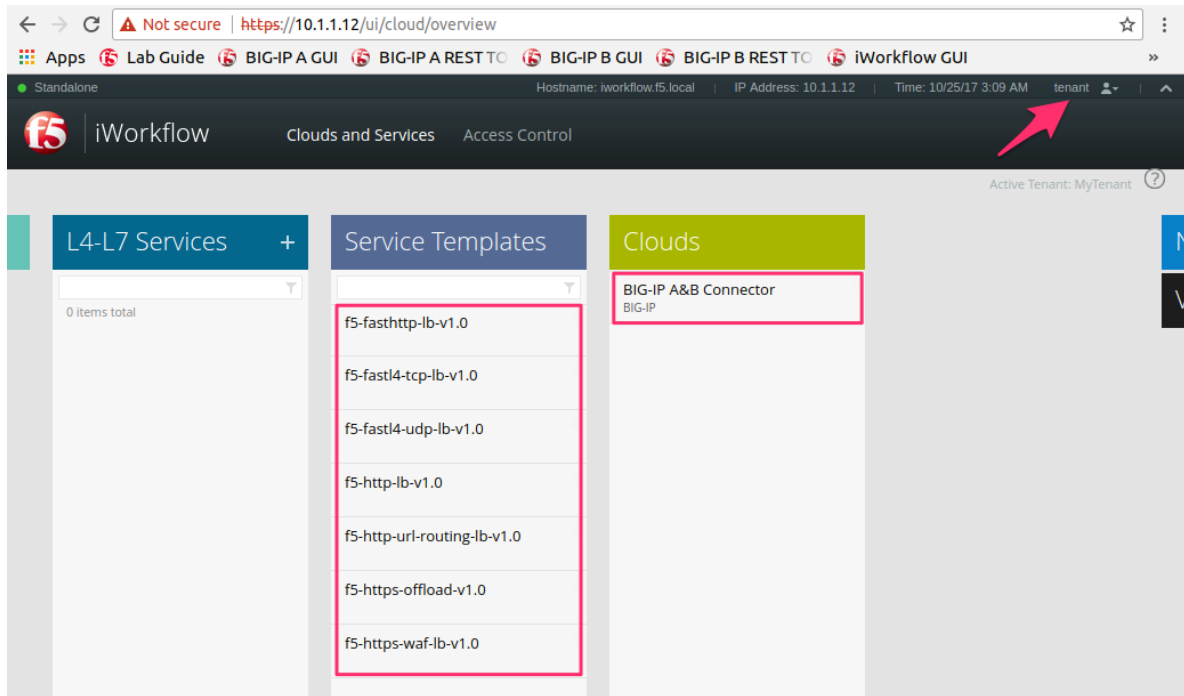
Note: Service Templates can also be assigned to specific Cloud Connectors, allowing you to restrict the use of Templates to a specific Tenant and set of BIG-IP resources.

Task 1 - Login to the iWorkflow Tenant UI

iWorkflow provides a Tenant UI that can act as a simple self-service portal for Tenants. In this lab we'll use the Tenant UI to monitor the results of various actions we take via the iWorkflow Tenant API.

Perform the following steps to complete this task:

1. Open a new Chrome window/tab and connect to `https://10.1.1.12`
2. Use the `MyTenant` Tenant User credentials to login:
 - Username: `tenant`
 - Password: `tenant`
3. You will see a user interface that looks similar to the Provider UI, however, the access is limited to Tenant specific objects. You can see a list of available *Service Templates* and *Clouds* with their associated Connectors:



Task 2 - Authenticate to the iWorkflow Tenant API

As described above, the Tenant interfaces to iWorkflow maintain their own access control mechanisms. As a result, when performing operations via the Tenant API you must authenticate with a Tenant User (`tenant` in this case).

Perform the following steps to complete this task:

1. In Postman expand the `Lab 3.3 - Deploy L4-7 Services` folder in the collection.
2. Click the `Authenticate and Obtain Token for Tenant User` request and examine the JSON request *Body*. Notice that we are sending the credentials for the Tenant User (`tenant`). This request will automatically populate the `iwf_tenant_auth_token` variable in the Postman environment so it can be used by subsequent requests.
3. Click the `Send` button on the `Authenticate and Obtain Token for Tenant User` request. Check the *Test Results* tab to ensure the token was populated.
4. Click the `Set Tenant Authentication Token Timeout` request and click the `Send` button. This request will increase the timeout value for the token so we can complete the lab without having to re-authenticate.

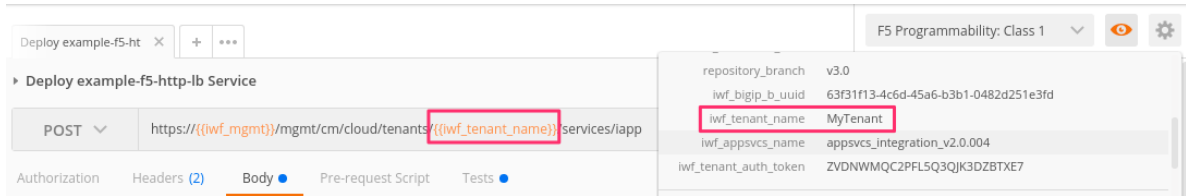
Task 3 - Perform Service Lifecycle Operations

In this task we will perform CRUD operations on Service Deployments demonstrating a full Service Lifecycle for a Tenant Service.

Create

Perform the following steps to complete this task:

1. Click the Deploy example-f5-http-lb Service request in the folder.
2. Examine the URI. Notice that the variable `iwf_tenant_name` is used to specify the Tenant we are performing the operation on. In this case `iwf_tenant_name` is set to `MyTenant` in the Postman environment:



3. Examine the JSON Request *Body*; it contains the following data:
 - Deployment name
 - A URI Reference to the Service Template `f5-http-lb-v1.0`
 - The input `vars` and `tables` for the deployment. These fields were marked `Tenant Editable` in the Service Template
 - A URI Reference to the Connector to use for deployment. This specifies which BIG-IP devices will be used for this deployment

The data in the list above is highlighted below:



4. Click the *Send* button to **Create** the Service Deployment
5. Switch to the Chrome iWorkflow Tenant UI window. The `example-f5-http-lb` Service is now present in the *L4-L7 Services* pane. Double click the Service and examine its properties. You can compare the values in the UI to the JSON Request *Body* from the step above.

L4-L7 Services + **example-f5-http-lb** Save Delete Cancel

1 item total

example-f5-http-lb
MyTenant
active member cnt: 1
clientside-bits in: 0

Properties **Statistics**

General Properties

Name	example-f5-http-lb
Status	
L4-L7 Service Template	f5-http-lb-v1.0
Cloud	BIG-IP A&B Connector

Customize L4-L7 Server Template

Virtual Server: Address	10.1.20.122
Virtual Server: Port	80
Pool: Members	
Min Rows: 0	
Max Rows: No Maximum	

IPAddress	State		
10.1.10.100	enabled	+	x
10.1.10.101	enabled	+	x

- Open a Chrome window/tab to the BIG-IP A GUI at <https://10.1.1.10> and login with admin/admin credentials. Navigate to *iApps* → *Application Services*. Select *example-f5-http-lb* from the list of deployed services and examine the *Components* of the deployed service:

iApps » Application Services : Applications » example-f5-http-lb

Properties **Reconfigure** **Components**

Name	Availability	Type
BIG-IP		
example-f5-http-lb		Application Service
example-f5-http-lb	Available	Virtual Server
example-f5-http-lb_pool_0	Available	Pool
http		Monitor
10.1.10.100:80	Available	Pool Member
10.1.10.100	Unknown	Node
10.1.10.101:80	Available	Pool Member
10.1.10.101	Unknown	Node
10.1.20.122%0		Virtual Address
example-f5-http-lb_profile_http		Profile
tcp-wan-optimized		Profile
publish_stats		icall_periodic_handler
publish_stats		icall_script
postdeploy_final		icall_script

Enable Disable Force Offline Refresh

Update

Perform the following steps to complete this task:

- Click the *Modify example-f5-http-lb Service request* in the folder.

2. We will send a `PUT` request to the Resource URI for the existing deployment and add a Pool Member as shown in the JSON Request *Body*:



3. Click the *Send* button to **Update** the Service Deployment.
4. Update the iWorkflow Tenant UI and notice that the Service has been updated:

example-f5-http-lb

SaveDeleteCancel

Properties
Statistics

General Properties

Name	example-f5-http-lb		
Status			
L4-L7 Service Template	f5-http-lb-v1.0		
Cloud	BIG-IP A&B Connector		

Customize L4-L7 Server Template

Virtual Server: Address	10.1.20.122		
Virtual Server: Port	80		

	IPAddress	State	
Pool: Members Min Rows: 0 Max Rows: No Maximum	10.1.10.100	enabled	+ x
	10.1.10.101	enabled	+ x
	10.1.10.102	enabled	+ x

5. Update the BIG-IP GUI and notice that the *Components* tree has been updated:

IApps » Application Services : Applications » example-f5-http-lb

Properties
Reconfigure
Components

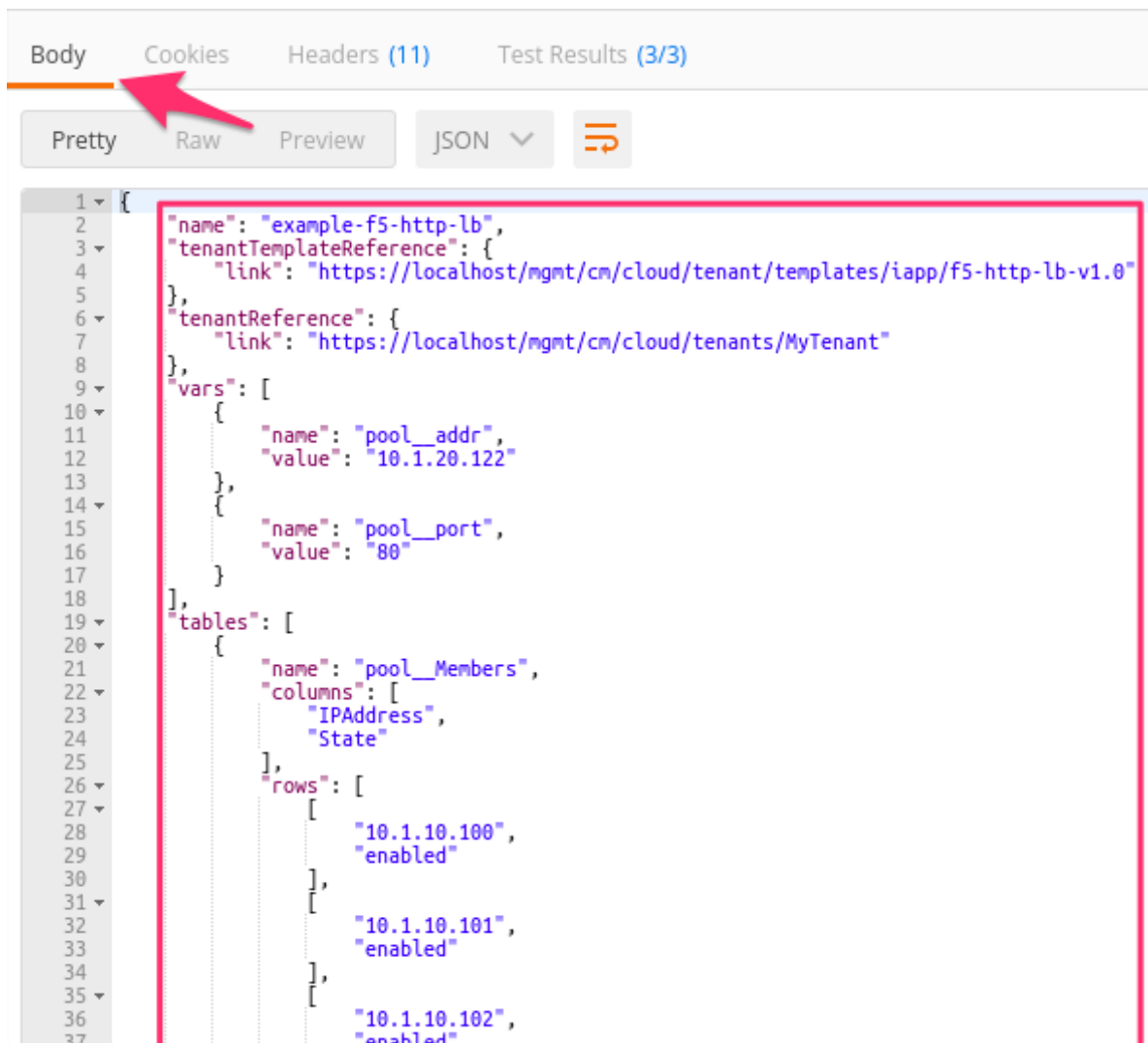
Name	Availability	Type
BIG-IP		
example-f5-http-lb		Application Service
example-f5-http-lb	Available	Virtual Server
example-f5-http-lb_pool_0	Available	Pool
http		Monitor
10.1.10.100:80	Available	Pool Member
10.1.10.100	Unknown	Node
10.1.10.101:80	Available	Pool Member
10.1.10.101	Unknown	Node
10.1.10.102:80	Available	Pool Member
10.1.10.102	Unknown	Node
10.1.20.122%0		Virtual Address
example-f5-http-lb_profile_http		Profile
tcp-wan-optimized		Profile
publish_stats		icall_periodic_handler
publish_stats		icall_script
postdeploy_final		icall_script

Enable
Disable
Force Offline
Refresh

Read

Perform the following steps to complete this task:

1. Click the `Get example-f5-http-lb` Service request in the folder.
2. We will send a `GET` request to the Resource URI for the existing deployment.
3. Click the `Send` button to **Read** the Service Deployment.
4. Examine the JSON Response *Body* to see the state of the current Service Deployment:



The screenshot shows an API client interface with tabs for Body, Cookies, Headers (11), and Test Results (3/3). The Body tab is selected, and a red arrow points to it. Below the tabs are buttons for Pretty, Raw, and Preview, and a dropdown menu set to JSON. The JSON response is displayed in a text area, with a red box highlighting the content. The JSON is as follows:

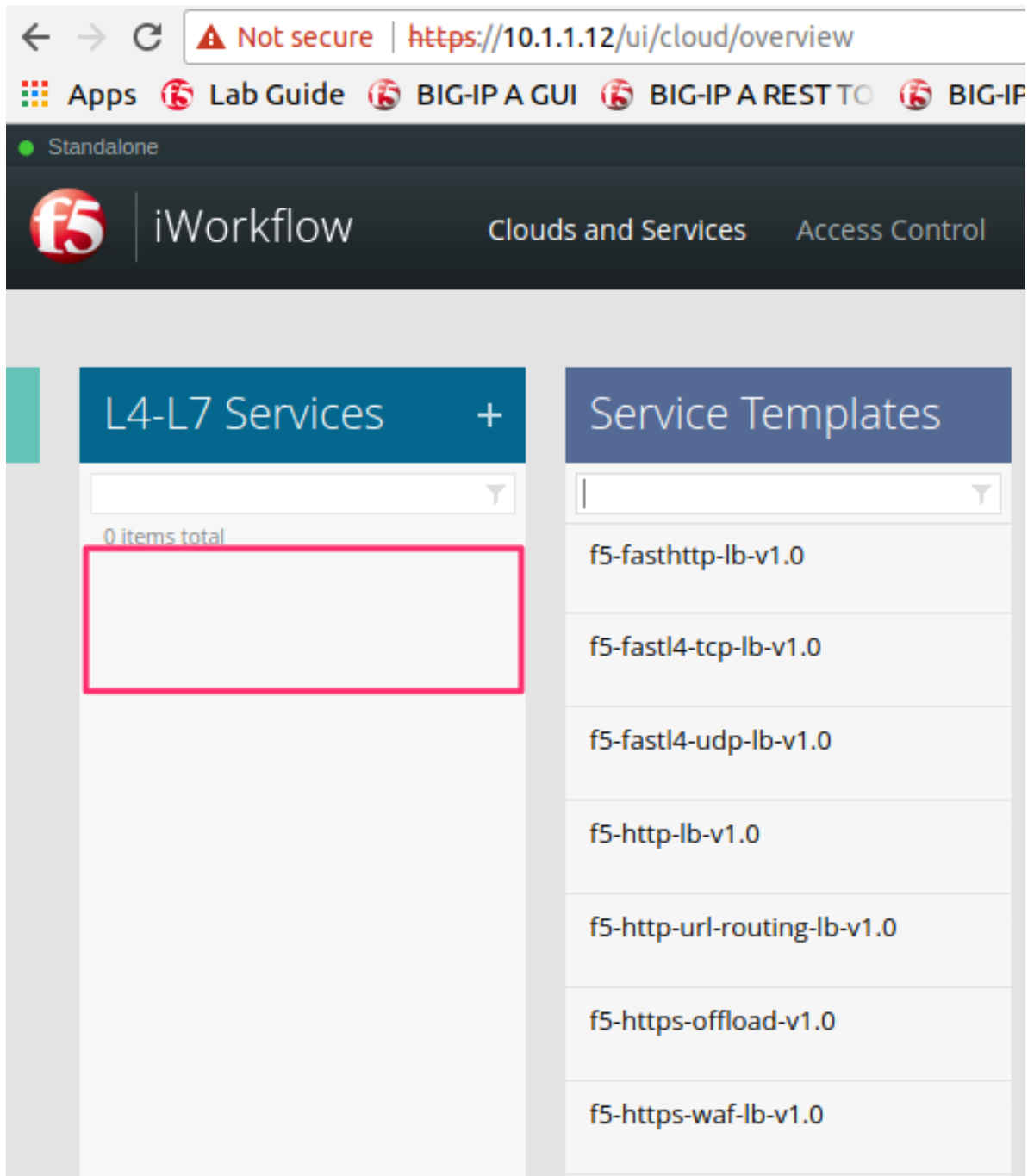
```
{
  "name": "example-f5-http-lb",
  "tenantTemplateReference": {
    "link": "https://localhost/mgmt/cm/cloud/tenant/templates/iapp/f5-http-lb-v1.0"
  },
  "tenantReference": {
    "link": "https://localhost/mgmt/cm/cloud/tenants/MyTenant"
  },
  "vars": [
    {
      "name": "pool_addr",
      "value": "10.1.20.122"
    },
    {
      "name": "pool_port",
      "value": "80"
    }
  ],
  "tables": [
    {
      "name": "pool_Members",
      "columns": [
        "IPAddress",
        "State"
      ],
      "rows": [
        [
          "10.1.10.100",
          "enabled"
        ],
        [
          "10.1.10.101",
          "enabled"
        ],
        [
          "10.1.10.102",
          "enabled"
        ]
      ]
    }
  ]
}
```

Delete

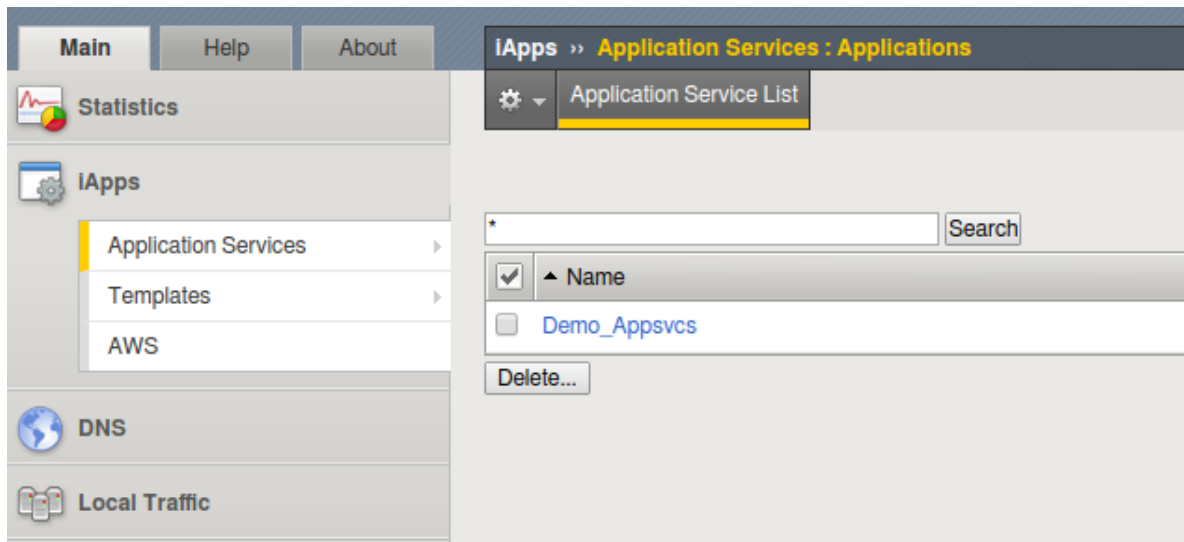
Perform the following steps to complete this task:

1. Click the `Delete example-f5-http-lb` Service request in the folder.
2. We will send a `DELETE` request to the Resource URI for the existing deployment.
3. Click the `Send` button to **Delete** the Service Deployment.

4. Update the iWorkflow Tenant UI and verify that the Service has been deleted:



5. In the BIG-IP GUI navigate to *iApps* → *Application Services* and verify the service was deleted.

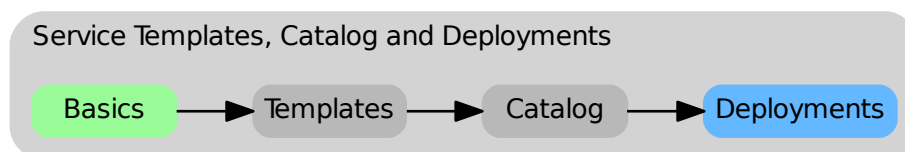


Task 3 - Deploy Additional Services

Examples **Create** requests are included in the Lab 3.3 - Deploy L4-7 Services folder. For the remaining services refer to the table below to see which ones apply most to your specific use cases. You can repeat the steps in Task 2 for the additional services by modifying the requests as needed.

Service Name	Description
f5-http-lb	HTTP Load Balancing to a Single Pool
f5-https-offload	HTTPS Offload and Load Balancing to a Single Pool
f5-fasthttp-lb	Performance-enhanced HTTP Load Balancing to a Single Pool
f5-fastl4-tcp-lb	Generic L4 TCP Load Balancing to a Single Pool
f5-fastl4-udp-lb	Generic L4 UDP Load Balancing to a Single Pool
f5-http-url-routing-lb	HTTP Load Balancing with URL Based Content Routing to Multiple Pools
f5-https-waf-lb	HTTPS Offload, Web Application Firewall Protection and Load Balancing to a Single Pool

Lab 3.4: iWorkflow REST Proxy



While the focus so far has been on building **Declarative Interfaces** with iWorkflow, it's important to note iWorkflow can also help simplify **Imperative** operations to BIG-IP devices when needed.

iWorkflow includes a REST proxy that allows pass-through of REST requests to devices discovered on iWorkflow. The REST proxy feature allows customers to simplify **Imperative** Automation by:

- Providing a centralized API endpoint for BIG-IP infrastructure
 - No need to communicate with individual BIG-IP devices, only with iWorkflow
- Simplified authentication
 - Strong authentication can be implemented at iWorkflow rather than on each BIG-IP
- Simplified Role Based Access Control (RBAC)
 - RBAC can be implemented at iWorkflow for all devices rather than on individual devices in the environment

The REST proxy works by passing data sent to a specific URL through to the BIG-IP device. The root URL for a particular devices REST proxy is:

```
/mgmt/shared/resolver/device-groups/cm-cloud-managed-devices/devices/  
<device_uuid>/rest-proxy/
```

Any URL segments included after `.../rest-proxy/` are forwarded unaltered to the BIG-IP device. Query parameters (e.g. `?expandSubcollections=true`) are also passed unaltered along with the request type and request body.


Task 1 - Perform REST operations via the REST Proxy


In this task we will perform a sample CRUD operation utilizing the REST Proxy. The intent of this task is to show the basic mechanism used to perform these tasks. Simply changing the URL to include the iWorkflow REST Proxy root for that device could easily change all the **Imperative** operations we have completed in this lab to use the REST Proxy.





Perform the following steps to complete this task:

1. Expand the `Lab 3.4 - iWorkflow REST Proxy` folder in the Postman collection.
2. Click the `Step 1: Create pool on BIG-IP A`. Examine the request type, URL and JSON body. Essentially we are performing a POST to the `/mgmt/tm/ltn/pool` collection on BIG-IP A. The last part of the URL includes this URI path (the part after `.../rest-proxy/`). The JSON body and all other parameters are passed unaltered. Also, notice that we are still using our iWorkflow Token to Authenticate, not the BIG-IP one in the *Headers* tab.

► Step 1: Create pool on BIGIP-A

POST  https://{iwf_mgmt}/mgmt/shared/resolver/device-groups/cm-cloud-managed-devices/devices/{iwf_bigip_a_uuid}/rest-proxy/mgmt/tm/ltn/pool

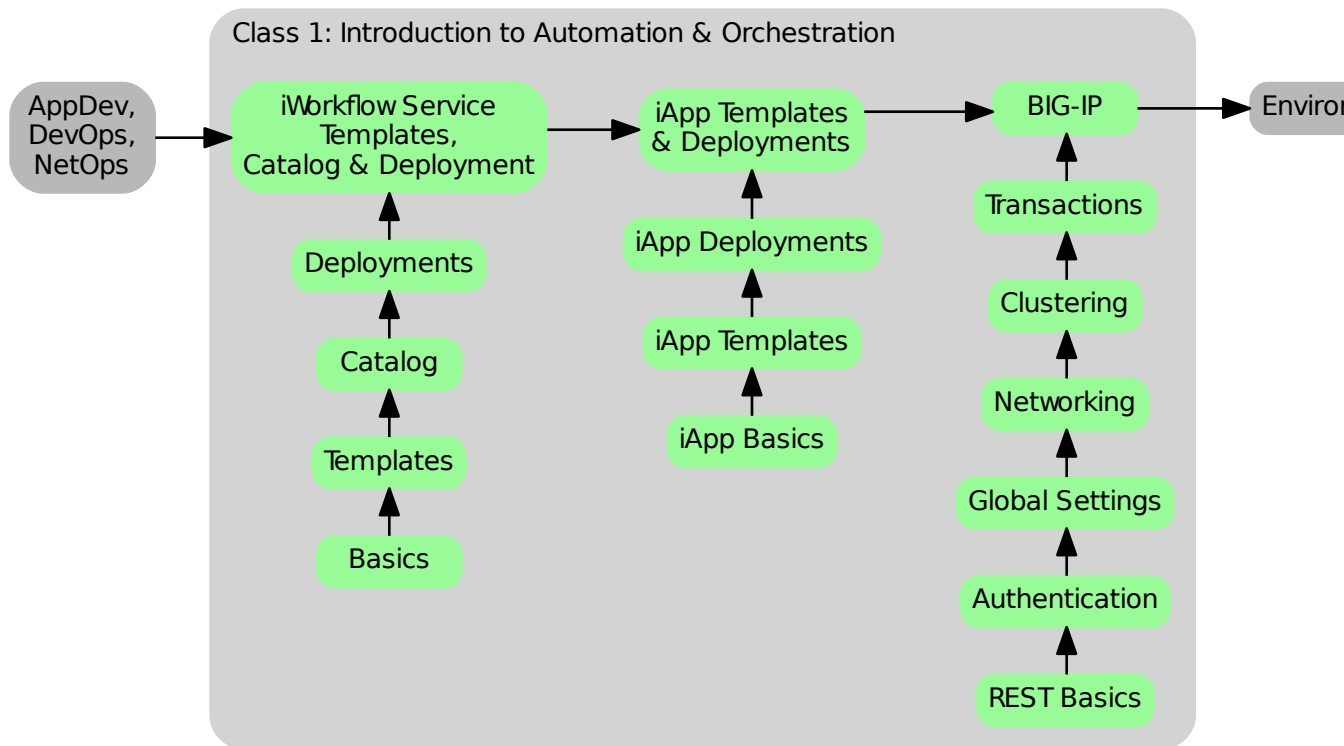
Authorization Headers (2) Body  Pre-request Script Tests 

 form-data  x-www-form-urlencoded  raw  binary JSON (application/json) 

```
1 {  
2   "name": "rest_proxy_pool",  
3   "partition": "Common",  
4   "allowNat": "yes",  
5   "allowSnat": "yes",  
6   "loadBalancingMode": "round-robin",  
7   "monitor": "/Common/http",  
8 }
```

3. Click the *Send* button and examine the response.
4. Complete Steps 2-5 for the remaining items in the Lab 3.4 – iWorkflow REST Proxy collection. Examine each request carefully so you understand what is happening.

2.6 Conclusion



In this class we learned the base concepts and skills required to effectively automate the F5 BIG-IP platform. The diagram above shows a high-level view of the different components to this base level of knowledge. In subsequent classes we will expand on the core concepts and knowledge learned in this class.

This content has been created with a DevOps methodology and fully Continuous Toolchain. All content contained here is sourced from the following GitHub repository:

<https://github.com/f5devcentral/f5-automation-labs/>

Bug Reports and Requests for Enhancement are handled in two ways:

- Fork the Github Repo, fix or enhance as required, and submit a Pull Request
 - <https://help.github.com/articles/creating-a-pull-request-from-a-fork/>
- Open an [Issue](#) within the repository.

Lastly, this content would not be possible without the contributions from many F5 Employees, Partners, and Customers. A full list of contributors to this content can be found at:

<https://github.com/f5devcentral/f5-automation-labs/graphs/contributors>

Class 2: Building Continuous Delivery Pipelines

This class covers the following topics:

- Continuous Integration(CI) and Continuous Delivery(CD) Concepts
- F5 Automation Toolkits:
 - F5-Super-NetOps-Container
 - F5 Postman Collections and f5-postman-workflows extensions
 - F5 f5-newman-wrapper for Automating Workflows
- Building CI/CD Pipelines with Jenkins
- Team Collaboration with Automated Slack Notifications

The entire class will be run from within the F5 Lab Created environment, for access to the lab please ask your instructor, or continue with the self-paced labs from f5.com/supernetops.

Note: If you are running this lab independent from Class 1 you will want to restore BIGIP-A from UCS `bigip-a-module3.ucs` located in the `in_case_of_emergency` folder. Not restoring BIGIP-A will result in services unable to be accessed and nodes/pool members offline. This restore **MUST** be done via TMSH with a `no-license` flag.

Expected time to complete: **3 hours**

3.1 Module 1: f5-super-netops-container Toolkit

In this module, we will explore how to use the **f5-super-netops-container** toolkit to easily integrate various F5 Automation, Orchestration, Super-NetOps and DevOps tools, along with framework technologies.

The f5-super-netops-container is meant to be provided as a technical leave behind, a functional solution that contains tools (which we will use in this Class) and documentation around F5 Cloud Solutions. The container is **continuously updated** to always include our latest information.

The labs in this module will show you how to install the f5-super-netops-container image; you can also start it in your local environment and access the same various tools and documentation.

To install the f5-super-netops-container, your system must support running Docker Community Edition (CE). Please refer to <https://docs.docker.com/engine/installation/#platform-support-matrix> for more information.

This toolkit is fully open source and is on GitHub at <https://github.com/f5devcentral/f5-super-netops-container>

3.1.1 Lab 1.1: Install Docker Community Edition (CE)

Task 1 - Test Docker CE

Open **Root Terminal** from your desktop and test your Docker CE setup is functional with the `hello-world` container; run the following command

```
docker run --rm hello-world
```

Example output:

```
$ docker run --rm hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
78445dd45222: Pull complete
Digest: sha256:c5515758d4c5e1e838e9cd307f6c6a0d620b5e07e6f927b07d05f6d12a1ac8d7
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

Share images, automate workflows, and more with a free Docker ID:
https://cloud.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/engine/userguide/
```

Note: The `--rm` option will delete the container as soon as it stops running.

If you see this message: **Cannot connect to the Docker daemon. Is the docker daemon running on this host?**, it is likely that you don't have enough privileges with your user, try to use **sudo** when executing docker commands.

If you want to remove the `hello-world` container, you can run the command `sudo docker rmi hello-world`. If your container is running, you cannot remove the image. You can issue the following commands in that case (this will stop ALL your container instances): `sudo docker stop $(docker ps -aq)`

3.1.2 Lab 1.2: Obtain & Start the f5-super-netops-container Image

In this lab we will use the `docker` cli tools to obtain and start the `f5-super-netops-container` image.

Task 1 - Obtain and verify the container image

Perform the following steps to complete this task:

1. Return to your open **Root Terminal**
2. Execute `docker pull f5devcentral/f5-super-netops-container:jenkins`

Example output:

```
$ docker pull f5devcentral/f5-super-netops-container:jenkins
jenkins: Pulling from f5devcentral/f5-super-netops-container
019300c8a437: Pull complete
2d6b38b56ae7: Pull complete
5fab9174d5b4: Pull complete
fc0251c85d81: Pull complete
d5c1476cba25: Pull complete
3f563aeb530f: Pull complete
56717b902584: Pull complete
3a973f5ee17d: Pull complete
68d52f474d41: Pull complete
604d6366bf0b: Pull complete
b3b4184aef22: Pull complete
2cebef5955c: Pull complete
2b7bce9d0d9e: Pull complete
259f696f7766: Pull complete
6d5f2e57c5b3: Pull complete
985706ad6d05: Pull complete
a29f68892227: Pull complete
7420ee096abd: Pull complete
0907797bbe90: Pull complete
5b8f2518bf01: Pull complete
2940be145e35: Pull complete
f2cb35cbf665: Pull complete
5cdfa1779954: Pull complete
61c1367b68d8: Pull complete
5bcd8c5223bb: Pull complete
b0defdb83b82: Pull complete
Digest: sha256:27563f98bf58c9d26eb5989acaf540a9ad7fb1806e4a4c373ad28769ebe63ef4
Status: Downloaded newer image for f5devcentral/f5-super-netops-container:jenkins
```

3. Execute `docker images`

Example output:

```
$ docker images
REPOSITORY                                TAG                IMAGE ID            SIZE
f5devcentral/f5-super-netops-container    jenkins            b71fc40407e4       490MB
↪2 weeks ago
```

Task 2 - Start the container image

To start the container we will execute the command:

1. Execute `docker run -p 8080:80 -p 2222:22 -p 10000:8080 --rm -it -e SNOPS_GH_BRANCH=master f5devcentral/f5-super-netops-container:jenkins`

Note: The image requires Internet connectivity to download the latest versions of tools and documentation. Please ensure you have proper connectivity from your host prior to starting the image. If you need to use a proxy please refer to the documentation at <https://docs.docker.com>

The image will now start and load resources from the Internet. This process may take a while depending on the speed of your connection. When the startup process is complete you will be presented in the `root` user prompt. You can interact with the image with standard Linux commands. In the next lab we will connect to the image via SSH and HTTP.

The `-p` option publishes a L4 port from the container to the host. For example the `-p 8080:80` option will redirect port 8080 on the host system to port 80 in the container.

The `-it` option will make the session interactive and allocate a pseudo-TTY

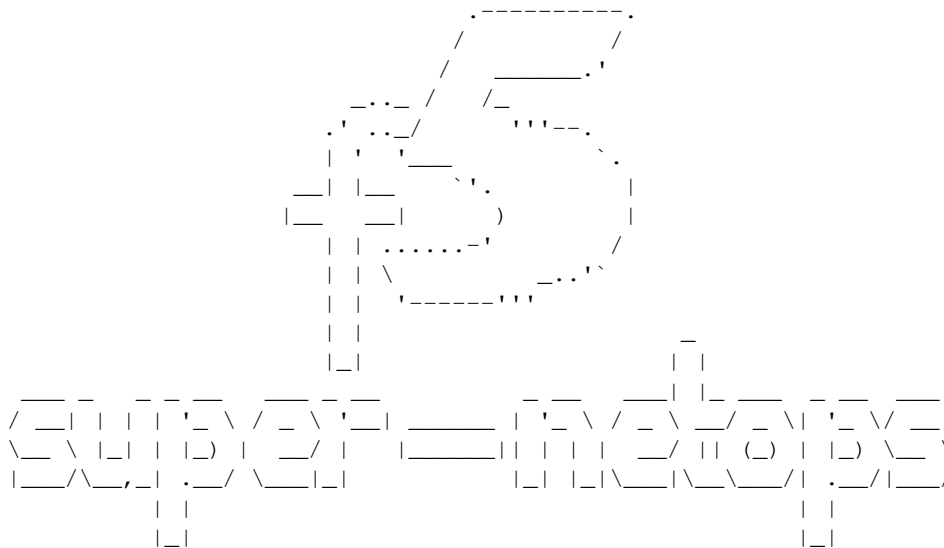
The `-e` option will specify a Github Branch, in this case we are pulling from `master`

The `f5devcentral/f5-super-netops-container:jenkins` option is the name associated with the image we obtained in Task 1.

Example startup output:

```
container:jenkins
[s6-init] making user provided files available at /var/run/s6/etc...exited 0.
[s6-init] ensuring user provided files have correct perms...exited 0.
[fix-attrs.d] applying ownership & permissions fixes...
[fix-attrs.d] done.
[cont-init.d] executing container initialization scripts...
[cont-init.d] done.
[services.d] starting services
[services.d] done.
[environment] SNOPS_HOST_SSH=2222
[environment] SNOPS_REPO=https://github.com/f5devcentral/f5-super-netops-container.git
[environment] SNOPS_AUTOCLONE=1
[environment] SNOPS_HOST_IP=172.17.0.2
[environment] SNOPS_ISALIVE=1
[environment] SNOPS_GIT_HOST=github.com
[environment] SNOPS_REVEALJS_DEV=0
[environment] SNOPS_HOST_HTTP=8080
[environment] SNOPS_IMAGE=jenkins
[environment] SNOPS_GH_BRANCH=master
Reticulating splines...
Becoming self-aware...
[cloneGitRepos] Retrieving repository list from https://github.com/f5devcentral/f5-
↪super-netops-container.git#develop
[updateRepos] Processing /tmp/snops-repo/images/jenkins/fs/etc/snopsrepo.d/jenkins.
↪json
[updateRepos] Processing /tmp/snops-repo/images/base/fs/etc/snopsrepo.d/base.json
[updateRepos] Processing /tmp/user_repos.json
[cloneGitRepos] Loading repositories from /home/snops/repos.json
[cloneGitRepos] Found 7 repositories to clone...
[cloneGitRepos][1/7] Cloning f5-sphinx-theme#master from https://github.com/
↪f5devcentral/f5-sphinx-theme.git
[cloneGitRepos][1/7] Installing f5-sphinx-theme#master
[cloneGitRepos][2/7] Cloning f5-super-netops-container#develop from https://github.
↪com/f5devcentral/f5-super-netops-container.git
[cloneGitRepos][2/7] Installing f5-super-netops-container#develop
[cloneGitRepos][3/7] Cloning f5-application-services-integration-iApp#develop from
↪https://github.com/F5Networks/f5-application-services-integration-iApp.git
[cloneGitRepos][3/7] Installing f5-application-services-integration-iApp#develop
```

```
[cloneGitRepos][4/7] Cloning f5-postman-workflows#develop from https://github.com/
↳ 0xHiteshPatel/f5-postman-workflows.git
[cloneGitRepos][4/7] Installing f5-postman-workflows#develop
[cloneGitRepos][5/7] Cloning f5-automation-labs#master from https://github.com/
↳ f5devcentral/f5-automation-labs.git
[cloneGitRepos][5/7] Installing f5-automation-labs#master
[cloneGitRepos][6/7] Cloning ultimate-vimrc#master from https://github.com/amix/vimrc.
↳ git
[cloneGitRepos][6/7] Installing ultimate-vimrc#master
[cloneGitRepos][7/7] Cloning reveal-js#master from https://github.com/hakimel/reveal.
↳ js.git
[cloneGitRepos][7/7] Installing reveal-js#master
```



Welcome to the f5-super-netops-container. This image has the following services running:

```
SSH tcp/22
HTTP tcp/80
```

To access these services you may need to remap ports on your host to the local container using the command:

```
docker run -p 8080:80 -p 2222:22 -it f5devcentral/f5-super-netops-container:base
```

From the HOST perspective, this results in:

```
localhost:2222 -> f5-super-netops-container:22
localhost:8080 -> f5-super-netops-container:80
```

You can then connect using the following:

```
HTTP: http://localhost:8080
SSH: ssh -p 2222 snops@localhost
```

Default Credentials:

```
snops/default
root/default
```

```
Go forth and automate!

(you can now detach by using Ctrl+P+Q)

[root@f5-super-netops] [/] #
```

Task 3 - Detach/Re-attach the Container

When running containers it's important to understand how you launched it, ours was launched as a **foreground process**, if you typed the `exit` command in the running container it will shutdown. In order to avoid this you should detach from the container once it has completed booting. You can still perform functions by using SSH to access the container as explained in the next lab.

Its likely that the installation of the `f5-super-netops-container` will not be on a localhost while running in a large environment, the steps below show how you can leave this instance running as a background process, if needed.

Detach the Container

1. Issue a `Ctrl+p+q` in the running TTY.

Example output:

```
[root@f5-super-netops] [/] #
[root@f5-super-netops] [/] #
[root@f5-super-netops] [/] # <enter Ctrl+p+q>
hostname:~ user$
```

2. Verify our container is still running by entering `docker ps`

Example output:

```
hostname:~ user$ docker ps
$ docker ps
CONTAINER ID        IMAGE               CREATED             STATUS              PORTS
↳COMMAND              CREATED             STATUS              PORTS
↳
↳NAMES
4cf75944bfbcc      f5devcentral/f5-super-netops-container:jenkins        "/
↳init /snopsboot/..."    2 minutes ago      Up 2 minutes        8000/tcp, 50000/
↳tcp, 0.0.0.0:2222->22/tcp, 0.0.0.0:8080->80/tcp, 0.0.0.0:10000->8080/tcp
↳loving_montalcini
```

Re-attach the Container

1. Execute `docker ps`

Example output:

```
hostname:~ user$ docker ps
$ docker ps
CONTAINER ID        IMAGE               CREATED             STATUS              PORTS
↳COMMAND              CREATED             STATUS              PORTS
↳
↳NAMES
```

```

4cf75944bfbcbf5devcentral/f5-super-netops-container:jenkins"/
↪init /snopsboot/..." 2 minutes agoUp 2 minutes8000/tcp, 50000/
↪tcp, 0.0.0.0:2222->22/tcp, 0.0.0.0:8080->80/tcp, 0.0.0.0:10000->8080/tcp
↪loving_montalcini
|-----|
^~ YOUR CONTAINER ID

```

2. Copy the value under the `CONTAINER ID` column that correspond to the `f5devcentral/f5-super-netops-container:jenkins` image.
3. Execute `docker attach <container_id>`
4. You may have to hit `<Enter>` twice to display the command prompt
5. Detach the container again by entering `<Ctrl+p+q>`

3.1.3 Lab 1.3: Connect to f5-super-netops-container

In the previous lab we started the container image and were presented in a root user terminal. In order to use the container and its associated tools properly we will connect via SSH and/or HTTP.

Task 1 - Connect via SSH

To connect to the image via SSH we must use the published port specified in the `docker run` command. **To review** the command used to start the container was:

```

docker run -p 8080:80 -p 2222:22 -p 10000:8080 --rm -it -e
SNOPS_GH_BRANCH=master f5devcentral/f5-super-netops-container:jenkins

```

This will publish the standard SSH service from `TCP/22` to `TCP/2222`. In the case of the SSH service the following mapping applies:

```
localhost:2222 -> f5-super-netops-container:22
```

The container includes the `snops` user with a password of `default`.

```
ssh -p 2222 snops@localhost
```

Note: The host SSH keys for our environment are regenerated each time the container boots, you may receive an error when trying to connect indicating the host key has changed. This error is safe to ignore in this case and can be resolved by removing the key from `~/.ssh/known_hosts`. You can also configure your local SSH config by adding the following to `~/.ssh/config`:

```

Host localhost
Port 2222
StrictHostKeyChecking no
UserKnownHostsFile /dev/null

```

Example output of connecting to the container:

```

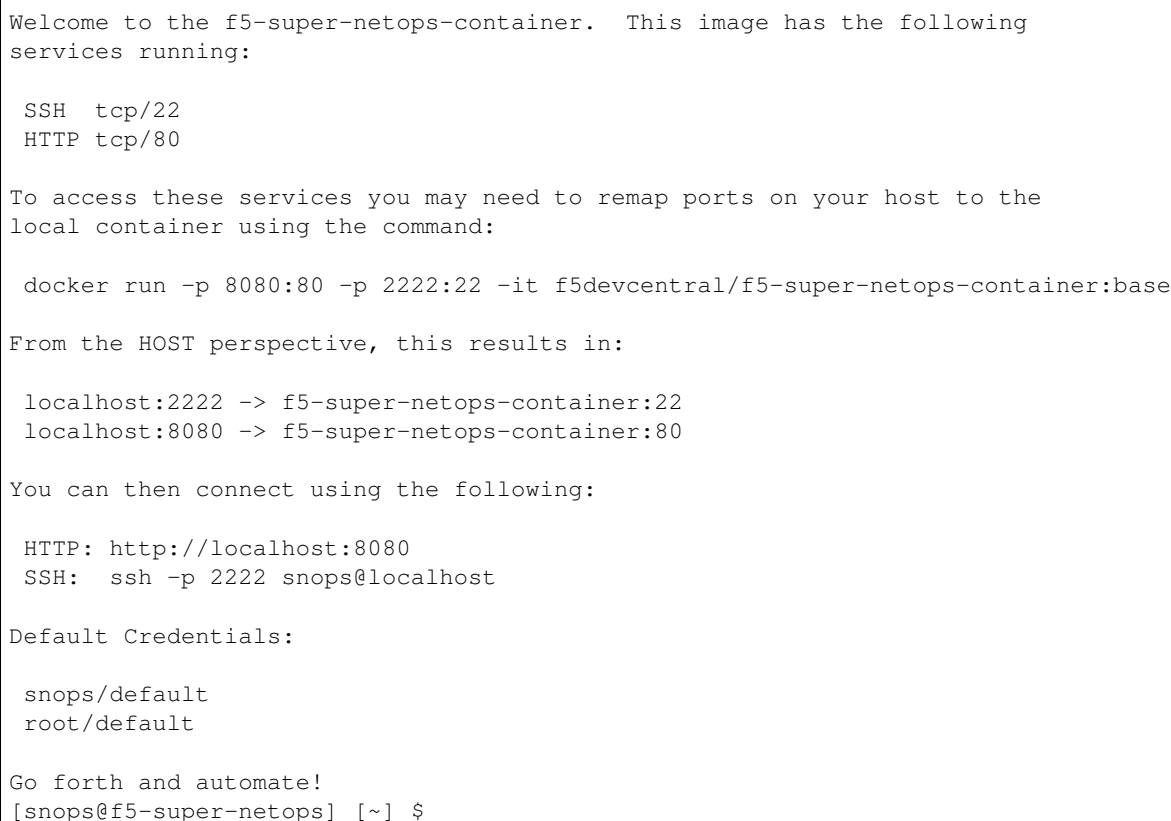
$ ssh -p 2222 snops@localhost
Warning: Permanently added '[localhost]:2222' (ECDSA) to the list of known hosts.
snops@localhost's password:

```

```

/-----/
/_____/

```



```
localhost:8080 -> f5-super-netops-container:80
```

Open Chrome on your Linux Jumphost and enter the URL:

```
http://localhost:8080/start
```

You should see a page like this:

Task 3 - Connect via Jenkins

To connect to the image via Jenkins we use the published port specified in the `docker run` command. **To review** the command used to start the container was:

```
docker run -p 8080:80 -p 2222:22 -p 10000:8080 --rm -it -e  
SNOPS_GH_BRANCH=master f5devcentral/f5-super-netops-container:jenkins
```

This will publish the standard Jenkins service from TCP/8080 to TCP/10000. In the case of the Jenkins service the following mapping applies:

```
10.1.1.8:10000 -> f5-super-netops-container:8080
```

To connect to Jenkins open a web browser and enter the URL:

```
http://localhost:10000
```

You should see a page like this:



User:

Password:

☐ Remember me on this computer

3.2 Module 2: F5 f5-postman-workflows & f5-newman-wrapper

In the previous Class you may have found the tasks associated with checking various response values and populating environment variables **very** tedious. In addition to being tedious, these tasks are not fundamentally automatable due to the requirement for human interaction.

In order to assist users with automating the F5 BIG-IP platform we have developed a set of tools that can be used with the Postman REST Client (<http://getpostman.com>).

The tools are:

- f5-postman-workflows
 - Provide re-usable JavaScript functions that ease testing of API responses and populating environment variables
 - Implement a delay-based polling mechanism
- f5-newman-wrapper
 - Allow users to easily assemble Postman collections into workflows
 - Enabled integration with third-party tools such as Ansible, Chef & Puppet

This framework allows collection developers to create automatable collections that include full testing of response values, population of environment variables to establish chains of requests and time-based polling to allow long-lived API processes time to complete.

Users can then interact with these collections via the Postman GUI client, run the collections with the Postman Runner or the Newman CLI client.

This lab module will walk you through using the tools. If you are interested in developing collections using the f5-postman-workflows framework please visit the official GitHub repository at <https://github.com/0xHiteshPatel/f5-postman-workflows>

3.2.1 Lab 2.1: Install the f5-postman-workflows Framework

In this lab you will walk through installing the f5-postman-workflows framework into the Postman REST Client.

Task 1 - Import the f5-postman-workflows Postman Collection

In this task you will Import a Postman Collection that contains Installation helpers, Examples and a automated Test Framework. The collection is installed from the f5-postman-workflows GitHub repository.

Perform the following steps to complete this task:



1. Open the Postman Client on your jump host by clicking the  icon
2. Click the 'Import' button in the top left of the Postman window
3. Click the 'Import from Link' tab. Paste the following URL into the text box and click 'Import'

```
https://raw.githubusercontent.com/0xHiteshPatel/f5-postman-workflows/master/F5_Postman_Workflows.postman_collection.json
```
4. You should now see a collection named `F5_Postman_Workflows` in your Postman Collections sidebar, in some cases the Collections don't appear until Postman has been closed and relaunched.

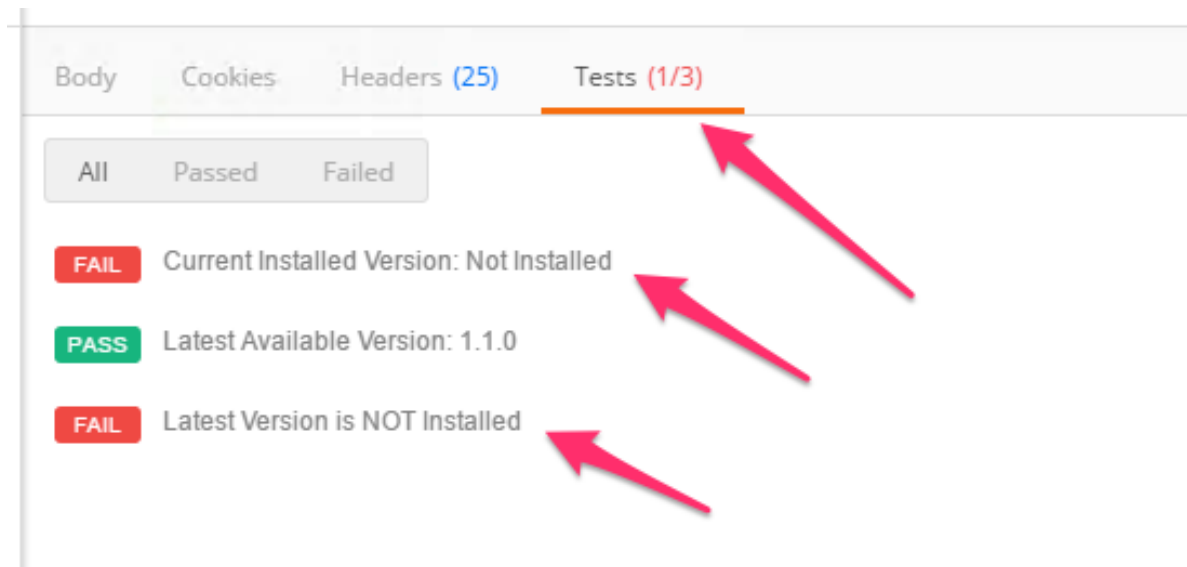
Task 2 - Install f5-postman-workflows into your Postman Client

To utilize the helper functions the framework includes, we must install those functions into the Postman Client. The installation helpers perform the following tasks:

1. Determine the most current version of the framework
2. Dynamically minify the JavaScript code from the f5-postman-workflows GitHub repository using Google's Closure Compiler
3. Install the minified JS code into a Postman Global Variable
4. Set a number of Global variables that allow you to configure various options

To install the framework complete the following tasks:

1. Open the `F5_Postman_Workflows` collection
2. Open the `Install` folder
3. Select the `Check f5-postman-workflows Version` item and click 'Send'
4. Examine the 'Tests' portion of the **RESPONSE**:



5. Select the `Install/Upgrade f5-postman-workflows` item and click 'Send'

6. Examine the 'Tests' again and ensure that Installation was successful:



7. Click the 'Eye' button in the top right of the Postman window and examine the Global variables that have been populated



The f5-postman-workflows framework is now installed in your Postman client.

3.2.2 Lab 2.2: Manually Execute a Workflow

In this lab we will walk through how to obtain two collections, and then we'll use the f5-postman-workflows framework to execute a simple workflow using the Postman GUI client. The f5-postman-workflows GitHub repository is continually updated with new collections that can be used as is, or customized, to automate the F5 platform. Additionally, the f5-super-netops-container automatically downloads these and other tools so users can rapidly execute workflows in their environments.

Postman collections also serve as a reference example of how various tasks can be accomplished using an **Imperative** process. When executing a collection you are actually providing a **Declarative** input to an **Imperative** process.

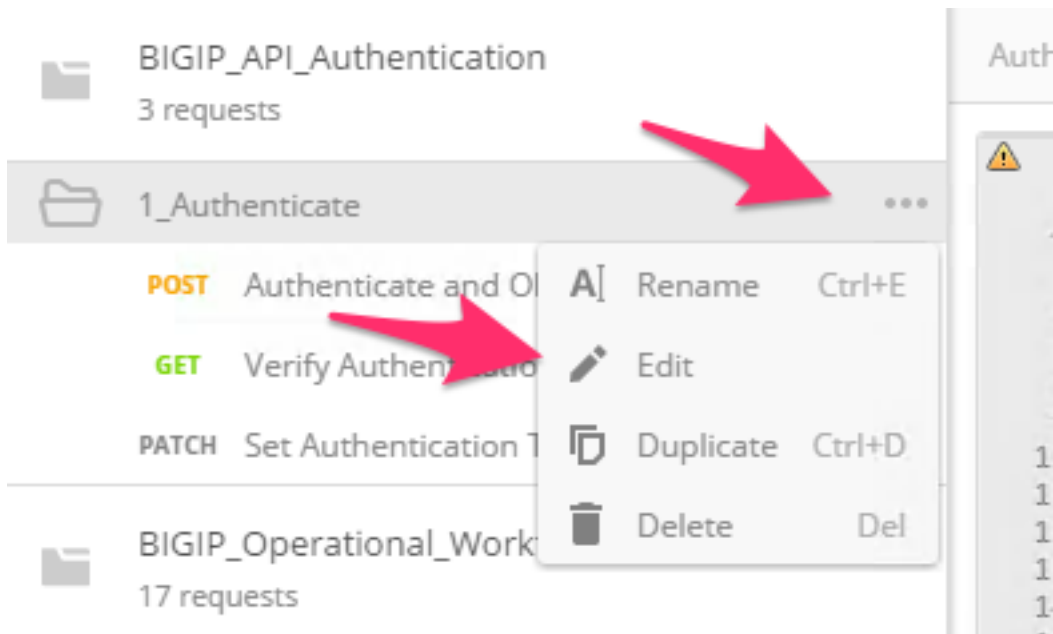
Collections are self-documenting, and we will explore how to access the included documentation to assemble a workflow from beginning to end. In the next lab we will use this base knowledge to create workflows as JSON templates that can be executed by the f5-newman-wrapper on the f5-super-netops-container image (or any system that has Newman installed)

Task 1 - Import and Explore BIG-IP Collections

First, we will import two collections to Postman using the same steps in the previous labs. The **two different** collections will allow us to perform REST **API Authentication** to BIG-IP devices and then execute **Operational** actions on the BIG-IP device. We are stitching together two **Imperative** process's.

Execute the following steps to complete this task:

1. Click Import -> Import from Link and import both of these collection URLs:
 - https://raw.githubusercontent.com/0xHiteshPatel/f5-postman-workflows/master/collections/BIG_IP/BIGIP_API_Authentication.postman_collection.json
 - https://raw.githubusercontent.com/0xHiteshPatel/f5-postman-workflows/master/collections/BIG_IP/BIGIP_Operational_Workflows.postman_collection.json
2. You should now have two additional Collections in the sidebar:
 - BIGIP_API_Authentication
 - BIGIP_Operational_Workflows
3. Expand the BIGIP_API_Authentication collection. Within the collection you will see one folder named 1_Authenticate. Folders are used to organize various workflows within a collection. In this case this collection performs exactly one task, authentication, therefore one folder is present.
4. Expand the 1_Authenticate folder. Notice there are three requests in the folder. These three requests will be executed in a synchronous manner (one-after-another).
5. Click the ... icon on the 1_Authenticate folder, then click Edit



6. In the opened window you will see documentation explaining what the requests in this folder accomplish. Additionally you will see a series of Input and Output variables. Unless marked otherwise it is assumed that all Input variables **are** required. In this case the `bigip_token_timeout` variable is optional.

Folders may also contain output variables that are set to pass data between requests in different collections (A Waterfall). In this case the output variable is named `bigip_token` and contains the authentication token that can be sent in the `X-F5-Auth-Token` HTTP header to perform authentication.

7. Close the window by clicking 'Cancel'
8. Repeat the steps above and explore the `BIGIP_Operational_Workflows` collection, specifically the `4A_Get_BIGIP_Version` folder

Task 2 - Manually Chain Folders into a Workflow

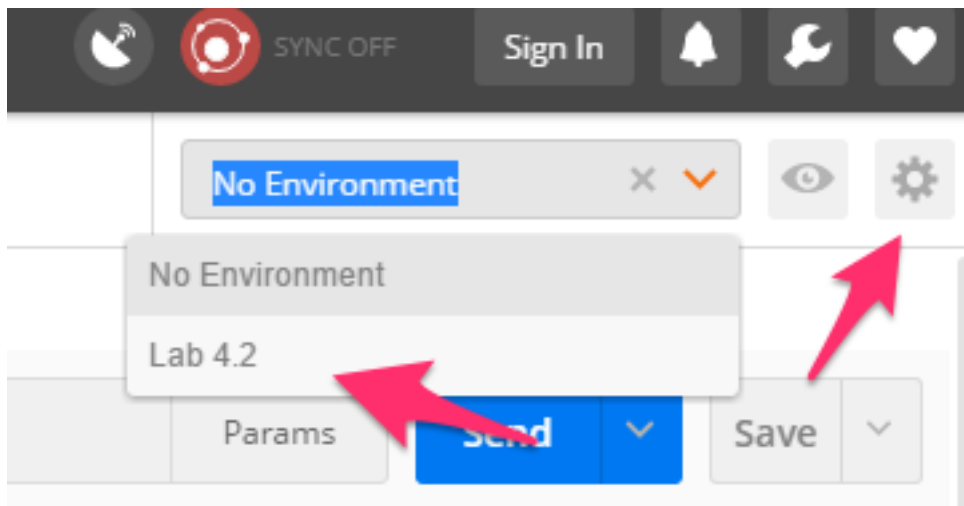
In this task we will explore how to chain two folders together and manually execute a workflow. This example is simple, but should help illustrate how we can use folders as building blocks that can be assembled or chained together to construct a workflow.

We will use the `1_Authenticate` folder in the `BIGIP_API_Authentication` collection and then pass the authentication token to the `4A_Get_BIGIP_Version` folder in the `BIGIP_Operational_Workflows` collection.

Execute the following steps to complete this task:

1. Create a new Postman environment by clicking the Gear icon -> Manage Environments -> Add.
2. Name the environment `Lab 2.2` and populate the following key/value pairs:
 - **bigip_mgmt**: 10.1.1.4
 - **bigip_username**: admin
 - **bigip_password**: admin
3. Click the 'Add' button, then close the 'Manage Environments' window.

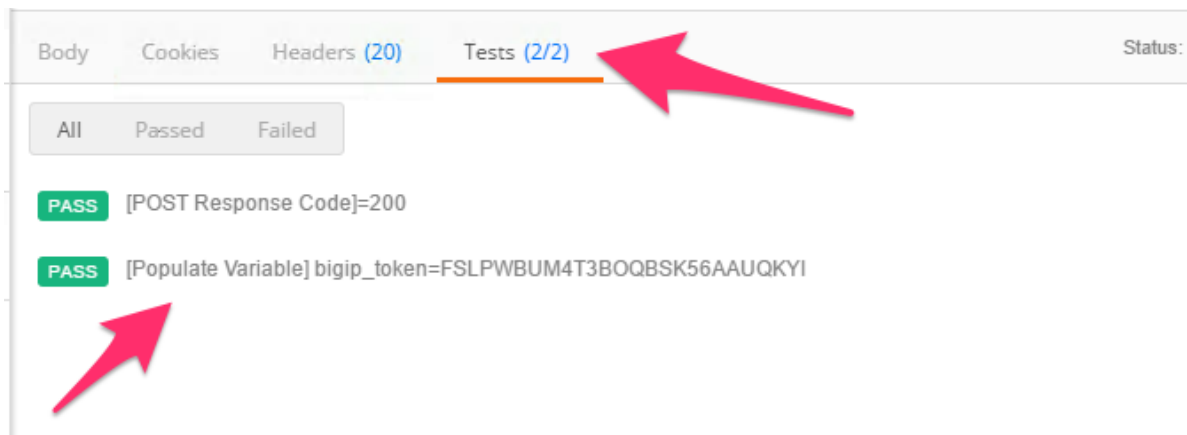
4. Select the Lab 2.2 environment:



The preceding steps configured the Input Variables required for all the folders that comprise our workflow. We will now manually execute all the requests in the folders.

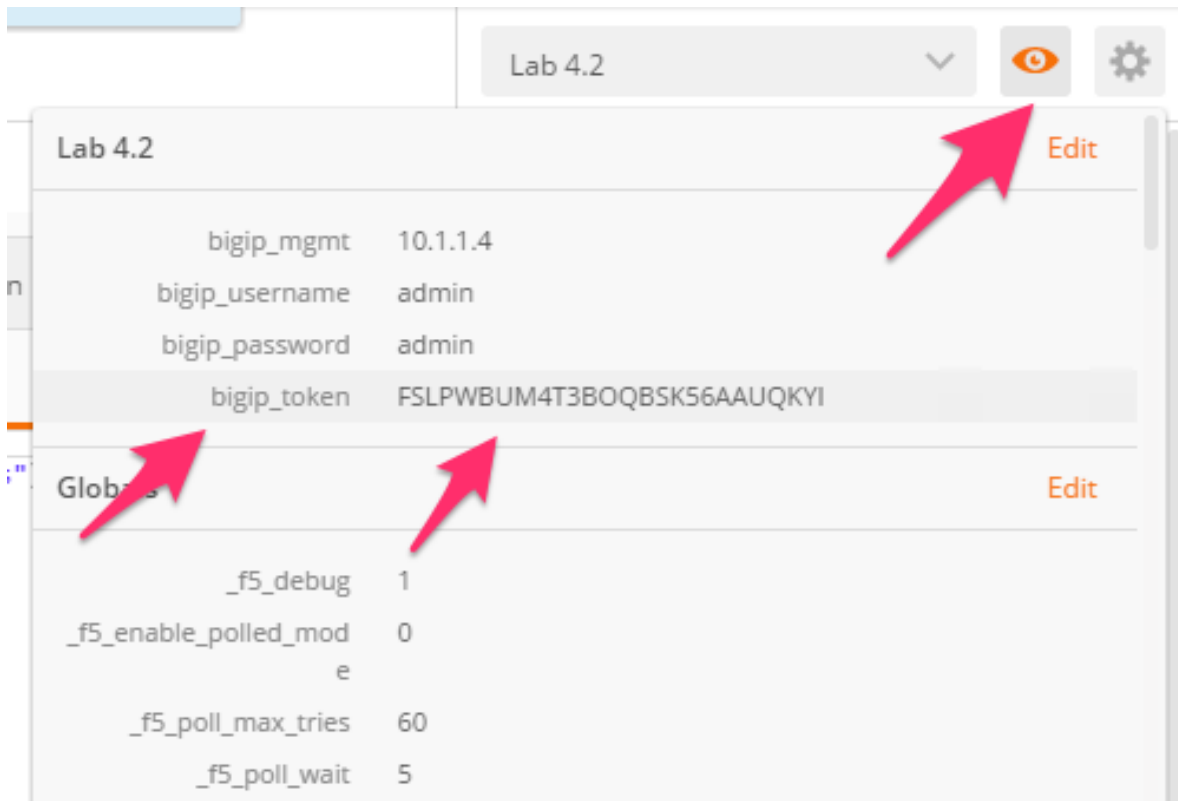
1. Expand the BIGIP_API_Authentication -> 1_Authenticate folder.
2. Select the Authenticate and Obtain Token item and click Send
3. Examine the Tests in the response portion of the request. All the tests should be passing. Additionally you should see a test similar to:

[Populate Variable] bigip_token=....



These test items and their corresponding actions (populating a variable in this case) are generated by the f5-postman-workflows framework.

4. Examine your Postman Environment variables and confirm that the bigip_token variable is present and populated.

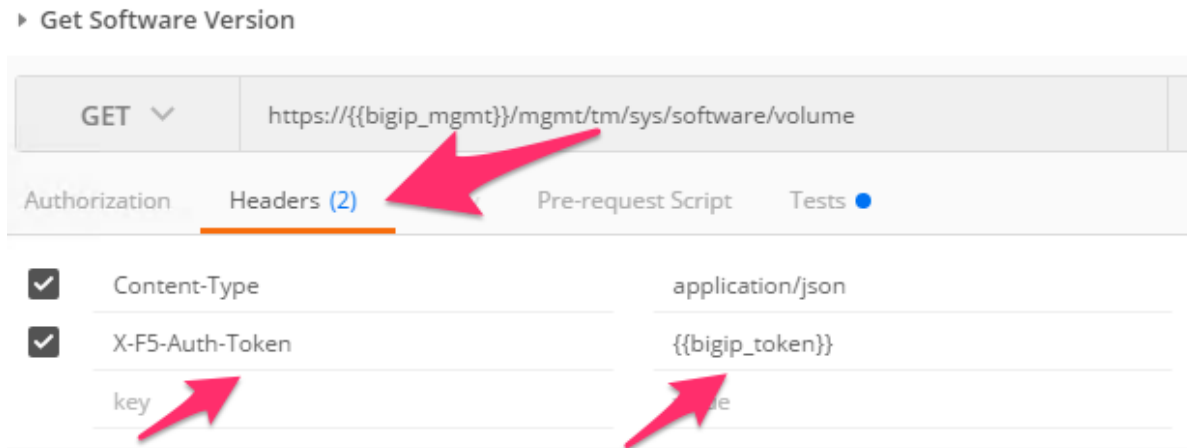


5. Select the `Verify Authentication Works` request in the folder and click 'Send'. Examine the Tests and ensure they are all passing
6. Select the `Set Authentication Token Timeout` request, click *Send* and verify all Tests pass.

At this point we have successfully authenticated to our device and stored the authentication token in the `bigip_token` environment variable. We will now execute a request in a **different** collection and folder that uses the `bigip_token` variable value to authenticate and perform its actions.

1. Expand the `BIGIP_Operational_Workflows` -> `4A_Get_BIGIP_Version` folder.
2. Click the `Get Software Version` request.
3. Click the 'Headers' tab. Notice that the value for the `X-F5-Auth-Token` header is populated with the `bigip_token` variable value.

Note: Postman uses the `{{variable_name}}` syntax to perform variable value substitution.



- Click 'Send' to send the request. Examine the Tests and ensure all tests have passed.
- Examine your environment variables and note that the `bigip_version` and `bigip_build` variables are now populated.

While the example above was simple, it should show how we can chain together different collections and folders to assemble custom workflows. The key concepts to understand are:

- The `f5-postman-workflows` framework and collection test-code performs unit tests on the response data, and verifies the request executed successfully.
- The framework also populates Output Variables as documented so they can be used in subsequent requests as Inputs to assemble a workflow

Next, we will explore how to use this base knowledge to assemble various collections and folders into workflows using Newman and the `f5-newman-wrapper`.

3.2.3 Lab 2.3: f5-newman-wrapper Introduction

As shown in the previous lab, we can manually execute collections and folders using the Postman GUI to achieve end results on BIG-IP devices. While this capability is important in a test/prototyping phase, we need to ensure we can execute these manual steps as an automated process.

To achieve this goal we can use the `f5-newman-wrapper` tool. This tool allows a user to specify a workflow in a JSON formatted file, this includes Input Variables, the collections and folders, and executes various output options to provide feedback and run details in a programmatic fashion.

The core element of a workflow that can be executed by `f5-newman-wrapper` is a JSON formatted input file. In this lab we will introduce the file format.

Task 1 - Explore the workflow JSON format

To introduce the format of the workflow file we will use an example that recreates the simple workflow we executed manually in the previous lab. We will explore the file in sections followed by showing the whole file.

Define Name and Description

```
1 {
2   "name": "Wrapper_Demo_1",
3   "description": "Execute a chained workflow that authenticates to a BIG-IP and_
↪retrieves it's software version"
4 }
```

Define Global Settings for the Run

This section defines how f5-newman-wrapper will run this workflow. The attributes are explained in the table below.

```
1 {
2   "globalEnvVars": "../framework/f5-postman-workflows.postman_globals.json",
3   "globalOptions": {
4     "insecure": true,
5     "reporters": ["cli"]
6   },
7   "saveEnvVars": true,
8   "outputFile": "Wrapper_Demo_1-run.json",
9   "envOutputFile": "Wrapper_Demo_1-env.json"
10 }
```

Attribute	Description
globalEnvVars	This is the file that contains the Global environment variables used by Newman. This file is generated by the f5-postman-workflows build scripts and contains the same global variables as we saw in the previous lab that installed the framework into the Postman GUI client
globalOptions	Specify the global options for newman. Available options are documented at: https://github.com/postmanlabs/newman#api-reference Note: Removing the <code>cli</code> option from the <code>reporters</code> array will disable verbose CLI output
saveEnvVars	Save the environment variables at the end of the run to a file
outputFile	The file to save the run details to.
envOutputFile	The file to save the environment variables at the end of the run to.

Define Input Variables

This section specifies the Input Variables for the workflow. The name `globalVars` conveys that the variables defined here will be present for each request in the defined workflow (the global scope from a workflow perspective). Variables can also be defined within each item in a workflow (the local scope from a item perspective). In the case of a global and local variable that is named identically, the local scope variable will take precedence.

```
1 {
2   "globalVars": {
3     "bigip_mgmt": "10.1.1.4",
```

```

4     "bigip_username": "admin",
5     "bigip_password": "admin"
6   }
7 }

```

Define the Workflow Collections and Ordering

This section defines the workflow and collections and folders that it is comprised of. The `workflow` attribute is an ordered array that contains objects defining each collection and folder to run.

```

1  {
2    "workflow": [
3      {
4        "name": "Authenticate to BIG-IP",
5        "options": {
6          "collection": "../collections/BIG_IP/BIGIP_API_Authentication.postman_
↪collection.json",
7          "folder": "1_Authenticate"
8        }
9      },
10     {
11       "name": "Get BIG-IP Software Version",
12       "options": {
13         "collection": "../collections/BIG_IP/BIGIP_Operational_Workflows.
↪postman_collection.json",
14         "folder": "4A_Get_BIGIP_Version"
15       }
16     }
17   ]
18 }

```

Lets look at the item in the workflow that performs authentication:

```

1  {
2    "name": "Authenticate to BIG-IP",
3    "options": {
4      "collection": "../collections/BIG_IP/BIGIP_API_
↪Authentication.postman_collection.json",
5      "folder": "1_Authenticate"
6    }
7  }

```

The `name` attribute specifies the name for this item. The `options` object specifies the parameters used to execute this particular item. In our case the `collection` attribute refers to the file containing the `BIGIP_API_Authentication` collection. The `folder` attribute specifies the name of the folder to run in the collection.

By default all output variables from a collection or folder are passed to the next item in the workflow. This allows us to chain collections together as needed to build workflows.

Final Workflow JSON

```

1  {
2    "name": "Wrapper_Demo_1",

```

```

3      "description": "Execute a chained workflow that authenticates to a BIG-IP
↪and retrieves it's software version",
4      "globalEnvVars": "../framework/f5-postman-workflows.postman_globals.json",
5      "globalOptions": {
6          "insecure": true,
7          "reporters": ["cli"]
8      },
9      "globalVars": {
10         "bigip_mgmt": "10.1.1.4",
11         "bigip_username": "admin",
12         "bigip_password": "admin"
13     },
14     "saveEnvVars": true,
15     "outputFile": "Wrapper_Demo_1-run.json",
16     "envOutputFile": "Wrapper_Demo_1-env.json",
17     "workflow": [
18         {
19             "name": "Authenticate to BIG-IP",
20             "options": {
21                 "collection": "../collections/BIG_IP/BIGIP_API_
↪Authentication. postman_collection.json",
22                 "folder": "1_Authenticate"
23             }
24         },
25         {
26             "name": "Get BIG-IP Software Version",
27             "skip": false,
28             "options": {
29                 "collection": "../collections/BIG_IP/BIGIP_
↪Operational_Workflows. postman_collection.json",
30                 "folder": "4A_Get_BIGIP_Version"
31             }
32         }
33     ]
34 }

```

3.2.4 Lab 2.4: Run a workflow with f5-newman-wrapper

In this lab we will use the f5-super-netops-container to run the workflow we reviewed in the previous lab. The advantage of using the f5-super-netops Container is that all the tools, collections and frameworks are pre-installed and ready to use.

Task 1 - Run a f5-newman-wrapper Workflow

1. Return to, or open an SSH session as described in the *previous lab*
2. Run `cd f5-postman-workflows/local`
3. Run `cp ../workflows/Wrapper_Demo_1.json .`
4. Edit the `Wrapper_Demo_1.json` file with `vim` and enter the `10.1.1.4` for the value of the `bigip_mgmt` variable

```

"globalVars": {
    "bigip_mgmt": "10.1.1.4",
    "bigip_username": "admin",

```

```
    "bigip_password": "admin"
  },
```

5. Run `f5-newman-wrapper Wrapper_Demo_1.json`
6. Examine the output to see how the workflow was executed. Notice that the same tests that we saw when using Postman are present during this run.

Example output:

```
[snops@f5-super-netops] [~/f5-postman-workflows/local] $ f5-newman-wrapper
↳ Wrapper_Demo_1.json
[Wrapper_Demo_1-2017-03-30-04-08-12] starting run
[Wrapper_Demo_1-2017-03-30-04-08-12] [runCollection][Authenticate to BIG-IP]
↳ running...
newman

BIGIP_API_Authentication

? 1_Authenticate
? Authenticate and Obtain Token
  POST https://10.1.1.4/mgmt/shared/authn/login [200 OK, 1.41KB, 108ms]
  ✓ [POST Response Code]=200
  ✓ [Populate Variable] bigip_token=WYKIVPHCNASNVEC55ZDVNH5002

? Verify Authentication Works
  GET https://10.1.1.4/mgmt/shared/authz/tokens/WYKIVPHCNASNVEC55ZDVNH5002 [200
↳ OK, 1.23KB, 8ms]
  ✓ [GET Response Code]=200
  ✓ [Current Value] token=WYKIVPHCNASNVEC55ZDVNH5002
  ✓ [Check Value] token == WYKIVPHCNASNVEC55ZDVNH5002

? Set Authentication Token Timeout
  PATCH https://10.1.1.4/mgmt/shared/authz/tokens/WYKIVPHCNASNVEC55ZDVNH5002 [200
↳ OK, 1.23KB, 14ms]
  ✓ [PATCH Response Code]=200
  ✓ [Current Value] timeout=1200
  ✓ [Check Value] timeout == 1200

?-----?-----?-----?
|                                     | executed |   failed |
?-----?-----?-----?
|               iterations |         1 |         0 |
?-----?-----?-----?
|               requests  |         3 |         0 |
?-----?-----?-----?
|             test-scripts |         3 |         0 |
?-----?-----?-----?
|    prerequest-scripts   |         1 |         0 |
?-----?-----?-----?
|             assertions   |         8 |         0 |
?-----?-----?-----?
| total run duration: 297ms |          |
?-----?-----?-----?
| total data received: 1.71KB (approx) |          |
?-----?-----?-----?
| average response time: 43ms |          |
?-----?-----?-----?
[Wrapper_Demo_1-2017-03-30-04-08-12] [runCollection][Get BIG-IP Software Version]
↳ running...
```

```

newman

BIGIP_Operational_Workflows

? 4A_Get_BIGIP_Version
? Get Software Version
  GET https://10.1.1.4/mgmt/tm/sys/software/volume [200 OK, 1.32KB, 16ms]
  ✓ [GET Response Code]=200
  ✓ [Populate Variable] bigip_version=12.1.1
  ✓ [Populate Variable] bigip_build=1.0.196
[Wrapper_Demo_1-2017-03-30-04-08-12] run completed

?-----?-----?-----?
|                                     | executed |    failed |
?-----?-----?-----?
|             iterations |         1 |          0 |
?-----?-----?-----?
|             requests  |         1 |          0 |
?-----?-----?-----?
|           test-scripts |         1 |          0 |
?-----?-----?-----?
|    prerequest-scripts |         0 |          0 |
?-----?-----?-----?
|           assertions  |         3 |          0 |
?-----?-----?-----?
| total run duration: 58ms                                     |
?-----?-----?-----?
| total data received: 611B (approx)                           |
?-----?-----?-----?
| average response time: 16ms                                   |
?-----?-----?-----?

```

7. Examine the environment variables that were saved at the end of the run by executing `cat Wrapper_Demo_1-env.json`

Example output:

```

1 {
2   "id": "c0550892-36d4-4412-bf35-ald9aa8d2efe",
3   "values": [
4     {
5       "type": "any",
6       "value": "10.1.1.4",
7       "key": "bigip_mgmt"
8     },
9     {
10      "type": "any",
11      "value": "admin",
12      "key": "bigip_username"
13    },
14    {
15      "type": "any",
16      "value": "admin",
17      "key": "bigip_password"
18    },
19    {
20      "type": "any",
21      "value": "WYKIVPHCNASNVEC55ZDVNH5002",

```

```

22     "key": "bigip_token"
23   },
24   {
25     "type": "any",
26     "value": "1200",
27     "key": "bigip_token_timeout"
28   },
29   {
30     "type": "any",
31     "value": "12.1.1",
32     "key": "bigip_version"
33   },
34   {
35     "type": "any",
36     "value": "1.0.196",
37     "key": "bigip_build"
38   }
39 ]
40 }

```

Notice that the `bigip_version` and `bigip_build` variables were saved, similar to how this was shown in the Postman GUI Environment Variables. This file is JSON formatted and can easily be used directly by other tools to drive further automation.

3.2.5 Lab 2.5: Building Complex Workflows

In the previous lab we reviewed and ran a very simple workflow. To support more complex use cases `f5-newman-wrapper` includes features to help build more complex workflows.

These features allow users to:

- Create infinitely nested items
- Rename/remap variables name pre and post run of an item
- Load variables from a saved environment file
- Define variables in the global (workflow) or local (item) scope

To explore all the available options currently implemented please refer to <https://raw.githubusercontent.com/0xHiteshPatel/f5-postman-workflows/master/framework/f5-newman-wrapper/workflow-schema.json>

Task 1 - Explore Nested Workflows & Variable Remapping

By using the 'children' array within an item in a workflow you can create nested items. In this task, we will create a more advanced version of the workflow we used in the previous lab. This workflow will perform authentication to two BIG-IP devices and then retrieve the software version running on each.

We will implement a workflow that is best depicted by the following branch diagram:

```

Start
|
|- Authenticate
|   |- Authenticate to BIG-IP A
|   |- Authenticate to BIG-IP B
|
|- Get BIGIP Version

```

```

|   |- Get BIGIP Version on BIG-IP A
|   |- Get BIGIP Version on BIG-IP B
|
Stop

```

To implement this workflow we need to consider how Input Variables are passed to each item in the workflow. Previously, we saw that the following variables are required to the `1_Authenticate` folder in the `BIGIP_API_Authentication` collection:

- `bigip_mgmt`
- `bigip_username`
- `bigip_password`

The issue we encounter when building this workflow is that we, at a minimum, have different values for `bigip_mgmt` because we are trying to communicate with two BIG-IP devices. To address this issue, we could define our input variables as follows:

- `bigip_a_mgmt = 10.1.1.4`
- `bigip_b_mgmt = 10.1.1.5`
- `bigip_username = admin`
- `bigip_password = admin`

This solves the problem of providing both BIG-IP management addresses, however, it introduces another issue. The `1_Authenticate` folder requires that the management IP address be passed in the `bigip_mgmt` input variable. To solve this issue, we will use variable name remapping to remap a globalVar to a different name before the `1_Authenticate` folder is run for each BIG-IP device. To illustrate this, we will add more information to our diagram:

```

Start
|
|   |- Define globalVars
|   |   |- bigip_a_mgmt = 10.1.1.4
|   |   |- bigip_b_mgmt = 10.1.1.5
|   |   |- bigip_username = admin
|   |   |- bigip_password = admin
|   |
|   |- Authenticate
|   |   |- Authenticate to BIG-IP A
|   |   |   | Pre-run: Remap bigip_a_mgmt -> bigip_mgmt
|   |   |   | Run: 1_Authenticate folder
|   |   |
|   |   |- Authenticate to BIG-IP B
|   |   |   | Pre-run: Remap bigip_b_mgmt -> bigip_mgmt
|   |   |   | Run: 1_Authenticate folder
|   |
|   |- Get BIGIP Version
|   |   |- Get BIGIP Version on BIG-IP A
|   |   |- Get BIGIP Version on BIG-IP B
|
Stop

```

We've now addressed our issues regarding defining and passing the BIG-IP management address, but have to consider one last problem. The **output variable** of the `1_Authenticate` folder is `bigip_token`. By default `f5-newman-wrapper` will store all output variables from one folder and automatically pass them to the next item. In this case, an issue occurs because the `Authenticate to BIG-IP B` item will overwrite

the `bigip_token` variable that was outputted by the `Authenticate` to BIG-IP A item. To resolve this issue, we can remap variables **AFTER** or post-run of an item. We can modify our diagram to handle this issue like this:

```
Start
|
|- Define globalVars
|   |- bigip_a_mgmt = 10.1.1.4
|   |- bigip_b_mgmt = 10.1.1.5
|   |- bigip_username = admin
|   |- bigip_password = admin
|
|- Authenticate
|   |- Authenticate to BIG-IP A
|   |   | Pre-run: Remap bigip_a_mgmt -> bigip_mgmt
|   |   | Run: 1_Authenticate folder
|   |   | Post-run: Remap bigip_token -> bigip_a_token
|   |
|   |- Authenticate to BIG-IP B
|   |   | Pre-run: Remap bigip_b_mgmt -> bigip_mgmt
|   |   | Run: 1_Authenticate folder
|   |   | Post-run: Remap bigip_token -> bigip_b_token
|   |
|- Get BIGIP Version
|   |- Get BIGIP Version on BIG-IP A
|   |- Get BIGIP Version on BIG-IP B
|
Stop
```

The last step is to perform some additional pre-run remapping to pass the correct token to the `4A_Get_BIGIP_Version` folder to get our BIG-IP software version. Additionally, we will perform some post-run remaps so we can save the output variables for each device:

```
Start
|
|- Define globalVars
|   |- bigip_a_mgmt = 10.1.1.4
|   |- bigip_b_mgmt = 10.1.1.5
|   |- bigip_username = admin
|   |- bigip_password = admin
|
|- Authenticate
|   |- Authenticate to BIG-IP A
|   |   | Pre-run: Remap bigip_a_mgmt -> bigip_mgmt
|   |   | Run: 1_Authenticate folder
|   |   | Post-run: Remap bigip_token -> bigip_a_token
|   |
|   |- Authenticate to BIG-IP B
|   |   | Pre-run: Remap bigip_b_mgmt -> bigip_mgmt
|   |   | Run: 1_Authenticate folder
|   |   | Post-run: Remap bigip_token -> bigip_b_token
|   |
|- Get BIGIP Version
|   |- Get BIGIP Version on BIG-IP A
|   |   | Pre-run: Remap bigip_a_mgmt -> bigip_mgmt
|   |   | Pre-run: Remap bigip_a_token -> bigip_token
|   |   | Run: 4A_Get_BIGIP_Version folder
|   |   | Post-run: Remap bigip_version -> bigip_a_version
```



```

| | | Post-run: Remap bigip_build -> bigip_a_build
| | |
| | - Get BIGIP Version on BIG-IP B
| | | Pre-run: Remap bigip_b_mgmt -> bigip_mgmt
| | | Pre-run: Remap bigip_b_token -> bigip_token
| | | Run: 4A_Get_BIGIP_Version folder
| | | Post-run: Remap bigip_version -> bigip_b_version
| | | Post-run: Remap bigip_build -> bigip_b_build
| | |
| - Save globalVars to file
|
Stop

```

Note: Collections and folders that are designed to act on multiple devices are designed to automatically use the `bigip_a...` and `bigip_b...` syntax to avoid having to remap variables. In this case the `BIGIP_Operational_Workflows` collection is designed to perform actions on **one** device at a time, thus the need for remapping of the `bigip_token` input variables.

Note: Another option that is available to solve this issue is to define all variables in the local scope for each item. This method is not preferred because it decreases portability and increases complexity in definition of input variables.

Task 2 - Build Complex Workflow JSON

Define Global Settings & Variables:

```

1 {
2   "name": "Wrapper_Demo_2",
3   "description": "Execute a chained workflow that authenticates to two BIG-IPs and
↪ retrieves their software version",
4   "globalEnvVars": "../framework/f5-postman-workflows.postman_globals.json",
5   "globalOptions": {
6     "insecure": true,
7     "reporters": ["cli"]
8   },
9   "globalVars": {
10    "bigip_a_mgmt": "10.1.1.4",
11    "bigip_b_mgmt": "10.1.1.5",
12    "bigip_username": "admin",
13    "bigip_password": "admin"
14  },
15  "saveEnvVars": true,
16  "outputFile": "Wrapper_Demo_2-run.json",
17  "envOutputFile": "Wrapper_Demo_2-env.json"
18 }

```

Define Authentication Items

Note: As shown below, we can use the `skip: true` attribute to signal f5-newman-wrapper to not run that particular item. The items children will still be processed. The `skip` attribute can be used to create a container for similar requests.

```
1 {
2   "workflow": [
3     {
4       "name": "Authenticate to BIG-IPs",
5       "skip": true,
6       "children": [
7         {
8           "name": "Authenticate to BIG-IP A",
9           "options": {
10            "collection": "../collections/BIG_IP/BIGIP_API_Authentication.postman_
↵collection.json",
11            "remapPreRun": {
12              "bigip_a_mgmt": "bigip_mgmt"
13            },
14            "folder": "1_Authenticate",
15            "remapPostRun": {
16              "bigip_token": "bigip_a_token"
17            }
18          }
19        },
20        {
21          "name": "Authenticate to BIG-IP B",
22          "options": {
23            "collection": "../collections/BIG_IP/BIGIP_API_Authentication.postman_
↵collection.json",
24            "remapPreRun": {
25              "bigip_b_mgmt": "bigip_mgmt"
26            },
27            "folder": "1_Authenticate",
28            "remapPostRun": {
29              "bigip_token": "bigip_b_token"
30            }
31          }
32        }
33      ]
34    }
35  ]
36 }
```

The JSON above implements the following part of our branch diagram:

```
| - Authenticate
|   | - Authenticate to BIG-IP A
|   |   | Pre-run: Remap bigip_a_mgmt -> bigip_mgmt
|   |   | Run: 1_Authenticate folder
|   |   | Post-run: Remap bigip_token -> bigip_a_token
|   |
|   | - Run: Authenticate to BIG-IP B
|   |   | Pre-run: Remap bigip_b_mgmt -> bigip_mgmt
|   |   | Run: 1_Authenticate folder
|   |   | Post-run: Remap bigip_token -> bigip_b_token
```

Specifically, note the use of the `skip` attribute on line 5 to create a container to group the items together.

Define Get Software Version Items

```
1 {
2   "workflow": [
3     {
4       "name": "Get BIG-IP Software Versions",
5       "skip": true,
6       "children": [
7         {
8           "name": "Get BIG-IP A Software Version",
9           "options": {
10            "collection": "../collections/BIG_IP/BIGIP_Operational_Workflows.postman_
↪collection.json",
11            "remapPreRun": {
12              "bigip_a_mgmt": "bigip_mgmt",
13              "bigip_a_token": "bigip_token"
14            },
15            "folder": "4A_Get_BIGIP_Version",
16            "remapPostRun": {
17              "bigip_version": "bigip_a_version",
18              "bigip_build": "bigip_a_build"
19            }
20          }
21        },
22        {
23          "name": "Get BIG-IP B Software Version",
24          "options": {
25            "collection": "../collections/BIG_IP/BIGIP_Operational_Workflows.postman_
↪collection.json",
26            "remapPreRun": {
27              "bigip_b_mgmt": "bigip_mgmt",
28              "bigip_b_token": "bigip_token"
29            },
30            "folder": "4A_Get_BIGIP_Version",
31            "remapPostRun": {
32              "bigip_version": "bigip_b_version",
33              "bigip_build": "bigip_b_build"
34            }
35          }
36        }
37      ]
38    }
39  ]
40 }
```

The JSON above implements the following part of our branch diagram:

```
| - Get BIGIP Version
|   | - Get BIGIP Version on BIG-IP A
|   |   | Pre-run: Remap bigip_a_mgmt -> bigip_mgmt
|   |   | Pre-run: Remap bigip_a_token -> bigip_token
|   |   | Run: 4A_Get_BIGIP_Version folder
|   |   | Post-run: Remap bigip_version -> bigip_a_version
|   |   | Post-run: Remap bigip_build -> bigip_a_build
|   |
```

```

|- Get BIGIP Version on BIG-IP B
| | Pre-run: Remap bigip_b_mgmt -> bigip_mgmt
| | Pre-run: Remap bigip_b_token -> bigip_token
| | Run: 4A_Get_BIGIP_Version folder
| | Post-run: Remap bigip_version -> bigip_b_version
| | Post-run: Remap bigip_build -> bigip_b_build

```

Final Workflow JSON

```

1  {
2    "name": "Wrapper_Demo_2",
3    "description": "Execute a chained workflow that authenticates to two BIG-IPs and_
↳ retrieves their software version",
4    "globalEnvVars": "../framework/f5-postman-workflows.postman_globals.json",
5    "globalOptions": {
6      "insecure": true,
7      "reporters": ["cli"]
8    },
9    "globalVars": {
10     "bigip_a_mgmt": "",
11     "bigip_b_mgmt": "",
12     "bigip_username": "admin",
13     "bigip_password": "admin"
14   },
15   "saveEnvVars": true,
16   "outputFile": "Wrapper_Demo_2-run.json",
17   "envOutputFile": "Wrapper_Demo_2-env.json",
18   "workflow": [
19     {
20       "name": "Authenticate to BIG-IPs",
21       "skip": true,
22       "children": [
23         {
24           "name": "Authenticate to BIG-IP A",
25           "options": {
26             "collection": "../collections/BIG_IP/BIGIP_API_Authentication.postman_
↳ collection.json",
27             "remapPreRun": {
28               "bigip_a_mgmt": "bigip_mgmt"
29             },
30             "folder": "1_Authenticate",
31             "remapPostRun": {
32               "bigip_token": "bigip_a_token"
33             }
34           }
35         },
36         {
37           "name": "Authenticate to BIG-IP B",
38           "options": {
39             "collection": "../collections/BIG_IP/BIGIP_API_Authentication.postman_
↳ collection.json",
40             "remapPreRun": {
41               "bigip_b_mgmt": "bigip_mgmt"
42             },
43             "folder": "1_Authenticate",
44             "remapPostRun": {

```

```

45         "bigip_token": "bigip_b_token"
46     }
47 }
48 }
49 ]
50 },
51 {
52     "name": "Get BIG-IP Software Versions",
53     "skip": true,
54     "children": [
55         {
56             "name": "Get BIG-IP A Software Version",
57             "options": {
58                 "collection": "../collections/BIG_IP/BIGIP_Operational_Workflows.postman_
↪collection.json",
59                 "remapPreRun": {
60                     "bigip_a_mgmt": "bigip_mgmt",
61                     "bigip_a_token": "bigip_token"
62                 },
63                 "folder": "4A_Get_BIGIP_Version",
64                 "remapPostRun": {
65                     "bigip_version": "bigip_a_version",
66                     "bigip_build": "bigip_a_build"
67                 }
68             }
69         },
70         {
71             "name": "Get BIG-IP B Software Version",
72             "options": {
73                 "collection": "../collections/BIG_IP/BIGIP_Operational_Workflows.postman_
↪collection.json",
74                 "remapPreRun": {
75                     "bigip_b_mgmt": "bigip_mgmt",
76                     "bigip_b_token": "bigip_token"
77                 },
78                 "folder": "4A_Get_BIGIP_Version",
79                 "remapPostRun": {
80                     "bigip_version": "bigip_b_version",
81                     "bigip_build": "bigip_b_build"
82                 }
83             }
84         }
85     ]
86 }
87 ]
88 }

```

Task 3 - Run the Workflow

1. Open an SSH session as described in the *previous lab*
2. Run `cd f5-postman-workflows/local`
3. Run `cp ../workflows/Wrapper_Demo_2.json .`
4. Edit the `Wrapper_Demo_2.json` file and enter you BIG-IP management addresses

```

1 {
2   "globalVars": {
3     "bigip_a_mgmt": "10.1.1.4",
4     "bigip_b_mgmt": "10.1.1.5",
5     "bigip_username": "admin",
6     "bigip_password": "admin"
7   }
8 }

```

5. Run `f5-newman-wrapper Wrapper_Demo_2.json`
6. Examine the output to see how the workflow was executed.

Example output:

```

[snops@f5-super-netops] [~/f5-postman-workflows/local] $ f5-newman-wrapper
↳ Wrapper_Demo_2.json
[Wrapper_Demo_2-2017-03-30-19-22-52] starting run
[Wrapper_Demo_2-2017-03-30-19-22-52] [runCollection][Authenticate to BIG-IP A]
↳ running...
newman

BIGIP_API_Authentication

? 1_Authenticate
? Authenticate and Obtain Token
  POST https://10.1.1.4/mgmt/shared/authn/login [200 OK, 1.41KB, 570ms]
  ✓ [POST Response Code]=200
  ✓ [Populate Variable] bigip_token=UE7W5CXWM5SJ6SZE5A7KTAI5Q

? Verify Authentication Works
  GET https://10.1.1.4/mgmt/shared/authz/tokens/UE7W5CXWM5SJ6SZE5A7KTAI5Q [200
↳ OK, 1.23KB, 9ms]
  ✓ [GET Response Code]=200
  ✓ [Current Value] token=UE7W5CXWM5SJ6SZE5A7KTAI5Q
  ✓ [Check Value] token == UE7W5CXWM5SJ6SZE5A7KTAI5Q

? Set Authentication Token Timeout
  PATCH https://10.1.1.4/mgmt/shared/authz/tokens/UE7W5CXWM5SJ6SZE5A7KTAI5Q [200
↳ OK, 1.23KB, 13ms]
  ✓ [PATCH Response Code]=200
  ✓ [Current Value] timeout=1200
  ✓ [Check Value] timeout == 1200

?-----?-----?-----?
|                               | executed | failed |
?-----?-----?-----?
|           iterations |           1 |           0 |
?-----?-----?-----?
|           requests |           3 |           0 |
?-----?-----?-----?
|       test-scripts |           3 |           0 |
?-----?-----?-----?
| prerequest-scripts |           1 |           0 |
?-----?-----?-----?
|       assertions |           8 |           0 |
?-----?-----?-----?
| total run duration: 740ms |
?-----?-----?-----?

```

```

| total data received: 1.71KB (approx) |
?-----?
| average response time: 197ms |
?-----?
[Wrapper_Demo_2-2017-03-30-19-22-52] [runCollection][Authenticate to BIG-IP B]
↪running...
newman

BIGIP_API_Authentication

? 1_Authenticate
? Authenticate and Obtain Token
  POST https://10.1.1.5/mgmt/shared/authn/login [200 OK, 1.41KB, 350ms]
  ✓ [POST Response Code]=200
  ✓ [Populate Variable] bigip_token=ONQXOQPNCVOHZELKIFSPHETL3I

? Verify Authentication Works
  GET https://10.1.1.5/mgmt/shared/authz/tokens/ONQXOQPNCVOHZELKIFSPHETL3I [200_
↪OK, 1.23KB, 9ms]
  ✓ [GET Response Code]=200
  ✓ [Current Value] token=ONQXOQPNCVOHZELKIFSPHETL3I
  ✓ [Check Value] token == ONQXOQPNCVOHZELKIFSPHETL3I

? Set Authentication Token Timeout
  PATCH https://10.1.1.5/mgmt/shared/authz/tokens/ONQXOQPNCVOHZELKIFSPHETL3I [200_
↪OK, 1.23KB, 12ms]
  ✓ [PATCH Response Code]=200
  ✓ [Current Value] timeout=1200
  ✓ [Check Value] timeout == 1200

?-----?-----?-----?
| | executed | failed |
?-----?-----?-----?
| iterations | 1 | 0 |
?-----?-----?-----?
| requests | 3 | 0 |
?-----?-----?-----?
| test-scripts | 3 | 0 |
?-----?-----?-----?
| prerequest-scripts | 1 | 0 |
?-----?-----?-----?
| assertions | 8 | 0 |
?-----?-----?-----?
| total run duration: 472ms |
?-----?
| total data received: 1.71KB (approx) |
?-----?
| average response time: 123ms |
?-----?
[Wrapper_Demo_2-2017-03-30-19-22-52] [runCollection][Get BIG-IP A Software_
↪Version] running...
newman

BIGIP_Operational_Workflows

? 4A_Get_BIGIP_Version
? Get Software Version
  GET https://10.1.1.4/mgmt/tm/sys/software/volume [200 OK, 1.32KB, 207ms]

```

```

✓ [GET Response Code]=200
✓ [Populate Variable] bigip_version=12.1.1
✓ [Populate Variable] bigip_build=1.0.196

?-----?-----?-----?
|                                     | executed |   failed |
?-----?-----?-----?
|             iterations |         1 |         0 |
?-----?-----?-----?
|             requests  |         1 |         0 |
?-----?-----?-----?
|          test-scripts |         1 |         0 |
?-----?-----?-----?
|    prerequest-scripts |         0 |         0 |
?-----?-----?-----?
|             assertions |         3 |         0 |
?-----?-----?-----?
| total run duration: 250ms                                     |
?-----?-----?-----?
| total data received: 611B (approx)                             |
?-----?-----?-----?
| average response time: 207ms                                    |
?-----?-----?-----?
[Wrapper_Demo_2-2017-03-30-19-22-52] [runCollection][Get BIG-IP B Software_
↪Version] running...
newman

BIGIP_Operational_Workflows

? 4A_Get_BIGIP_Version
? Get Software Version
GET https://10.1.1.5/mgmt/tm/sys/software/volume [200 OK, 1.32KB, 191ms]
✓ [GET Response Code]=200
✓ [Populate Variable] bigip_version=12.1.1
✓ [Populate Variable] bigip_build=1.0.196

?-----?-----?-----?
|                                     | executed |   failed |
?-----?-----?-----?
|             iterations |         1 |         0 |
?-----?-----?-----?
|             requests  |         1 |         0 |
?-----?-----?-----?
|          test-scripts |         1 |         0 |
?-----?-----?-----?
|    prerequest-scripts |         0 |         0 |
?-----?-----?-----?
|             assertions |         3 |         0 |
?-----?-----?-----?
| total run duration: 230ms                                     |
?-----?-----?-----?
| total data received: 611B (approx)                             |
?-----?-----?-----?
| average response time: 191ms                                    |
?-----?-----?-----?
[Wrapper_Demo_2-2017-03-30-19-22-52] run completed in 3s, 316.921 ms

```

7. Examine the environment variables that were saved at the end of the run by executing `cat`

Wrapper_Demo_2-env.json. The resulting BIG-IP software versions are now present and have been highlighted below.

Example output:

```
1 {
2   "id": "d459e491-4936-4be7-a910-567f711a636a",
3   "values": [
4     {
5       "type": "any",
6       "value": "10.1.1.4",
7       "key": "bigip_a_mgmt"
8     },
9     {
10      "type": "any",
11      "value": "10.1.1.5",
12      "key": "bigip_b_mgmt"
13    },
14    {
15      "type": "any",
16      "value": "10.1.1.5",
17      "key": "bigip_mgmt"
18    },
19    {
20      "type": "any",
21      "value": "admin",
22      "key": "bigip_username"
23    },
24    {
25      "type": "any",
26      "value": "admin",
27      "key": "bigip_password"
28    },
29    {
30      "type": "any",
31      "value": "UE7W5CXWM5SJ6SZEVS7KTAI5Q",
32      "key": "bigip_a_token"
33    },
34    {
35      "type": "any",
36      "value": "ONQXOQPNCVOHZELKIFSPHETL3I",
37      "key": "bigip_b_token"
38    },
39    {
40      "type": "any",
41      "value": "ONQXOQPNCVOHZELKIFSPHETL3I",
42      "key": "bigip_token"
43    },
44    {
45      "type": "any",
46      "value": "12.1.1",
47      "key": "bigip_a_version"
48    },
49    {
50      "type": "any",
51      "value": "1.0.196",
52      "key": "bigip_a_build"
53    },
54    {
```

```

55     "type": "any",
56     "value": "1200",
57     "key": "bigip_token_timeout"
58   },
59   {
60     "type": "any",
61     "value": "12.1.1",
62     "key": "bigip_b_version"
63   },
64   {
65     "type": "any",
66     "value": "1.0.196",
67     "key": "bigip_b_build"
68   }
69 ]
70 }

```

3.3 Module 3: Stitching Workflows from Class 1 into new Orchestratable Collections

In the previous module we saw the example of stitching together the Authentication Folder and some facts gathering. We will now stitch together the Postman Collection from Class 1 and the Authentication Collection from Module 2. Once we validate the new file we'll use f5-newman-wrapper to execute.

Stitching together the collections and workflows allows Super-NetOps engineers the ability to start quickly Orchestrating calls running Automation workflows. This also allows BIG-IP to be Orchestrated from upper level orchestration toolkits.

Using this structure allows you to build your own solutions, to manage BIG-IP quickly as native REST calls are used.

3.3.1 Lab 3.1 - Files used and locations

The `f5-super-netops-container` is a self contained toolkit, meaning everything we need is already in the solution. It will also always be up-to-date, received either from restarting the container or running the update git clones scripts.

Task 1 - Review the super-netops-container files and collections used

1. During the installation of the `super-netops-container` there were several github repositories cloned, all of which are mapped to the `/home/snops/` directory.

Let's make sure all repositories were mapped correctly.

Execute: `cd /home/snops`

The Collections we will be using are located here:

```

|- /f5-automation-labs
  |- /postman_collections
    |   f5-programmability-class-2.postman_collection.json

```

```
| - /f5-postman-workflows
| - /collections
|   | /BIG_IP
|   |     BIGIP_Operational_Workflows.postman_collection.json
```

The f5-newman-wrapper configuration files are located here:

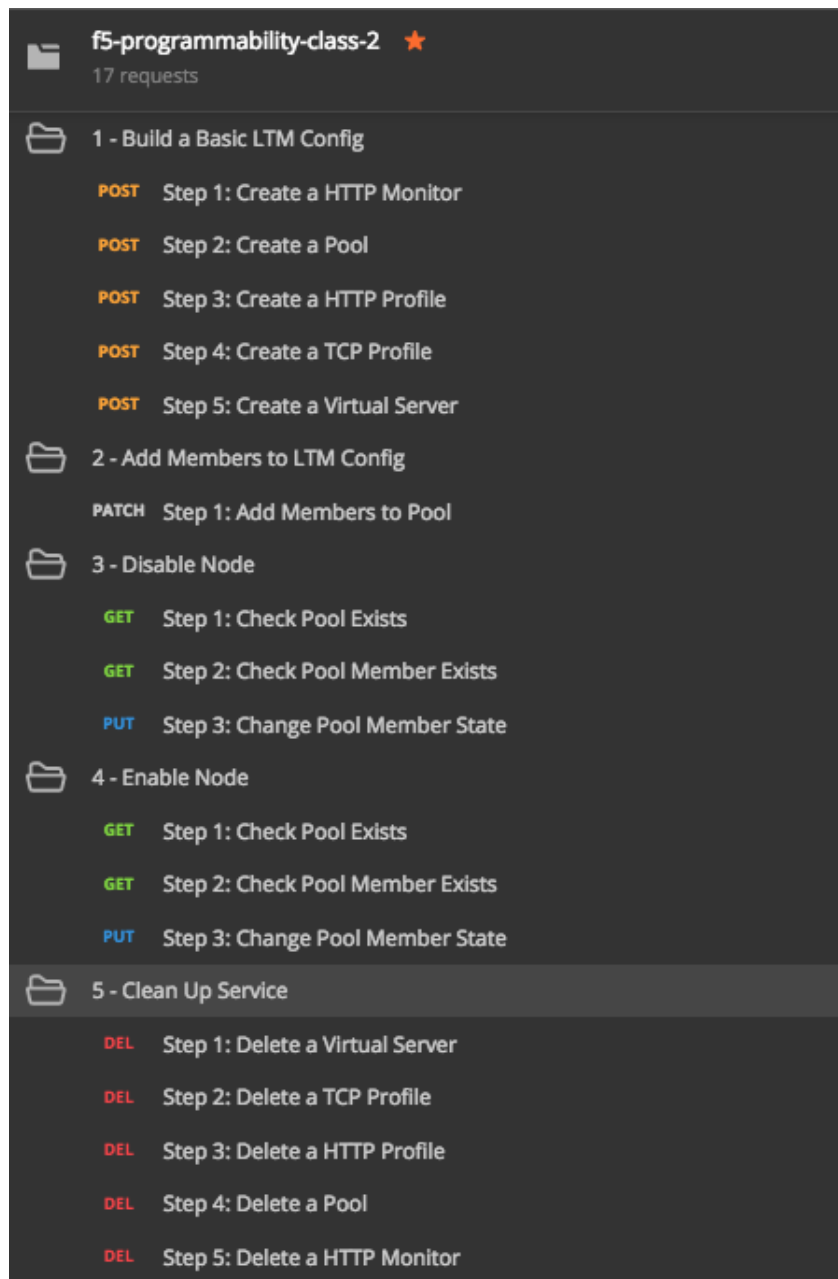
```
| - /f5-automation-labs
|   | - /jenkins
|     | /f5-newman-build
|     |     f5-newman-build-1
|     |     f5-newman-build-2
|     |     f5-newman-build-5
|     | /f5-newman-operation
|     |     f5-newman-build-3
|     |     f5-newman-build-4
```

3.3.2 Lab 3.2 - Execute f5-newman-wrapper for a Build Workflow

Your environment has already been seeded with 5 `f5-newman-wrapper` files, these files will execute against the collections noted in the previous lab. This lab will cover the **Build** aspect, creating a Virtual Server Framework containing all the pieces required for this demo service.

Note: This is a Postman Collection, and can also be imported into the Postman GUI client for viewing

For a visual reference of what `f5-programmability-class-2.postman_collection.json` looks like:



Note: You do not need to have all these operations individually broken out, it is shown this way to educate that Workflows can be as small (update a pool member) or as large (deploy a whole service) as needed

Task 1 - Examine f5-newman-build-1

Note: The contents of this folder contain files for this lab, and upcoming labs in this class

1. Navigate to the location containing the f5-newman-wrapper files `cd ~/f5-automation-labs/jenkins/f5-newman-build`

2. Let's examine the contents of the first f5-newman-wrapper file `cat f5-newman-build-1`

```
1 {
2     "name": "f5-newman-build-1",
3     "description": "Execute a chained workflow that authenticates to a BIG-IP_
4     ↪and builds configuration",
5     "globalEnvVars": "/home/snops/f5-postman-workflows/framework/f5-postman-
6     ↪workflows.postman_globals.json",
7     "globalOptions": {
8         "insecure": true,
9         "reporters": ["cli"]
10    },
11    "globalVars": {
12        "bigip_mgmt": "10.1.1.4",
13        "bigip_username": "admin",
14        "bigip_password": "admin",
15        "bigip_partition": "Common",
16        "bigip_pool_name": "module_3_pool",
17        "bigip_pool_member": "75.67.228.133:80",
18        "bigip_object_state": "user-up",
19        "bigip_object_session": "user-enabled",
20        "bigip_vs_name": "module_3_vs",
21        "bigip_vs_destination": "10.1.20.129:80",
22        "bigip_node_name": "75.67.228.133",
23        "bigip_http_monitor": "module_3_http_monitor",
24        "bigip_http_profile": "module_3_http",
25        "bigip_tcp_profile": "module_3_tcp_clientside"
26    },
27    "workflow": [
28        {
29            "name": "Authenticate to BIG-IP",
30            "options": {
31                "collection": "/home/snops/f5-postman-workflows/
32                ↪collections/BIG_IP/BIGIP_API_Authentication.postman_collection.json",
33                "folder": "1_Authenticate"
34            }
35        }, (REMOVE THIS TEXT AND ADD YOUR CODE BELOW)
36    ]
37 }
```

#. The above f5-newman-wrapper file only has the Authenticate to BIG-IP Collection/Folder referenced, **we will need to add in another collection**. You are going to add this code snippet after the last },. This shows the method for chaining together multiple calls from multiple sources, shown in a previous lab. For editing files VIM/VI is installed on the container, if you **do not know** how to use VIM/VI please let the instructor know.

```
1 {
2     "name": "1 - Build a Basic LTM Config",
3     "skip": false,
4     "options": {
5         "collection": "/home/snops/f5-automation-labs/postman_
6         ↪collections/f5-programmability-class-2.postman_collection.json",
7         "folder": "1 - Build a Basic LTM Config"
8     }
9 }
```

1. Now that you have the full file you can see what it will look like with `cat f5-newman-build-1`. The

environment variables will float into both Collections, and the returned Global Variables will persist during the whole run.

Example of a complete file:

```
1 {
2     "name": "f5-newman-build-1",
3     "description": "Execute a chained workflow that authenticates to a BIG-IP and
↳ builds configuration",
4     "globalEnvVars": "/home/snops/f5-postman-workflows/framework/f5-postman-
↳ workflows.postman_globals.json",
5     "globalOptions": {
6         "insecure": true,
7         "reporters": ["cli"]
8     },
9     "globalVars": {
10         "bigip_mgmt": "10.1.1.4",
11         "bigip_username": "admin",
12         "bigip_password": "admin",
13         "bigip_partition": "Common",
14         "bigip_pool_name": "module_3_pool",
15         "bigip_pool_member": "75.67.228.133:80",
16         "bigip_object_state": "user-up",
17         "bigip_object_session": "user-enabled",
18         "bigip_vs_name": "module_3_vs",
19         "bigip_vs_destination": "10.1.20.129:80",
20         "bigip_node_name": "75.67.228.133",
21         "bigip_http_monitor": "module_3_http_monitor",
22         "bigip_http_profile": "module_3_http",
23         "bigip_tcp_profile": "module_3_tcp_clientside"
24     },
25     "workflow": [
26         {
27             "name": "Authenticate to BIG-IP",
28             "options": {
29                 "collection": "/home/snops/f5-postman-workflows/
↳ collections/BIG_IP/BIGIP_API_Authentication.postman_collection.json",
30                 "folder": "1_Authenticate"
31             }
32         },
33         {
34             "name": "1 - Build a Basic LTM Config",
35             "skip": false,
36             "options": {
37                 "collection": "/home/snops/f5-automation-labs/postman_
↳ collections/f5-programmability-class-2.postman_collection.json",
38                 "folder": "1 - Build a Basic LTM Config"
39             }
40         }
41     ]
42 }
```

Task 2 - Execute the first f5-newman-wrapper file

1. Login to your BIG-IP lab machine and verify you do not have any Virtual Servers or Pools

Note: If you are using the F5 lab systems there are already shortcuts in your Chrome browser

```

46 newman
47
48 f5-programmability-class-2
49
50 ? 1 - Build a Basic LTM Config
51 ? Step 1: Create a HTTP Monitor
52   POST https://10.1.1.4/mgmt/tm/ltm/monitor/http [200 OK, 1.32KB, 625ms]
53
54 ? Step 2: Create a Pool
55   POST https://10.1.1.4/mgmt/tm/ltm/pool [200 OK, 1.56KB, 157ms]
56
57 ? Step 3: Create a HTTP Profile
58   POST https://10.1.1.4/mgmt/tm/ltm/profile/http [200 OK, 1.96KB, 183ms]
59
60 ? Step 4: Create a TCP Profile
61   POST https://10.1.1.4/mgmt/tm/ltm/profile/tcp [200 OK, 2.68KB, 64ms]
62
63 ? Step 5: Create a Virtual Server
64   POST https://10.1.1.4/mgmt/tm/ltm/virtual [200 OK, 1.9KB, 230ms]
65
66 ?-----?-----?-----?
67 |                               | executed |   failed |
68 ?-----?-----?-----?
69 |             iterations |         1 |         0 |
70 ?-----?-----?-----?
71 |             requests  |         5 |         0 |
72 ?-----?-----?-----?
73 |          test-scripts |         0 |         0 |
74 ?-----?-----?-----?
75 |    prerequest-scripts |         0 |         0 |
76 ?-----?-----?-----?
77 |             assertions |         0 |         0 |
78 ?-----?-----?-----?
79 | total run duration: 1406ms                               |
80 ?-----?-----?-----?
81 | total data received: 5.79KB (approx)                       |
82 ?-----?-----?-----?
83 | average response time: 251ms                               |
84 ?-----?-----?-----?
85 [f5-newman-build-1-2017-07-26-08-23-00] run completed in 6s, 90.207 ms

```

Note: Notice the 200 OK responses, the number of requests etc., we're building in testing and logging, look back at BIGIP-A for the newly created Application Service Framework

3. On BIG-IP A, examine Virtual Server `module_3_vs`:

<input checked="" type="checkbox"/>	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
<input type="checkbox"/>		module_3_vs			10.1.20.129	80 (HTTP)	Standard	Edit...	Common

4. On BIG-IP A, examine Pool `module_3_pool`:

<input checked="" type="checkbox"/>	Status	Name	Description	Application	Members	Partition / Path
<input type="checkbox"/>		module_3_pool			0	Common

Task 3 - Execute the second f5-newman-wrapper file

1. f5-newman-build-2 contains calls to add pool members to the Application Service Framework created above; this is done independently of the build, to show Service staging as a possible use case.

Execute: f5-newman-wrapper f5-newman-build-2

Output should look like:


```
1 $ f5-newman-wrapper f5-newman-build-2
2 [f5-newman-build-2-2017-07-26-08-40-52] starting run
3 [f5-newman-build-2-2017-07-26-08-40-52] [runCollection][Authenticate to BIG-IP]
  ↳running...
4 newman
5
6 BIGIP_API_Authentication
7
8 ? 1_Authenticate
9 ? Authenticate and Obtain Token
10 POST https://10.1.1.4/mgmt/shared/authn/login [200 OK, 1.41KB, 272ms]
11 ✓ [POST Response Code]=200
12 ✓ [Populate Variable] bigip_token=WSNAXWTCWNZGJG7MDBVF6CRXTB
13
14 ? Verify Authentication Works
15 GET https://10.1.1.4/mgmt/shared/authz/tokens/WSNAXWTCWNZGJG7MDBVF6CRXTB [200 OK,
  ↳ 1.23KB, 15ms]
16 ✓ [GET Response Code]=200
17 ✓ [Current Value] token=WSNAXWTCWNZGJG7MDBVF6CRXTB
18 ✓ [Check Value] token == WSNAXWTCWNZGJG7MDBVF6CRXTB
19
20 ? Set Authentication Token Timeout
21 PATCH https://10.1.1.4/mgmt/shared/authz/tokens/WSNAXWTCWNZGJG7MDBVF6CRXTB [200
  ↳OK, 1.23KB, 61ms]
22 ✓ [PATCH Response Code]=200
23 ✓ [Current Value] timeout=1200
24 ✓ [Check Value] timeout == 1200
25
26 ?-----?-----?-----?
27 | | | executed | failed |
28 ?-----?-----?-----?
29 | iterations | 1 | 0 |
30 ?-----?-----?-----?
31 | requests | 3 | 0 |
32 ?-----?-----?-----?
33 | test-scripts | 3 | 0 |
34 ?-----?-----?-----?
35 | prerequest-scripts | 1 | 0 |
36 ?-----?-----?-----?
37 | assertions | 8 | 0 |
38 ?-----?-----?-----?
39 | total run duration: 1034ms |
40 ?-----?-----?-----?
41 | total data received: 1.71KB (approx) |
42 ?-----?-----?-----?
43 | average response time: 116ms |
44 ?-----?-----?-----?
45 [f5-newman-build-2-2017-07-26-08-40-52] [runCollection][2 - Add Members to LTM
  ↳Config] running...
```

```

46 newman
47
48 f5-programmability-class-2
49
50 ? 2 - Add Members to LTM Config
51 ? Step 1: Add Members to Pool
52 PATCH https://10.1.1.4/mgmt/tm/ltm/pool/module_3_pool [200 OK, 1.52KB, 143ms]
53
54 ?-----?-----?-----?
55 | | | executed | failed |
56 ?-----?-----?-----?
57 | iterations | 1 | 0 |
58 ?-----?-----?-----?
59 | requests | 1 | 0 |
60 ?-----?-----?-----?
61 | test-scripts | 0 | 0 |
62 ?-----?-----?-----?
63 | prerequest-scripts | 0 | 0 |
64 ?-----?-----?-----?
65 | assertions | 0 | 0 |
66 ?-----?-----?-----?
67 | total run duration: 182ms |
68 ?-----?-----?-----?
69 | total data received: 818B (approx) |
70 ?-----?-----?-----?
71 | average response time: 143ms |
72 ?-----?-----?-----?
73 [f5-newman-build-2-2017-07-26-08-40-52] run completed in 4s, 328.497 ms

```

2. On BIG-IP A examine Virtual Server `module_3_vs`, the Virtual Server should be healthy and Green:

<input checked="" type="checkbox"/>	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
<input type="checkbox"/>		module_3_vs			10.1.20.129	80 (HTTP)	Standard	Edit...	Common

3. On BIG-IP A examine Pool `module_3_pool`:

<input checked="" type="checkbox"/>	Status	Name	Description	Application	Members	Partition / Path
<input type="checkbox"/>		module_3_pool			2	Common

3.3.3 Lab 3.3 - Execute f5-newman-wrapper for an Operations Workflow

In the last lab we walked through creating an Application Service Framework, and then updating the Service Framework in a separate call. This lab has 2 f5-newman-files also, one used to user-down a pool member, and another to user-up the same member. These could be used as individual calls from another toolkit (which we'll see later) or run independently as a single commands.

Task 1 - Execute f5-newman-build-3

1. Navigate to the location containing the f5-newman-wrapper files `cd ~/f5-automation-labs/jenkins/f5-newman-operation`
2. On BIGIP-A, examine the pool `module_3_pool`, you should see 2 active (Green) pool members:

Local Traffic » Pools : Pool List » **module_3_pool**

Load Balancing

Load Balancing Method: Round Robin ▼

Priority Group Activation: Disabled ▼

Current Members

<input checked="" type="checkbox"/>	Status	Member	Address	Service Port	FQDN	Ephemeral
<input type="checkbox"/>	●	75.67.228.133:80	75.67.228.133	80		No
<input type="checkbox"/>	●	216.16.74.15:80	216.16.74.15	80		No

3. f5-newman-build-3 contains calls to change the node state to **user-down** for "bigip_pool_member": "10.1.10.101:8002", both of these are specified as variables in the f5-newman-wrapper files.

Execute: f5-newman-wrapper f5-newman-build-3

Output should look like:

```

1  $ f5-newman-wrapper f5-newman-build-3
2  [f5-newman-build-3-2017-07-26-09-06-53] starting run
3  [f5-newman-build-3-2017-07-26-09-06-53] [runCollection][Authenticate to BIG-IP]
4  ↪running...
5  newman
6  BIGIP_API_Authentication
7
8  ? 1_Authenticate
9  ? Authenticate and Obtain Token
10  POST https://10.1.1.4/mgmt/shared/authn/login [200 OK, 1.41KB, 267ms]
11  ✓ [POST Response Code]=200
12  ✓ [Populate Variable] bigip_token=JFN6TNIRAWEKNR5QPM26VT4QFE
13
14  ? Verify Authentication Works
15  GET https://10.1.1.4/mgmt/shared/authz/tokens/JFN6TNIRAWEKNR5QPM26VT4QFE [200
16  ↪OK, 1.23KB, 22ms]
17  ✓ [GET Response Code]=200
18  ✓ [Current Value] token=JFN6TNIRAWEKNR5QPM26VT4QFE
19  ✓ [Check Value] token == JFN6TNIRAWEKNR5QPM26VT4QFE
20
21  ? Set Authentication Token Timeout
22  PATCH https://10.1.1.4/mgmt/shared/authz/tokens/JFN6TNIRAWEKNR5QPM26VT4QFE [200
23  ↪OK, 1.23KB, 26ms]
24  ✓ [PATCH Response Code]=200
25  ✓ [Current Value] timeout=1200
26  ✓ [Check Value] timeout == 1200

```

```

26 ?-----?-----?-----?
27 |                               | executed |    failed |
28 ?-----?-----?-----?
29 |             iterations |         1 |         0 |
30 ?-----?-----?-----?
31 |             requests  |         3 |         0 |
32 ?-----?-----?-----?
33 |             test-scripts |         3 |         0 |
34 ?-----?-----?-----?
35 |    prerequest-scripts |         1 |         0 |
36 ?-----?-----?-----?
37 |             assertions |         8 |         0 |
38 ?-----?-----?-----?
39 | total run duration: 1243ms                               |
40 ?-----?-----?-----?
41 | total data received: 1.71KB (approx)                       |
42 ?-----?-----?-----?
43 | average response time: 105ms                               |
44 ?-----?-----?-----?
45 [f5-newman-build-3-2017-07-26-09-06-53] [runCollection][3 - Disable Node] running.
46 ↳..
47 newman
48 f5-programmability-class-2
49
50 ? 3 - Disable Node
51 ? Step 1: Check Pool Exists
52   GET https://10.1.1.4/mgmt/tm/ltn/pool/~Common~module_3_pool [200 OK, 1.56KB, ↳
53   ↳39ms]
54   ✓ [GET Response Code]=200
55
56 ? Step 2: Check Pool Member Exists
57   GET https://10.1.1.4/mgmt/tm/ltn/pool/~Common~module_3_pool/members/~Common~10.
58   ↳1.10.101:8002 [200 OK, 1.25KB, 33ms]
59   ✓ [GET Response Code]=200
60
61 ? Step 3: Change Pool Member State
62   PUT https://10.1.1.4/mgmt/tm/ltn/pool/~Common~module_3_pool/members/~Common~10.
63   ↳1.10.101:8002 [200 OK, 1.25KB, 298ms]
64   ✓ [PUT Response Code]=200
65
66 ?-----?-----?-----?
67 |                               | executed |    failed |
68 ?-----?-----?-----?
69 |             iterations |         1 |         0 |
70 ?-----?-----?-----?
71 |             requests  |         3 |         0 |
72 ?-----?-----?-----?
73 |             test-scripts |         3 |         0 |
74 ?-----?-----?-----?
75 |    prerequest-scripts |         1 |         0 |
76 ?-----?-----?-----?
77 |             assertions |         3 |         0 |
78 ?-----?-----?-----?
79 | total run duration: 1092ms                               |
80 ?-----?-----?-----?
81 | total data received: 1.89KB (approx)                       |
82 ?-----?-----?-----?

```

```

80 | average response time: 123ms |
81 ?-----?
82 [f5-newman-build-3-2017-07-26-09-06-53] run completed in 6s, 564.868 ms

```

Note: Notice the 200 OK responses, as it completed successfully

4. Log back into BIG-IP A examine the pool `module_3_pool` status page you should see on black diamond node and another node green and online:

Local Traffic » Pools : Pool List » **module_3_pool**

Load Balancing

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

Current Members

<input checked="" type="checkbox"/>	Status	Member	Address	Service Port	FQDN	Ephemeral
<input type="checkbox"/>		75.67.228.133:80	75.67.228.133	80		No
<input type="checkbox"/>		216.16.74.15:80	216.16.74.15	80		No

Task 2 - Execute f5-newman-build-4

1. Navigate to the location containing the f5-newman-wrapper files `cd ~/f5-automation-labs/jenkins/f5-newman-operation`
2. On BIG-IP A examine the pool `module_3_pool`, you should show only 1 Active and Green:

Local Traffic » Pools : Pool List » **module_3_pool**

Load Balancing

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

Current Members

<input checked="" type="checkbox"/>	Status	Member	Address	Service Port	FQDN	Ephemeral
<input type="checkbox"/>		75.67.228.133:80	75.67.228.133	80		No
<input type="checkbox"/>		216.16.74.15:80	216.16.74.15	80		No

3. f5-newman-build-3 contains calls to **user-up** variable node "bigip_pool_member":"10.1.10.101:8002"

Execute: f5-newman-wrapper f5-newman-build-4

Output should look like:

```

1  $ f5-newman-wrapper f5-newman-build-4
2  [f5-newman-build-4-2017-07-26-09-12-47] starting run
3  [f5-newman-build-4-2017-07-26-09-12-47] [runCollection][Authenticate to BIG-IP]
4  ↳running...
5  newman
6  BIGIP_API_Authentication
7
8  ? 1_Authenticate
9  ? Authenticate and Obtain Token
10  POST https://10.1.1.4/mgmt/shared/authn/login [200 OK, 1.41KB, 240ms]
11  ✓ [POST Response Code]=200
12  ✓ [Populate Variable] bigip_token=LN5IEBCKW5TTNXZLX5VYRUTOW5
13
14  ? Verify Authentication Works
15  GET https://10.1.1.4/mgmt/shared/authz/tokens/LN5IEBCKW5TTNXZLX5VYRUTOW5 [200
16  ↳OK, 1.23KB, 15ms]
17  ✓ [GET Response Code]=200
18  ✓ [Current Value] token=LN5IEBCKW5TTNXZLX5VYRUTOW5
19  ✓ [Check Value] token == LN5IEBCKW5TTNXZLX5VYRUTOW5
20
21  ? Set Authentication Token Timeout
22  PATCH https://10.1.1.4/mgmt/shared/authz/tokens/LN5IEBCKW5TTNXZLX5VYRUTOW5 [200
23  ↳OK, 1.23KB, 27ms]
24  ✓ [PATCH Response Code]=200
25  ✓ [Current Value] timeout=1200
26  ✓ [Check Value] timeout == 1200
27
28  ?-----?-----?-----?

```

```

27 | | executed | failed |
28 ?-----?-----?
29 | iterations | 1 | 0 |
30 ?-----?-----?
31 | requests | 3 | 0 |
32 ?-----?-----?
33 | test-scripts | 3 | 0 |
34 ?-----?-----?
35 | prerequest-scripts | 1 | 0 |
36 ?-----?-----?
37 | assertions | 8 | 0 |
38 ?-----?-----?
39 | total run duration: 922ms |
40 ?-----?
41 | total data received: 1.71KB (approx) |
42 ?-----?
43 | average response time: 94ms |
44 ?-----?
45 [f5-newman-build-4-2017-07-26-09-12-47] [runCollection][4 - Enable Node] running..
46 ↪.
47 newman
48 f5-programmability-class-2
49
50 ? 4 - Enable Node
51 ? Step 1: Check Pool Exists
52 GET https://10.1.1.4/mgmt/tm/ltm/pool/~Common~module_3_pool [200 OK, 1.56KB, ↪
53 ↪31ms]
54 ✓ [GET Response Code]=200
55
56 ? Step 2: Check Pool Member Exists
57 GET https://10.1.1.4/mgmt/tm/ltm/pool/~Common~module_3_pool/members/~Common~10.
58 ↪1.10.101:8002 [200 OK, 1.25KB, 28ms]
59 ✓ [GET Response Code]=200
60
61 ? Step 3: Change Pool Member State
62 PUT https://10.1.1.4/mgmt/tm/ltm/pool/~Common~module_3_pool/members/~Common~10.
63 ↪1.10.101:8002 [200 OK, 1.25KB, 62ms]
64 ✓ [PUT Response Code]=200
65
66 ?-----?-----?
67 | | executed | failed |
68 ?-----?-----?
69 | iterations | 1 | 0 |
70 ?-----?-----?
71 | requests | 3 | 0 |
72 ?-----?-----?
73 | test-scripts | 3 | 0 |
74 ?-----?-----?
75 | prerequest-scripts | 1 | 0 |
76 ?-----?-----?
77 | assertions | 3 | 0 |
78 ?-----?-----?
79 | total run duration: 519ms |
80 ?-----?
81 | total data received: 1.89KB (approx) |
82 ?-----?
83 | average response time: 40ms |

```

```

81 ?-----?
82 [f5-newman-build-4-2017-07-26-09-12-47] run completed in 4s, 510.429 ms

```

Note: Notice the 200 OK responses, as it completed successfully

- On BIG-IP A examine Pool `module_3_pool` all Nodes should be back to the beginning state:

Local Traffic » Pools : Pool List » module_3_pool

Properties Members Statistics

Load Balancing

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

Update

Current Members

<input checked="" type="checkbox"/>	Status	Member	Address	Service Port	FQDN	Ephemeral
<input type="checkbox"/>	Green	75.67.228.133:80	75.67.228.133	80		No
<input type="checkbox"/>	Green	216.16.74.15:80	216.16.74.15	80		No

Enable Disable Force Offline Remove

3.3.4 Lab 3.3 - Execute an f5-newman-wrapper for Teardown

To get ready for the next module, we're going to execute one last f5-newman-wrapper directly. This file is designed to delete the framework and service we created in the last few labs. We used 2 f5-newman-wrapper files to create our service, but for the deletion we will only use 1. This is important because we can separate the service nodes availability into Infrastructure as Code concepts loosely coupled from the service and calls needed.

Task 1 - Execute f5-newman-build-5

- Navigate to the location containing the f5-newman-wrapper files `cd ~/f5-automation-labs/jenkins/f5-newman-build`
- On BIG-IP A examine the virtual server `module_3_vs`, it should be active and Green:

<input checked="" type="checkbox"/>	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
<input type="checkbox"/>	Green	module_3_vs			10.1.20.129	80 (HTTP)	Standard	Edit...	Common

- On BIGIP-A examine the pool `module_3_pool`, you should show 2 active members Green:

<input checked="" type="checkbox"/>	Status	Name	Description	Application	Members	Partition / Path
<input type="checkbox"/>	Green	module_3_pool			2	Common

4. f5-newman-build-5 contains calls to delete all items we've created in the last few modules

Execute: f5-newman-wrapper f5-newman-build-5

Output should look like:

```
1 $ f5-newman-wrapper f5-newman-build-5
2 [f5-newman-build-5-2017-07-26-09-28-13] starting run
3 [f5-newman-build-5-2017-07-26-09-28-13] [runCollection][Authenticate to BIG-IP]_
  ↳running...
4 newman
5
6 BIGIP_API_Authentication
7
8 ? 1_Authenticate
9 ? Authenticate and Obtain Token
10 POST https://10.1.1.4/mgmt/shared/authn/login [200 OK, 1.41KB, 194ms]
11 ✓ [POST Response Code]=200
12 ✓ [Populate Variable] bigip_token=NGEHHD6ZDJFD2MNF2UL3UXTGVH
13
14 ? Verify Authentication Works
15 GET https://10.1.1.4/mgmt/shared/authz/tokens/NGEHHD6ZDJFD2MNF2UL3UXTGVH [200_
  ↳OK, 1.23KB, 16ms]
16 ✓ [GET Response Code]=200
17 ✓ [Current Value] token=NGEHHD6ZDJFD2MNF2UL3UXTGVH
18 ✓ [Check Value] token == NGEHHD6ZDJFD2MNF2UL3UXTGVH
19
20 ? Set Authentication Token Timeout
21 PATCH https://10.1.1.4/mgmt/shared/authz/tokens/NGEHHD6ZDJFD2MNF2UL3UXTGVH [200_
  ↳OK, 1.23KB, 17ms]
22 ✓ [PATCH Response Code]=200
23 ✓ [Current Value] timeout=1200
24 ✓ [Check Value] timeout == 1200
25
26 ?-----?-----?-----?
27 | | | executed | failed |
28 ?-----?-----?-----?
29 | iterations | 1 | 0 |
30 ?-----?-----?-----?
31 | requests | 3 | 0 |
32 ?-----?-----?-----?
33 | test-scripts | 3 | 0 |
34 ?-----?-----?-----?
35 | prerequest-scripts | 1 | 0 |
36 ?-----?-----?-----?
37 | assertions | 8 | 0 |
38 ?-----?-----?-----?
39 | total run duration: 835ms |
40 ?-----?-----?-----?
41 | total data received: 1.71KB (approx) |
42 ?-----?-----?-----?
43 | average response time: 75ms |
44 ?-----?-----?-----?
45 [f5-newman-build-5-2017-07-26-09-28-13] [runCollection][5 - Clean Up Service]_
  ↳running...
46 newman
47
48 f5-programmability-class-2
49
```

```

50 ? 5 - Clean Up Service
51 ? Step 1: Delete a Virtual Server
52   DELETE https://10.1.1.4/mgmt/tm/lrm/virtual/module_3_vs [200 OK, 740B, 57ms]
53
54 ? Step 2: Delete a TCP Profile
55   DELETE https://10.1.1.4/mgmt/tm/lrm/profile/tcp/module_3_tcp_clientside [200 OK,
56   ↪ 740B, 88ms]
57
58 ? Step 3: Delete a HTTP Profile
59   DELETE https://10.1.1.4/mgmt/tm/lrm/profile/http/module_3_http [200 OK, 740B, ↪
60   ↪ 56ms]
61
62 ? Step 4: Delete a Pool
63   DELETE https://10.1.1.4/mgmt/tm/lrm/pool/module_3_pool [200 OK, 740B, 47ms]
64
65 ? Step 5: Delete a HTTP Monitor
66   DELETE https://10.1.1.4/mgmt/tm/lrm/monitor/http/module_3_http_monitor [200 OK, ↪
67   ↪ 740B, 59ms]
68
69 ?-----?-----?-----?
70 |               | executed |   failed |
71 ?-----?-----?-----?
72 |               | iterations |         1 |         0 |
73 ?-----?-----?-----?
74 |               | requests |         5 |         0 |
75 ?-----?-----?-----?
76 |               | test-scripts |         0 |         0 |
77 ?-----?-----?-----?
78 |               | prerequest-scripts |         0 |         0 |
79 ?-----?-----?-----?
80 |               | assertions |         0 |         0 |
81 ?-----?-----?-----?
82 | total run duration: 445ms |
83 ?-----?-----?-----?
84 | total data received: 0B (approx) |
85 ?-----?-----?-----?
86 | average response time: 61ms |
87 ?-----?-----?-----?
88 [f5-newman-build-5-2017-07-26-09-28-13] run completed in 4s, 267.464 ms

```

Note: Notice the 200 OK responses, as it completed successfully

5. On BIG-IP A examine Virtual `module_3_vs` and Pool `module_3_pool` are deleted

3.4 Module 4: Continuous Integration / Continuous Delivery

This Module will continue to build up our Infrastructure to a Self-Service or CI/CD goal. We will be building on the code that was utilized in the previous modules and labs, though now we'll use Jenkins to provide a CI/CD mechanism. This lab will also use Slack to notify users of changes going on in real time.

Tools we will be using:

- f5-newman-wrapper & previous workflows
 - The previous 5 wrapper workflows files will be executed, but from a Jenkins Pipeline

- f5-super-netops-container
 - Continuing delivery of F5 configuration from a self contained toolkit
 - This version or **variant** of the container has Jenkins installed for you, this is depicted from tag associated to the Docker Image `f5devcentral/f5-super-netops-container:jenkins`
- Slack
 - There has been a Slack channel already setup on your behalf, which we will all be monitoring for environment changes
 - Any person with an @f5.com email address can join the Slack Channel. To join and view the transactions use <https://f5agilitydevops.slack.com/signup>
- Jenkins
 - Jenkins is installed on the f5-super-netops-container, accessed via `http://localhost:10000` (Web) user credentials are `admin/default`

From the previous labs you should already have your Super-NetOps-Container already running, if it's not please refer to Class 2 Module 2 on starting the service.

3.4.1 Lab 4.1 - File Locations and Jenkins setup

We've been executing all our commands locally from Automated scripts; we are now going to take the different toolkits and tie them together to form a **Pipeline**. Pipelines will vary in deployments and even within solutions. Our lab will show you just one way one could be utilized.

Task 1 - Locating the Jenkins files and how they are setup

1. Lets make sure the Jenkins files were mapped correctly.

Execute: `cd ~/f5-automation-labs/jenkins` to access our folder containing the Jenkins Pipeline Files

2. The Jenkins files are located alongside the f5-newman-wrapper files we've used in the previous labs, setup this way was for ease of learning. You may place tools in different structures in your environment.

File Locations:

```
| - /f5-automation-labs
|   | - /jenkins
|   |   | /f5-newman-build
|   |   |   Jenkinsfile1-2
|   |   |   Jenkinsfile5
|   |   | /f5-newman-operation
|   |   |   Jenkinsfile3
|   |   |   Jenkinsfile4
```

3. Lets review the first Jenkins file, from the current folder structure execute `cat Jenkinsfile1-2`

File output:

```
1 node {
2   stage('Testing') {
3     //Run the tests
4     //sh "python -m /home/snops/f5-automation-labs/jenkins/f5-newman-build/f5-
↪newman-build-1"
5     //sh "python -m /home/snops/f5-automation-labs/jenkins/f5-newman-build/f5-
↪newman-build-2"
```

```

6   }
7   stage('Framework-Deployment') {
8       //Run SNOOPS Container Newman Package Virtual and Pool
9       sh "f5-newman-wrapper /home/snops/f5-automation-labs/jenkins/f5-newman-
↳build/f5-newman-build-1"
10      //chatops slack message that run has completed
11      slackSend(
12          channel: '#jenkins_builds',
13          color: 'good',
14          message: 'Super-NetOps Engineer is about to deploy an F5 Service_
↳Framework, Approval Needed!',
15          teamDomain: 'f5agilitydevops',
16          token: 'vLMQmBq2tiyiCcZoNlbnAi0Z'
17      )
18  }
19  stage('Approval') {
20      //Gate the process and require approval
21      input 'Proceed?'
22      //chatops slack message that run has completed
23      slackSend(
24          channel: '#jenkins_builds',
25          color: 'good',
26          message: 'Super-NetOps Engineer just approved a new F5 Service_
↳Framework, thats some serious Continuous Delivery!',
27          teamDomain: 'f5agilitydevops',
28          token: 'vLMQmBq2tiyiCcZoNlbnAi0Z'
29      )
30  }
31  stage('Add-Sevice-Node') {
32      //Run SNOOPS Container Newman Package add Node to Pool
33      sh "f5-newman-wrapper /home/snops/f5-automation-labs/jenkins/f5-newman-
↳build/f5-newman-build-2"
34      //chatops slack message that run has completed
35      slackSend(
36          channel: '#jenkins_builds',
37          color: 'good',
38          message: 'Super-NetOps Engineer just added a Node to a Service,
↳Production is Online!',
39          teamDomain: 'f5agilitydevops',
40          token: 'vLMQmBq2tiyiCcZoNlbnAi0Z'
41      )
42  }
43  }

```

- This is a Jenkins Pipeline file, which we will be inputing into a Pipeline deployment via our Jenkins Toolkit.
- The file should be human readable even without Jenkins experience, a `stage` can be thought of as a step in the Pipeline (or a work-center in manufacturing terms); right after the stage is its name, followed by some commands. Since the super-netops-container is running this Jenkins installation locally, we can use local mappings to file structure.
- In more common deployments the Jenkins file would be stored in a SCM (like Github) and called during an Event (Build/Pull Request) or a Polling Timer, or even some other kind of scripting launch.
- Testing in Pipeline before executing code with tools like `linter` or python scripts can make sure formatting is valid, reducing errors from happening during builds.

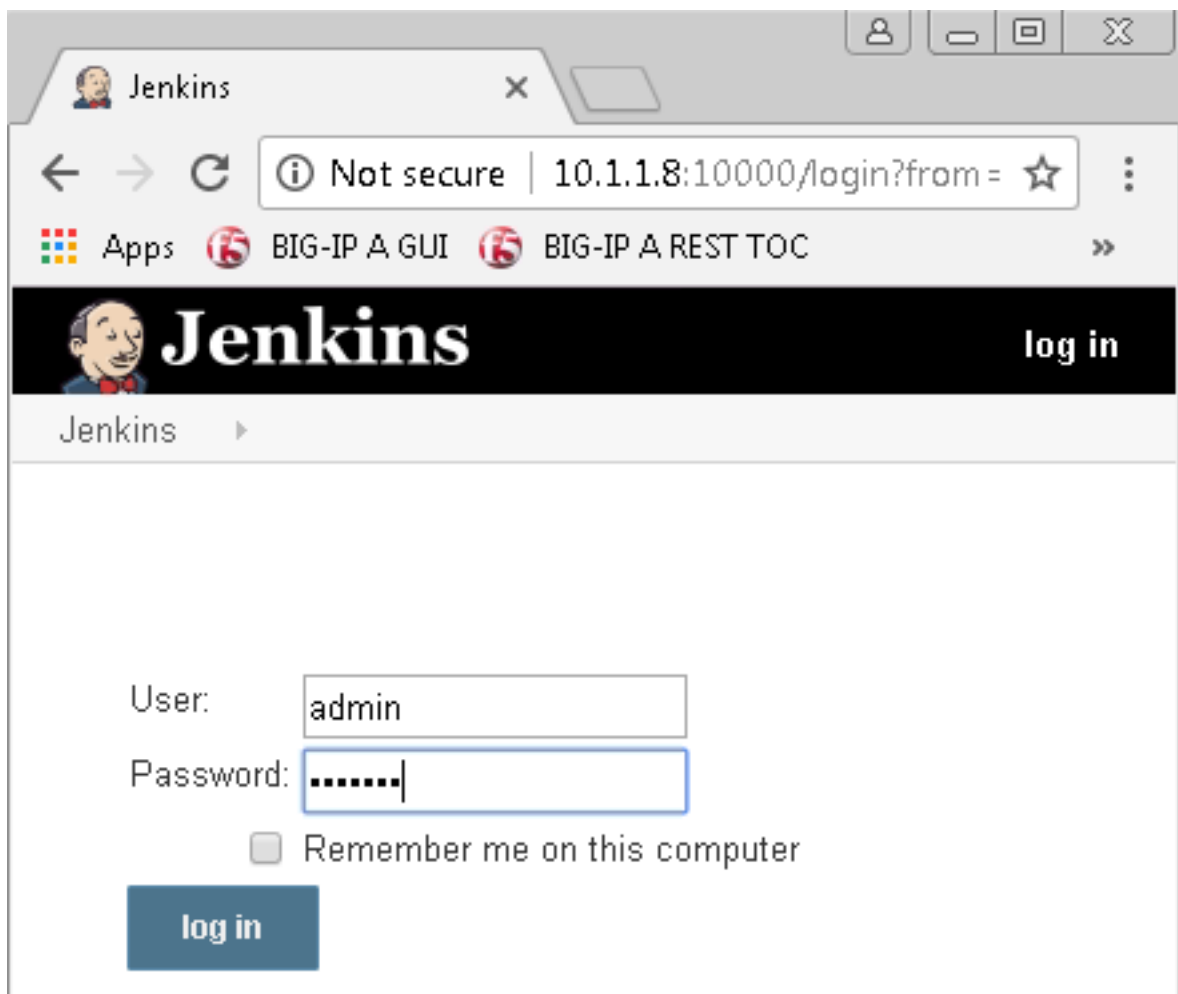
Our installation also has some Slack calls. Which we will setup next.

Task 2 - Accessing Jenkins and Installing the Slack-Notifier Plug-in

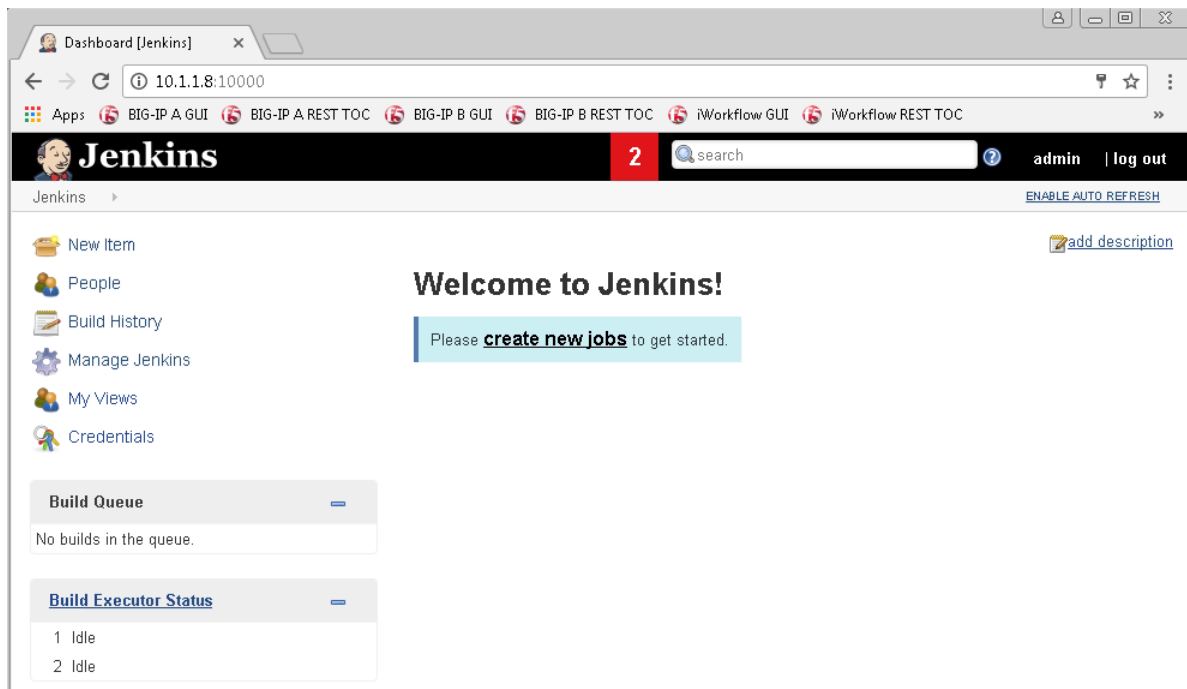
Slack is a ChatOps toolkit, think of Skype, Teams, Messenger, or IIRC! Except Slack also has the ability to take in bots. slackbots are used to interact with services, they might query for something when asked, or give you information when they notice something. In our case our Jenkins Pipeline file will use Slack to notify all of us when an action happens, collaborative teamwork.

Note: In the Jenkins Files, the `message` piece is sent to the Slack channel, if you would like to modify your messages for our lab **change the text!**

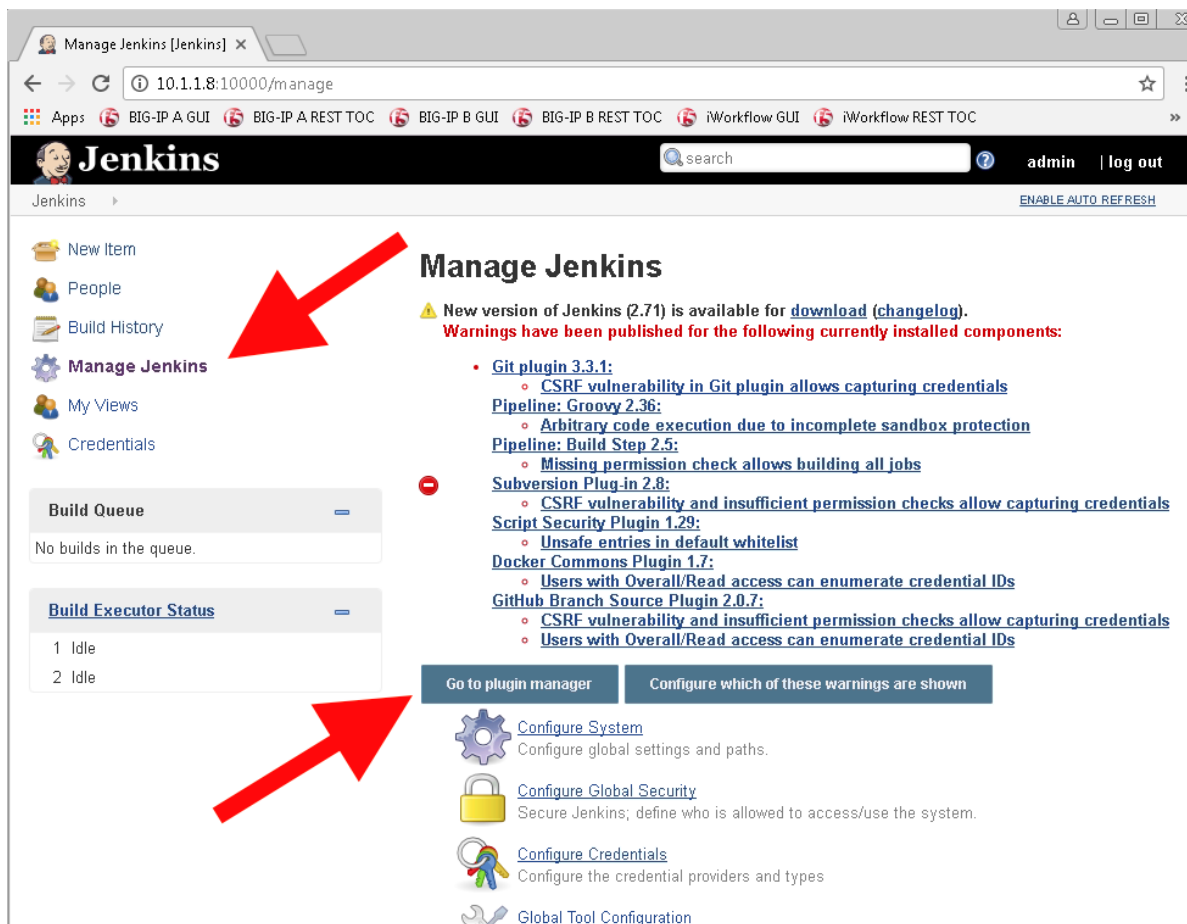
1. Access Jenkins via Chrome, open a new tab to `http://localhost:10000`, the user credentials are `admin\default`.



2. Once you are logged into Jenkins it should look like below

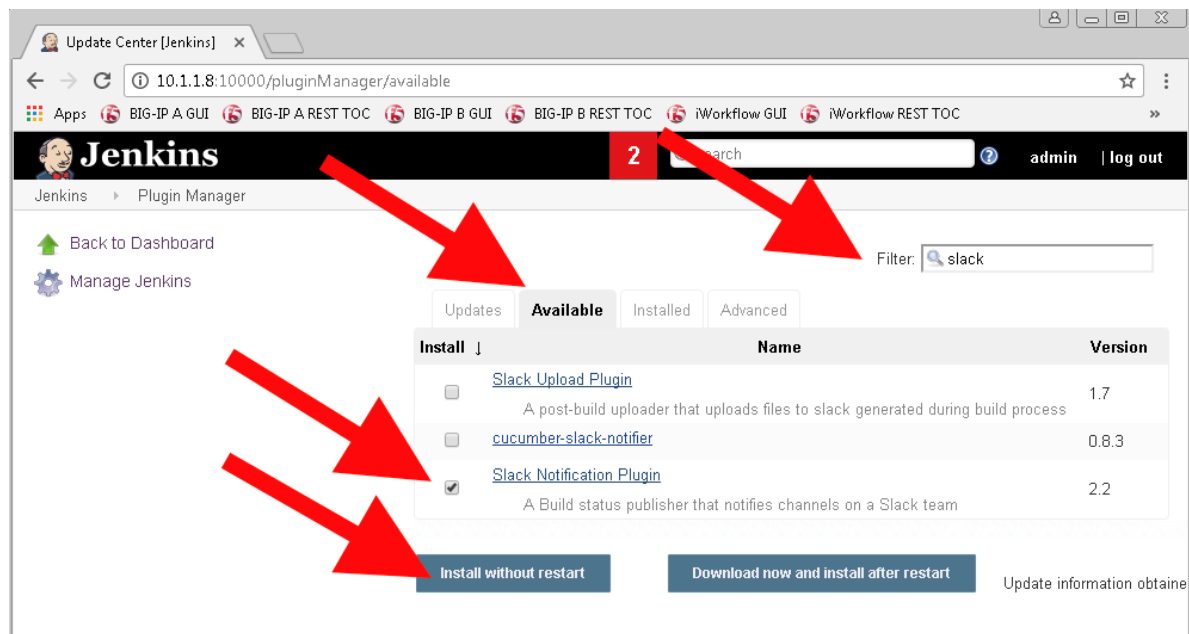


3. Click on Manage Jenkins

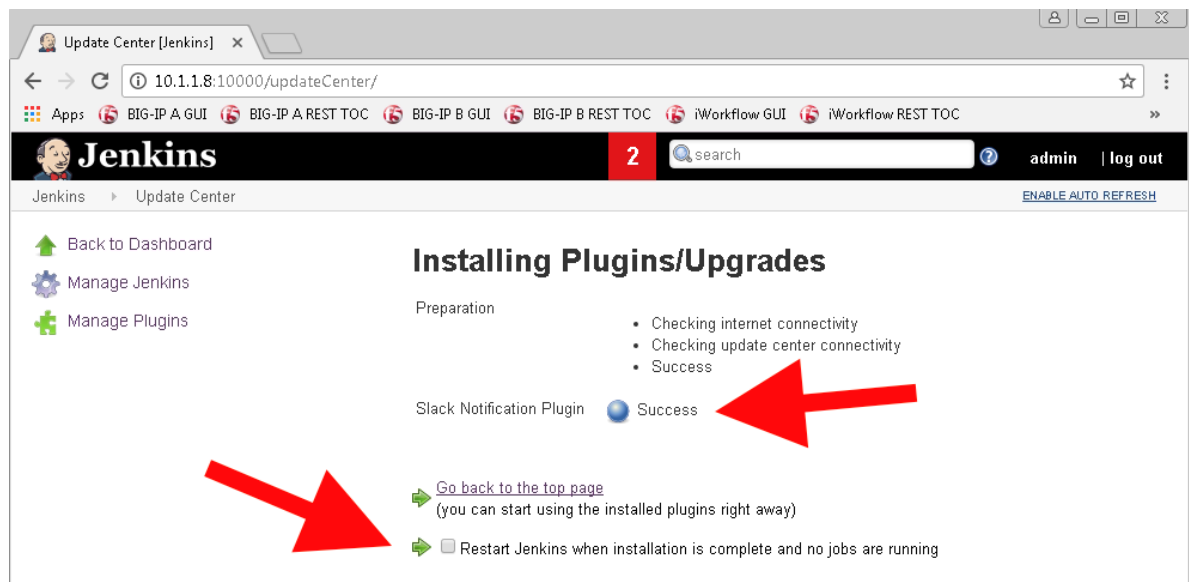


4. On the Manage Jenkins tab Select Available then filter on slack, once the filter is complete choose

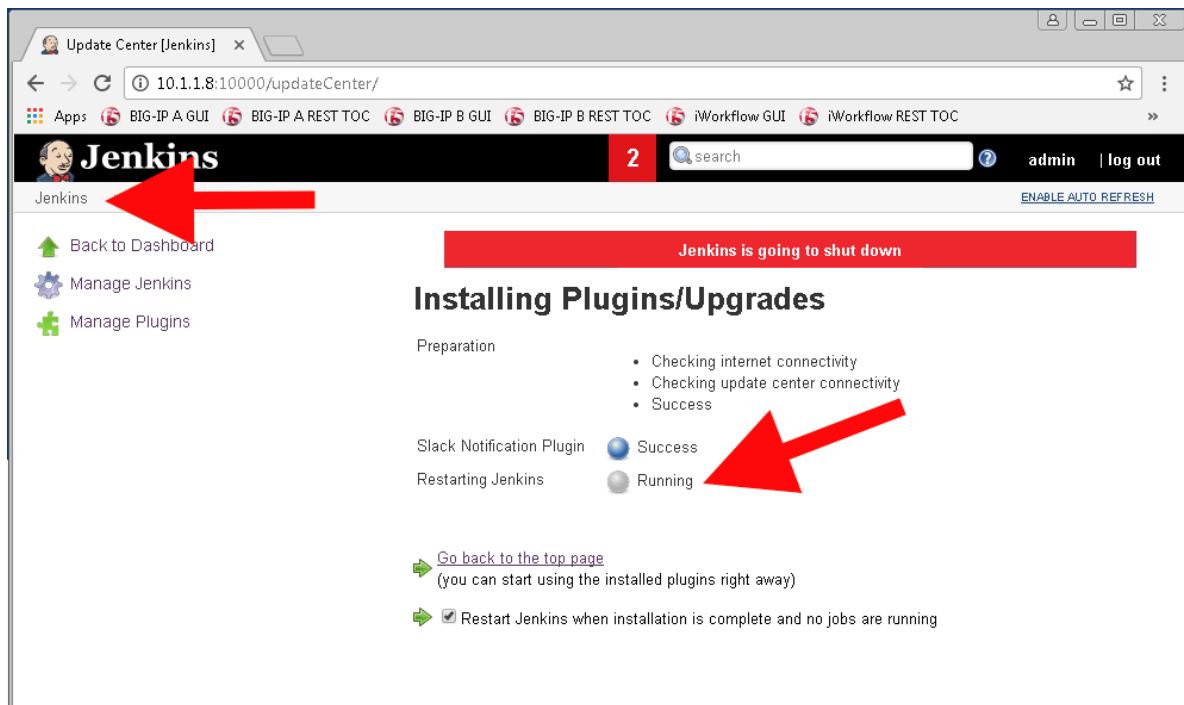
Slack Notification Plugin and execute Install without Restart



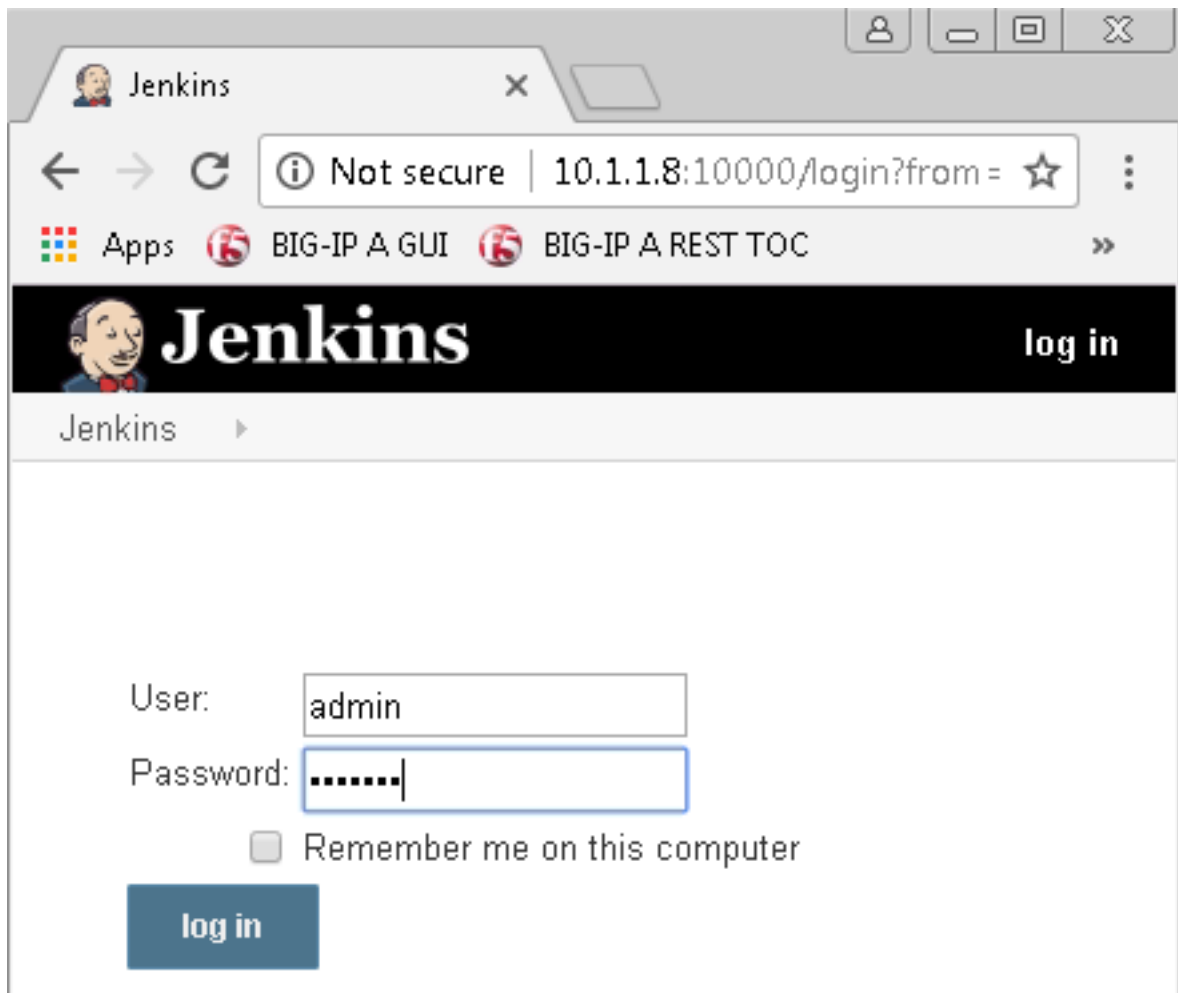
5. Once the Slack Notification Plugin has changed to Success, tick the radio button for Restart Jenkins when installation is complete and no jobs are running



6. Slack can take a few minutes to install in the background (give it 30 seconds), once the Restarting Jenkins globe is grey and the status is Running go back to Jenkins Home



7. Executing a restart of Jenkins will stop your session, you will need to log back into the system



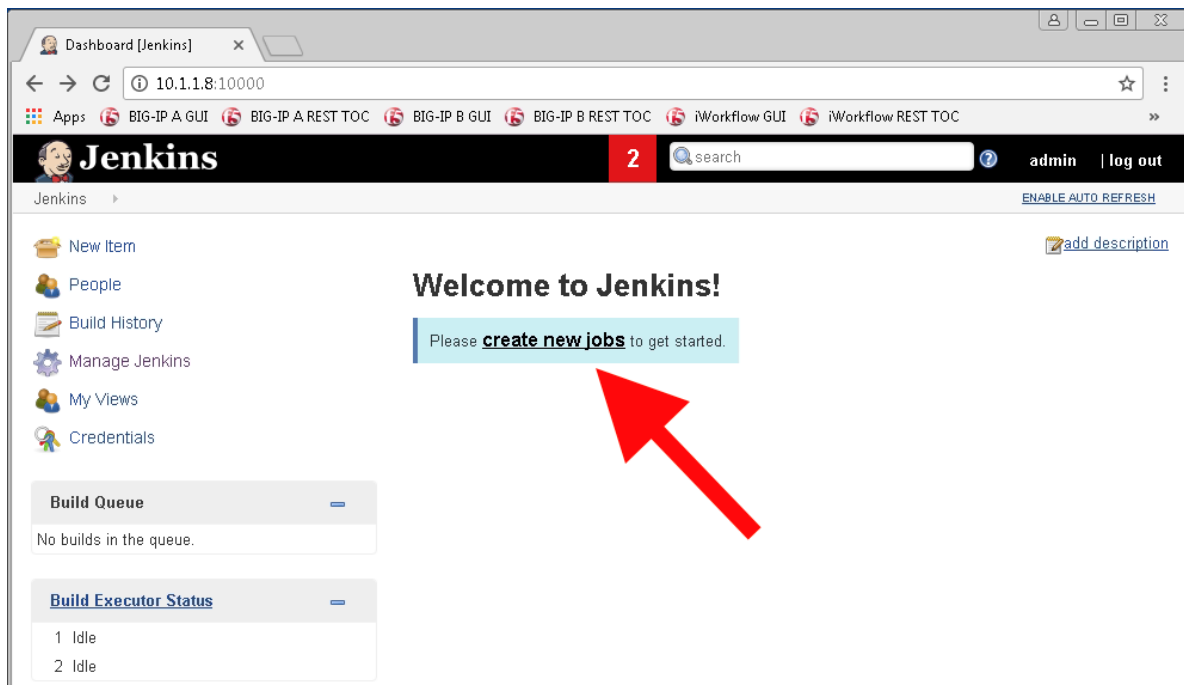
3.4.2 Lab 4.2 - Executing Jenkins Jobs for Creation or Modify

Now that we have Jenkins running, and the dependent Slack Plugin installed we can utilize our Jenkins Pipeline Scripts successfully.

Task 1 - Building the Application Service Framework via Jenkins

This step is executing the f5-newman-wrapper files. Instead of having to run the two different builds (Application Service Framework and Pool member add) individually we'll use a **pause**. Jenkins has a pause functionality which pauses a deployment looking for an approval to continue. After the approving step the node will be added; using the 2 f5-newman-wrapper files, but in conjunction with a single solution (Jenkins). Jenkins will continue to update the class via Slack as people are progressing. Jenkins also keeps a running console for logging, which we will also review.

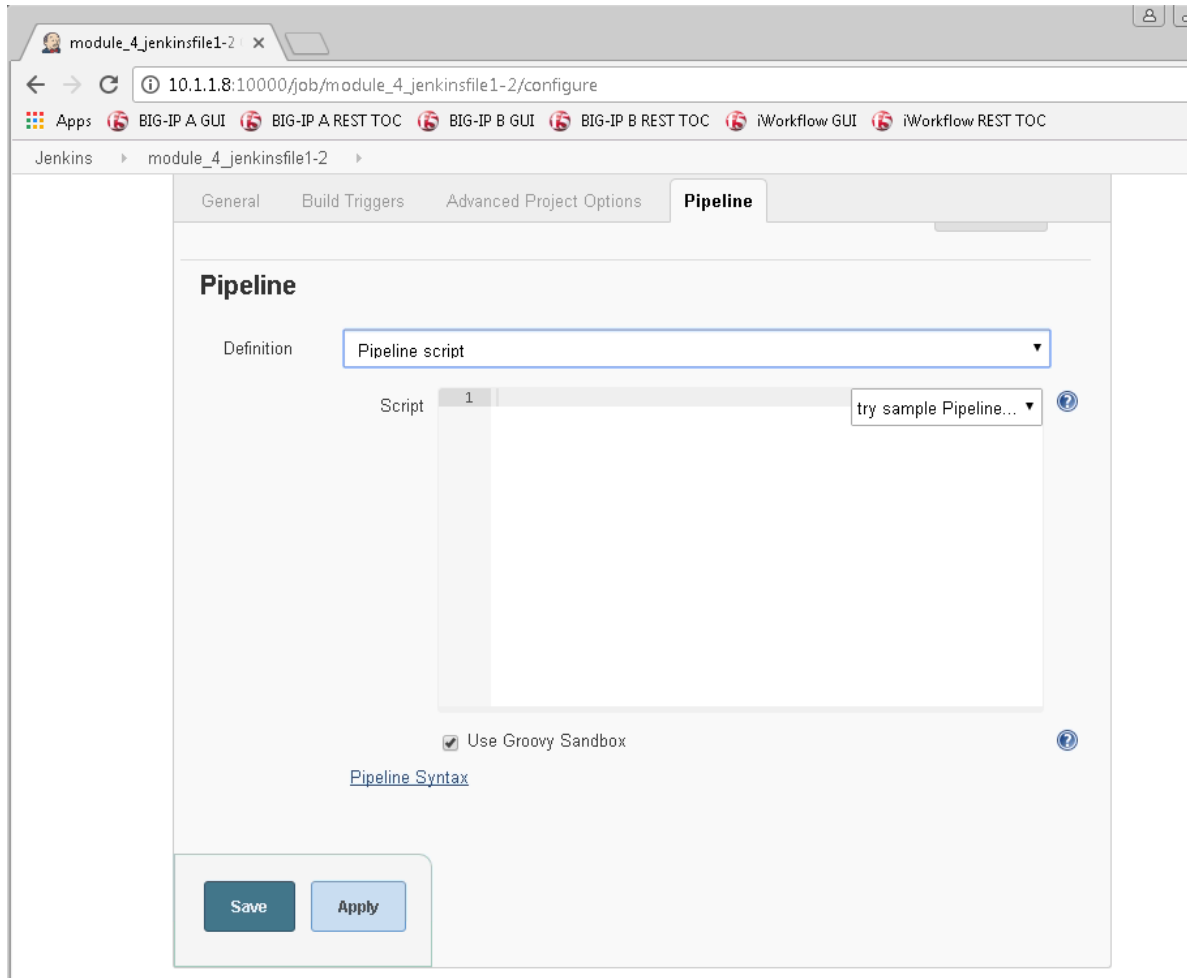
1. From the Jenkins Dashboard click on `create new jobs`



2. We are going to create our first Pipeline Job. Name the item `module_4_jenkinsfile1-2`, choose the Pipeline project style and select OK



3. We are going to be using the raw Jenkinsfile1-2 right in the Pipeline Script option at the end of the config page. Scroll to the bottom of the page but **please look at the other options** which can deploy a Pipeline. The different options in here are for an SCM (like GitHub), the Polling or Commit methods enable Continuous Deployment, as Jenkins will deploy the change on an event basis. Tie this with automatic testing to make sure you're not breaking the build!



4. We need to enter the contents of the Jenkinsfile1-2 into the Script section under Pipeline. After the contents are added click the Save Option.

```
1 node {
2   stage('Testing') {
3     //Run the tests
4     //sh "python -m /home/snops/f5-automation-labs/jenkins/f5-newman-build/f5-
↵newman-build-1"
5     //sh "python -m /home/snops/f5-automation-labs/jenkins/f5-newman-build/f5-
↵newman-build-2"
6   }
7   stage('Frameword-Deployment') {
8     //Run SNOPS Container Newman Package Virtual and Pool
9     sh "f5-newman-wrapper /home/snops/f5-automation-labs/jenkins/f5-newman-build/
↵f5-newman-build-1"
10    //chatops slack message that run has completed
11    slackSend(
12      channel: '#jenkins_builds',
```

```

13     color: 'good',
14     message: 'Super-NetOps Engineer is about to deploy an F5 Service Framework,
↪Approval Needed!',
15     teamDomain: 'f5agilitydevops',
16     token: 'vLMQmBq2tiyiCcZoNlbmAi0Z'
17 )
18 }
19 stage('Approval') {
20     //Gate the process and require approval
21     input 'Proceed?'
22     //chatops slack message that run has completed
23     slackSend(
24         channel: '#jenkins_builds',
25         color: 'good',
26         message: 'Super-NetOps Engineer just approved a new F5 Service Framework,
↪thats some serious Continuous Delivery!',
27         teamDomain: 'f5agilitydevops',
28         token: 'vLMQmBq2tiyiCcZoNlbmAi0Z'
29     )
30 }
31 stage('Add-Sevice-Node') {
32     //Run SNOPS Container Newman Package add Node to Pool
33     sh "f5-newman-wrapper /home/snops/f5-automation-labs/jenkins/f5-newman-build/
↪f5-newman-build-2"
34     //chatops slack message that run has completed
35     slackSend(
36         channel: '#jenkins_builds',
37         color: 'good',
38         message: 'Super-NetOps Engineer just added a Node to a Service, Production
↪is Online!',
39         teamDomain: 'f5agilitydevops',
40         token: 'vLMQmBq2tiyiCcZoNlbmAi0Z'
41     )
42 }
43 }

```

Contents in Pipeline:

module_4_jenkinsfile1-2

10.1.1.8:10000/job/module_4_jenkinsfile1-2/configure

Apps BIG-IP A GUI BIG-IP A REST TOC BIG-IP B GUI BIG-IP B REST TOC iWorkflow GUI iWorkflow REST TOC

Jenkins > module_4_jenkinsfile1-2

General Build Triggers Advanced Project Options **Pipeline**

Pipeline

Definition Pipeline script

Script

```
27 token: 'vLMQmBq2tiyiCcZoN1bm'
28 )
29 }
30 }
31 stage('Add-Service-Node') {
32 //Run SNOPS Container Newman Package add Node to F
33 sh "f5-newman-wrapper /home/snops/Local_Mapped_Repo
34 //chatops slack message that run has completed
35 slackSend(
36 channel: '#jenkins_builds',
37 color: 'good',
38 message: 'Super-NetOps Engineer just added a Node
39 teamDomain: 'f5agilitydevops',
40 token: 'vLMQmBq2tiyiCcZoN1bmAi0Z'
41 )
42 }
43 }
44 }
```

☒ Use Groovy Sandbox

[Pipeline Syntax](#)

Save Apply

1. Once the Job is saved, you will be taken to the stage view page, from here we are going to execute our Pipeline build, choose the **Build Now** option.

module_4_jenkinsfile1-2

10.1.1.8:10000/job/module_4_jenkinsfile1-2/

Apps BIG-IP A GUI BIG-IP A REST TOC BIG-IP B GUI BIG-IP B REST TOC iWorkflow GUI iWorkflow REST TOC

Jenkins 2 search admin | log out

Jenkins > module_4_jenkinsfile1-2 > [ENABLE AUTO REFRESH](#)

Back to Dashboard

Status

Changes

Build Now

Delete Pipeline

Configure

Full Stage View

Pipeline Syntax

Build History trend

find

RSS for all RSS for failures

Pipeline module_4_jenkinsfile1-2

[add description](#)

Disable Project

Recent Changes

Stage View

No data available. This Pipeline has not yet run.

Permalinks

- The Build is now running, and the stages are being executed in order. However, on our third stage we have a **pause** and an approval **needed**. Also at the same time Slack has begun to notify us that a new service is being deployed, and someone needs to approve it.

Jenkins 2 search

Jenkins > module_4_jenkinsfile1-2 >

Back to Dashboard

Status

Changes

Build Now

Delete Pipeline

Configure

Full Stage View

Pipeline Syntax

Build History trend

find

RSS for all RSS for failures

Pipeline module_4_jenkinsfile1-2

Recent Changes

Stage View

Average stage times:


Testing	Framework-Deployment	Approval
58ms	14s	81ms

#1 Jul 27 02:39 No Changes

58ms 14s

Approval


Permalinks


Jenkins


Jenkins
 module_4_jenkinsfile1-2


[Back to Dashboard](#)
[Status](#)
[Changes](#)
[Build Now](#)
[Delete Pipeline](#)
[Configure](#)
[Full Stage View](#)
[Pipeline Syntax](#)

Pipeline module_4_j




[Recent Changes](#)

Stage View



Build History
[trend](#)


#1

Jul 27, 2017 6:39 AM


[RSS for all](#)

[RSS for failures](#)

Average stage times:


#1

Jul 27
02:39

No
Changes

Permalinks

Highlight over the third Stage to prompt for the Approval

jenkins APP 11:40 PM

Super-NetOps Engineer is about to deploy an F5 Service Framework, Approval Needed!

3. Approve the change in Jenkins to allow the build to finish. Once this is done, the approval and finished Slack notification will be sent.

Jenkins
2

[Jenkins](#) > [module_4_jenkinsfile1-2](#) >

[Back to Dashboard](#)
[Status](#)
[Changes](#)
[Build Now](#)
[Delete Pipeline](#)
[Configure](#)
[Full Stage View](#)
[Pipeline Syntax](#)

Pipeline module_4_jenkinsfile1-2

[Recent Changes](#)

Stage View

#1

Jul 27, 2017 6:39 AM

[RSS for all](#)
[RSS for failures](#)

Testing	Framework-Deployment	Approval
58ms	14s	81ms

#1

Jul 27 02:39

No Changes

Proceed?

Proceed

Abort

globe icon

Average stage times:

Permalinks

Jenkins
2

[Jenkins](#) > [module_4_jenkinsfile1-2](#) >

[Back to Dashboard](#)
[Status](#)
[Changes](#)
[Build Now](#)
[Delete Pipeline](#)
[Configure](#)
[Full Stage View](#)
[Pipeline Syntax](#)

Pipeline module_4_jenkinsfile1-2

[Recent Changes](#)

Stage View

#1

Jul 27, 2017 6:39 AM

[RSS for all](#)
[RSS for failures](#)

Testing	Framework-Deployment	Approval
58ms	14s	81ms

#1

Jul 27 02:39

No Changes

Proceed?

Proceed

Abort

globe icon

Average stage times:

Permalinks

- At the end of the Build event (success or failure) there is a console output from Jenkins. Select the blue globe on the left to see the outputs

Jenkins 2

Jenkins > module_4_jenkinsfile1-2 >

- Back to Dashboard
- Status
- Changes
- Build Now
- Delete Pipeline
- Configure
- Full Stage View
- Pipeline Syntax

Build History trend

find

#1 Jul 27, 2017 6:39 AM

[RSS for all](#) [RSS for failures](#)

Pipeline module_4_jenkinsfile1-2

[Recent Changes](#)

Stage View

Average stage times:

Testing	Framework-Deployment	Approval	Add-Service-Node
58ms	14s	478ms	9s

#1

Jul 27 02:39

No Changes

Testing	Framework-Deployment	Approval	Add-Service-Node
58ms	14s	478ms <small>(cached 61.36s)</small>	9s

5. The Console Output file not only contains the Jenkins output from the Build, but also the f5-newman-wrapper toolkit logs for easy troubleshooting

Jenkins > module_4_jenkinsfile1-2 > #1

	executed	failed
iterations	1	0
requests	1	0
test-scripts	0	0
prerequisite-scripts	0	0
assertions	0	0

total run duration: 116ms

total data received: 818B (approx)

average response time: 87ms

```
[f5-newman-build-2-2017-07-27-06-40-54] run completed in 4s, 431.764 ms
[Pipeline] slackSend
run slackstepsend, step vLMQmBq2tiyiCcZoNlhmAiOZ:false, desc null:false
Slack Send Pipeline step configured values from global config - baseUrl: true, teamDomain: false, token: false, channel: false, color: false
[Pipeline] )
[Pipeline] // stage
[Pipeline] )
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

6. Check Slack for the completion of everything!

Today new messages

jenkins APP 11:40 PM

Super-NetOps Engineer is about to deploy an F5 Service Framework, Approval Needed!

11:40 ☆ Super-NetOps Engineer just approved a new F5 Service Framework, thats some serious Continuous Delivery!

Super-NetOps Engineer just added a Node to a Service, Production is Online!

7. Verify on the BIG-IP that the pool module_3_vs has been created and the services are Green

Local Traffic » Virtual Servers : Virtual Server List									
<div> <div>Virtual Server List</div> <div>Virtual Address List</div> <div>Statistics</div> </div>									
<div> <div>Search</div> <div>Create...</div> </div>									
<input checked="" type="checkbox"/>	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
<input type="checkbox"/>		module_3_vs			10.1.20.129	80 (HTTP)	Standard	Edit...	Common
<div> <div>Enable</div> <div>Disable</div> <div>Delete...</div> </div>									

Task 2 - Jenkinsfile3 and Jenkinsfile4

These two Jenkins files were completed to show the ability of creating smaller deployments. In our case we will use the f5-newman-wrapper toolkit to again change the user selected state of a pool member. The different Pipelines notifications also have different Slack Color depictions, helping to quickly identify issues to team members.

1. Return to the Jenkins Dashboard and select New Item

The screenshot shows the Jenkins Dashboard. A red arrow points to the 'New Item' button in the left sidebar. The main area displays a table of Jenkins jobs. The table has columns: S, W, Name, Last Success, Last Failure, and Last Duration. One job is listed: 'module_4_jenkinsfile1-2' with a last success of '1 hr 41 min - #1' and a last failure of 'N/A'. Below the table, there are links for 'Icon: S M L', 'Legend', 'RSS for all', 'RSS for failures', and 'RSS for just latest builds'.

2. Repeat steps 2 & 3 of the last module, creating 2 new Jenkins jobs, one for each desired node state.
3. Create and Execute module_4_jenkinsfile_3 for a down node

Pipeline Job Name: module_4_jenkinsfile_3

```

1 node {
2   stage('Testing') {
3     //Run the tests
4     //sh "python -m /home/snops/f5-automation-labs/jenkins/f5-newman-operation/
↪ f5-newman-build-3"
5   }
6   stage('Disable-Node') {
7     //Run SNOPS Container Newman Package Virtual and Pool
8     sh "f5-newman-wrapper /home/snops/f5-automation-labs/jenkins/f5-newman-
↪ operation/f5-newman-build-3"
9     //chatops slack message that run has completed
10    slackSend(
11      channel: '#jenkins_builds',
12      color: 'bad',
13      message: 'Super-NetOps Engineer just disabled a Service Node!',
14      teamDomain: 'f5agilitydevops',
15      token: 'vLMQmBq2tiyiCcZoNlbnAi0Z'
16    )
17  }
18 }

```

4. Verify on the BIG-IP that the pool `module_3_pool` has a down node
5. Create and Execute `module_4_jenkinsfile_4` for an up node

Pipeline Job Name: `module_4_jenkinsfile_4`

```

1 node {
2   stage('Testing') {
3     //Run the tests
4     //sh "python -m /home/snops/f5-automation-labs/jenkins/f5-newman-operation/
↪f5-newman-build-4"
5   }
6   stage('Enable-Node') {
7     //Run SNOOPS Container Newman Package Virtual and Pool
8     sh "f5-newman-wrapper /home/snops/f5-automation-labs/jenkins/f5-newman-
↪operation/f5-newman-build-4"
9     //chatops slack message that run has completed
10    slackSend(
11      channel: '#jenkins_builds',
12      color: 'good',
13      message: 'Super-NetOps Engineer just enabled a Service Node!',
14      teamDomain: 'f5agilitydevops',
15      token: 'vLMQmBq2tiyiCcZoNlbnAi0Z'
16    )
17  }
18 }

```

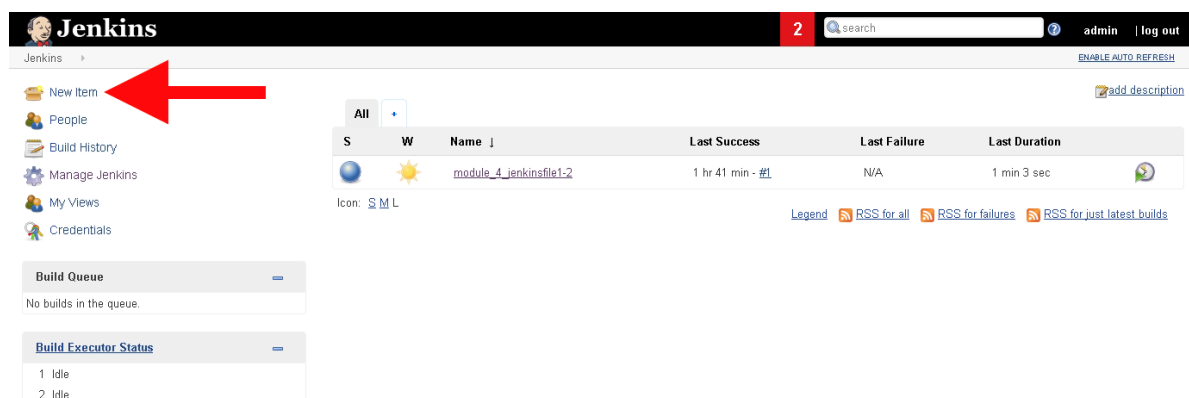
6. Verify on the BIG-IP that the pool `module_3_pool` has an up node

3.4.3 Lab 4.3 - Destroying a Service with Jenkins

For the last module we will teardown the Application Service we've been working with today. Destruction of an Application Services is an easy step often overlooked because of the perceived complexity it takes to reverse engineer a build. Utilizing Postman and the `f5-newman-wrapper` this is actually a very easy step, and will be incredibly valuable to teams seeking to strive for better Application Lifecycle Management. Because Postman and Newman operate in sequential order, simply reversing the order of creation will result in the correct teardown order. Also, since we're using the native F5 REST endpoints, all you need is a Resource with a DELETE method.

Task 1 - Teardown the Application via Jenkins

1. Return to the Jenkins Dashboard and select New Item



The screenshot shows the Jenkins web interface. On the left sidebar, the 'New Item' button is highlighted with a red arrow. The main content area displays a table of build jobs. The table has columns for status (S), icon (W), name, last success, last failure, and last duration. One build is listed: 'module_4_jenkinsfile1:2' with a success status and a duration of 1 min 3 sec. Below the table, there are sections for 'Build Queue' (showing 'No builds in the queue.') and 'Build Executor Status' (showing 1 idle and 2 idle executors).

2. Repeat steps 2 & 3 of the first module, creating the final Jenkins job
3. Create and Execute module_4_jenkinsfile_5 to destroy our Application Service

Pipeline Job Name: module_4_jenkinsfile_5

```

1 node {
2     stage('Testing') {
3         //Run the tests
4         //sh "python -m /home/snops/f5-automation-labs/jenkins/f5-newman-build/f5-
↪newman-build-5"
5     }
6     stage('Removal-Notification') {
7         //Run SNOOPS Container Newman Package Delete Service
8         //chatops slack message that run has completed
9         slackSend(
10             channel: '#jenkins_builds',
11             color: 'bad',
12             message: 'Super-NetOps Engineer is about to remove an F5 Service!',
13             teamDomain: 'f5agilitydevops',
14             token: 'vLMQmBq2tiyiCcZoNlbnAi0Z'
15         )
16     }
17     stage('Approval') {
18         //Gate the process and require approval
19         input 'Delete?'
20     }
21     stage('Service-Delete') {
22         //Run SNOOPS Container Newman Package add Node to Pool
23         sh "f5-newman-wrapper /home/snops/f5-automation-labs/jenkins/f5-newman-
↪build/f5-newman-build-5"
24         //chatops slack message that run has completed
25         slackSend(
26             channel: '#jenkins_builds',
27             color: 'good',
28             message: 'Super-NetOps Engineer removed an F5 Service successfully!',
29             teamDomain: 'f5agilitydevops',
30             token: 'vLMQmBq2tiyiCcZoNlbnAi0Z'
31         )
32     }
33 }

```

4. Verify the on the BIG-IP the service has been Deleted
5. Class 2 is Complete! if you have extra time, please give us feedback! <https://www.surveymonkey.com/r/W2SZDYK>

Class 3: Introduction to SecDevOps

This hands-on lab will demonstrate how to secure applications programmatically using a BIG-IP's iControl based REST API.

Leveraging programmability to deploy security policies and/or adhere to best practices during an application's lifecycle reduces the operational (e.g. time and money) cost of a defense in depth strategy. Programmatic workflows can be developed and deployed for specific security use cases, and integrated into the SDLC process, allowing for the protection of an application to iterate in parallel with the development of the application.

This course will feature the following topics.

- General interaction with tmm via BIG-IPs REST APIs
- Create, modify and assign an AFM policy
- Create, modify and assign an ASM policy

Lab Guide

This lab is divided into three modules. Each module of the lab, will require configuration of the BIG-IP, AFM, or ASM using the iControl REST based API. It is recommended that each lab be executed in order.

To perform the steps required in the lab, [Postman](#) will be used from the Windows jump box.

Prior to beginning the exercises, it is recommended to review the [Lab Topology](#).

1. Module 1: Configuring BIG-IP
2. Module 2: Configuring AFM (Advanced Firewall Module)
3. Module 3: Configuring ASM (Application Security Module)

Support

Bugs and enhancements can be made by opening an [issue](#) within the [GitHub](#) repository.

Getting Started

Please follow the instructions provided by the instructor to start your lab and access your jump host.

Note: All work for this lab will be performed exclusively from the Windows jumphost. No software installation or interaction with your local system is required.

Expected time to complete: **3 hours**

4.1 Lab Topology

The network topology implemented for this lab is very simple. Since the focus of the lab is Control Plane programmability rather than Data Plane traffic flow we can keep the data plane fairly simple. The following components have been included in your lab environment:

- 1 x F5 BIG-IP (v13.0)
- 1 x Linux webserver (Ubuntu 16.04)
- 1 x Windows 7 jump box

The following table lists VLANs, IP Addresses and Credentials for all components:

Component	VLAN/IP Address(es)	Credentials
Windows Jump Box	<ul style="list-style-type: none">• Management: 10.1.1.250• External: 10.1.10.250	external_user/available in instance details
BIG-IP	<ul style="list-style-type: none">• Management: 10.1.1.5• External: 10.1.10.5• Internal: 10.1.20.5	admin/admin
Linux Server	<ul style="list-style-type: none">• Management: 10.1.1.10• Internal: 10.1.20.10	ubuntu/ubuntu

4.2 Module 1: iControl REST API Refresher

- Explore the iControl REST API on a BIG-IP
- Use Postman to interact with the iControl REST API
- Authenticate to the BIG-IP using a username/password and token
- Modify the authentication token timeout
- Build a basic LTM configuration

4.2.1 Lab 1.1: Exploring iControl

The iControl REST API available via TMOS can be directly accessed and endpoints explored.

1. Open Google Chrome and navigate to the following bookmarks: BIG-IP A GUI and BIG-IP API ToC. Accept any SSL warnings/errors that appear and ensure that you can access both login prompts.
2. Click on the **BIG-IP API ToC** bookmark to access the API Table of Contents for BIG-IP A. The `/mgmt/toc` path in the URL is available on all TMOS versions 11.6 or newer.
3. Authenticate using the default **admin/admin** credentials.
4. After successfully authenticating, you will be presented with a top-level list of REST resources available on the BIG-IP. At the top of the page is a search box that can be used to search for specific REST resources.

4.2.2 Lab 1.2: API Authentication

This lab utilizes the Postman Chrome extension to facilitate the sending data to and receiving data from the iControl REST API.

REST API Authentication

One of the many basic concepts related to interaction with REST API's is how a particular consumer is authenticated to the system. BIG-IP, BIG-IQ and iWorkflow support two types of authentication: HTTP BASIC and Token based. It's important to understand both of these authentication mechanisms, as consumers of the API will often make use of both types depending on the use case. This lab will demonstrate how to interact with both types of authentication.

Task 1 - Basic Authentication

Warning: Prior to performing any of the below steps, ensure that you can log into the BIG-IP with Chrome after accepting the invalid certificate. Postman relies on the Chrome certificate store and if the self-signed cert has not been accepted via Chrome, this extension will not work properly.


In this task we will use the Postman tool to send API requests using HTTP BASIC authentication. As its name implies this method of authentication encodes the user credentials via the existing BASIC authentication method provided by the HTTP protocol. The mechanism this method uses is to insert an HTTP header named 'Authorization' with a value that is built by Base 64 encoding the string "<username>:<password>". The resulting header takes this form:

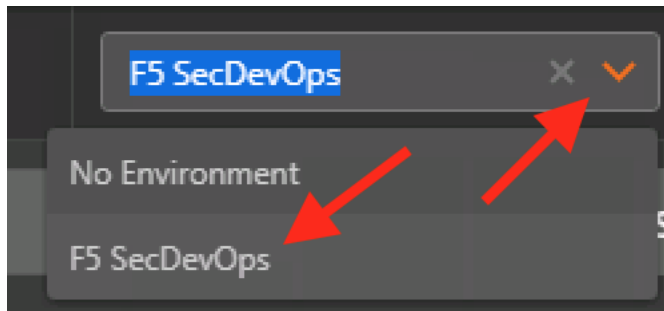
```
Authorization: Basic YWRtaW46YWRtaW4=
```

It should be noted that cracking the method of authentication is TRIVIAL; as a result API calls should always be performed using HTTPS (F5 default) rather than HTTP.

Perform the following steps to complete this task:

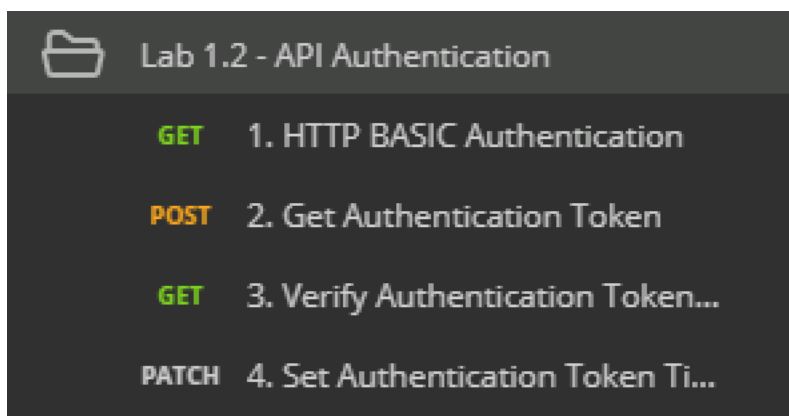


1. Open the Postman Client on your jumphost by clicking the  icon.
2. To assist in multi-step procedures we make heavy use of the 'Environments' capability in Postman. This capability allows us to set various global variables that are then substituted into a request before it's sent. When you open Postman please verify that your environment is set the **F5 SecDevOps** environment:

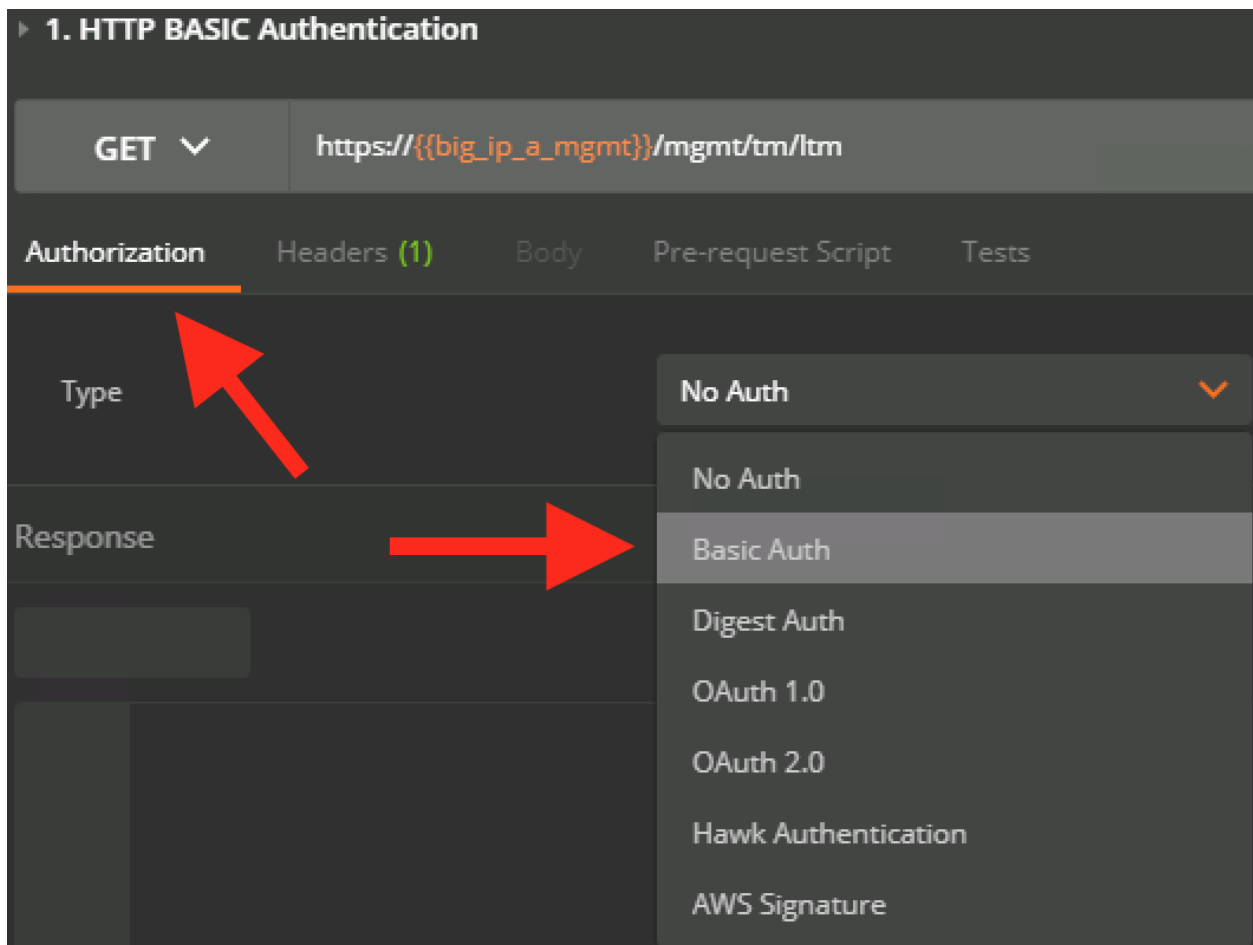


3. Click the 'Collections' tab on the left side of the screen, expand the 'F5 SecDevOps' collection on the left side of the screen, expand the **Lab 1.2 - API Authentication** folder:

(Ignore the # of requests on the screen below versus what you might see, the # of requests will grow and change as this lab grows)

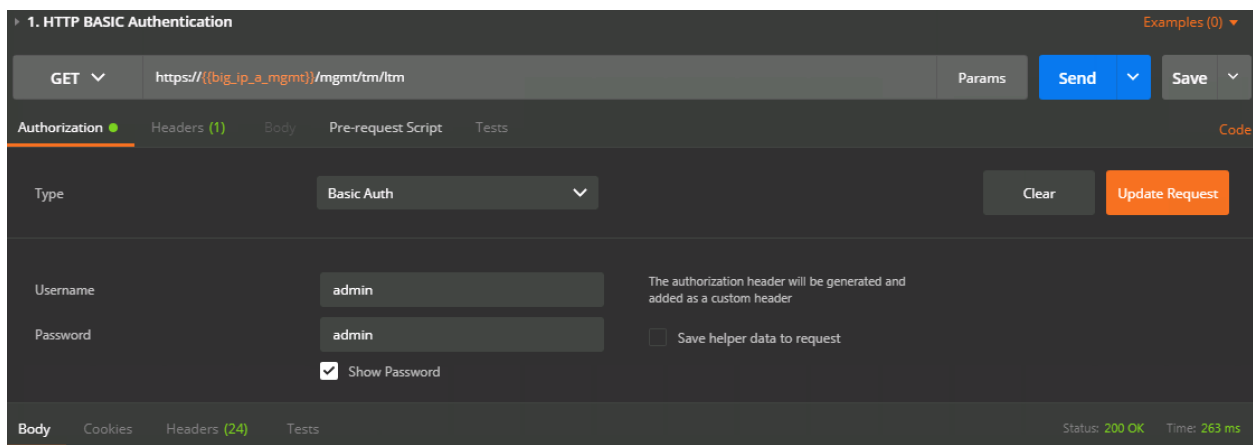


4. Click the **1. HTTP BASIC Authentication** item. Click the 'Authorization' tab and select 'Basic Auth' as the Type. Fill in the username and password (admin/admin) and click the 'Update Request' button. Notice that the number of Headers in the Headers tab changed from 1 to 2. This is because Postman automatically created the HTTP header and updated your request to include it. Click the 'Headers' tab and examine the HTTP header:



5. Click the 'Send' button to send the request. If the request succeeds you should be presented with a listing of the '/mgmt/tm/ltn' Organizing Collection.

Tip: Pay attention to the Status response i.e. **200 OK**



Task 2 - Token Based Authentication

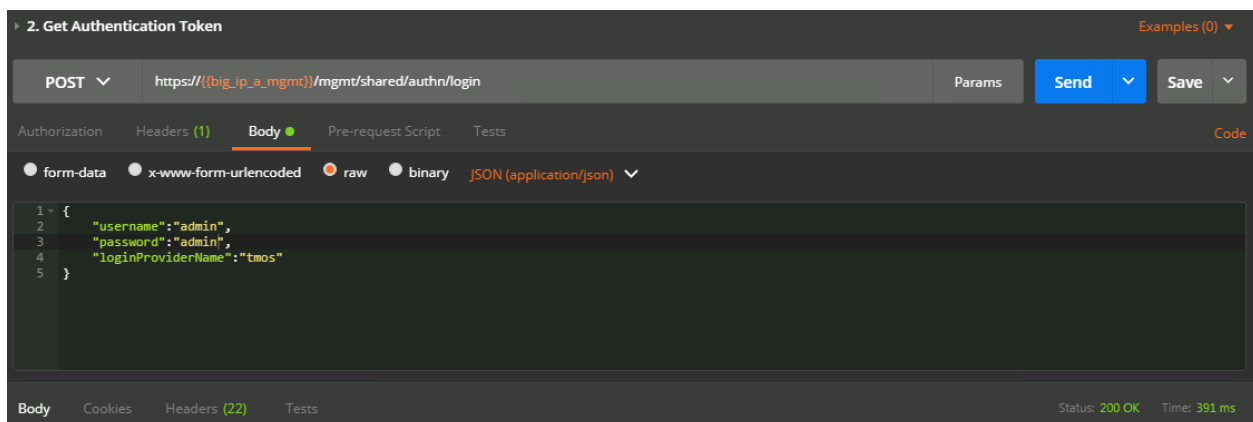
One of the disadvantages of BASIC Authentication is that credentials are sent with each and every request. This can result in a much greater attack surface being exposed unnecessarily. As a result Token Based Authentication (TBA) is preferred in many cases. This method only sends the credentials once, on the first request. The system then responds with a unique token for that session and the consumer then uses that token for all subsequent requests. BIG-IP, BIG-IQ and iWorkflow support token-based authentication that drops down to the underlying authentication subsystems available in TMOS. As a result the system can be configured to support external authentication providers (RADIUS, TACACS, AD, etc) and those authentication methods can flow through to the REST API. In this task we will demonstrate TBA using the local authentication database, however, authentication to external providers is fully supported.

Tip: For more information about external authentication providers see the section titled “About external authentication providers with iControl REST” in the iControl REST API User Guide available at <https://devcentral.f5.com>

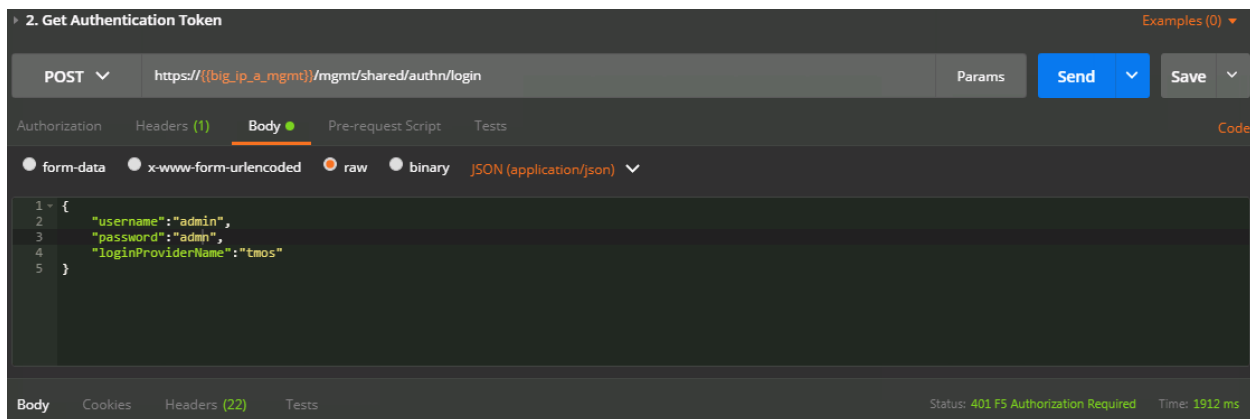
Perform the following steps to complete this task:

1. Click the **2: Get Authentication Token** item in the **Lab 1.2 - API Authentication** Postman Collection
2. Notice that we send a POST request to the `/mgmt/shared/authn/login` endpoint. Note that BASIC authentication is NOT required for this step. The token is provided based on the credentials located within the JSON payload.
3. Click the 'Body' tab and examine the JSON that we will send to BIG-IP to provide credentials and the authentication provider:
4. Modify the JSON body and add the required credentials (admin/admin). Then click the 'Send' button.
5. Examine the response status code. If authentication succeeded and a token was generated, the response will have a 200 OK status code. If the status code is 401 then check your credentials. View the response body to see the token that was provided:

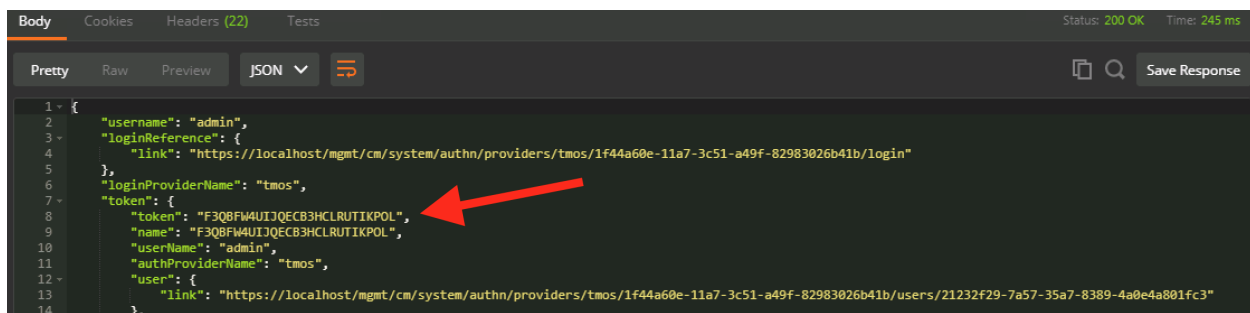
Successful:



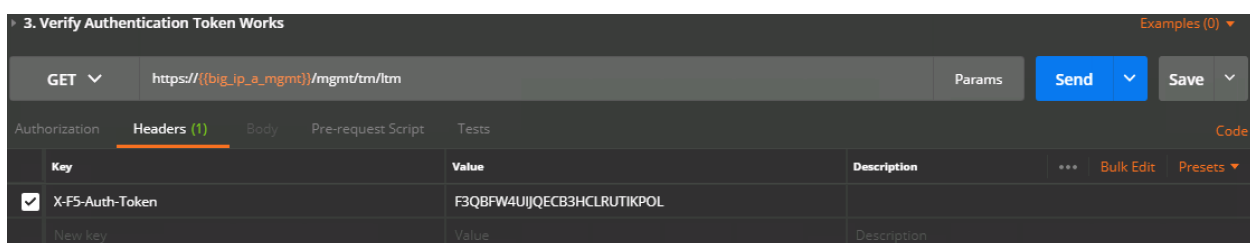
Unsuccessful:



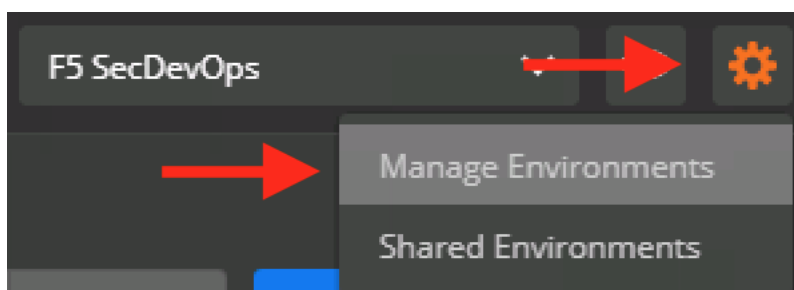
- Once you receive a 200 OK status code examine the response body. The various attributes show the parameters assigned to the particular token. Find the 'token' attribute and copy it into your clipboard (Ctrl+c) for use in the next step:



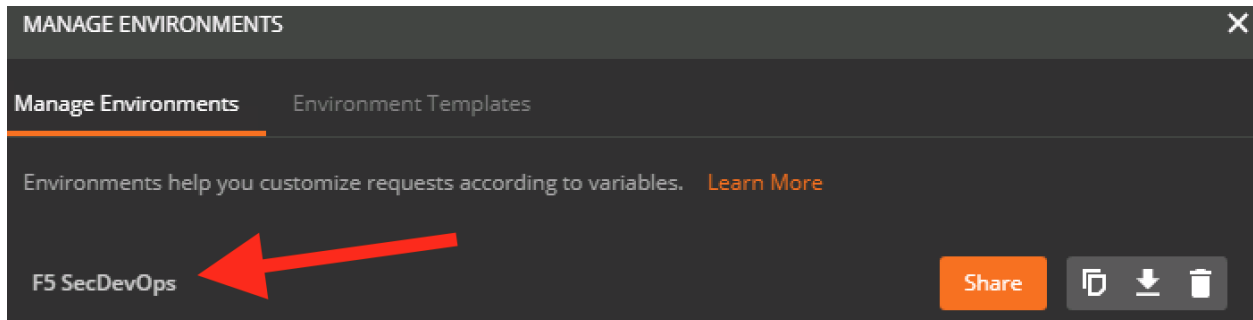
- Click the **3: Verify Authentication Works** item in the **Lab 1.2 - API Authentication** Postman collection. Click the 'Headers' tab and paste the token value copied above as the VALUE for the 'X-F5-Auth-Token' header. This header is required to be sent on all requests when using token based authentication.



- Click the 'Send' button. If your request is successful you should see a '200 OK' status and a listing of the 'itm' Organizing Collection.
- We will now update your Postman environment to use this auth token for the remainder of the lab. Click the Environment menu in the top right of the Postman window and click 'Manage Environments':

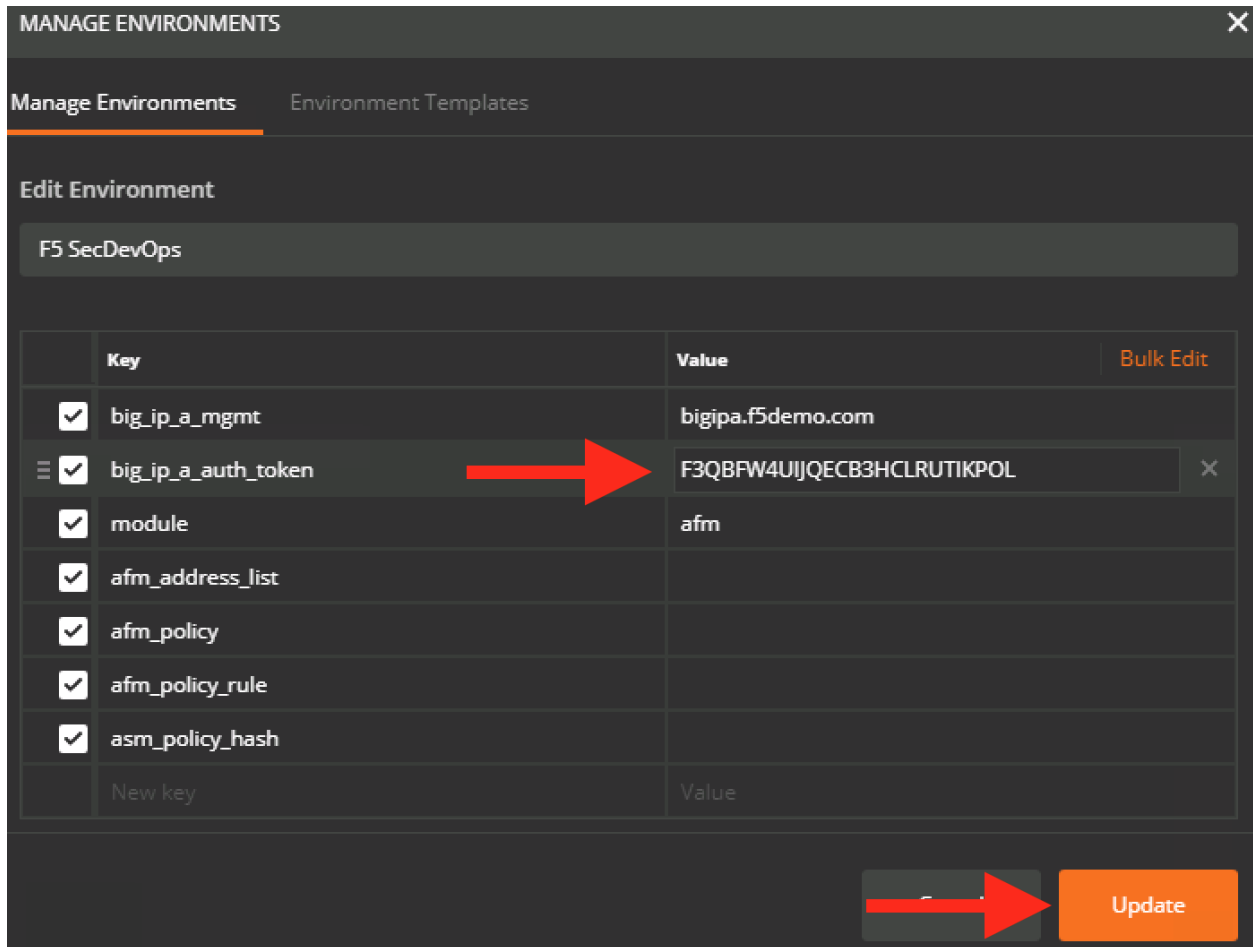


10. Click the **F5 SecDevOps** item:



11. Update the value for 'big_ip_a_auth_token' by Pasting (Ctrl-v) in your auth token:

12. Click the 'Update' button and then close the 'Manage Environments' window. You're subsequent requests will now automatically substitute the token's value where the `{{big_ip_a_auth_token}}` environmental variable is used.



13. Click the **4: Set Authentication Token Timeout** item in the **Lab 1.2 - API Authentication** Postman collection. This request will PATCH your token Resource (check the URI) and update the timeout attribute so we can complete the lab easily. Examine the request type and JSON Body and then click the 'Send' button. Verify that the timeout has been changed to '36000' in the response:

```
Body Cookies Headers (20) Tests Status: 200 OK Time: 48 ms Size: 1.54 KB
Pretty Raw Preview JSON Save Response
1 {
2   "token": "6AV324CMVZVIDZU5407NUMLSVQ",
3   "name": "6AV324CMVZVIDZU5407NUMLSVQ",
4   "userName": "admin",
5   "authProviderName": "tmos",
6   "user": {
7     "link": "https://localhost/mgmt/cm/system/authn/providers/tmos/1f44a60e-11a7-3c51-a49f-82983026b41b/users/21232f29-7a57-35a7-8389-4a0e4a801fc3"
8   },
9   "groupReferences": [
10    {
11      "link": "https://localhost/mgmt/cm/system/authn/providers/tmos/1f44a60e-11a7-3c51-a49f-82983026b41b/user-groups/21232f29-7a57-35a7-8389-4a0e4a801fc3"
12    }
13  ],
14  "timeout": 36000,
15  "startTime": "2017-07-27T22:37:40.427-0400",
16  "address": "10.1.1.250",
17  "partition": "[All]",
18  "generation": 2,
19  "lastUpdateMicros": 1501209585888708,
20  "expirationMicros": 1501245460427000,
21  "kind": "shared:authz:tokens:authtokenitemstate",
22  "selfLink": "https://localhost/mgmt/shared/authz/tokens/6AV324CMVZVIDZU5407NUMLSVQ"
23 }
```

4.2.3 Lab 1.3: Building a Basic LTM Config

Overview

In this lab, the iControl REST API will be used to build a basic monitor, node, pool, and virtual server configuration on the BIG-IP.

Specific Instructions

Prior to performing the below steps, validate that the Hackazon web site is not accessible via the Windows jump box by clicking on the Hackazon bookmark in the Chrome toolbar.

Follow the below steps in order found in the Postman collection to complete this portion of the lab. The requests and responses have been included below for reference.

Attention: Some response content has been removed for brevity.

1. Create an HTTP Monitor

An HTTP POST to the `/mgmt/tm/ltn/monitor/http` endpoint with a body containing the monitor configuration creates a monitor.

Request

POST `https://{{big_ip_a_mgmt}}/mgmt/tm/ltn/monitor/http`

Headers

Content-Type: `application/json`
X-F5-Auth-Token: `{{big_ip_a_auth_token}}`

Body

```
{
  "name": "hackazon_monitor",
  "send": "GET /\r\n"
}
```

Example Response

```
{
  "kind": "tm:ltm:monitor:http:httpstate",
  "name": "hackazon_monitor",
  "partition": "Common",
  "fullPath": "/Common/hackazon_monitor",
  "generation": 0,
  "selfLink": "https://localhost/mgmt/tm/ltm/monitor/http/~Common~hackazon_monitor?
↪ver=13.0.0",
  "adaptive": "disabled",
  "adaptiveDivergenceType": "relative",
  "adaptiveDivergenceValue": 25,
  "adaptiveLimit": 200,
  "adaptiveSamplingTimespan": 300,
  "defaultsFrom": "/Common/http",
  "destination": ":*:*",
  "interval": 5,
  "ipDscp": 0,
  "manualResume": "disabled",
  "reverse": "disabled",
  "send": "GET / HTTP/\r\n",
  "timeUntilUp": 0,
  "timeout": 16,
  "transparent": "disabled",
  "upInterval": 0
}
```

2. Create a Pool

An HTTP POST to the `/mgmt/tm/ltm/pool` endpoint with a body containing the configuration creates a pool with a node(s).

Request

```
POST https://{big_ip_a_mgmt}/mgmt/tm/ltm/pool
```

Headers

```
Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{
  "name": "hackazon_pool",
  "monitor": "/Common/hackazon_monitor",
  "members": ["10.1.20.10:80"]
}
```

Example Response

```
{
  "kind": "tm:ltm:pool:poolstate",
  "name": "hackazon_pool",
  "partition": "Common",
  "fullPath": "/Common/hackazon_pool",
  "generation": 10781,
  "selfLink": "https://localhost/mgmt/tm/ltm/pool/~Common~hackazon_pool?ver=13.0.0",
  "allowNat": "yes",
  "allowSnat": "yes",
  "ignorePersistedWeight": "disabled",
  "ipTosToClient": "pass-through",
  "ipTosToServer": "pass-through",
  "linkQosToClient": "pass-through",
  "linkQosToServer": "pass-through",
  "loadBalancingMode": "round-robin",
  "minActiveMembers": 0,
  "minUpMembers": 0,
  "minUpMembersAction": "failover",
  "minUpMembersChecking": "disabled",
  "monitor": "/Common/hackazon_monitor ",
  "queueDepthLimit": 0,
  "queueOnConnectionLimit": "disabled",
  "queueTimeLimit": 0,
  "reselectTries": 0,
  "serviceDownAction": "none",
  "slowRampTime": 10,
  "membersReference": {
    "link": "https://localhost/mgmt/tm/ltm/pool/~Common~hackazon_pool/members?
↪ver=13.0.0",
    "isSubcollection": true
  }
}
```

3. Create a HTTP Profile

An HTTP POST to the `/mgmt/tm/ltm/profile/http` endpoint with a body containing the configuration creates a profile.

Request

```
POST https://{{big_ip_a_mgmt}}/mgmt/tm/ltm/profile/http
```

Headers

```
Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{
  "name": "hackazon_http_profile",
  "insertXforwardedFor": "enabled",
  "serverAgentName": "hackazon"
}
```

Example Response

```
{
  "kind": "tm:ltm:profile:http:httpstate",
  "name": "hackazon_http_profile",
  "partition": "Common",
  "fullPath": "/Common/hackazon_http_profile",
  "generation": 10783,
  "selfLink": "https://localhost/mgmt/tm/ltm/profile/http/~Common~hackazon_http_
↪profile?ver=13.0.0",
  "acceptXff": "disabled",
  "appService": "none",
  "basicAuthRealm": "none",
  "defaultsFrom": "/Common/http",
  "defaultsFromReference": {
    "link": "https://localhost/mgmt/tm/ltm/profile/http/~Common~http?ver=13.0.0"
  },
  "description": "none",
  "encryptCookies": [],
  "insertXforwardedFor": "enabled",
  "serverAgentName": "hackazon"
}
```

4. Create a TCP profile

An HTTP POST to the `/mgmt/tm/ltm/profile/tcp` endpoint with a body containing the configuration creates a TCP profile.

Request

```
POST https://{big_ip_a_mgmt}/mgmt/tm/ltm/profile/tcp
```

Headers

```
Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{
  "name": "hackazon_tcp_clientside_profile",
  "nagle": "disabled",
  "sendBufferSize": "16000"
}
```

Example Response

```
{
  "kind": "tm:ltm:profile:tcp:tcpstate",
  "name": "hackazon_tcp_clientside_profile",
  "partition": "Common",
  "fullPath": "/Common/hackazon_tcp_clientside_profile",
  "generation": 10784,
  "selfLink": "https://localhost/mgmt/tm/ltm/profile/tcp/~Common~hackazon_tcp_
↪clientside_profile?ver=13.0.0",
  "abc": "enabled",
  "ackOnPush": "enabled",
  "appService": "none",
  "autoProxyBufferSize": "disabled",
}
```



```

    "autoReceiveWindowSize": "disabled",
    "autoSendBufferSize": "disabled",
    "closeWaitTimeout": 5,
    "cmetricsCache": "enabled",
    "cmetricsCacheTimeout": 0,
    "congestionControl": "high-speed",
    "defaultsFrom": "/Common/tcp",
    "defaultsFromReference": {
      "link": "https://localhost/mgmt/tm/ltm/profile/tcp/~Common~tcp?ver=13.0.0"
    },
    "keepAliveInterval": 1800,
    "nagle": "disabled",
    "sendBufferSize": 16000
  }
}

```

5. Create a Virtual Server

An HTTP POST to the `/mgmt/tm/ltm/virtual` endpoint with a body containing the configuration creates a virtual server.

Request

```
POST https://{{big_ip_a_mgmt}}/mgmt/tm/ltm/virtual
```

Headers

```

Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}

```

Body

```

{
  "name": "hackazon_vs",
  "destination": "10.1.10.10:80",
  "ipProtocol": "tcp",
  "pool": "hackazon_pool",
  "sourceAddressTranslation": { "type": "automap" },
  "profiles": [
    { "name": "/Common/hackazon_tcp_clientside_profile", "context": "clientside" },
    { "name": "/Common/tcp-wan-optimized", "context": "serverside" },
    "/Common/hackazon_http_profile"
  ]
}

```

Example Response

Note: The profiles for this virtual server is a subcollection. This collection can be access by performing a GET on the profiles endpoint for this specific virtual server `https://{{big_ip_a_mgmt}}/mgmt/tm/ltm/virtual/~Common~hackazon_vs/profiles`.

```

{
  "kind": "tm:ltm:virtual:virtualstate",
  "name": "hackazon_vs",
  "partition": "Common",
  "fullPath": "/Common/hackazon_vs",

```

```

"generation": 10785,
"selfLink": "https://localhost/mgmt/tm/ltm/virtual/~Common~hackazon_vs?ver=13.0.0
↪",
"addressStatus": "yes",
"autoLasthop": "default",
"cmpEnabled": "yes",
"connectionLimit": 0,
"destination": "/Common/10.1.10.20:80",
"enabled": true,
"gtmScore": 0,
"ipProtocol": "tcp",
"mask": "255.255.255.255",
"mirror": "disabled",
"mobileAppTunnel": "disabled",
"nat64": "disabled",
"pool": "/Common/hackazon_pool",
"poolReference": {
  "link": "https://localhost/mgmt/tm/ltm/pool/~Common~hackazon_pool?ver=13.0.0"
},
"rateLimit": "disabled",
"rateLimitDstMask": 0,
"rateLimitMode": "object",
"rateLimitSrcMask": 0,
"serviceDownImmediateAction": "none",
"source": "0.0.0.0/0",
"sourceAddressTranslation": {
  "type": "automap"
},
"sourcePort": "preserve",
"synCookieStatus": "not-activated",
"translateAddress": "enabled",
"translatePort": "enabled",
"vlansDisabled": true,
"vsIndex": 9,
"policiesReference": {
  "link": "https://localhost/mgmt/tm/ltm/virtual/~Common~hackazon_vs/policies?
↪ver=13.0.0",
  "isSubcollection": true
},
"profilesReference": {
  "link": "https://localhost/mgmt/tm/ltm/virtual/~Common~hackazon_vs/profiles?
↪ver=13.0.0",
  "isSubcollection": true
}
}

```

6. Retrieve VS information

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/ltm/virtual/~Common~hackazon_vs/
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```

{
  "kind": "tm:ltm:virtual:virtualstate",
  "name": "hackazon_vs",
  "partition": "Common",
  "fullPath": "/Common/hackazon_vs",
  "generation": 10785,
  "selfLink": "https://localhost/mgmt/tm/ltm/virtual/~Common~hackazon_vs?ver=13.0.0",
  ↪",
  "addressStatus": "yes",
  "autoLasthop": "default",
  "cmpEnabled": "yes",
  "connectionLimit": 0,
  "destination": "/Common/10.1.10.20:80",
  "enabled": true,
  "gtmScore": 0,
  "ipProtocol": "tcp",
  "mask": "255.255.255.255",
  "mirror": "disabled",
  "mobileAppTunnel": "disabled",
  "nat64": "disabled",
  "pool": "/Common/hackazon_pool",
  "poolReference": {
    "link": "https://localhost/mgmt/tm/ltm/pool/~Common~hackazon_pool?ver=13.0.0"
  },
  "rateLimit": "disabled",
  "rateLimitDstMask": 0,
  "rateLimitMode": "object",
  "rateLimitSrcMask": 0,
  "serviceDownImmediateAction": "none",
  "source": "0.0.0.0/0",
  "sourceAddressTranslation": {
    "type": "automap"
  },
  "sourcePort": "preserve",
  "synCookieStatus": "not-activated",
  "translateAddress": "enabled",
  "translatePort": "enabled",
  "vlansDisabled": true,
  "vsIndex": 9,
  "policiesReference": {
    "link": "https://localhost/mgmt/tm/ltm/virtual/~Common~hackazon_vs/policies?
↪ver=13.0.0",
    "isSubcollection": true
  },
  "profilesReference": {
    "link": "https://localhost/mgmt/tm/ltm/virtual/~Common~hackazon_vs/profiles?
↪ver=13.0.0",
    "isSubcollection": true
  }
}

```

7. Validate the virtual server

Click on the Hackazon bookmark in the Chrome toolbar and validate that the Hackazon web site is now accessible.

4.3 Module 2: Programmatic Control of Firewall Services

- Provision AFM module on BIG-IP
- Interact with AFM related REST endpoints on a BIG-IP
- Create and modify an AFM address list
- Create and modify an AFM policy

4.3.1 Lab 2.1: Provisioning AFM

Overview

In this lab, the iControl REST API will be used to provision a module on the BIG-IP. More specifically, the Advanced Firewall Manager (AFM) module will be provisioned for use in **Module 2: Configuring AFM (Advanced Firewall Module)**.

Specific Instructions

Prior to performing the below steps, validate the `{{module}}` Postman environment variable. The `{{module}}` should be set to **afm**.

Follow the below steps in order found in the Postman collection to complete this portion of the lab. The requests and responses have been included below for reference.

Attention: Some response content has been removed for brevity.

1. Retrieve all module provision states

Request

```
GET https://{{big_ip_a_mgmt}}/mgmt/tm/sys/provision
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

Note: The **afm** module is currently provisioned for **none** while the **ltm** module is provisioned for **nominal**.

```
{
  "kind": "tm:sys:provision:provisioncollectionstate",
  "selfLink": "https://localhost/mgmt/tm/sys/provision?ver=13.0.0",
  "items": [
    {
      "kind": "tm:sys:provision:provisionstate",
      "name": "afm",
      "fullPath": "afm",
      "generation": 5609,

```

```

        "selfLink": "https://localhost/mgmt/tm/sys/provision/afm?ver=13.0.0",
        "cpuRatio": 0,
        "diskRatio": 0,
        "level": "none",
        "memoryRatio": 0
    },
    {
        "kind": "tm:sys:provision:provisionstate",
        "name": "ltm",
        "fullPath": "ltm",
        "generation": 1,
        "selfLink": "https://localhost/mgmt/tm/sys/provision/ltm?ver=13.0.0",
        "cpuRatio": 0,
        "diskRatio": 0,
        "level": "nominal",
        "memoryRatio": 0
    }
]
}

```

2. Retrieve single module provision state

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/sys/provision/{module}
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

Note: The **afm** module should still be provisioned after performing the steps in Lab 1.

```

{
    "kind": "tm:sys:provision:provisionstate",
    "name": "afm",
    "fullPath": "afm",
    "generation": 5609,
    "selfLink": "https://localhost/mgmt/tm/sys/provision/afm?ver=13.0.0",
    "cpuRatio": 0,
    "diskRatio": 0,
    "level": "none",
    "memoryRatio": 0
}

```

3.1. Provision module (OPTIONAL)

Warning: This step is optional and should only be performed if **afm** is not provisioned.

The **afm** module is provisioned using an HTTP PATCH with a body containing a provisioning level to the REST endpoint for `mgmt/tm/sys/provision/{{module}}`.

Note: Performing a provision/deprovision operation takes some time to complete. If the original request is still being processed, the below error may be encountered.

```
{
  "code": 400,
  "message": "01071003:3: A previous provisioning operation is in progress. Try_
↪again when the BIGIP is active.",
  "errorStack": [],
  "apiError": 3
}
```

Request

```
PATCH https://{{big_ip_a_mgmt}}/mgmt/tm/sys/provision/{{module}}
```

Headers

```
Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{
  "level": "nominal"
}
```

Example Response

Note: The **afm** module has been provisioned with a **level of nominal**.

```
{
  "kind": "tm:sys:provision:provisionstate",
  "name": "afm",
  "fullPath": "afm",
  "generation": 10636,
  "selfLink": "https://localhost/mgmt/tm/sys/provision/afm?ver=13.0.0",
  "cpuRatio": 0,
  "diskRatio": 0,
  "level": "nominal",
  "memoryRatio": 0
}
```

3.2. Deprovision module

This request will serve as an example of how to deprovision a BIG-IP module.

Request

```
PATCH https://{{big_ip_a_mgmt}}/mgmt/tm/sys/provision/{{module}}
```

Headers

```
Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{
  "level": "none"
}
```

Example Response

```
{
  "kind": "tm:sys:provision:provisionstate",
  "name": "afm",
  "fullPath": "afm",
  "generation": 10714,
  "selfLink": "https://localhost/mgmt/tm/sys/provision/afm?ver=13.0.0",
  "cpuRatio": 0,
  "diskRatio": 0,
  "level": "none",
  "memoryRatio": 0
}
```

3.3. Re-provision module

Re-provision the **afm** module if previously deprovisioned.

Request

```
PATCH https://{{big_ip_a_mgmt}}/mgmt/tm/sys/provision/{{module}}
```

Headers

```
Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{
  "level": "nominal"
}
```

Example Response

```
{
  "kind": "tm:sys:provision:provisionstate",
  "name": "afm",
  "fullPath": "afm",
  "generation": 10636,
  "selfLink": "https://localhost/mgmt/tm/sys/provision/afm?ver=13.0.0",
  "cpuRatio": 0,
  "diskRatio": 0,
  "level": "nominal",
  "memoryRatio": 0
}
```

4.3.2 Lab 2.2: Create AFM Address List

Overview

In this lab, the iControl REST based API will be used to create an address list that will be used with an AFM policy in a later lab.

Specific Instructions

Follow the below steps in order found in the Postman collection to complete this portion of the lab. The requests and responses have been included below for reference.

Attention: Some response content has been removed for brevity.

1. List Firewall Policies

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/security/firewall/policy
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

Note: A test policy has already been created on the BIG-IP for demonstration purposes.

```
{
  "kind": "tm:security:firewall:policy:polycollectionstate",
  "selfLink": "https://localhost/mgmt/tm/security/firewall/policy?ver=13.0.0",
  "items": [
    {
      "kind": "tm:security:firewall:policy:polycystate",
      "name": "block_all",
      "partition": "Common",
      "fullPath": "/Common/block_all",
      "generation": 5789,
      "selfLink": "https://localhost/mgmt/tm/security/firewall/policy/~Common~
↪block_all?ver=13.0.0",
      "rulesReference": {
        "link": "https://localhost/mgmt/tm/security/firewall/policy/~Common~
↪block_all/rules?ver=13.0.0",
        "isSubcollection": true
      }
    }
  ]
}
```


2. List all Firewall Address Lists

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/security/firewall/address-list
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

Note: A test address list has already been created on the BIG-IP for demonstration purposes.

```
{
  "kind": "tm:security:firewall:address-list:address-listcollectionstate",
  "selfLink": "https://localhost/mgmt/tm/security/firewall/address-list?ver=13.0.0",
  "items": [
    {
      "kind": "tm:security:firewall:address-list:address-liststate",
      "name": "test_address_list",
      "partition": "Common",
      "fullPath": "/Common/test_address_list",
      "generation": 6326,
      "selfLink": "https://localhost/mgmt/tm/security/firewall/address-list/~
↪Common~test_address_list?ver=13.0.0",
      "addresses": [
        {
          "name": "1.1.1.1"
        }
      ]
    }
  ]
}
```

3. Create an Address List

An HTTP POST to the `/mgmt/tm/security/firewall/address-list/` endpoint with a body containing the configuration creates an address list that can be used with a firewall policy.

Request

```
POST https://{big_ip_a_mgmt}/mgmt/tm/security/firewall/address-list/
```

Headers

```
Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{
  "name": "google-dns_address_list",
  "addresses": [
    {
```

```
        "name": "8.8.4.4"
      }
    ]
  }
}
```

Example Response

Note: Copy the **name** of the address list, highlighted below, from the response into the **afm_address_list** Postman environment variable.

```
{
  "kind": "tm:security:firewall:address-list:address-liststate",
  "name": "google-dns_address_list",
  "partition": "Common",
  "fullPath": "/Common/google-dns_address_list",
  "generation": 11436,
  "selfLink": "https://localhost/mgmt/tm/security/firewall/address-list/~Common~
↪google-dns_address_list?ver=13.0.0",
  "addresses": [
    {
      "name": "8.8.4.4"
    }
  ]
}
```

4. List Single Firewall Address List

Note: Ensure that the **afm_address_list** Postman environment variable has been populated with the name of the address list.

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/security/firewall/address-list/{afm_address_
↪list}}
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```
{
  "kind": "tm:security:firewall:address-list:address-liststate",
  "name": "google-dns_address_list",
  "partition": "Common",
  "fullPath": "/Common/google-dns_address_list",
  "generation": 11436,
  "selfLink": "https://localhost/mgmt/tm/security/firewall/address-list/~Common~
↪google-dns_address_list?ver=13.0.0",
  "addresses": [
    {
      "name": "8.8.4.4"
    }
  ]
}
```

```
}
  ]
}
```

5. Update Firewall Address List

An HTTP PATCH to the `/mgmt/tm/security/firewall/address-list/{afm_address_list}` endpoint with a body containing all addresses that should exist in the address list will update this collection.

Request

```
PATCH https://{big_ip_a_mgmt}/mgmt/tm/security/firewall/address-list/{afm_address_
↪list}}
```

Headers

```
Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Note: Include the contents of the address list plus the new address(es) to ensure that the contents are not overwritten.

Body

Warning: When patching an address list, be sure to include all addresses (e.g. existing and new) to ensure that the list does not get overwritten.

```
{
  "addresses": [
    {
      "name": "8.8.4.4"
    },
    {
      "name": "8.8.8.8"
    }
  ]
}
```

Example Response

```
{
  "kind": "tm:security:firewall:address-list:address-liststate",
  "name": "google-dns_address_list",
  "partition": "Common",
  "fullPath": "/Common/google-dns_address_list",
  "generation": 11436,
  "selfLink": "https://localhost/mgmt/tm/security/firewall/address-list/~Common~
↪google-dns_address_list?ver=13.0.0",
  "addresses": [
    {
      "name": "8.8.4.4"
    },
    {
      "name": "8.8.8.8"
    }
  ]
}
```

```
{
  {
    "name": "8.8.8.8"
  }
}
```

4.3.3 Lab 2.3: Create AFM Policy

Overview

In this lab, the iControl REST based API will be used to create a firewall policy that will leverage the previously created address list.

Specific Instructions

Follow the below steps in order found in the Postman collection to complete this portion of the lab. The requests and responses have been included below for reference.

Attention: Some response content has been removed for brevity.

1. List AFM policies

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/security/firewall/policy
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```
{
  "kind": "tm:security:firewall:policy:polycollectionstate",
  "selfLink": "https://localhost/mgmt/tm/security/firewall/policy?ver=13.0.0",
  "items": [
    {
      "kind": "tm:security:firewall:policy:polycystate",
      "name": "block_all",
      "partition": "Common",
      "fullPath": "/Common/block_all",
      "generation": 5789,
      "selfLink": "https://localhost/mgmt/tm/security/firewall/policy/~Common~
↪block_all?ver=13.0.0",
      "rulesReference": {
        "link": "https://localhost/mgmt/tm/security/firewall/policy/~Common~
↪block_all/rules?ver=13.0.0",
        "isSubcollection": true
      }
    }
  ]
}
```

2. Create AFM policy

An HTTP POST to the `/mgmt/tm/security/firewall/policy` endpoint with a body containing just a policy name creates a firewall policy.

Request

```
POST https://{{big_ip_a_mgmt}}/mgmt/tm/security/firewall/policy
```

Headers

```
Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{
  "name": "global_default_deny"
}
```

Example Response

Note: Copy the full policy name as it appears in the `"selfLink": "https://localhost/mgmt/tm/security/firewall/policy/~Common~global_default_deny?ver=13.0.0"` line of the response and populate the `{{afm_policy}}` Postman environment variable. In this case, the name of the policy is `~Common~global_default_deny`.

```
{
  "kind": "tm:security:firewall:policy:polycystate",
  "name": "global_default_deny",
  "partition": "Common",
  "fullPath": "/Common/global_default_deny",
  "generation": 11451,
  "selfLink": "https://localhost/mgmt/tm/security/firewall/policy/~Common~global_
↪default_deny?ver=13.0.0",
  "rulesReference": {
    "link": "https://localhost/mgmt/tm/security/firewall/policy/~Common~global_
↪default_deny/rules?ver=13.0.0",
    "isSubcollection": true
  }
}
```

3. List AFM policy rules

Request

```
GET https://{{big_ip_a_mgmt}}/mgmt/tm/security/firewall/policy/{{afm_policy}}/rules
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

Note: There will be no rules listed in the newly created policy. Rules are populated in the "items": [] sub collection.

```
{
  "kind": "tm:security:firewall:policy:rules:rulescollectionstate",
  "selfLink": "https://localhost/mgmt/tm/security/firewall/policy/~Common~global_
  ↳ default_deny/rules?ver=13.0.0",
  "items": []
}
```

4. Add default deny rule to policy

An HTTP POST to the /mgmt/tm/security/firewall/policy/{{afm_policy}}/rules endpoint with a body containing a new rule will add the rule to the firewall policy.

Request

```
POST https://{{big_ip_a_mgmt}}/mgmt/tm/security/firewall/policy/{{afm_policy}}/rules
```

Headers

```
Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{
  "name": "default_deny",
  "fullPath": "default_deny",
  "action": "drop",
  "ipProtocol": "any",
  "iruleSampleRate": 1,
  "log": "no",
  "status": "enabled",
  "destination": { }
  "place-before": "none"
}
```

Example Response

```
{
  "kind": "tm:security:firewall:policy:rules:rulesstate",
  "name": "default_deny",
  "fullPath": "default_deny",
  "generation": 11464,
  "selfLink": "https://localhost/mgmt/tm/security/firewall/policy/~Common~global_
  ↳ default_deny/rules/default_deny?ver=13.0.0",
  "action": "drop",
  "ipProtocol": "any",
  "iruleSampleRate": 1,
  "log": "no",
  "status": "enabled",
  "destination": {},
  "source": {
    "identity": {}
  }
}
```

```
}  
}
```

5. Add address list rule to policy

An HTTP POST to the `/mgmt/tm/security/firewall/policy/{{afm_policy}}/rules` endpoint with a body containing a new rule will add the rule to the firewall policy. The status of the rule can be specified when the POST is made.

Request

```
POST https://{{big_ip_a_mgmt}}/mgmt/tm/security/firewall/policy/{{afm_policy}}/rules
```

Headers

```
Content-Type: application/json  
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{  
  "name": "allow_google-dns",  
  "fullPath": "allow_google-dns",  
  "action": "accept",  
  "ipProtocol": "any",  
  "iruleSampleRate": 1,  
  "log": "no",  
  "status": "enabled",  
  "placeBefore": "default_deny",  
  "destination": {  
    "addressLists": [  
      "/Common/google-dns_address_list"  
    ]  
  }  
}
```

Example Response

Note: Copy the newly created rule name `allow_google-dns` and populate the `{{afm_policy_rule}}` Postman environment variable.

```
{  
  "kind": "tm:security:firewall:policy:rules:rulesstate",  
  "name": "allow_google-dns",  
  "fullPath": "allow_google-dns",  
  "generation": 13210,  
  "selfLink": "https://localhost/mgmt/tm/security/firewall/policy/~Common~global_  
→default_deny/rules/allow_google-dns?ver=13.0.0",  
  "action": "accept",  
  "ipProtocol": "any",  
  "iruleSampleRate": 1,  
  "log": "no",  
  "status": "enabled",  
  "destination": {  
    "addressLists": [  

```

```

        "/Common/google-dns_address_list"
    ],
    "addressListsReference": [
        {
            "link": "https://localhost/mgmt/tm/security/firewall/address-list/~Common~
↪allow_google-dns?ver=13.0.0"
        }
    ]
},
"source": {
    "identity": {}
}
}

```

6. List policy rules

The "items" sub collection will now be populated with the all the firewall rules when performing an HTTP GET on the rules endpoint of the **{{afm_policy}}**.

Request

```
GET https://{{big_ip_a_mgmt}}/mgmt/tm/security/firewall/policy/{{afm_policy}}/rules
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```

{
    "kind": "tm:security:firewall:policy:rules:rulescollectionstate",
    "selfLink": "https://localhost/mgmt/tm/security/firewall/policy/~Common~global_
↪default_deny/rules?ver=13.0.0",
    "items": [
        {
            "kind": "tm:security:firewall:policy:rules:rulesstate",
            "name": "allow_google-dns",
            "fullPath": "allow_google-dns",
            "generation": 11483,
            "selfLink": "https://localhost/mgmt/tm/security/firewall/policy/~
↪Common~global_default_deny/rules/allow_google-dns?ver=13.0.0",
            "action": "accept",
            "ipProtocol": "any",
            "iruleSampleRate": 1,
            "log": "yes",
            "status": "enabled",
            "destination": {
                "addressLists": [
                    "/Common/google-dns_address_list"
                ],
                "addressListsReference": [
                    {
                        "link": "https://localhost/mgmt/tm/security/firewall/address-
↪list/~Common~google-dns_address_list?ver=13.0.0"
                    }
                ]
            },

```



```

        "source": {
            "identity": {}
        },
        {
            "kind": "tm:security:firewall:policy:rules:rulesstate",
            "name": "default_deny",
            "fullPath": "default_deny",
            "generation": 11464,
            "selfLink": "https://localhost/mgmt/tm/security/firewall/policy/~
↪Common~global_default_deny/rules/default_deny?ver=13.0.0",
            "action": "drop",
            "ipProtocol": "any",
            "iruleSampleRate": 1,
            "log": "no",
            "status": "enabled",
            "destination": {},
            "source": {
                "identity": {}
            }
        }
    ]
}

```

7. Disable Policy rule

An HTTP PATCH to the `/mgmt/tm/security/firewall/policy/{{afm_policy}}/rules/{{afm_policy_rule}}` endpoint with a body containing a name of an existing rule can set the `"status": "disabled"` to deactivate a single rule.

Request

```

PATCH https://{{big_ip_a_mgmt}}/mgmt/tm/security/firewall/policy/{{afm_policy}}/rules/
↪{{afm_policy_rule}}

```

Headers

```

Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}

```

Body

```

{
    "status": "disabled"
}

```

Example Response

```

{
    "kind": "tm:security:firewall:policy:rules:rulesstate",
    "name": "allow_google-dns",
    "fullPath": "allow_google-dns",
    "generation": 11470,
    "selfLink": "https://localhost/mgmt/tm/security/firewall/policy/~Common~global_
↪default_deny/rules/allow_google-dns?ver=13.0.0",
    "action": "accept",

```

```

    "ipProtocol": "any",
    "iruleSampleRate": 1,
    "log": "no",
    "status": "disabled",
    "destination": {
      "addressLists": [
        "/Common/google-dns_address_list"
      ],
      "addressListsReference": [
        {
          "link": "https://localhost/mgmt/tm/security/firewall/address-list/~
↪Common~google-dns_address_list?ver=13.0.0"
        }
      ]
    },
    "source": {
      "identity": {}
    }
  }
}

```

8. List policy rule

Request

```

GET https://{big_ip_a_mgmt}/mgmt/tm/security/firewall/policy/{afm_policy}/rules/{
↪afm_policy_rule}

```

Headers

```

X-F5-Auth-Token: {big_ip_a_auth_token}

```

Example Response

```

{
  "kind": "tm:security:firewall:policy:rules:rulesstate",
  "name": "allow_google-dns",
  "fullPath": "allow_google-dns",
  "generation": 11483,
  "selfLink": "https://localhost/mgmt/tm/security/firewall/policy/~Common~global_
↪default_deny/rules/allow_google-dns?ver=13.0.0",
  "action": "accept",
  "ipProtocol": "any",
  "iruleSampleRate": 1,
  "log": "yes",
  "status": "disabled",
  "destination": {
    "addressLists": [
      "/Common/google-dns_address_list"
    ],
    "addressListsReference": [
      {
        "link": "https://localhost/mgmt/tm/security/firewall/address-list/~Common~
↪google-dns_address_list?ver=13.0.0"
      }
    ]
  },
}

```

```
"source": {  
  "identity": {}  
}  
}
```

4.4 Module 3: Programmatic Control of Web Application Firewall Services

- Provision ASM module on BIG-IP
- Interact with ASM related REST endpoints on a BIG-IP
- Create and modify an ASM policy
- Apply the ASM policy to a virtual server

4.4.1 Lab 3.1: Provisioning ASM

Overview

In this lab, the iControl REST API will be used to provision a module on the BIG-IP. More specifically, the Application Security Manager (ASM) module will be provisioned for use in **Module 3: Configuring ASM (Application Security Module)**.

Specific Instructions

Prior to performing the steps below, validate the **{{module}}** Postman environment variable. The **{{module}}** should be set to **asm**.

Follow the below steps in order found in the Postman collection to complete this portion of the lab. The requests and responses have been included below for reference.

Attention: Some response content has been removed for brevity.

1. Deprovision AFM module

This request will serve as an example of how to deprovision a BIG-IP module.

Request

```
PATCH https://{{big_ip_a_mgmt}}/mgmt/tm/sys/provision/afm
```

Headers

```
Content-Type: application/json  
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{
  "level": "none"
}
```

Example Response

```
{
  "kind": "tm:sys:provision:provisionstate",
  "name": "afm",
  "fullPath": "afm",
  "generation": 10714,
  "selfLink": "https://localhost/mgmt/tm/sys/provision/afm?ver=13.0.0",
  "cpuRatio": 0,
  "diskRatio": 0,
  "level": "none",
  "memoryRatio": 0
}
```

2. Retrieve all module provision states

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/sys/provision
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

Note: The **asm** module is currently provisioned for **none** while the **ltm** module is provisioned for **nominal**.

```
{
  "kind": "tm:sys:provision:provisioncollectionstate",
  "selfLink": "https://localhost/mgmt/tm/sys/provision?ver=13.0.0",
  "items": [
    {
      "kind": "tm:sys:provision:provisionstate",
      "name": "asm",
      "fullPath": "asm",
      "generation": 5609,
      "selfLink": "https://localhost/mgmt/tm/sys/provision/asm?ver=13.0.0",
      "cpuRatio": 0,
      "diskRatio": 0,
      "level": "none",
      "memoryRatio": 0
    },
    {
      "kind": "tm:sys:provision:provisionstate",
      "name": "ltm",
      "fullPath": "ltm",
      "generation": 1,
      "selfLink": "https://localhost/mgmt/tm/sys/provision/ltm?ver=13.0.0",
      "cpuRatio": 0,

```

```
        "diskRatio": 0,
        "level": "nominal",
        "memoryRatio": 0
      }
    ]
  }
```

3. Retrieve single module provision state

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/sys/provision/{module}
```

Headers

```
X-F5-Auth-Token: {big_ip_a_auth_token}
```

Example Response

Note: The **asm** module is currently not provisioned.

```
{
  "kind": "tm:sys:provision:provisionstate",
  "name": "asm",
  "fullPath": "asm",
  "generation": 5609,
  "selfLink": "https://localhost/mgmt/tm/sys/provision/asm?ver=13.0.0",
  "cpuRatio": 0,
  "diskRatio": 0,
  "level": "none",
  "memoryRatio": 0
}
```

4. Provision ASM module

The **asm** module is provisioned using an HTTP PATCH with a body containing a provisioning level to the REST endpoint for `mgmt/tm/sys/provision/{module}`.

Request

```
PATCH https://{big_ip_a_mgmt}/mgmt/tm/sys/provision/{module}
```

Headers

```
X-F5-Auth-Token: {big_ip_a_auth_token}
```

Body

```
{
  "level": "nominal"
}
```

Example Response

Note: The **asm** module has been provisioned with a **level** of **nominal**.

```
{
  "kind": "tm:sys:provision:provisionstate",
  "name": "asm",
  "fullPath": "asm",
  "generation": 10636,
  "selfLink": "https://localhost/mgmt/tm/sys/provision/asm?ver=13.0.0",
  "cpuRatio": 0,
  "diskRatio": 0,
  "level": "nominal",
  "memoryRatio": 0
}
```

4.4.2 Lab 3.2: Interact with ASM

Overview

In this lab, the iControl REST based API will be used to explore some of the ASM related endpoints.

Specific Instructions

Follow the below steps in order found in the Postman collection to complete this portion of the lab. The requests and responses have been included below for reference.

Attention: Some response content has been removed for brevity.

1.0. Retrieve ASM resources

Request

```
GET https://{{big_ip_a_mgmt}}/mgmt/tm/asm
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```
{
  "kind": "tm:asm:asmcollectionstate",
  "selfLink": "https://localhost/mgmt/tm/asm?ver=13.0.0",
  "items": [
    {
      "reference": {
        "link": "https://localhost/mgmt/tm/asm/policies?ver=13.0.0"
      }
    },
  ],
}
```

```

        {
          "reference": {
            "link": "https://localhost/mgmt/tm/asm/server-technologies?ver=13.0.0"
          }
        }
      ]
    }
  }
}

```

1.1. Retrieve ASM server technologies

Request

```
GET https://{{big_ip_a_mgmt}}/mgmt/tm/asm/server-technologies
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```

{
  "kind": "tm:asm:server-technologies:server-technologycollectionstate",
  "selfLink": "https://localhost/mgmt/tm/asm/server-technologies?ver=13.0.0",
  "totalItems": 40,
  "items": [
    {
      "serverTechnologyDisplayName": "jQuery",
      "serverTechnologyName": "jQuery",
      "logoFileName": "jquery.png",
      "lastUpdateMicros": 1476919661000000,
      "description": "jQuery is a cross-platform JavaScript library designed to_
↪simplify the client-side scripting of HTML.",
      "kind": "tm:asm:server-technologies:server-technologystate",
      "serverTechnologyReferences": [],
      "selfLink": "https://localhost/mgmt/tm/asm/server-technologies/9ZC0_aLDC-
↪KN08jDyvXHew?ver=13.0.0",
      "id": "9ZC0_aLDC-KN08jDyvXHew"
    },
    {
      "serverTechnologyDisplayName": "Java Servlets/JSP",
      "serverTechnologyName": "Java Servlets/JSP",
      "logoFileName": "java.png",
      "lastUpdateMicros": 1476919661000000,
      "description": "A Java servlet is a Java program that extends the_
↪capabilities of a server.",
      "kind": "tm:asm:server-technologies:server-technologystate",
      "serverTechnologyReferences": [],
      "selfLink": "https://localhost/mgmt/tm/asm/server-technologies/
↪9ySigIBMpBbYU4r8FNAt4g?ver=13.0.0",
      "id": "9ySigIBMpBbYU4r8FNAt4g"
    }
  ]
}

```

2.0. Retrieve ASM policies

A test policy named `test_asm_policy` has already been created on the BIG-IP for demonstration purposes.

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/asm/policies
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

Note: Copy the ASM policy hash as it appears in the "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaUOag/plain-text-profiles?ver=13.0.0", line of the response and populate the `{{asm_policy_hash}}` Postman environment variable.

```
{
  "kind": "tm:asm:policies:policycollectionstate",
  "selfLink": "https://localhost/mgmt/tm/asm/policies?ver=13.0.0",
  "totalItems": 1,
  "items": [
    {
      "plainTextProfileReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaUOag/
↪plain-text-profiles?ver=13.0.0",
        "isSubCollection": true
      },
      "dataGuardReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaUOag/
↪data-guard?ver=13.0.0"
      }
    }
  ]
}
```

2.1. Retrieve ASM policy

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/asm/policies/{{asm_policy_hash}}
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```
{
  "plainTextProfileReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaUOag/plain-
↪text-profiles?ver=13.0.0",
    "isSubCollection": true
  },
}
```



```

    "dataGuardReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaU0ag/data-
↪guard?ver=13.0.0"
    },
    "createdDatetime": "2017-06-02T04:37:22Z",
    "cookieSettingsReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaU0ag/cookie-
↪settings?ver=13.0.0"
    },
    "versionLastChange": " Security Policy /Common/test_asm_policy [add]: Type was_
↪set to Security.\nEncoding Selected was set to false.\nApplication Language was set_
↪to utf-8.\nCase Sensitivity was set to Case Sensitive.\nTemplate was set to POLICY_
↪TEMPLATE_FUNDAMENTAL.\nActive was set to false.\nDifferentiate between HTTP and_
↪HTTPS URLs was set to Protocol Specific.\nPolicy Name was set to /Common/test_asm_
↪policy.\nEnforcement Mode was set to Blocking. { audit: policy = /Common/test_asm_
↪policy, username = admin, client IP = 192.168.2.111 }",
    "name": "test_asm_policy",
    "caseInsensitive": false,
    "headerSettingsReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaU0ag/header-
↪settings?ver=13.0.0"
    },
    "versionPolicyName": "/Common/test_asm_policy",
    "generalReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaU0ag/
↪general?ver=13.0.0"
    }
  }
}

```

3. Search for ASM policy

An HTTP GET to the /mgmt/tm/asm/policies endpoint with a parameter of filter=name eq test, allows ASM policies to be searched by name.

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/asm/policies?filter=name eq test
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```

{
  "plainTextProfileReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaU0ag/plain-
↪text-profiles?ver=13.0.0",
    "isSubCollection": true
  },
  "dataGuardReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaU0ag/data-
↪guard?ver=13.0.0"
  },
  "createdDatetime": "2017-06-02T04:37:22Z",
  "cookieSettingsReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaU0ag/cookie-
↪settings?ver=13.0.0"
  }
}

```

```

    },
    "versionLastChange": " Security Policy /Common/test_asm_policy [add]: Type was_
↪set to Security.\nEncoding Selected was set to false.\nApplication Language was set_
↪to utf-8.\nCase Sensitivity was set to Case Sensitive.\nTemplate was set to POLICY_
↪TEMPLATE_FUNDAMENTAL.\nActive was set to false.\nDifferentiate between HTTP and_
↪HTTPS URLs was set to Protocol Specific.\nPolicy Name was set to /Common/test_asm_
↪policy.\nEnforcement Mode was set to Blocking. { audit: policy = /Common/test_asm_
↪policy, username = admin, client IP = 192.168.2.111 }",
    "name": "test_asm_policy",
    "caseInsensitive": false,
    "headerSettingsReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaU0ag/header-
↪settings?ver=13.0.0"
    },
    "versionPolicyName": "/Common/test_asm_policy",
    "generalReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaU0ag/
↪general?ver=13.0.0"
    }
}

```

4.0. List ASM tasks

An HTTP GET to the `/mgmt/tm/asm/tasks/` endpoint lists the various ASM related tasks that can be performed via the iControl REST API.

Request

```
GET https://{{big_ip_a_mgmt}}/mgmt/tm/asm/tasks/
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```

{
  "kind": "tm:asm:tasks",
  "selfLink": "https://localhost/mgmt/tm/asm/tasks?ver=13.0.0",
  "items": [
    {
      "reference": {
        "link": "https://localhost/mgmt/tm/asm/tasks/export-policy?ver=13.0.0"
      }
    },
    {
      "reference": {
        "link": "https://localhost/mgmt/tm/asm/tasks/resolve-vulnerabilities?
↪ver=13.0.0"
      }
    },
    {
      "reference": {
        "link": "https://localhost/mgmt/tm/asm/tasks/check-signatures?ver=13.
↪0.0"
      }
    }
  ],
}

```

```

        {
            "reference": {
                "link": "https://localhost/mgmt/tm/asm/tasks/terminate-vulnerability-
↪assessment?ver=13.0.0"
            }
        },
        {
            "reference": {
                "link": "https://localhost/mgmt/tm/asm/tasks/apply-server-
↪technologies?ver=13.0.0"
            }
        },
        {
            "reference": {
                "link": "https://localhost/mgmt/tm/asm/tasks/associate-xml-validation-
↪files-to-xml-profile?ver=13.0.0"
            }
        },
        {
            "reference": {
                "link": "https://localhost/mgmt/tm/asm/tasks/export-policy-template?
↪ver=13.0.0"
            }
        },
        {
            "reference": {
                "link": "https://localhost/mgmt/tm/asm/tasks/export-requests?ver=13.0.
↪0"
            }
        },
        {
            "reference": {
                "link": "https://localhost/mgmt/tm/asm/tasks/initiate-vulnerability-
↪assessment?ver=13.0.0"
            }
        },
        {
            "reference": {
                "link": "https://localhost/mgmt/tm/asm/tasks/import-policy-template?
↪ver=13.0.0"
            }
        },
        {
            "reference": {
                "link": "https://localhost/mgmt/tm/asm/tasks/update-signatures?ver=13.
↪0.0"
            }
        },
        {
            "reference": {
                "link": "https://localhost/mgmt/tm/asm/tasks/import-policy?ver=13.0.0"
            }
        },
        {
            "reference": {
                "link": "https://localhost/mgmt/tm/asm/tasks/bulk?ver=13.0.0"
            }
        },
    ],

```

```

    {
      "reference": {
        "link": "https://localhost/mgmt/tm/asm/tasks/get-vulnerability-
↪assessment-subscriptions?ver=13.0.0"
      }
    },
    {
      "reference": {
        "link": "https://localhost/mgmt/tm/asm/tasks/apply-policy?ver=13.0.0"
      }
    },
    {
      "reference": {
        "link": "https://localhost/mgmt/tm/asm/tasks/export-signatures?ver=13.
↪0.0"
      }
    },
    {
      "reference": {
        "link": "https://localhost/mgmt/tm/asm/tasks/import-vulnerabilities?
↪ver=13.0.0"
      }
    }
  ]
}

```

4.1. List specific ASM task

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/asm/tasks/export-policy
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```

{
  "kind": "tm:asm:tasks:export-policy:export-policy-taskcollectionstate",
  "selfLink": "https://localhost/mgmt/tm/asm/tasks/export-policy?ver=13.0.0",
  "totalItems": 0,
  "items": []
}

```

5. Retrieve ASM policy templates

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/asm/policy-templates
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```
{
  "kind": "tm:asm:policy-templates:policy-templatecollectionstate",
  "selfLink": "https://localhost/mgmt/tm/asm/policy-templates?ver=13.0.0",
  "totalItems": 32,
  "items": [
    {
      "policyType": "security",
      "name": "POLICY_TEMPLATE_SHAREPOINT_2007_HTTP",
      "description": "Generic template for SharePoint 2007 (http)",
      "kind": "tm:asm:policy-templates:policy-templatestate",
      "templateType": "application-ready",
      "selfLink": "https://localhost/mgmt/tm/asm/policy-templates/jmHjN-Fpm-
      ↪SGwYQsrZp57A?ver=13.0.0",
      "templateDefaults": {
        "caseInsensitive": true,
        "learningSpeed": {
          "untrustedTrafficSiteChangeTracking": {
            "maxDaysBetweenSamples": 7,
            "differentSources": 10,
            "minMinutesBetweenSamples": 5
          },
          "untrustedTrafficLoosen": {
            "maxDaysBetweenSamples": 7,
            "differentSources": 20,
            "minHoursBetweenSamples": 1
          },
          "trustedTrafficSiteChangeTracking": {
            "maxDaysBetweenSamples": 7,
            "differentSources": 1,
            "minMinutesBetweenSamples": 0
          },
          "trustedTrafficLoosen": {
            "maxDaysBetweenSamples": 7,
            "differentSources": 1,
            "minHoursBetweenSamples": 0
          },
          "trafficTighten": {
            "minDaysBetweenSamples": 1,
            "totalRequests": 15000,
            "maxModificationSuggestionScore": 50
          }
        },
        "enforcementReadinessPeriod": 7,
        "learningMode": "disabled",
        "applicationLanguage": "utf-8",
        "enforcementMode": "transparent",
        "signatureStaging": true,
        "type": "security",
        "protocolIndependent": false
      },
      "title": "SharePoint 2007 (http)",
      "id": "jmHjN-Fpm-SGwYQsrZp57A"
    }
  ]
}
```

6. Retrieve ASM signature sets

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/asm/signature-sets
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```
{
  "kind": "tm:asm:signature-sets:signature-setcollectionstate",
  "selfLink": "https://localhost/mgmt/tm/asm/signature-sets?ver=13.0.0",
  "totalItems": 29,
  "items": [
    {
      "filter": {
        "riskFilter": "all",
        "accuracyFilter": "all",
        "userDefinedFilter": "all",
        "lastUpdatedFilter": "all",
        "accuracyValue": "all",
        "riskValue": "all",
        "signatureType": "all"
      },
      "isUserDefined": false,
      "name": "Generic Detection Signatures",
      "assignToPolicyByDefault": true,
      "lastUpdateMicros": 0,
      "kind": "tm:asm:signature-sets:signature-setstate",
      "selfLink": "https://localhost/mgmt/tm/asm/signature-sets/pBeUaadz6x-Z55_
↪GkLxfsg?ver=13.0.0",
      "defaultAlarm": true,
      "systems": [
        {
          "systemReference": {
            "link": "https://localhost/mgmt/tm/asm/signature-systems/
↪ESdDgGiP9nSPgKBhSlDyvQ?ver=13.0.0"
          }
        },
        {
          "systemReference": {
            "link": "https://localhost/mgmt/tm/asm/signature-systems/
↪rMiBJmL6DLmnfmW_pXHmdw?ver=13.0.0"
          }
        },
        {
          "systemReference": {
            "link": "https://localhost/mgmt/tm/asm/signature-systems/
↪b9hIlsIulARJ09bbdy0VQw?ver=13.0.0"
          }
        }
      ],
      "id": "pBeUaadz6x-Z55_GkLxfsg",
      "type": "filter-based",
      "signatureReferences": [
```

```

        {
          "link": "https://localhost/mgmt/tm/asm/signatures/nHU-8zUxj8ldUevwMgFpvw?
↪ver=13.0.0"
        },
        {
          "link": "https://localhost/mgmt/tm/asm/signatures/RTFj6E66sH7g7XMa9ihQQQ?
↪ver=13.0.0"
        }
      ],
      "category": "User-defined",
      "defaultBlock": true,
      "defaultLearn": true
    }
  ]
}

```

7. Retrieve ASM signature systems

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/asm/signature-systems
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```

{
  "kind": "tm:asm:signature-systems:signature-systemcollectionstate",
  "selfLink": "https://localhost/mgmt/tm/asm/signature-systems?ver=13.0.0",
  "totalItems": 44,
  "items": [
    {
      "kind": "tm:asm:signature-systems:signature-systemstate",
      "selfLink": "https://localhost/mgmt/tm/asm/signature-systems/
↪EstDgGiP9nSPgKBhSlDyvQ?ver=13.0.0",
      "name": "General Database",
      "id": "EstDgGiP9nSPgKBhSlDyvQ"
    },
    {
      "kind": "tm:asm:signature-systems:signature-systemstate",
      "selfLink": "https://localhost/mgmt/tm/asm/signature-systems/
↪rMiBJmL6DLmnfmW_pXHmdw?ver=13.0.0",
      "name": "Various systems",
      "id": "rMiBJmL6DLmnfmW_pXHmdw"
    }
  ]
}

```

8. Retrieve ASM attack types

Request

```
GET https://{{big_ip_a_mgmt}}/mgmt/tm/asm/attack-types
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```
{
  "kind": "tm:asm:attack-types:attack-typecollectionstate",
  "selfLink": "https://localhost/mgmt/tm/asm/attack-types?ver=13.0.0",
  "totalItems": 37,
  "items": [
    {
      "kind": "tm:asm:attack-types:attack-typestate",
      "selfLink": "https://localhost/mgmt/tm/asm/attack-types/9yL3q5_
↪p00E3pK1Uz9x2cw?ver=13.0.0",
      "name": "Remote File Include",
      "id": "9yL3q5_p00E3pK1Uz9x2cw",
      "description": "Remote File Inclusion attacks allow attackers to run_
↪arbitrary code on a vulnerable website."
    },
    {
      "kind": "tm:asm:attack-types:attack-typestate",
      "selfLink": "https://localhost/mgmt/tm/asm/attack-types/
↪ufg0smEkZrpmkoDHfSPGdQ?ver=13.0.0",
      "name": "Non-browser Client",
      "id": "ufg0smEkZrpmkoDHfSPGdQ",
      "description": "An attempt is made by a non-browser client to explore the_
↪site."
    }
  ]
}
```

9. Retrieve ASM policy urls

Request

```
GET https://{{big_ip_a_mgmt}}/mgmt/tm/asm/policies/{{asm_policy_hash}}/urls
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```
{
  "kind": "tm:asm:policies:urls:urlcollectionstate",
  "selfLink": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaU0ag/urls?
↪ver=13.0.0",
  "totalItems": 2,
  "items": [
    {
      "protocol": "http",
      "wildcardIncludesSlash": true,
      "lastLearnedNewEntityDatetime": "2017-06-02T04:37:25Z",
    }
  ]
}
```



```

    "html5CrossOriginRequestsEnforcement": {
      "enforcementMode": "disabled"
    },
    "kind": "tm:asm:policies:urls:urlstate",
    "selfLink": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaUOag/
↪urls/faiefv884qtHRU3Qva2AbQ?ver=13.0.0",
    "methodsOverrideOnUrlCheck": false,
    "id": "faiefv884qtHRU3Qva2AbQ",
    "isAllowed": true,
    "metacharsOnUrlCheck": false,
    "name": "*",
    "lastUpdateMicros": 1496378251000000,
    "description": "",
    "parameterReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaUOag/
↪urls/faiefv884qtHRU3Qva2AbQ/parameters?ver=13.0.0",
      "isSubCollection": true
    },
    "attackSignaturesCheck": true,
    "signatureOverrides": [],
    "clickjackingProtection": false,
    "urlContentProfiles": [
      {
        "headerValue": "*",
        "headerName": "*",
        "headerOrder": "default",
        "type": "apply-value-and-content-signatures"
      },
      {
        "headerValue": "*form*",
        "headerName": "Content-Type",
        "headerOrder": "1",
        "type": "form-data"
      },
      {
        "contentProfileReference": {
          "link": "https://localhost/mgmt/tm/asm/policies/W-
↪w3q351kYbr1A90EaUOag/json-profiles/X8FbXF48VWJ5Tecp5ATd4A?ver=13.0.0"
        },
        "headerValue": "*json*",
        "headerName": "Content-Type",
        "headerOrder": "2",
        "type": "json"
      },
      {
        "contentProfileReference": {
          "link": "https://localhost/mgmt/tm/asm/policies/W-
↪w3q351kYbr1A90EaUOag/xml-profiles/jwQd_XYZPfNGYnc3l7P4Pg?ver=13.0.0"
        },
        "headerValue": "*xml*",
        "headerName": "Content-Type",
        "headerOrder": "3",
        "type": "xml"
      }
    ],
    "performStaging": true,
    "type": "wildcard",
    "wildcardOrder": 2

```

```

    },
    {
      "protocol": "https",
      "wildcardIncludesSlash": true,
      "lastLearnedNewEntityDatetime": "2017-06-02T04:37:25Z",
      "html5CrossOriginRequestsEnforcement": {
        "enforcementMode": "disabled"
      },
      "kind": "tm:asm:policies:urls:urlstate",
      "selfLink": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaUOag/
↪urls/N_a3D1S7OKDehYEPb-mgCg?ver=13.0.0",
      "methodsOverrideOnUrlCheck": false,
      "id": "N_a3D1S7OKDehYEPb-mgCg",
      "isAllowed": true,
      "metacharsOnUrlCheck": false,
      "name": "*",
      "lastUpdateMicros": 1496378251000000,
      "description": "",
      "parameterReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaUOag/
↪urls/N_a3D1S7OKDehYEPb-mgCg/parameters?ver=13.0.0",
        "isSubCollection": true
      },
      "attackSignaturesCheck": true,
      "signatureOverrides": [],
      "clickjackingProtection": false,
      "urlContentProfiles": [
        {
          "headerValue": "*",
          "headerName": "*",
          "headerOrder": "default",
          "type": "apply-value-and-content-signatures"
        },
        {
          "headerValue": "*form*",
          "headerName": "Content-Type",
          "headerOrder": "1",
          "type": "form-data"
        },
        {
          "contentProfileReference": {
            "link": "https://localhost/mgmt/tm/asm/policies/W-
↪w3q351kYbr1A90EaUOag/json-profiles/X8FbXF48VWJ5Tecp5ATd4A?ver=13.0.0"
          },
          "headerValue": "*json*",
          "headerName": "Content-Type",
          "headerOrder": "2",
          "type": "json"
        },
        {
          "contentProfileReference": {
            "link": "https://localhost/mgmt/tm/asm/policies/W-
↪w3q351kYbr1A90EaUOag/xml-profiles/jwQd_XYZPfNGYnc3l7P4Pg?ver=13.0.0"
          },
          "headerValue": "*xml*",
          "headerName": "Content-Type",
          "headerOrder": "3",
          "type": "xml"
        }
      ]
    }
  ]
}

```

```

    }
  ],
  "performStaging": true,
  "type": "wildcard",
  "wildcardOrder": 1
}
]
}

```

10. Retrieve ASM policy signature sets

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/asm/policies/{asm_policy_hash}/signature-sets
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```

{
  "kind": "tm:asm:policies:signature-sets:signature-setcollectionstate",
  "selfLink": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaUOag/
↪signature-sets?ver=13.0.0",
  "totalItems": 1,
  "items": [
    {
      "signatureSetReference": {
        "link": "https://localhost/mgmt/tm/asm/signature-sets/pBeUaadz6x-Z55_
↪GkLxfsg?ver=13.0.0"
      },
      "lastUpdateMicros": 1496378251000000,
      "selfLink": "https://localhost/mgmt/tm/asm/policies/W-w3q351kYbr1A90EaUOag/
↪signature-sets/xMpCOKC5I4INzFCab3WEmw?ver=13.0.0",
      "kind": "tm:asm:policies:signature-sets:signature-setstate",
      "alarm": true,
      "block": true,
      "id": "xMpCOKC5I4INzFCab3WEmw",
      "learn": true
    }
  ]
}

```

4.4.3 Lab 3.3: Create ASM Policy

Overview

In this lab, the iControl REST based API will be used to create both an ASM parent and child policy.

Specific Instructions

Follow the below steps in order found in the Postman collection to complete this portion of the lab. The requests and responses have been included below for reference.

Attention: Some response content has been removed for brevity.

1. Retrieve ASM policy

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/asm/policies
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```
{
  "kind": "tm:asm:policies:policycollectionstate",
  "selfLink": "https://localhost/mgmt/tm/asm/policies?ver=13.0.0",
  "totalItems": 1,
  "items": [
    {
      "plainTextProfileReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/8JuF2s3Lb26BYwLXpaHLIg/
↪plain-text-profiles?ver=13.0.0",
        "isSubCollection": true
      },
      "dataGuardReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/8JuF2s3Lb26BYwLXpaHLIg/
↪data-guard?ver=13.0.0"
      }
    }
  ]
}
```

2.0. Create ASM parent policy

An HTTP POST to the `/mgmt/tm/asm/policies` endpoint with a body containing basic policy configuration including `"type": "parent"` will create a new ASM parent policy which can then be used for inheritance when a child policy is created.

Request

```
POST https://{big_ip_a_mgmt}/mgmt/tm/asm/policies
```

Headers

```
Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{
  "name": "API_ASM_POLICY_TEST",
  "description": "Test ASM policy",
  "applicationLanguage": "utf-8",
  "type": "parent",
}
```

```
    "enforcementMode": "transparent",
    "protocolIndependent": "true",
    "learningMode": "disabled",
    "serverTechnologyName": "Unix/Linux"
}
```

Example Response

Note: Copy the ASM policy hash for the newly created policy and populate the {{asm_policy_hash}} Postman environment variable. The hash in the example below is JEQPVWeJcdso_rEC7Xxo6Q

```
{
  "historyRevisionReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q/
↪history-revisions?ver=13.0.0",
    "isSubCollection": true
  },
  "childPolicyCount": 0,
  "responsePageReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q/
↪response-pages?ver=13.0.0",
    "isSubCollection": true
  },
  "policyBuilderReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q/policy-
↪builder?ver=13.0.0"
  },
  "serverTechnologyReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q/server-
↪technologies?ver=13.0.0",
    "isSubCollection": true
  },
  "blockingSettingReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q/
↪blocking-settings?ver=13.0.0",
    "isSubCollection": true
  },
  "hostNameReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q/host-
↪names?ver=13.0.0",
    "isSubCollection": true
  },
  "dataGuardReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q/data-
↪guard?ver=13.0.0"
  },
  "selfLink": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q?ver=13.
↪0.0",
  "signatureReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q/
↪signatures?ver=13.0.0",
    "isSubCollection": true
  },
  "filetypeReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q/
↪filetypes?ver=13.0.0",

```

```

        "isSubCollection": true
    },
    "createdDatetime": "2017-05-30T15:02:11Z",
    "modifierName": "",
    "id": "JEqPVWeJcdso_rEC7Xxo6Q",
    "subPath": "/Common",
    "name": "API_ASM_POLICY_TEST",
    "caseInsensitive": false,
    "headerSettingsReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/JEqPVWeJcdso_rEC7Xxo6Q/header-
↪settings?ver=13.0.0"
    }
}

```

2.1. Retrieve ASM parent policy

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/asm/policies/{asm_policy_hash}
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```

{
    "historyRevisionReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/JEqPVWeJcdso_rEC7Xxo6Q/
↪history-revisions?ver=13.0.0",
        "isSubCollection": true
    },
    "childPolicyCount": 0,
    "responsePageReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/JEqPVWeJcdso_rEC7Xxo6Q/
↪response-pages?ver=13.0.0",
        "isSubCollection": true
    },
    "policyBuilderReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/JEqPVWeJcdso_rEC7Xxo6Q/policy-
↪builder?ver=13.0.0"
    },
    "serverTechnologyReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/JEqPVWeJcdso_rEC7Xxo6Q/server-
↪technologies?ver=13.0.0",
        "isSubCollection": true
    }
}

```

3.0. Create ASM child policy

An HTTP POST to the `/mgmt/tm/asm/policies` endpoint with a body containing basic policy configuration including `"parentPolicyName": "/Common/API_ASM_POLICY_TEST"` will create a new child policy which inherits a base configuration from the specified parent.

Request

```
POST https://{{big_ip_a_mgmt}}/mgmt/tm/asm/policies
```

Headers

```
Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{
  "name": "API_ASM_POLICY_CHILD_TEST",
  "description": "Test ASM policy",
  "applicationLanguage": "utf-8",
  "parentPolicyName": "/Common/API_ASM_POLICY_TEST",
  "enforcementMode": "transparent",
  "protocolIndependent": "true",
  "learningMode": "automatic",
  "learningSpeed": "slow",
  "serverTechnologyName": "Apache Tomcat"
}
```

Example Response

Note: Take note of the ASM policy hash for the newly created policy. Copy this value into your Postman's collection environmental variable for `{{asm_policy_hash}}`

The hash in the example below is `zD8sehZULw6Ni7GJG2XwJQ`

```
{
  "plainTextProfileReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/plain-
↪text-profiles?ver=13.0.0",
    "isSubCollection": true
  },
  "dataGuardReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/data-
↪guard?ver=13.0.0"
  },
  "createdDatetime": "2017-05-30T15:45:59Z",
  "cookieSettingsReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/cookie-
↪settings?ver=13.0.0"
  },
  "name": "API_ASM_POLICY_CHILD_TEST",
  "caseInsensitive": false,
  "headerSettingsReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/header-
↪settings?ver=13.0.0"
  },
  "sectionReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/
↪sections?ver=13.0.0",
    "isSubCollection": true
  },
  "loginPageReference": {
```

```

    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/login-
↪pages?ver=13.0.0",
    "isSubCollection": true
  },
  "description": "Test ASM policy",
  "fullPath": "/Common/API_ASM_POLICY_CHILD_TEST",
  "policyBuilderParameterReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/policy-
↪builder-parameter?ver=13.0.0"
  },
  "hasParent": true,
  "partition": "Common",
  "parentPolicyReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q?ver=13.
↪0.0"
  }
}

```

3.1. Retrieve ASM child policy

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/asm/policies/{asm_policy_hash}
```

Headers

```
X-F5-Auth-Token: {big_ip_a_auth_token}
```

Example Response

```

{
  "plainTextProfileReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/plain-
↪text-profiles?ver=13.0.0",
    "isSubCollection": true
  },
  "dataGuardReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/data-
↪guard?ver=13.0.0"
  },
  "createdDatetime": "2017-05-30T15:45:59Z",
  "cookieSettingsReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/cookie-
↪settings?ver=13.0.0"
  },
  "versionLastChange": " Security Policy /Common/API_ASM_POLICY_CHILD_TEST [add]:
↪Parent Policy was set to /Common/API_ASM_POLICY_TEST.\nType was set to Security.
↪\nEncoding Selected was set to true.\nApplication Language was set to utf-8.\nCase
↪Sensitivity was set to Case Sensitive.\nSecurity Policy Description was set to
↪Fundamental Policy.\nLearning Mode was set to Automatic.\nActive was set to false.
↪\nDifferentiate between HTTP and HTTPS URLs was set to Protocol Specific.\nPolicy
↪Name was set to /Common/API_ASM_POLICY_CHILD_TEST.\nEnforcement Mode was set to
↪Blocking. { audit: policy = /Common/API_ASM_POLICY_CHILD_TEST, username = admin,
↪client IP = 192.168.2.112 }",
  "name": "API_ASM_POLICY_CHILD_TEST",
  "caseInsensitive": false,

```



```

    "headerSettingsReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/header-
↪ settings?ver=13.0.0"
    },
    "sectionReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/
↪ sections?ver=13.0.0",
      "isSubCollection": true
    },
    "loginPageReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/login-
↪ pages?ver=13.0.0",
      "isSubCollection": true
    },
    "description": "Test ASM policy",
    "fullPath": "/Common/API_ASM_POLICY_CHILD_TEST",
    "policyBuilderParameterReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/policy-
↪ builder-parameter?ver=13.0.0"
    },
    "hasParent": true,
    "partition": "Common",
    "parentPolicyReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q?ver=13.
↪ 0.0"
    },
    "webScrapingReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/web-
↪ scraping?ver=13.0.0"
    },
    "csrfProtectionReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/csrf-
↪ protection?ver=13.0.0"
    },
    "policyAntivirusReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/
↪ antivirus?ver=13.0.0"
    },
    "kind": "tm:asm:policies:polycystate",
    "virtualServers": [],
    "policyBuilderCookieReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/policy-
↪ builder-cookie?ver=13.0.0"
    }
  }
}

```

4.4.4 Lab 3.4: Apply ASM Policy to VS

Overview

In this lab, the previously created ASM policy will be applied to a virtual server using the iControl REST API.

Specific Instructions

Follow the below steps in order found in the Postman collection to complete this portion of the lab. The requests and responses have been included below for reference.

Attention: Some response content has been removed for brevity.

1. Apply ASM Policy to VS

An HTTP PATCH to the `/mgmt/tm/asm/policies/{{asm_policy_hash}}` endpoint with a body containing the name of a virtual server(s), in this case `"virtualServers":["/Common/hackazon_vs"]`, will apply the ASM policy.

Request

```
PATCH https://{{big_ip_a_mgmt}}/mgmt/tm/asm/policies/{{asm_policy_hash}}
```

Headers

```
Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Body

```
{
  "virtualServers":["/Common/hackazon_vs"]
}
```

Example Response

```
{
  "plainTextProfileReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/plain-
    ↪text-profiles?ver=13.0.0",
    "isSubCollection": true
  },
  "dataGuardReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/data-
    ↪guard?ver=13.0.0"
  },
  "createdDatetime": "2017-05-30T15:45:59Z",
  "cookieSettingsReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/cookie-
    ↪settings?ver=13.0.0"
  },
  "versionLastChange": " Security Policy /Common/API_ASM_POLICY_CHILD_TEST [add]:
  ↪Parent Policy was set to /Common/API_ASM_POLICY_TEST.\nType was set to Security.
  ↪\nEncoding Selected was set to true.\nApplication Language was set to utf-8.\nCase
  ↪Sensitivity was set to Case Sensitive.\nSecurity Policy Description was set to
  ↪Fundamental Policy.\nLearning Mode was set to Automatic.\nActive was set to false.
  ↪\nDifferentiate between HTTP and HTTPS URLs was set to Protocol Specific.\nPolicy
  ↪Name was set to /Common/API_ASM_POLICY_CHILD_TEST.\nEnforcement Mode was set to
  ↪Blocking. { audit: policy = /Common/API_ASM_POLICY_CHILD_TEST, username = admin,
  ↪client IP = 192.168.2.112 }",
  "name": "API_ASM_POLICY_CHILD_TEST",
```

```

    "caseInsensitive": false,
    "headerSettingsReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/header-
↪ settings?ver=13.0.0"
    },
    "sectionReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/
↪ sections?ver=13.0.0",
      "isSubCollection": true
    },
    "loginPageReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/login-
↪ pages?ver=13.0.0",
      "isSubCollection": true
    },
    "description": "Test ASM policy",
    "fullPath": "/Common/API_ASM_POLICY_CHILD_TEST",
    "policyBuilderParameterReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/policy-
↪ builder-parameter?ver=13.0.0"
    },
    "hasParent": true,
    "partition": "Common",
    "parentPolicyReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q?ver=13.
↪ 0.0"
    },
  },
}

```

2. Retrieve ASM policy

Request

```
GET https://{big_ip_a_mgmt}/mgmt/tm/asm/policies/{asm_policy_hash}
```

Headers

```
X-F5-Auth-Token: {big_ip_a_auth_token}
```

Example Response

```

{
  "plainTextProfileReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/plain-
↪ text-profiles?ver=13.0.0",
    "isSubCollection": true
  },
  "dataGuardReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/data-
↪ guard?ver=13.0.0"
  },
  "createdDatetime": "2017-05-30T15:45:59Z",
  "cookieSettingsReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/cookie-
↪ settings?ver=13.0.0"
  },
}

```

```

    "versionLastChange": "Policy Building Settings Policy Building Settings [update]:
↪Internal Statistics have been updated { audit: policy = /Common/API_ASM_POLICY_
↪CHILD_TEST, component = Policy Builder }",
    "name": "API_ASM_POLICY_CHILD_TEST",
    "caseInsensitive": false,
    "headerSettingsReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/header-
↪settings?ver=13.0.0"
    }
}

```

3. Remove ASM Policy from VS

An HTTP PATCH to the `/mgmt/tm/asm/policies/{{asm_policy_hash}}` endpoint with a body removing the name of a virtual server(s), in this case `"virtualServers": [""]`, will remove the ASM policy from the absent virtual serves.

Request

```
PATCH https://{{big_ip_a_mgmt}}/mgmt/tm/asm/policies/{{asm_policy_hash}}
```

Headers

```

Content-Type: application/json
X-F5-Auth-Token: {{big_ip_a_auth_token}}

```

Body

```

{
    "virtualServers":[""]
}

```

Example Response

```

{
    "plainTextProfileReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/plain-
↪text-profiles?ver=13.0.0",
        "isSubCollection": true
    },
    "dataGuardReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/data-
↪guard?ver=13.0.0"
    },
    "createdDatetime": "2017-05-30T15:45:59Z",
    "cookieSettingsReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/cookie-
↪settings?ver=13.0.0"
    },
    "versionLastChange": "Policy Building Settings Policy Building Settings [update]:
↪Internal Statistics have been updated { audit: policy = /Common/API_ASM_POLICY_
↪CHILD_TEST, component = Policy Builder }",
    "name": "API_ASM_POLICY_CHILD_TEST",
    "caseInsensitive": false,
    "headerSettingsReference": {
        "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/header-
↪settings?ver=13.0.0"
    }
}

```

```

    },
    "sectionReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/
↪sections?ver=13.0.0",
      "isSubCollection": true
    },
    "loginPageReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/login-
↪pages?ver=13.0.0",
      "isSubCollection": true
    },
    "description": "Test ASM policy",
    "fullPath": "/Common/API_ASM_POLICY_CHILD_TEST",
    "policyBuilderParameterReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/policy-
↪builder-parameter?ver=13.0.0"
    },
    "hasParent": true,
    "partition": "Common",
    "parentPolicyReference": {
      "link": "https://localhost/mgmt/tm/asm/policies/JEQPVWeJcdso_rEC7Xxo6Q?ver=13.
↪0.0"
    }
  }
}

```

4. Delete ASM policy

An HTTP DELETE to the `/mgmt/tm/asm/policies/{{asm_policy_hash}}` endpoint will delete the ASM policy from the BIG-IP.

Request

```
DELETE https://{{big_ip_a_mgmt}}/mgmt/tm/asm/policies/{{asm_policy_hash}}
```

Headers

```
X-F5-Auth-Token: {{big_ip_a_auth_token}}
```

Example Response

```

{
  "plainTextProfileReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/plain-
↪text-profiles?ver=13.0.0",
    "isSubCollection": true
  },
  "dataGuardReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/data-
↪guard?ver=13.0.0"
  },
  "createdDatetime": "2017-05-30T15:45:59Z",
  "cookieSettingsReference": {
    "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/cookie-
↪settings?ver=13.0.0"
  },
  "versionLastChange": "Policy Building Settings Policy Building Settings [update]:_
↪Internal Statistics have been updated { audit: policy = /Common/API_ASM_POLICY_
↪CHILD_TEST, component = Policy Builder }",

```

```
"name": "API_ASM_POLICY_CHILD_TEST",
"caseInsensitive": false,
"headerSettingsReference": {
  "link": "https://localhost/mgmt/tm/asm/policies/zD8sehZULw6Ni7GJG2XwJQ/header-
↪ settings?ver=13.0.0"
}
```

This section contains useful HOWTOs

5.1 HOWTO - Update Existing iApp templates to Work with iWorkflow v2.1

This HOWTO document describes the minimal changes required to update an existing iApp template and add a version number to the template name.

Adding the version number allows the iApp template to be used by iWorkflow v2.1 and later. Versioning is required to enable iApp templates to be installed across many BIG-IP devices in a production-safe manner.

Without version information it is possible that iApp templates could be overwritten leading to deployment failures and/or outages.

5.1.1 Task 1 - Export the existing iApp from BIG-IP

The iApp template can be exported from a BIG-IP system where it has been installed. The file has a `.tmpl` extension and is a plaintext, readable format.

Complete the following steps:

1. Login to the BIG-IP GUI with admin credentials
2. Click iApps -> Templates
3. Find the desired template in the list and click the template name to open it
4. Scroll to the bottom of the page and click the 'Export' button
5. Click the Download: . . . button and save the file to your computer

5.1.2 Task 2 - Edit the Exported template

We will now edit the template name to add a version number. iWorkflow currently supports the following formats:

- `template_name_v1.0_0`

- `template_name.v.1.0.0`
- `/<partition>/template_name.v1.0.0`

Complete the following steps:

1. Open the previously saved `.tmpl` file in a text editor
2. Perform a text search for `sys application template`

Example:

```

1 cli admin-partitions {
2     update-partition Common
3 }
4
5 sys application template my_template_name {
6     actions {
7         definition {
8             implementation {

```

3. Modify the template name to include a version number using one of the formats specified at the beginning of this task.

Example:

```

1 cli admin-partitions {
2     update-partition Common
3 }
4
5 sys application template my_template_name.v1.0.0 {
6     actions {
7         definition {
8             implementation {

```

4. Save the file

5.1.3 Task 3 - Import the iApp template to iWorkflow

The updated iApp template is now ready to be imported to iWorkflow. Instructions on how to do this can be found at:

https://devcentral.f5.com/wiki/iWorkflow.iWorkflowOpsGuide_7.ashx

WE MAKE APPS  FASTER.
SMARTER.
SAFER.

F5 Networks, Inc. | f5.com



US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com
©2017 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. These training materials and documentation are F5 Confidential Information and are subject to the F5 Networks Reseller Agreement. You may not share these training materials and documentation with any third party without the express written permission of F5.