Programmability with SD-WAN

DEVWKS-1671

Jairo Leon

Marcelo Garcia

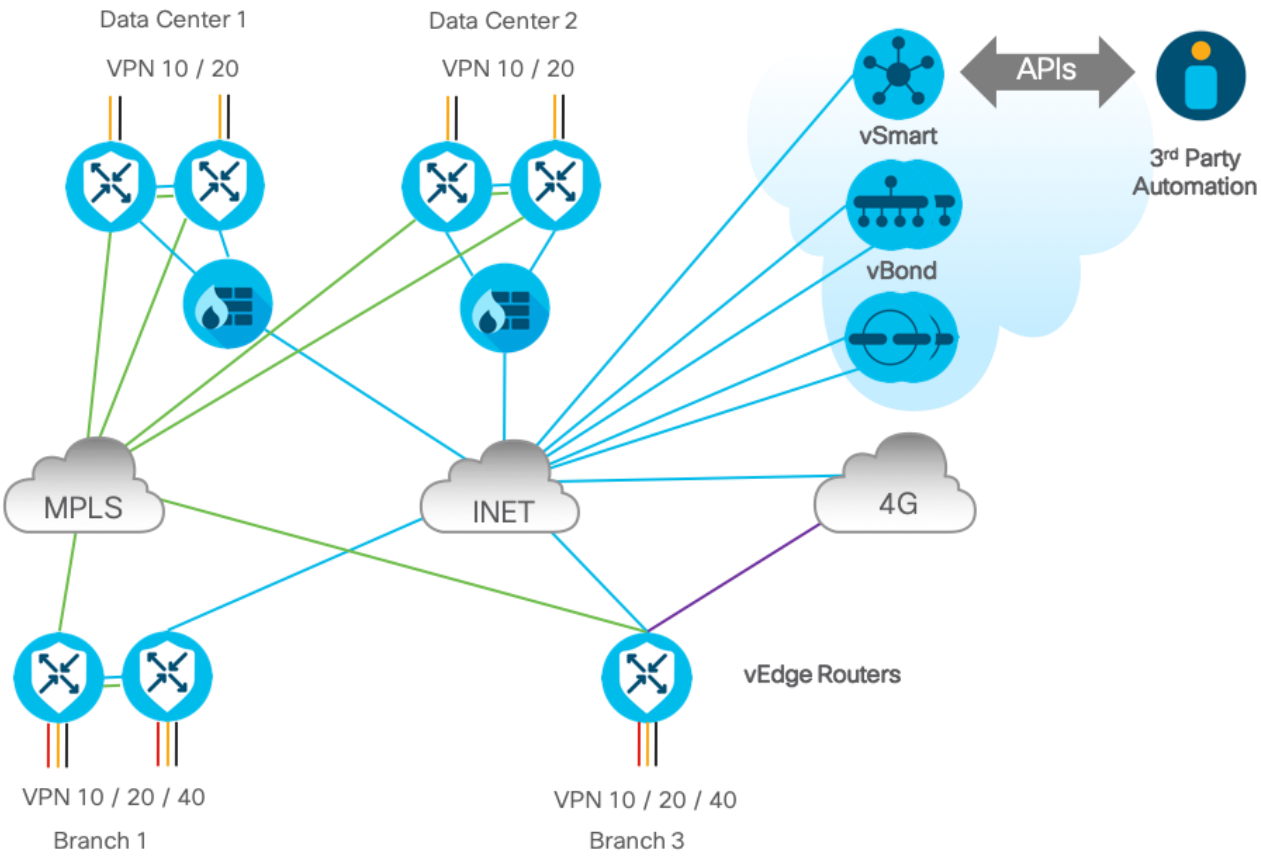
Table of Contents

Learning Objectives

In this lab activity, you will learn how to interact with the Cisco SD WAN solutions through the use of vMANAGE REST APIs.
vMANAGE API Docs Tool, Postman and Python scripts will be used as different tools to access these APIs.
This document provides a step-by-step guide for two labs:

1- Use Case 1: Using vMANAGE Rest APIs, reconfigure a template associated to a particular device, re-apply it and verify the changes.
2- Use Case 2: Using vMANAGE Rest APIs, configure a brand-new policy in order to switch traffic between DC and a particular branch from Internet to MPLS VPN.

Network Diagram



IP Address Plan

Note: This is just for your reference (if you are using traceroute these tables will be helpful). Since we will only use DC vEDGE routers and Branch-3 cEDGE Router all other routers in the topology are excluded from these tables.
Static routing, BGP and other protocols are configured and out of the scope of this lab and document.

Management IP Address Table

HOSTNAME	Management IP ADDRESS
DC1-VEDGE1	198.18.134.100
DC1-VEDGE2	198.18.134.101
DC2-VEDGE1	198.18.134.102
DC2-VEDGE2	198.18.134.103
BR1-CEDGE1	198.18.134.104
BR2-CEDGE2	198.18.134.105
BR3-CEDGE1	198.18.134.107

Hosts available in each site (per VPN) Table

SITE	Host IP in VPN 10	Host IP in VPN 20	Host IP in VPN 40
DC1	10.1.10.10	10.1.20.10	--
DC2	10.2.10.10	10.2.20.10	--
BR1	10.3.0.10	10.3.20.10	10.3.40.10
BR3	10.5.0.10	10.5.20.10	10.5.40.10

DC1-Edge1 IP Address

NEIGHBOR DEVICE	WAN IP ADDRESS
Ge 0/1 - VPN 0 (to MPLS-PE)	100.64.0.2/30
Ge 0/2 - VPN 0 (to INET-PE)	100.64.2.26/30
Ge 0/0 - VPN 10 (to FW)	10.1.100.2/30
Ge 0/3 - VPN 20 (to FW)	10.1.200.2/30

DC1-Edge2 IP Address

NEIGHBOR DEVICE	WAN IP ADDRESS
Ge 0/1 - VPN 0 (to MPLS-PE)	100.64.0.6/30
Ge 0/2 - VPN 0 (to INET-PE)	100.64.2.30/30
Ge 0/0 - VPN 10 (to FW)	10.1.101.2/30
Ge 0/3 - VPN 20 (to FW)	10.1.201.2/30

Branch 3 IP Address

NEIGHBOR DEVICE	WAN IP ADDRESS
GigabitEthernet 2 (to MPLS-PE)	100.64.0.22/30
GigabitEthernet 3 (to INET-PE)	100.64.2.10/30
GigabitEthernet 4 (VPN 10)	10.5.0.1/24
GigabitEthernet 5 (to LTE -PE)	100.64.4.10/30
GigabitEthernet 6 (VPN 20)	10.5.20.1/24
GigabitEthernet 7 (VPN 40)	10.5.40.1/24

MPLS PE ROUTER (Emulating MPLS Network) Table

NEIGHBOR DEVICE	WAN IP ADDRESS
GigabitEthernet 1 (to DC1-VEDGE1)	100.64.0.1/30
GigabitEthernet 2 (to DC1-VEDGE2)	100.64.0.5/30
GigabitEthernet 3 (to DC2-VEDGE1)	100.64.0.9/30
GigabitEthernet 4 (to DC2-VEDGE1)	100.64.0.13/30
GigabitEthernet 5 (to BR1-VEDGE1)	100.64.0.17/30
GigabitEthernet 6 (INET EDGE)	198.18.1.2/24
GigabitEthernet 7 (BR3-EDGE1)	100.64.0.21/30
GigabitEthernet 8 (BR2-EDGE1)	100.64.0.25/30

INET PE ROUTER (Emulating Internet Network) Table

NEIGHBOR DEVICE	WAN IP ADDRESS
GigabitEthernet 1 (to BR1)	100.64.2.1/30
GigabitEthernet 2 (to BR2)	100.64.2.5/30
GigabitEthernet 3 (to BR3)	100.64.2.9/30
GigabitEthernet 4 (to DC2 FTD)	100.64.2.13/30
GigabitEthernet 5 (to DC1 FTD)	100.64.2.17/29
GigabitEthernet 6 (to INET EDGE)	198.18.1.3/24

INET ROUTER (Emulating LTE Access – Internet Network) Table

NEIGHBOR DEVICE	WAN IP ADDRESS
GigabitEthernet 7 (to INET EDGE)	198.18.1.5/24
GigabitEthernet 8 (to BR1 CEDGE 2)	100.64.4.1/30
GigabitEthernet 9 (to BR2 CEDGE 1)	100.64.4.5/30
GigabitEthernet 10 (to BR3 CEDGE 1)	100.64.4.9/30

INTERNET ACCESS GATEWAY Table

NEIGHBOR DEVICE	WAN IP ADDRESS
GigabitEthernet 1 (to INET-PE / LTE-PE)	198.18.1.254/24
GigabitEthernet 2 (to INTERNET)	198.18.2.254/24

Use Case 1 / LAB1 – Change system configuration with vMANAGE APIs and feature templates

This first lab is just to show how you can use vMANAGE REST APIs to change a particular system configuration. In this case we will change the banner login and banner motd for branch 3 vedge router. Since in our environment we have a template assigned to the device, we will change this template and reapply it.
Summary steps are:

1. vMANAGE authentication.
2. Get the template ID assigned to the device (BR3 IP ADDRESS = 10.5.0.1) and verify the banner template assigned to it.
3. Configure a new banner template.
4. Associate the brand-new banner template with the device template.
5. Re-apply the device template to branch 3 vEDGE.
6. Log in to branch 3 vEDGE device (SSH) and verify the banner login and banner MOTD.

In this lab we are going to use post-man app. In each step you will see a post-man screenshot related to the task as an additional tool for guidance.
We have created a postman collection, please feel free to download and use it.

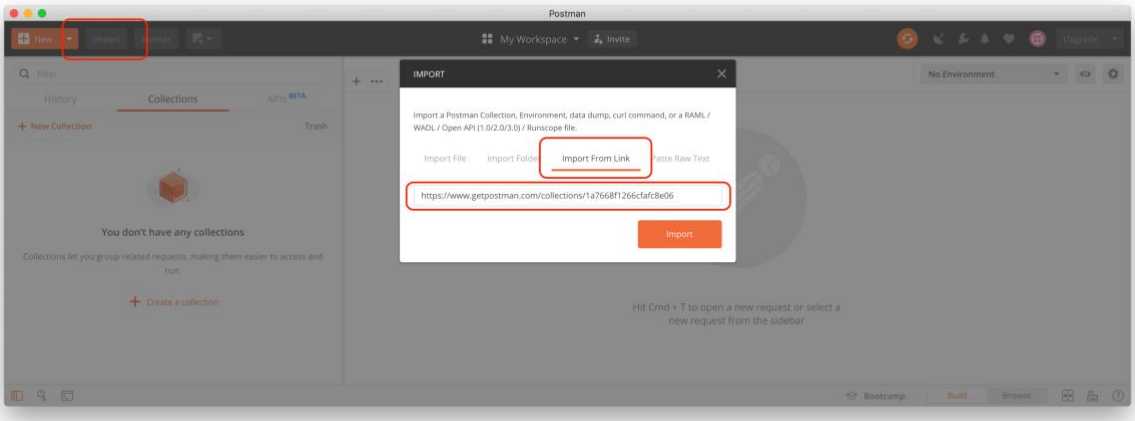
Postman collection link:

https://www.getpostman.com/collections/a15b3e29d99f54a56d86

Quick postman review:

If you are not familiar with Postman here is a brief review on how you can import a collection:

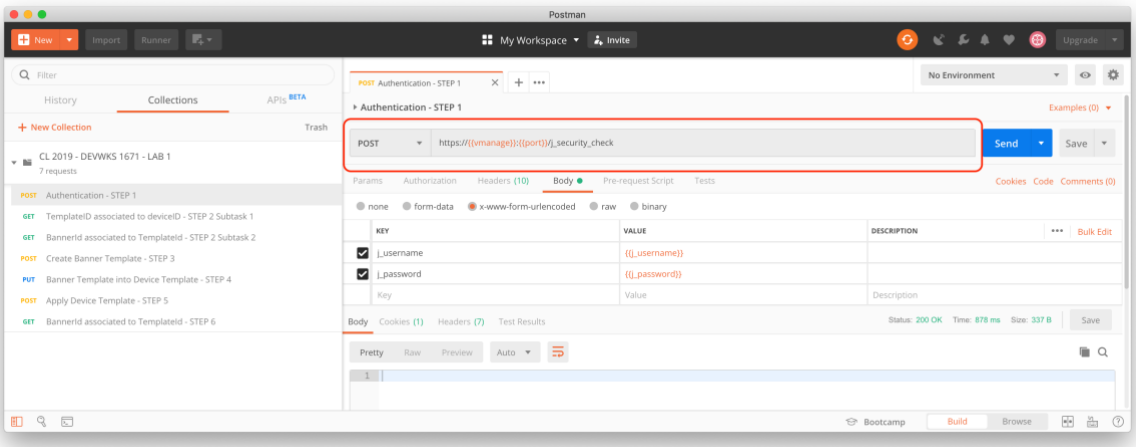
1- Go to “File”, then “Import”.
2- Click on “Import From Link”, then paste the link: https://www.getpostman.com/collections/a15b3e29d99f54a56d86



Step 1: Authentication

- Login to vMANAGE using post-man application.
    - POST: https://198.18.1.10:443/j_security_check

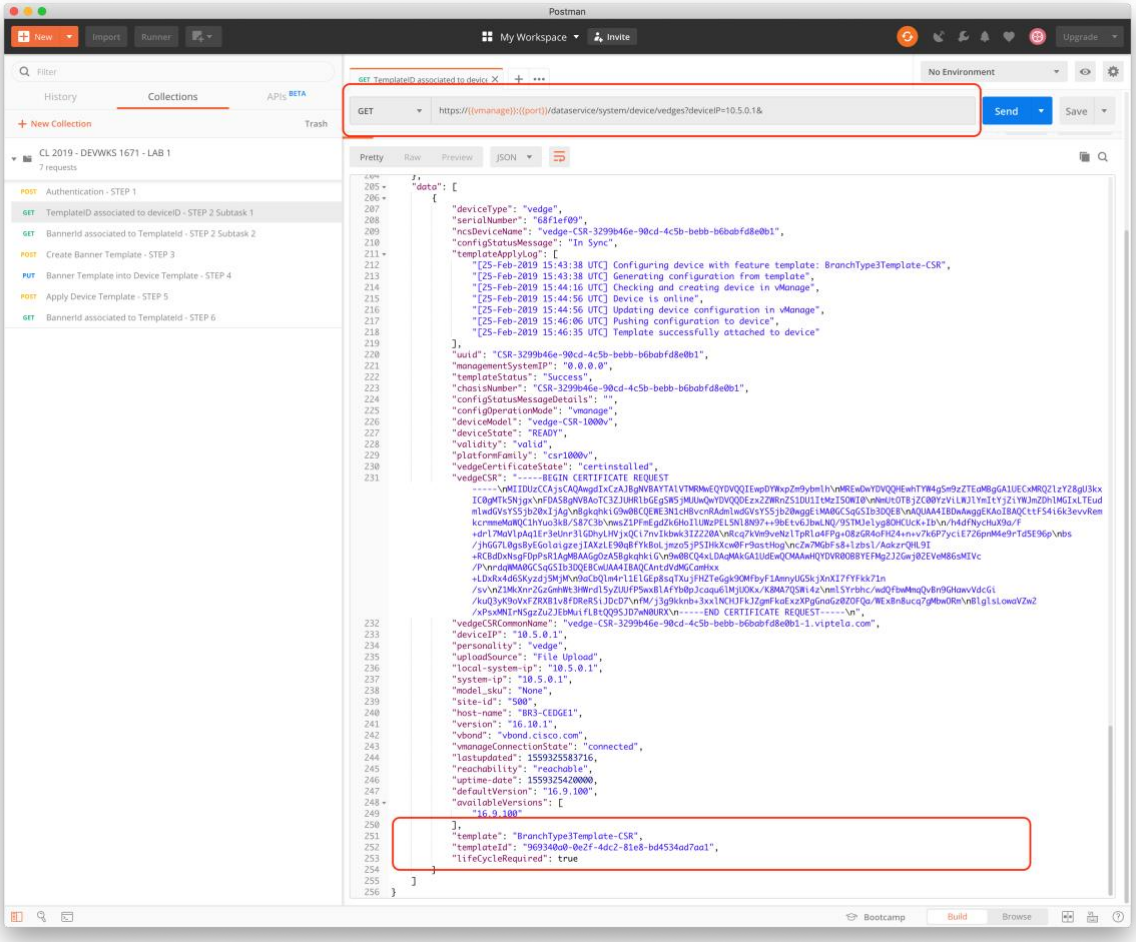
Variable	Initial Value	Current Value
vmanage	198.18.1.10	198.18.1.10
j_username	admin	admin
j_password	admin	admin
Port	443	443



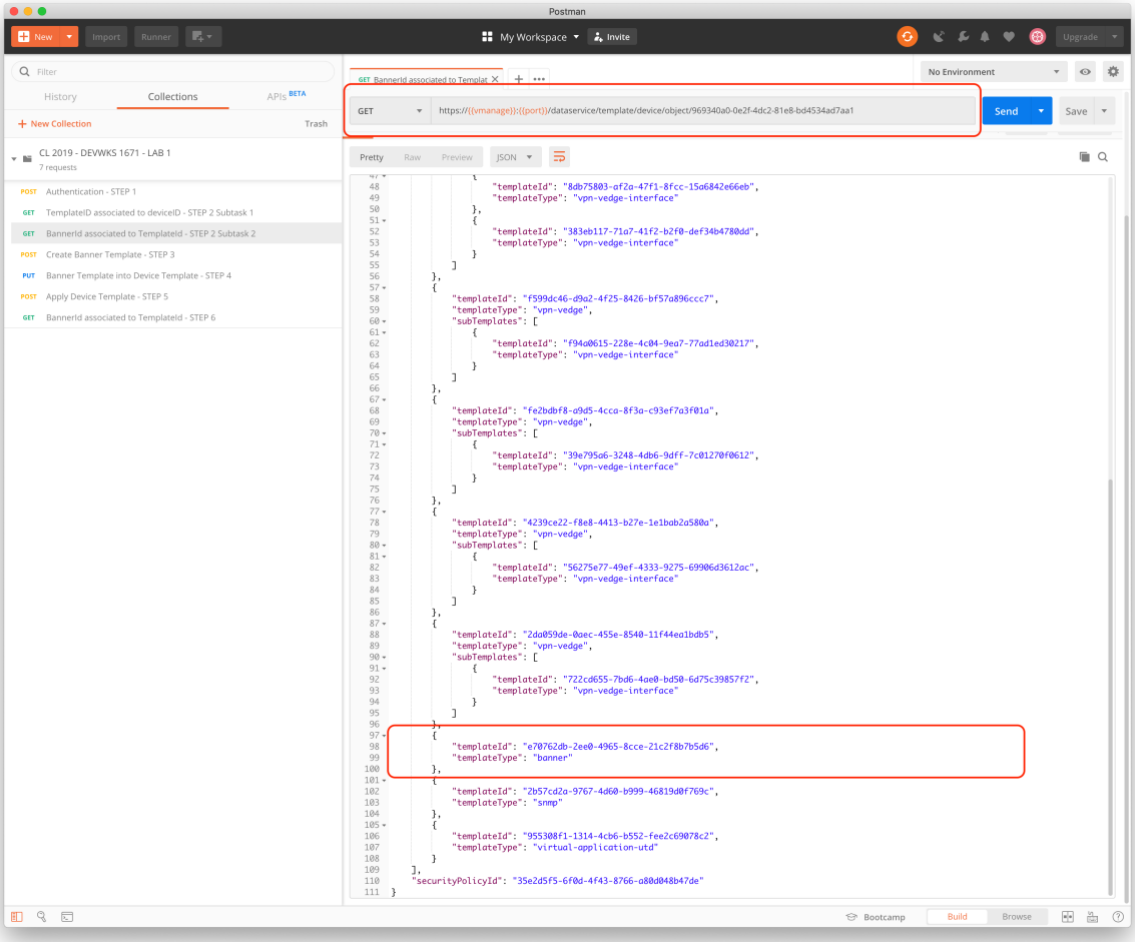
Step 2: Get the templateID associated to a deviceID

In our lab we are going to work with Branch 3 vEDGE. In this case we must have the template ID associated to the branch 3 vEDGE device ID.

- Subtask 1 – Get template ID associated to BR3 (IP ADDRESS 10.5.0.1)
    - GET https://198.18.1.10:443/dataservice/system/device/vedges?deviceIP=10.5.0.1&



- Subtask 2 – Identify the banner template ID associated with the general template ID of the BR3-vEDGE
    - GET https://198.18.1.10:443/dataservice/template/device/object/969340a0-0e2f-4dc2-81e8-bd4534ad7aa1

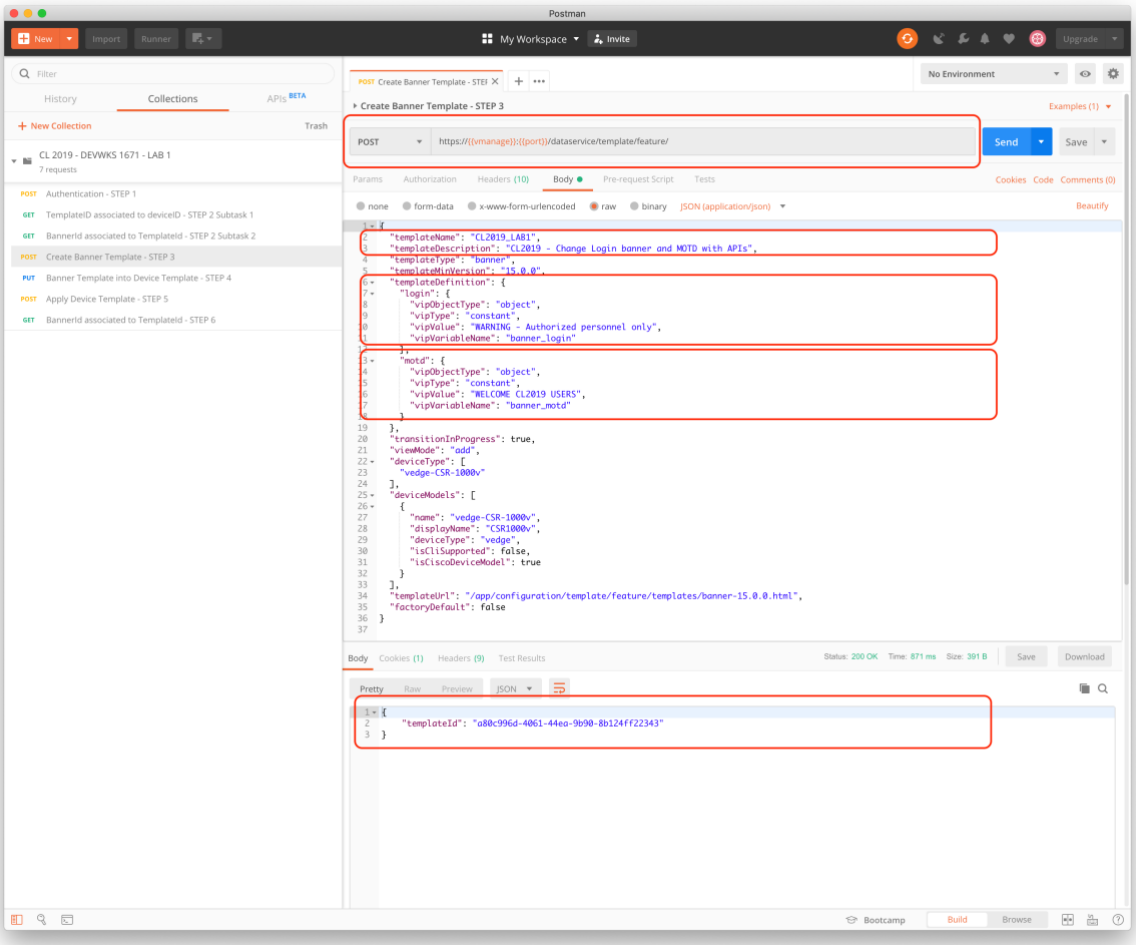


Step 3: Create BANNER template

- Create a new banner template
  - POST https://198.18.1.10/dataservice/template/feature/

```
{
  "templateName": "CL2019_LAB1",
  "templateDescription": "CL2019 - Change Login banner and MOTD with APIs",
  "templateType": "banner",
  "templateMinVersion": "15.0.0",
  "templateDefinition": {
    "login": {
      "vipObjectType": "object",
      "vipType": "constant",
      "vipValue": "WARNING - Authorized personnel only",
      "vipVariableName": "banner_login"
    },
    "motd": {
      "vipObjectType": "object",
      "vipType": "constant",
      "vipValue": "WELCOME CL2019 USERS",
      "vipVariableName": "banner_motd"
```

```
    }
  },
  "transitionInProgress": true,
  "viewMode": "add",
  "deviceType": [
    "vedge-CSR-1000v"
  ],
  "deviceModels": [
    {
      "name": "vedge-CSR-1000v",
      "displayName": "CSR1000v",
      "deviceType": "vedge",
      "isCliSupported": false,
      "isCiscoDeviceModel": true
    }
  ],
  "templateUrl": "/app/configuration/template/feature/templates/banner-
15.0.0.html",
  "factoryDefault": false
}
```



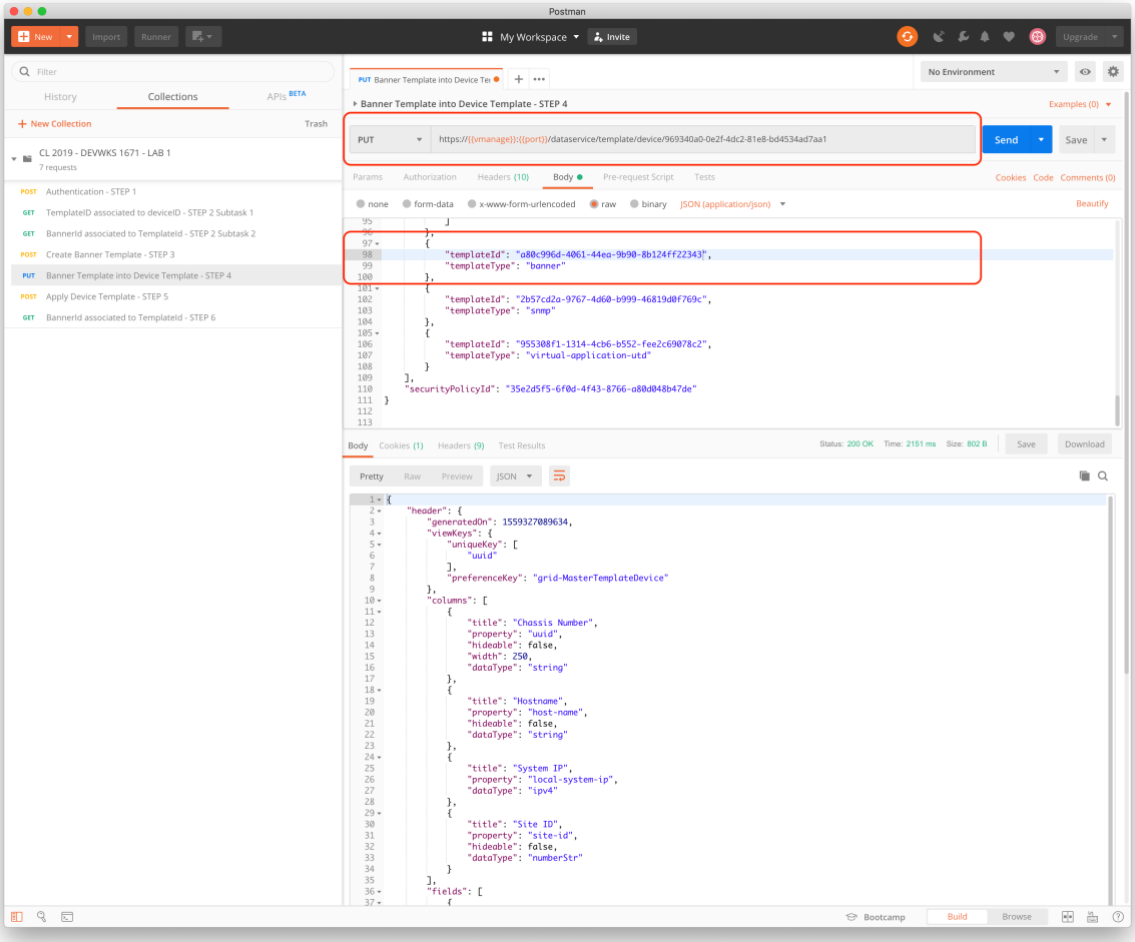
Step 4: Associate the new banner template with the device template

- Subtask 1 – Reference the new banner template in the device template associated with BR3-vEDGE
    - PUT https://198.18.1.10/dataservice/template/device/969340a0-0e2f-4dc2-81e8-bd4534ad7aa1
    - BODY:

```
{
    "templateId": "969340a0-0e2f-4dc2-81e8-bd4534ad7aa1",
    "templateName": "BranchType3Template-CSR",
    "templateDescription": "Branch Type 3 Template for CSR Routers",
    "deviceType": "vedge-CSR-1000v",
    "configType": "template",
    "factoryDefault": false,
    "policyId": "f73b285f-72eb-4f6d-865f-eae0e453bd8e",
    "featureTemplateUidRange": [],
    "connectionPreferenceRequired": true,
    "connectionPreference": true,
    "generalTemplates": [
        {
            "templateId": "3b30e089-2e26-44f1-b5b2-ac44f3f4279e",
            "templateType": "aaa"
        },
        {
            "templateId": "20d77367-06c8-4531-bad7-7e507b0c5829",
            "templateType": "bfd-vedge"
        },
        {
            "templateId": "7adf5770-deff-4472-9355-b4080b4594bd",
            "templateType": "omp-vedge"
        },
        {
            "templateId": "486d419f-4e6c-44a5-a6fb-7b5ccf94ff90",
            "templateType": "security-vedge"
        },
        {
            "templateId": "c70e876a-9ade-4e12-95e2-95fbd4691dbe",
            "templateType": "system-vedge",
            "subTemplates": [
                {
                    "templateId": "edf3d309-91d4-45be-98d9-cfd57a05a479",
                    "templateType": "logging"
                }
            ]
        },
```

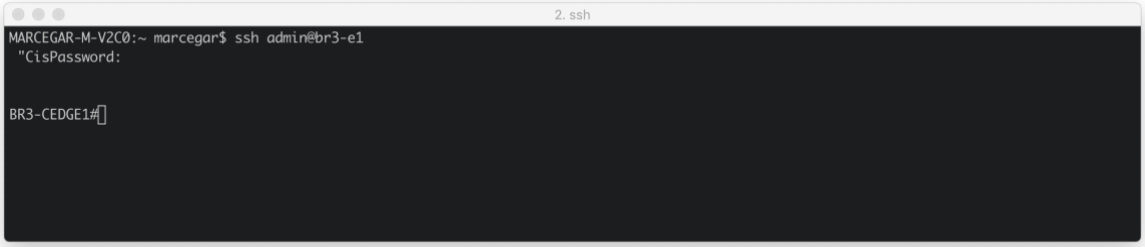
```
        {
            "templateId": "3a01b356-16c7-4115-a6c0-f068f88cd85c",
            "templateType": "vpn-vedge",
            "subTemplates": [
                {
                    "templateId": "cba76e7b-584a-4b70-b625-be1537dc3568",
                    "templateType": "vpn-vedge-interface"
                },
                {
                    "templateId": "8db75803-af2a-47f1-8fcc-15a6842e66eb",
                    "templateType": "vpn-vedge-interface"
                },
                {
                    "templateId": "383eb117-71a7-41f2-b2f0-def34b4780dd",
                    "templateType": "vpn-vedge-interface"
                }
            ]
        },
        {
            "templateId": "f599dc46-d9a2-4f25-8426-bf57a896ccc7",
            "templateType": "vpn-vedge",
            "subTemplates": [
                {
                    "templateId": "f94a0615-228e-4c04-9ea7-77ad1ed30217",
                    "templateType": "vpn-vedge-interface"
                }
            ]
        },
        {
            "templateId": "fe2bdbf8-a9d5-4cca-8f3a-c93ef7a3f01a",
            "templateType": "vpn-vedge",
            "subTemplates": [
                {
                    "templateId": "39e795a6-3248-4db6-9dff-7c01270f0612",
                    "templateType": "vpn-vedge-interface"
                }
            ]
        },
        {
            "templateId": "4239ce22-f8e8-4413-b27e-1e1bab2a580a",
            "templateType": "vpn-vedge",
            "subTemplates": [
                {
                    "templateId": "56275e77-49ef-4333-9275-69906d3612ac",
                    "templateType": "vpn-vedge-interface"
```

```
                }
            ]
        },
        {
            "templateId": "2da059de-0aec-455e-8540-11f44ea1bdb5",
            "templateType": "vpn-vedge",
            "subTemplates": [
                {
                    "templateId": "722cd655-7bd6-4ae0-bd50-6d75c39857f2",
                    "templateType": "vpn-vedge-interface"
                }
            ]
        },
        {
            "templateId": "<NEW ID TO BE COMPLETED BY THE USER>",
            "templateType": "banner"
        },
        {
            "templateId": "2b57cd2a-9767-4d60-b999-46819d0f769c",
            "templateType": "snmp"
        },
        {
            "templateId": "955308f1-1314-4cb6-b552-fee2c69078c2",
            "templateType": "virtual-application-utd"
        }
    ],
    "securityPolicyId": "35e2d5f5-6f0d-4f43-8766-a80d048b47de"
}
```



Step 5: Re-apply the template associated with BR3-vEDGE

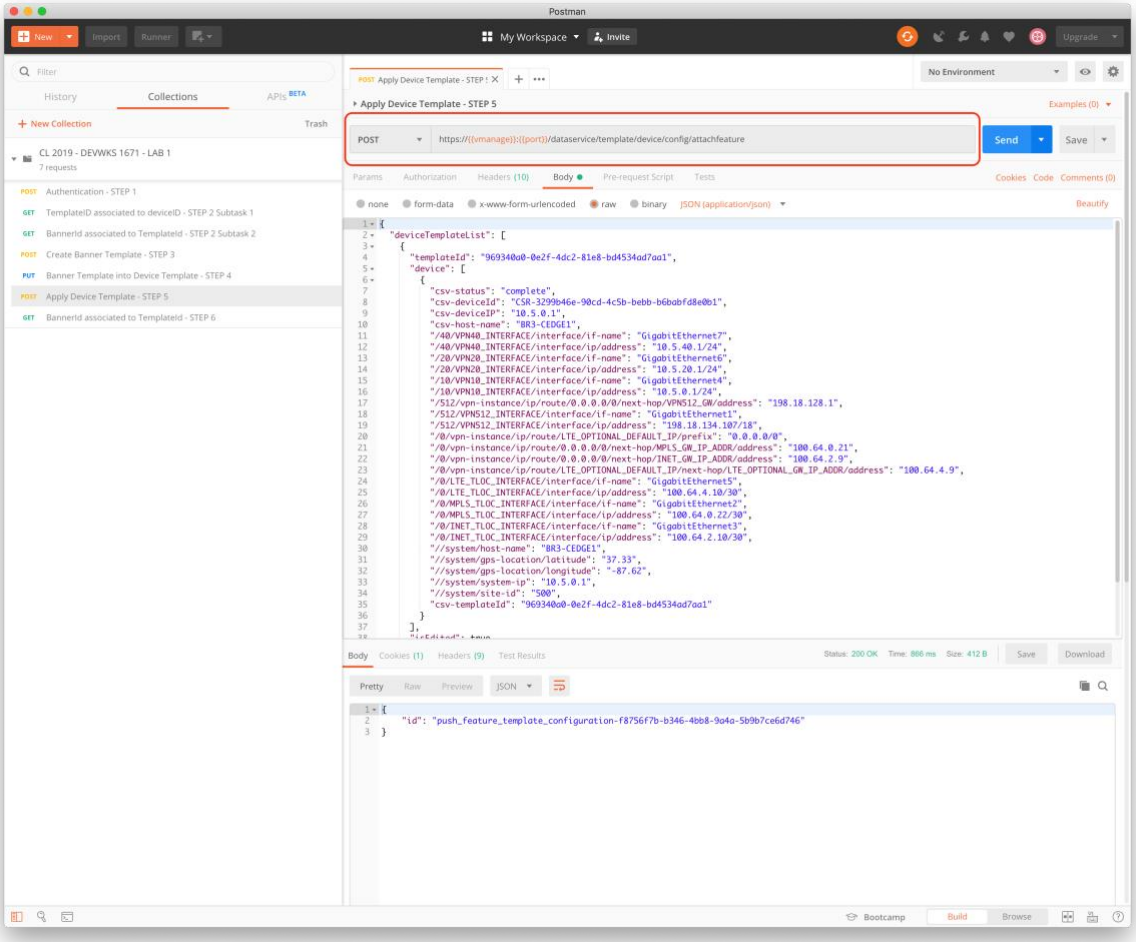
- Subtask 1 – Prior to apply the template, log in to the BR3-vEDGE (198.18.134.107) router and verify what is the login and MOTD banner.



- Subtask 2 – Apply the template.
  - POST https://198.18.1.10/dataservice/template/device/config/attachfeature
  - BODY:

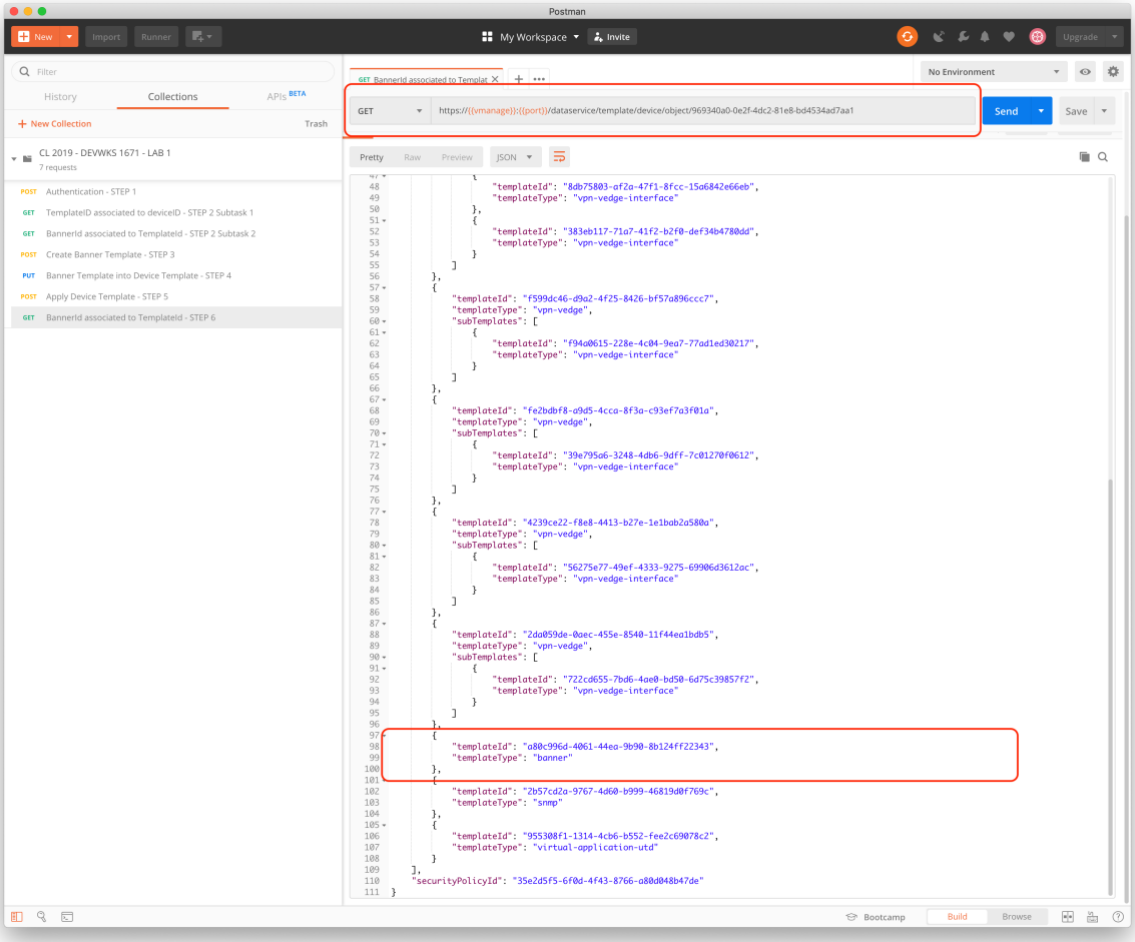
```
{
  "deviceTemplateList": [
    {
      "templateId": "969340a0-0e2f-4dc2-81e8-bd4534ad7aa1",
      "device": [
```

```
        {
          "csv-status": "complete",
          "csv-deviceId": "CSR-3299b46e-90cd-4c5b-bebb-b6babfd8e0b1",
          "csv-deviceIP": "10.5.0.1",
          "csv-host-name": "BR3-CEDGE1",
          "/40/VPN40_INTERFACE/interface/if-name": "GigabitEthernet7",
          "/40/VPN40_INTERFACE/interface/ip/address": "10.5.40.1/24",
          "/20/VPN20_INTERFACE/interface/if-name": "GigabitEthernet6",
          "/20/VPN20_INTERFACE/interface/ip/address": "10.5.20.1/24",
          "/10/VPN10_INTERFACE/interface/if-name": "GigabitEthernet4",
          "/10/VPN10_INTERFACE/interface/ip/address": "10.5.0.1/24",
          "/512/vpn-instance/ip/route/0.0.0.0/0/next-hop/VPN512_GW/address":
"198.18.128.1",
          "/512/VPN512_INTERFACE/interface/if-name": "GigabitEthernet1",
          "/512/VPN512_INTERFACE/interface/ip/address": "198.18.134.107/18",
          "/0/vpn-instance/ip/route/LTE_OPTIONAL_DEFAULT_IP/prefix": "0.0.0.0/0",
          "/0/vpn-instance/ip/route/0.0.0.0/0/next-hop/MPLS_GW_IP_ADDR/address":
"100.64.0.21",
          "/0/vpn-instance/ip/route/0.0.0.0/0/next-hop/INET_GW_IP_ADDR/address":
"100.64.2.9",
          "/0/vpn-instance/ip/route/LTE_OPTIONAL_DEFAULT_IP/next-
hop/LTE_OPTIONAL_GW_IP_ADDR/address": "100.64.4.9",
          "/0/LTE_TLOC_INTERFACE/interface/if-name": "GigabitEthernet5",
          "/0/LTE_TLOC_INTERFACE/interface/ip/address": "100.64.4.10/30",
          "/0/MPLS_TLOC_INTERFACE/interface/if-name": "GigabitEthernet2",
          "/0/MPLS_TLOC_INTERFACE/interface/ip/address": "100.64.0.22/30",
          "/0/INET_TLOC_INTERFACE/interface/if-name": "GigabitEthernet3",
          "/0/INET_TLOC_INTERFACE/interface/ip/address": "100.64.2.10/30",
          "//system/host-name": "BR3-CEDGE1",
          "//system/gps-location/latitude": "37.33",
          "//system/gps-location/longitude": "-87.62",
          "//system/system-ip": "10.5.0.1",
          "//system/site-id": "500",
          "csv-templateId": "969340a0-0e2f-4dc2-81e8-bd4534ad7aa1"
        }
      ],
      "isEdited": true,
      "isMasterEdited": false
    }
  ]
}
```

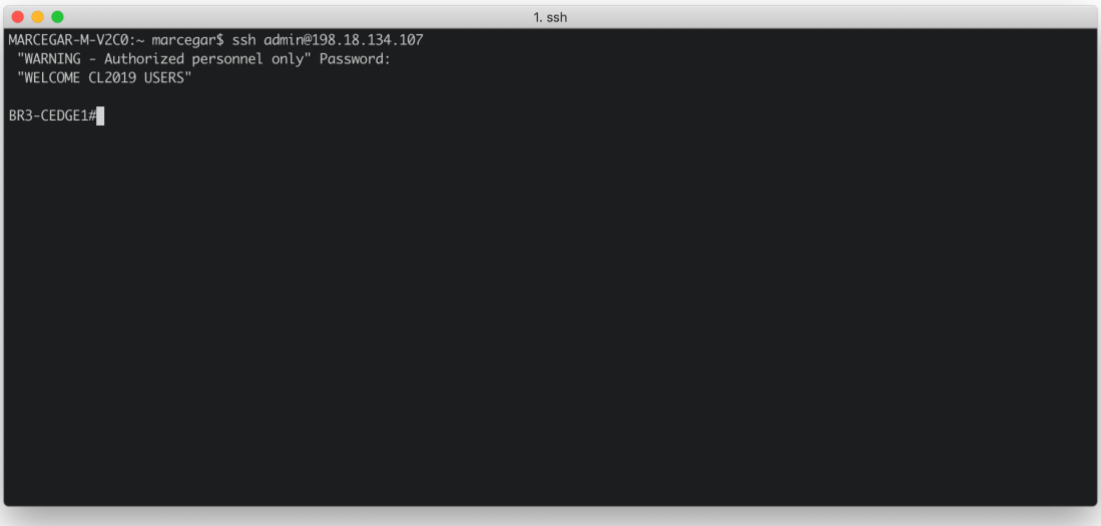


Step 6: Verification

- Subtask 1 – Verify device template (should be configured with the new banner template ID).
  - GET https://198.18.1.10:443/dataservice/template/device/object/969340a0-0e2f-4dc2-81e8-bd4534ad7aa1



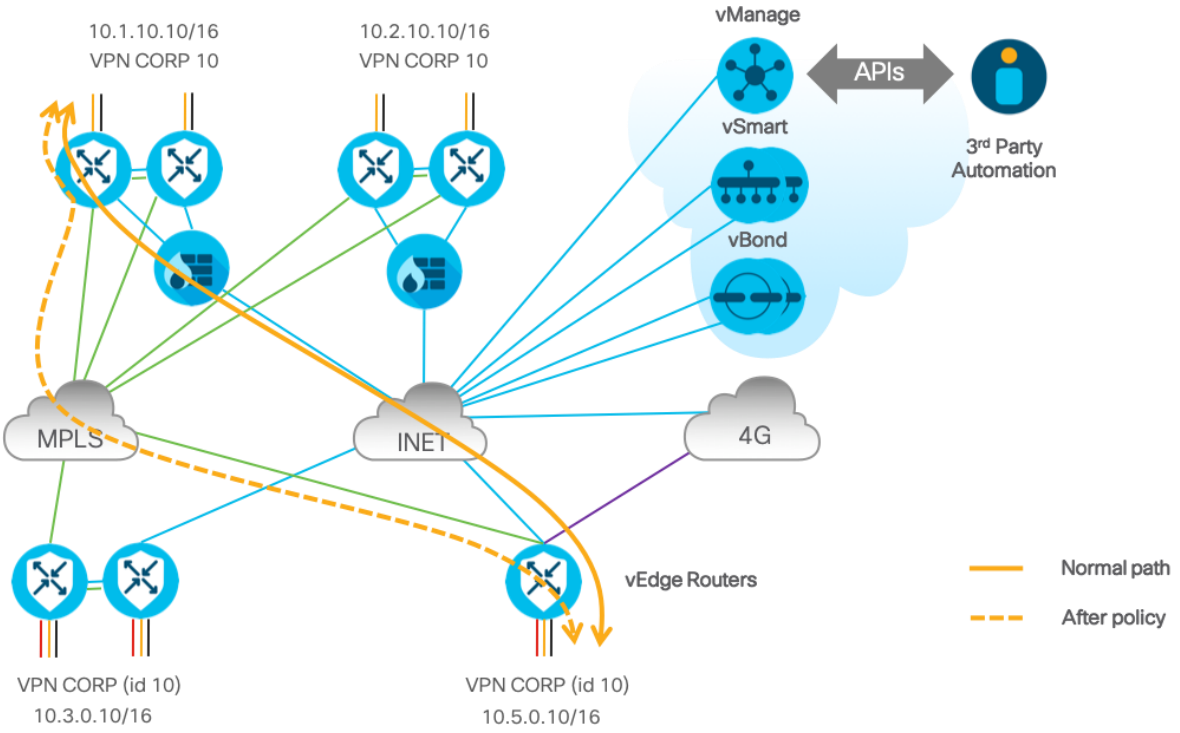
- Subtask 2 – Login to BR3-vEDGE (198.18.134.107) and verify locally the new banner configuration.



Use Case 2 / LAB 2 - Policies

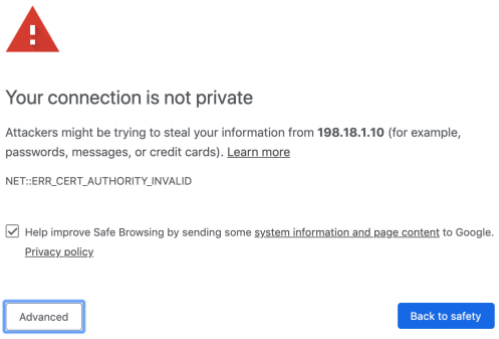
Policy is used to influence the flow of data traffic among the vEdge routers in the overlay network. To implement enterprise-specific traffic control requirements, you create basic policies, and you deploy advanced features of the Cisco SD-WAN (Viptela) software that are activated by means of the policy configuration infrastructure, the policies apply either to control plane or data plane traffic, and they are configured either centrally (on vMANAGE controllers) or locally (on vEdge routers). In our scenario we'll use centralized policy.

The following figure illustrates how influences on the traffic path using policies:



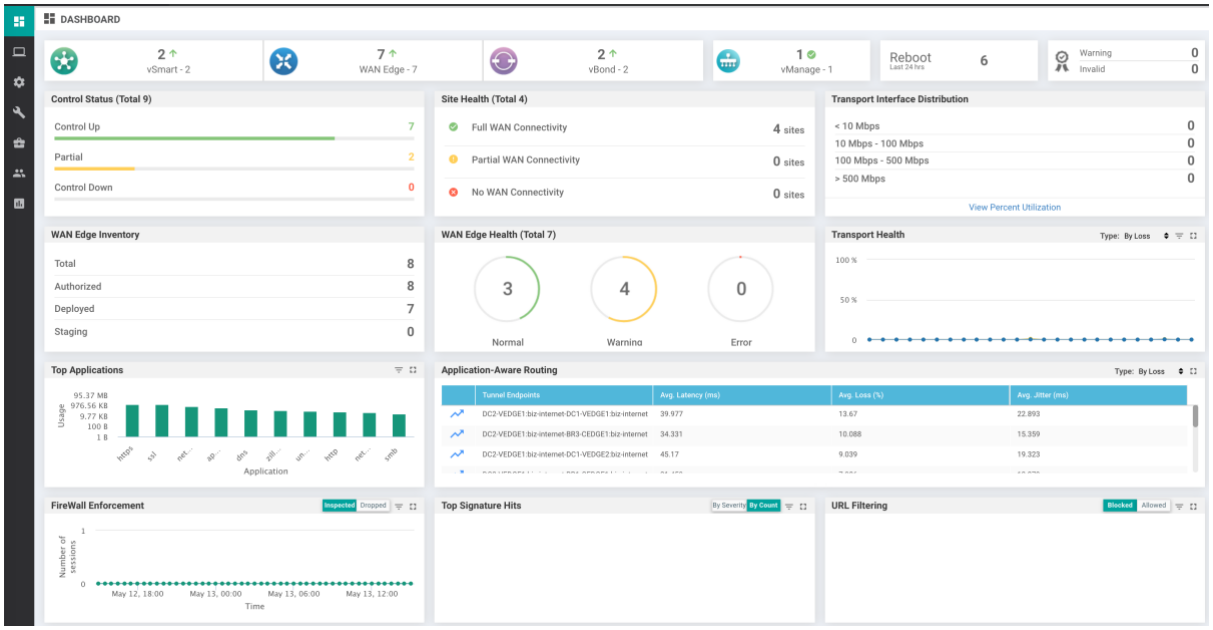
Step 1: Login into vManage and validate the Policies

- Subtask 1: Log into the SD-WAN User Interface
  - Lunch your Chrome web browser and enter the following URL: https://198.18.1.10/. If you see a Certificate Error similar to the following, please accept it.

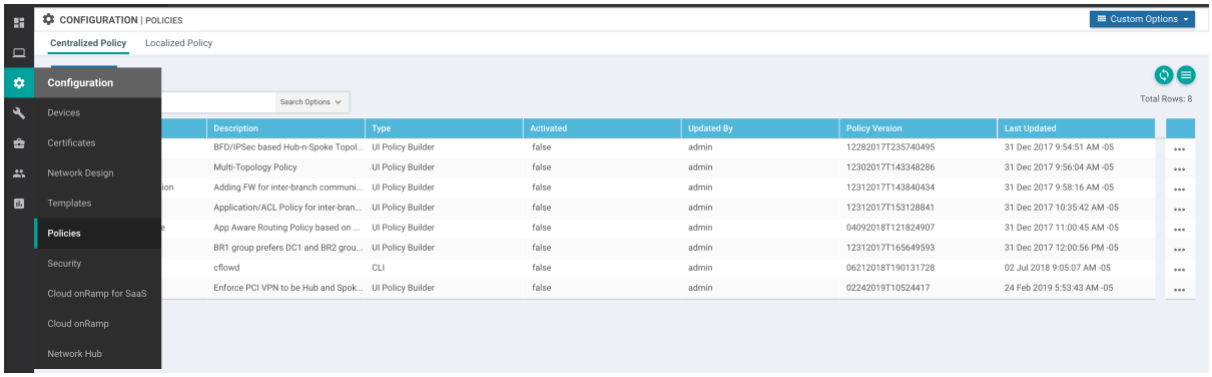


  - You can log into the SD-WAN solution by entering the following:
    - User: **admin**
    - Password: **admin**

- Once you have logged into the SD-WAN UI, you should see the following screen:

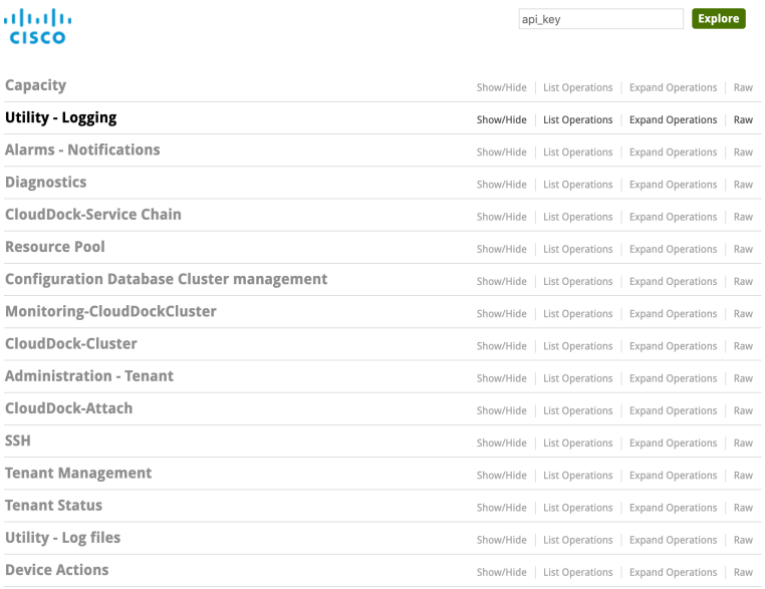


- Subtask 2: Validate Policies Created
  - To validate the policies created, from SD-WAN UI browse to **Configuration > Policies**. You should see all the policies created under Centralized Policy and Localized Policy, keep in mind that we'll work with Centralized policies

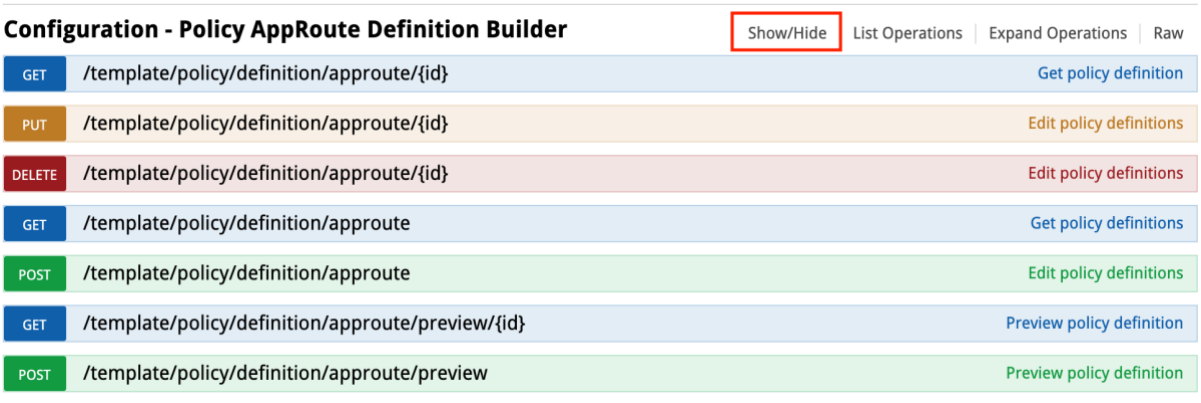


Step 2: Create application aware policy

- Subtask 1: Create new policy using APIs
  - Duplicate your Chrome web browser and add "apidocs/" to the original URL: https://198.18.1.10/apidocs/ .
  - You should be able to see all the API options available to interact with Cisco SD-WAN solution:

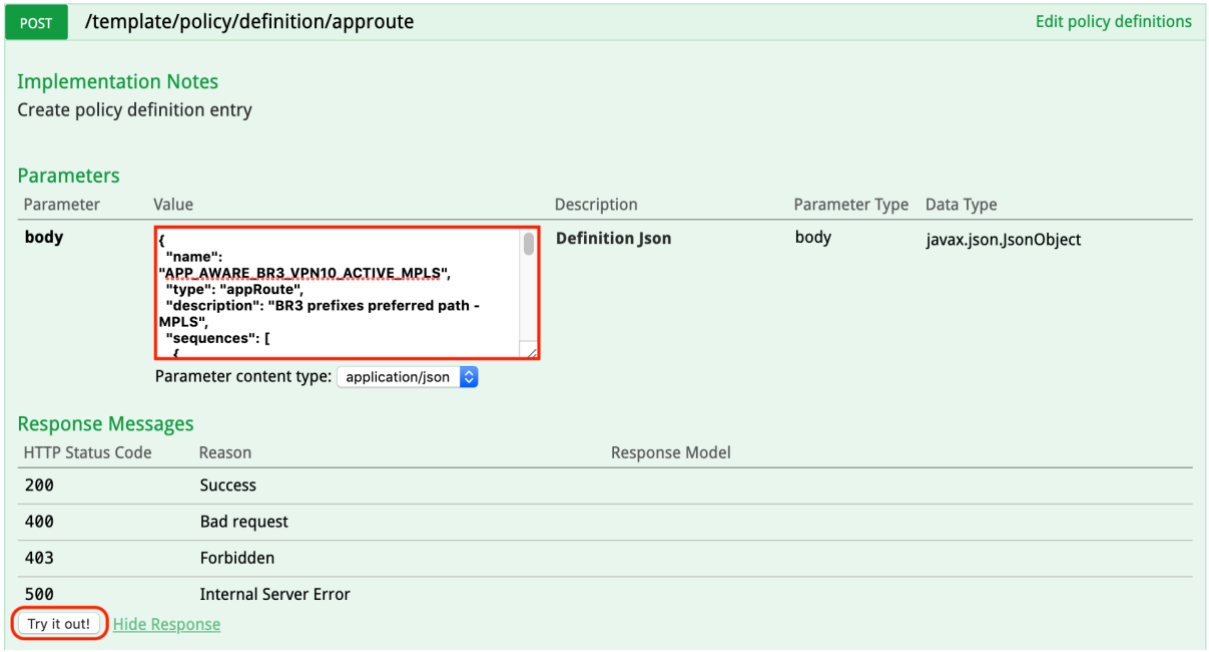


  - Then locate "**Configuration - Policy AppRoute Definition Builder**" and expand it doing click on **Show/Hide** to see all the options.



- Use the POST "**/template/policy/definition/approute**" to create an Application Aware Routing Policy and copy the following configuration as body.

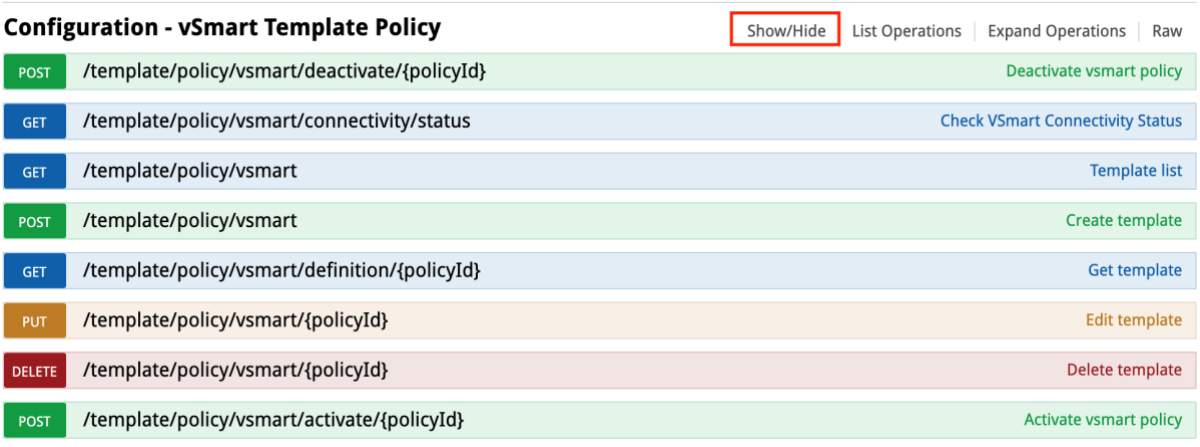
```
{
  "name": "APP_AWARE_BR3_VPN10_ACTIVE_MPLS",
  "type": "appRoute",
  "description": "BR3 prefixes preferred path - MPLS",
  "sequences": [
    {
      "sequenceId": 1,
      "sequenceName": "App Route",
      "sequenceType": "appRoute",
      "sequenceIpType": "ipv4",
      "match": {
        "entries": [
          {
            "field": "destinationDataPrefixList",
            "ref": "81387e80-c3b2-41d7-9804-9a58a375021c"
          }
        ]
      },
      "actions": [
        {
          "type": "backupSlaPreferredColor",
          "parameter": "mpls"
        }
      ]
    }
  ]
}
```



- Then click on "**Try it out**"
  - Under Response Body you will see the definition ID.
  - Copy this value because you will use it on the next step.

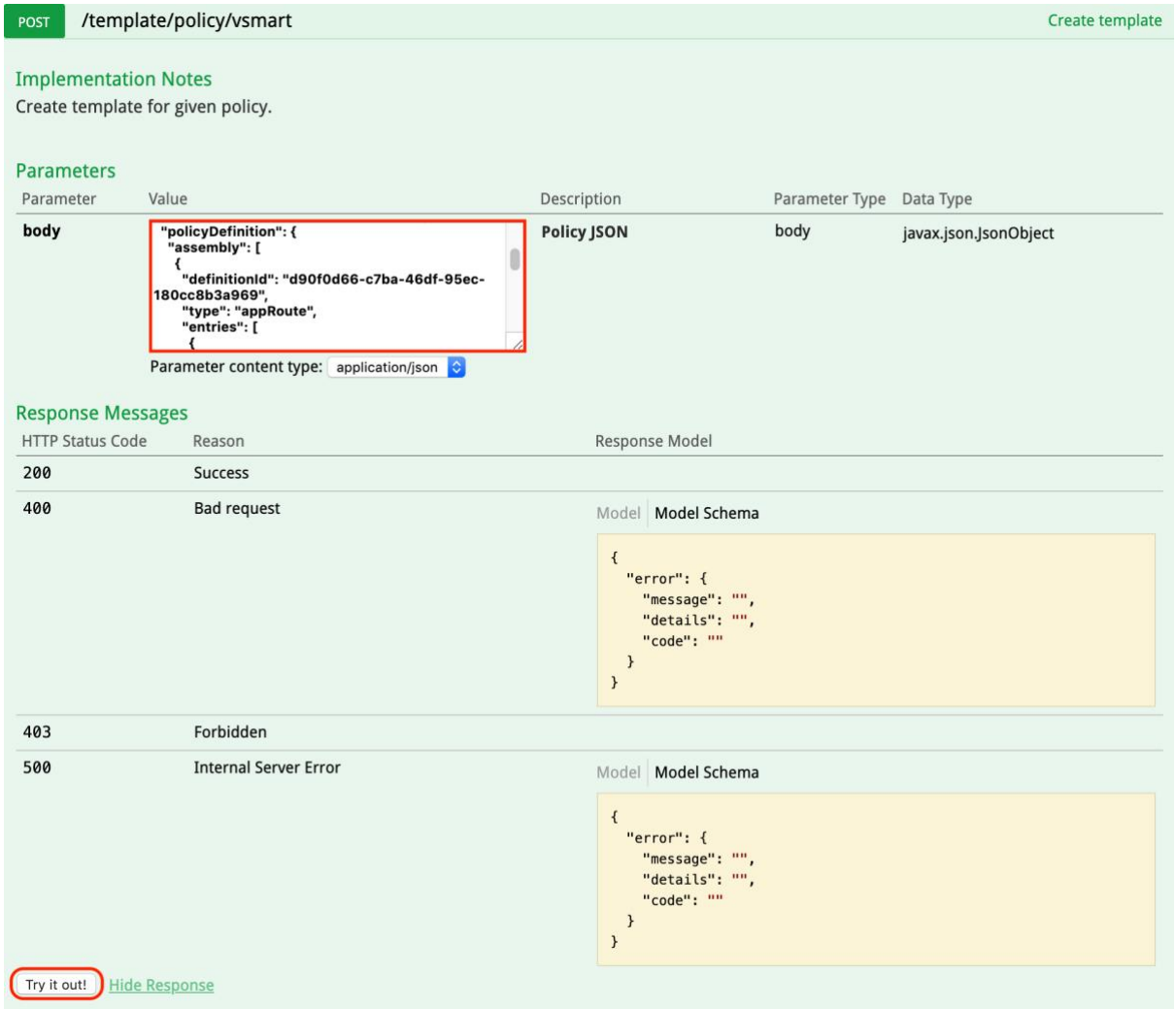
Step 3: Create a template policy using the application aware policy (configured in step 1) and a prefix list

- Subtask 1: Locate "**Configuration - vSmart Template Policy**" and expand it doing click on **Show/Hide** to see all the options.

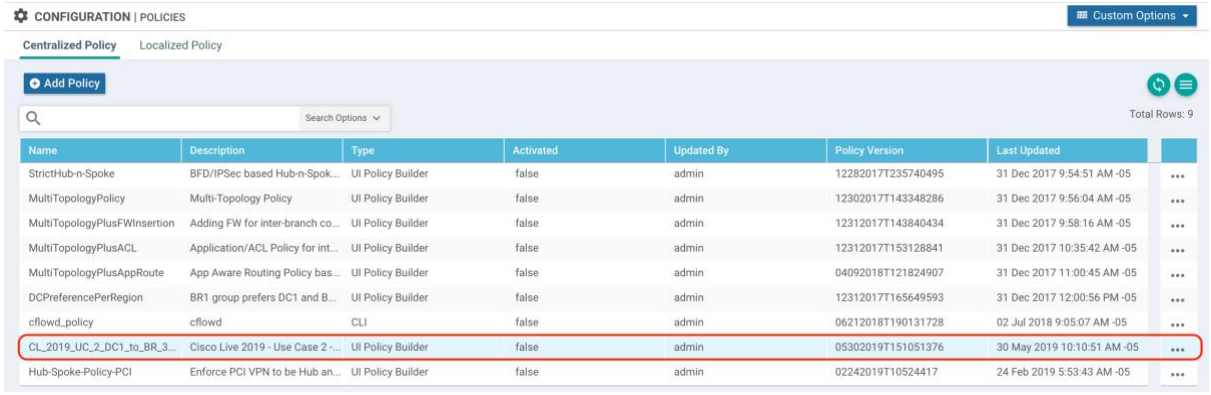


- Choose the POST "**/template/policy/vsmart**" to create a policy using the application aware policy created on step 1.
- Copy the following configuration on the body field and change the "**definitionId**" using the value saved on the previous step.

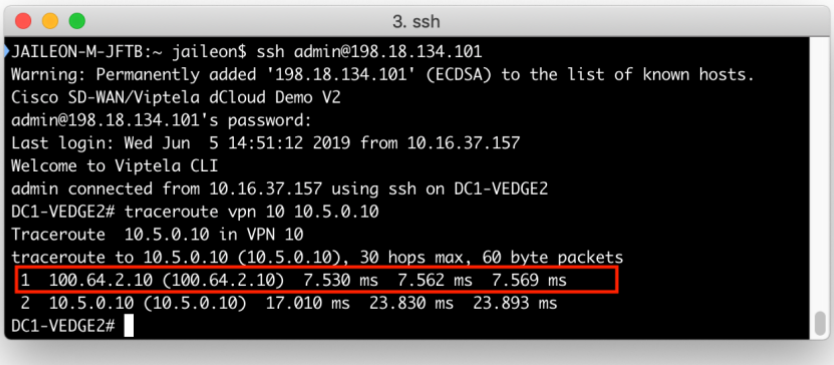
```
{
  "policyDescription": "Cisco Live 2019 - Use Case 2 - Policy applied to branch 3
vpn10 prefixes",
  "policyType": "feature",
  "policyName": "CL_2019_UC_2_DC1_to_BR_3_P_VPN10",
  "policyDefinition": {
    "assembly": [
      {
        "definitionId": "<NEW ID TO BE COMPLETED BY THE USER>",
        "type": "appRoute",
        "entries": [
          {
            "siteLists": [
              "cf4bbb13-0a3f-4302-adfa-6cfce6b3950c"
            ],
            "vpnLists": [
              "67c9a7e1-e1b2-4a31-bd7c-7d0bbf9b7bbb"
            ]
          }
        ]
      }
    ]
  },
  "isPolicyActivated": false
}
```



- Then click on "**Try it out**".
- At this point you should be able to see the policy created under policies using the SD-WAN UI.



- Subtask 2: Policy verification on the data path.
  - Login to DC1 EDGE2 using terminal console "**ssh admin@198.18.134.101**" the password is "**admin**"
  - Traceroute from DC1 EDGE2 to BR3 and verify the change in the path. Use the following command "**traceroute vpn 10 10.5.0.10**" The trace should show the IP address of the link between the INET and BR3 (100.64.2.10)

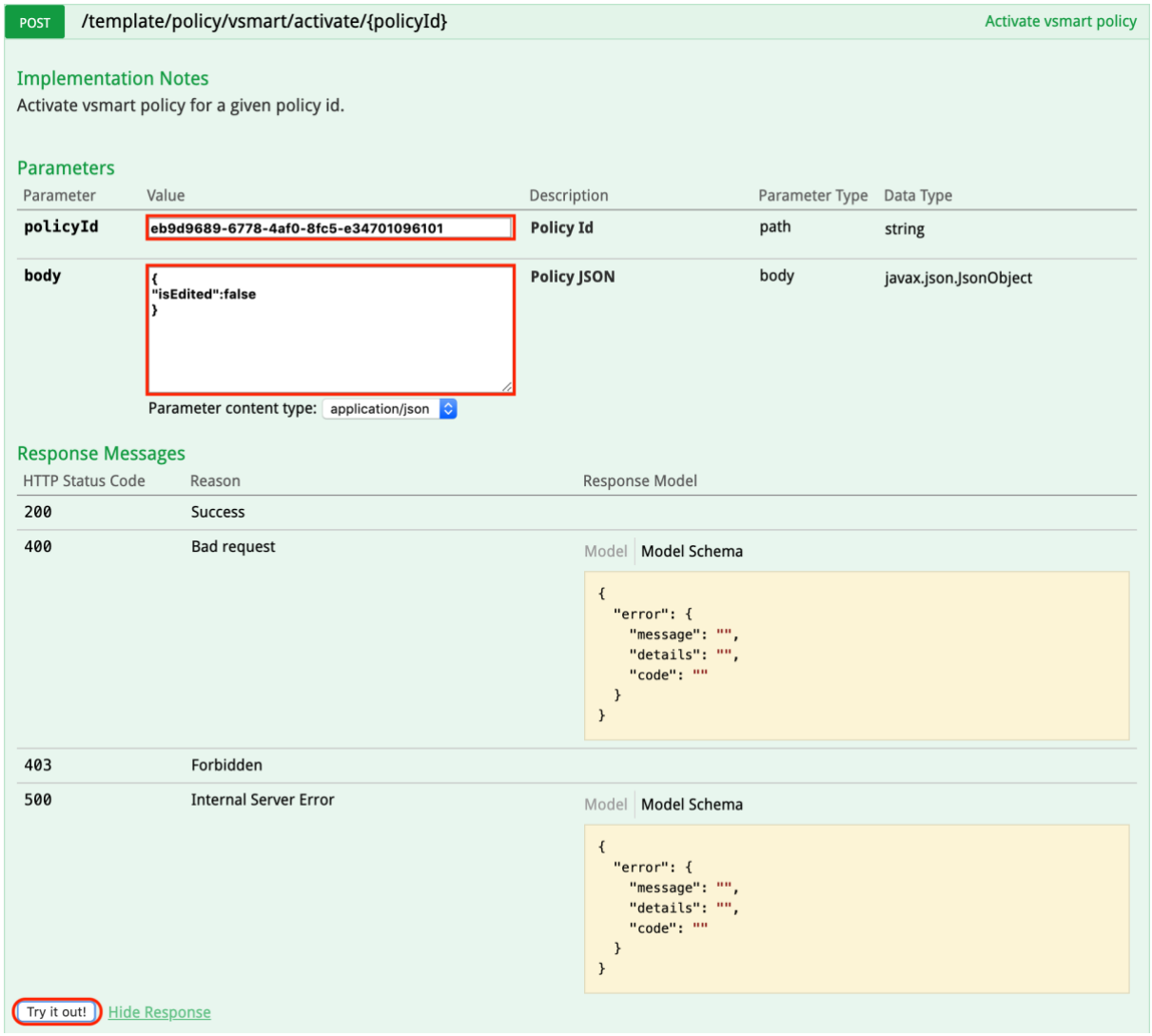


Step 4: Activate policy

- Subtask 1: To activate the policy you must have the "policyId" value of the policy created.
  - To get this value use the option GET "**/template/policy/vsmart**" under "**Configuration - vSmart Template Policy**".
  - Look the response body for the description of the policy configured in "Step 2", then look for the attribute associated to "policyId" and copy it.

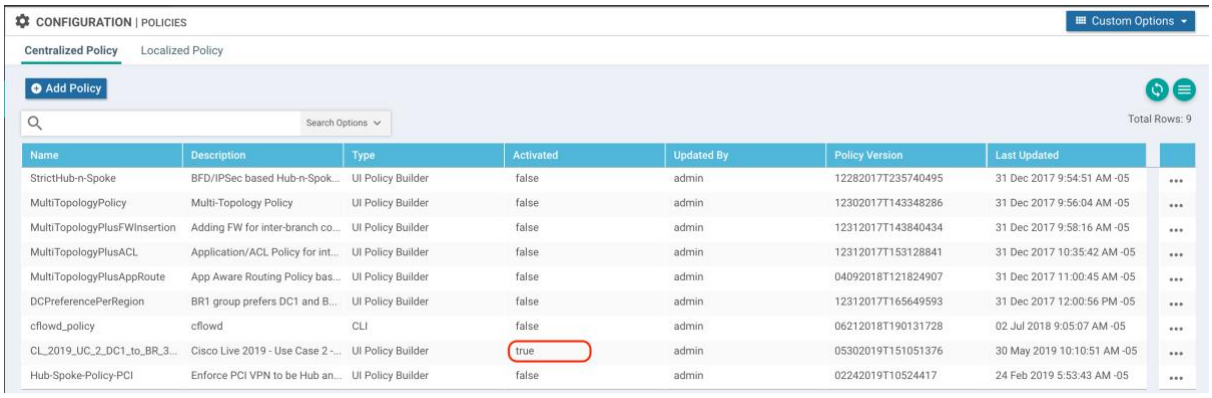
  - Under "**Configuration - vSmart Template Policy**" use the POST "**/template/policy/vsmart/activate/{policyId}**" option.
  - Copy the value previously identified (policyId attribute) and paste into the policyId field.
  - Finally, on the body field paste the following.

```
{
"isEdited":false
}
```



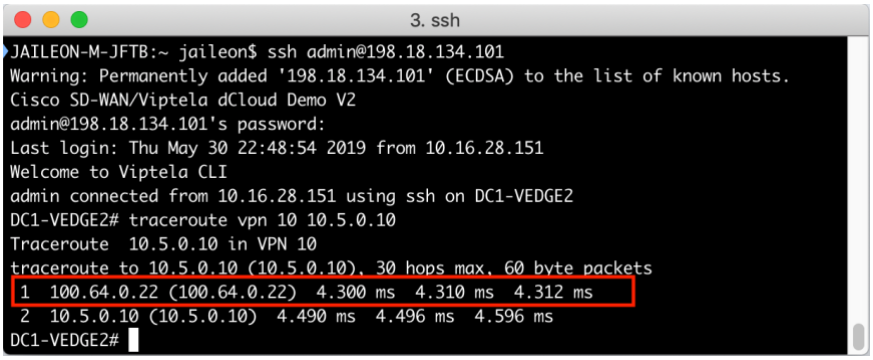
Step 5: Verification

- Subtask 1: Policy verification on vMANAGE.
    - Return to the configuration policies on vMANAGE UI and verify that the policy is activated:



- Subtask 2: Policy verification on the data path.
    - Login to DC1 EDGE2 using terminal console "**ssh admin@198.18.134.101**" the password is "**admin**"

- Traceroute from DC1 EDGE2 to BR3 and verify the change in the path. Use the following command "**traceroute vpn 10 10.5.0.10**" The trace should show you the IP address of the link between the MPLS-PE and BR3 (100.64.0.22)

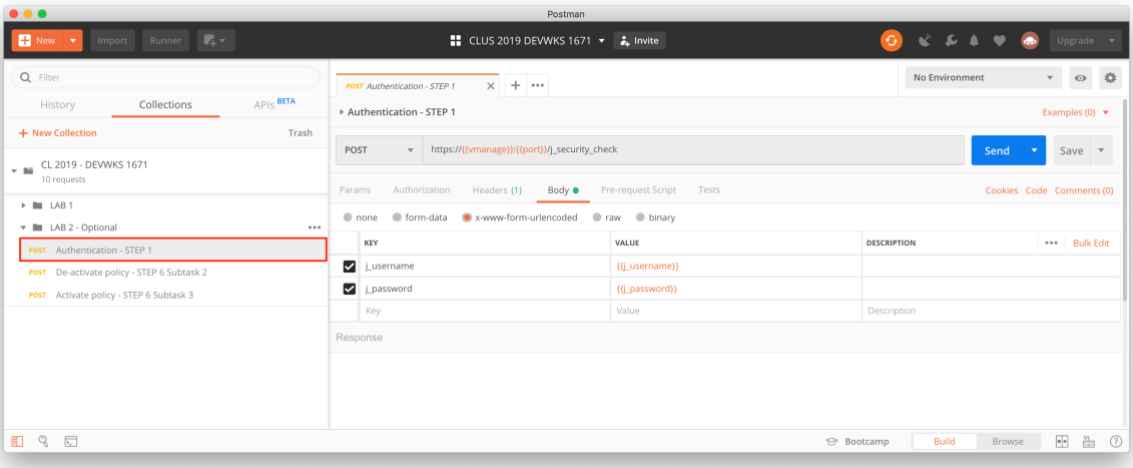


Step 6: Deactivate policy using Postman (OPTIONAL)

You can use postman as another tool to interact with vManage APIs.

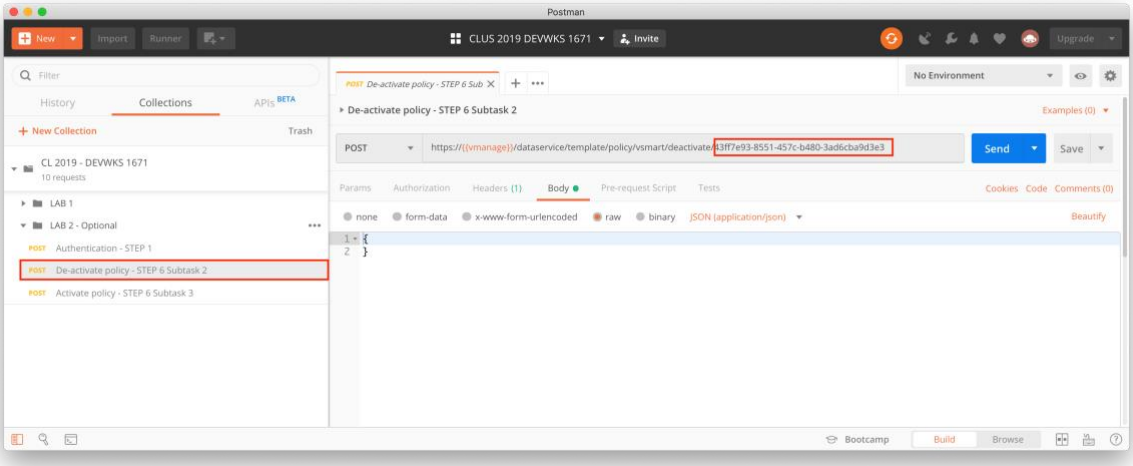
- Subtask 1: Open Postman and use the same collection imported during LAB1, but in this case use the scripts under LAB 2 folder.

    - Execute the "**POST Login**" to get the cookie from vmanage

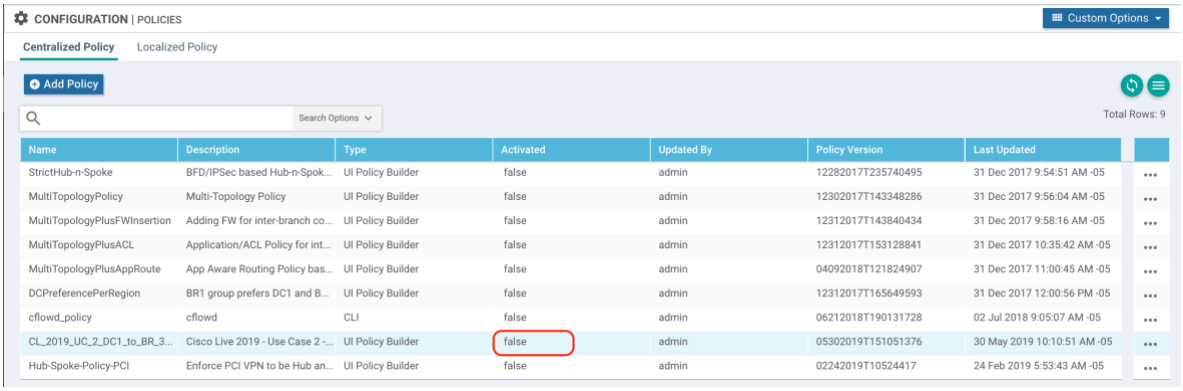


- Subtask 2: De-activate the policy:

    - Execute the "**POST de-activate policy**", to proceed with this step you need change the PolicyID on the URL, the PolicyID is the same value that you used on the step 4



- Then, go to SD-WAN UI browse to **Configuration > Policies** and verify that the policy is disabled (false under Activated column).



- Subtask 3: Activate the policy:

  - Execute the "**POST activate policy**", to proceed with this step you need change the PolicyID on the URL, the PolicyID is the same value that you used on the step 4

References

- Github repository:
  - https://github.com/jaileon/DEVWKS-1671.git

- Postman Collection:
  - https://www.getpostman.com/collections/a15b3e29d99f54a56d86