# **Reference Architecture Documentation**

F5 Networks, Inc.

Mar 26, 2020



## GSLB Build Guide 2020

# Reference Architecture

900

F5 Networks, Inc.





## Contents

| 1 | WAF |                          | 7        |
|---|-----|--------------------------|----------|
|   | 1.1 | Onboarding               | 7        |
|   |     | 1.1.1 Networking         | 8        |
|   |     | 1.1.1.1 VLAN'S           | 8        |
|   |     | 1112 SELEIP's            | 2        |
|   |     | 1 1 1 3 Default Boute 14 | <u>_</u> |
|   |     | 1 1 1 4 Deculte          | -<br>7   |
|   |     | 1.1.0 Cluster            | /<br>0   |
|   |     |                          | 5<br>0   |
|   |     |                          | 3        |
|   |     | 1.1.2.2 Irust Members    | 1        |
|   |     | 1.1.2.3 Changes Pending  | 3        |
|   |     | 1.1.2.4 Device Groups    | 5        |
|   |     | 1.1.2.5 Sync Again       | 7        |
|   |     | 1.1.3 Shared Objects     | 9        |
|   |     | 1.1.3.1 Sync Folder      | 9        |
|   |     | 1.1.3.2 HTTP Profile     | 1        |
|   |     | 1.1.3.3 TCP Profile      | 3        |
|   |     | 1.1.3.4 Health Monitor   | 5        |
|   |     | 1.1.3.5 Pools            | 7        |
|   |     | 114 Virtuals             | n        |
|   |     | 115 Security Policy      | ð        |
|   |     | 1151 Sync                | ົ້       |
|   |     | 1.1.5.1 Sync             | 3<br>⊿   |
|   |     | 1.1.5.2 Parent Onito     | +<br>~   |
|   |     |                          | 0        |
|   |     | 1.1.6 Cut-Over           | 8        |
|   | 1.2 | Policy luning            | 1        |
|   | 1.3 | Hack and Defend          | 1        |
| ~ | DNO |                          | _        |
| 2 | DNS | 50                       | 3        |
|   | 2.1 | Availability             | 3        |
|   |     | 2.1.1 Network Map        | 3        |
|   |     | 2.1.2 System             | 8        |
|   |     | 2.1.3 Settings           | 2        |
|   |     | 2.1.4 Listeners          | 3        |
|   |     | 2.1.4.1 DNS Profile      | 4        |

|     |        | 2.1.4.2  | UDP Profile                         |     |
|-----|--------|----------|-------------------------------------|-----|
|     |        | 2.1.4.3  | TCP Profile                         |     |
|     |        | 2.1.4.4  | UDP IP Address                      |     |
|     |        | 2.1.4.5  | TCP IP Address                      |     |
|     | 2.1.5  | Data C   | enters                              |     |
|     |        | 2.1.5.1  | Servers                             |     |
|     |        | 2        | 1.5.1.1 gtm1.SITE1                  |     |
|     |        | 2        | 1512 atm1 SITE2                     | 79  |
|     |        | 2        | 1513 site1 ha-pair                  | 84  |
|     |        | 2        | 1514 site2 ha-pair                  | 90  |
|     |        | 2152     | Device Trust                        | 97  |
|     |        | 2153     | Sync Group                          | 10  |
|     | 216    | Pools    |                                     | 10/ |
|     | 2.1.0  |          |                                     | 104 |
|     | 2.1.7  |          |                                     |     |
|     | 2.1.8  | Delega   | (ION                                |     |
|     |        | 2.1.8.1  |                                     | 14  |
|     |        | 2.1.8.2  |                                     |     |
|     |        | 2.1.8.3  | CNAME                               |     |
|     |        | 2.1.8.4  | Results                             |     |
|     | 2.1.9  | Failure  | Condition                           |     |
|     | 2.1.10 | ) Rest A | ··································· |     |
|     |        | 2.1.10.1 | Authenticate                        |     |
|     |        | 2.1.10.2 | POST                                |     |
|     |        | 2.1.10.3 | Results                             |     |
|     |        | 2.1.10.4 | Active/Standby                      |     |
|     |        | 2.1.10.5 | API Extras (Optional)               |     |
|     | 2.1.1  | 1 Congra | tulations                           |     |
| 2.2 | Secu   | rity     |                                     |     |
|     | 2.2.1  | Transp   | arent Cache                         |     |
|     |        | 2.2.1.1  | Monitors                            |     |
|     |        | 2212     | Load Balancing                      | 146 |
|     |        | 2213     | Results                             | 140 |
|     | 222    | Listone  | re                                  | 154 |
|     | 6.6.6  | 2221     | Log Profilo                         | 150 |
|     |        | 2.2.2.1  |                                     | 160 |
|     |        | 2.2.2.2  |                                     |     |
|     |        | 2.2.2.3  |                                     |     |
|     |        | 2.2.2.4  |                                     |     |
|     |        | 2.2.2.5  | DNS Servers                         |     |
|     |        | 2.2.2.6  | UDP Listener                        |     |
|     |        | 2.2.2.7  |                                     |     |
|     |        | 2.2.2.8  | Results                             |     |
|     | 2.2.3  | Hidden   | Master                              |     |
|     |        | 2.2.3.1  | Name Server                         |     |
|     |        | 2.2.3.2  | DNS Express                         |     |
|     |        | 2.2.3.3  | Results                             |     |
|     | 2.2.4  | DNSSe    | с                                   |     |
|     |        | 2.2.4.1  | Zone Signing Key                    |     |
|     |        | 2.2.4.2  | Key Signing Key                     |     |
|     |        | 2.2.4.3  | Signed Zone                         |     |
|     |        | 2.2.4.4  | Results                             | 19  |
|     | 2.25   | Validati | na Resolver                         | 192 |
|     | 0      | 2251     | Trust Anchors                       | 192 |
|     |        | 2252     | Modify DNS Profile                  | 10/ |
|     |        | 2.2.3.2  | Regulte                             | 100 |
|     |        |          |                                     | 197 |

| 2.2 | 2.6 | RPZ .   |                  |
|-----|-----|---------|------------------|
|     |     | 2.2.6.1 | Zone Runner      |
|     |     | 2.2.6.2 | Name Server      |
|     |     | 2.2.6.3 | DNS Express      |
|     |     | 2.2.6.4 | Local Zone       |
|     |     | 2.2.6.5 | Walled Garden    |
|     |     | 2.2.6.6 | Results          |
| 2.2 | 2.7 | URL C   | ategorization    |
|     |     | 2.2.7.1 | Create an iRule  |
|     |     | 2.2.7.2 | iRule assignment |
|     |     | 2.2.7.3 | Results          |
| 2.2 | 2.8 | Title . |                  |
|     |     |         |                  |

WAF

## 1.1 Onboarding



Four dedicated WAF instances are deployed across two datacenters.

Each WAF device has already been licensed, and a base configuration including hostname, and DNS settings.

Standalone WAF instances are load balanced by an existing HA pair of F5 LTM's.

## 1.1.1 Networking



Complete the tasks required to get the WAF devices onto a network.

### 1.1.1.1 VLAN's



Create a vlan on each WAF

1. \_

Note: It is required to complete the following task on both asm1.site1 asm2.site1

| Main Help About   | Network » VLANs : VLAN List                       |
|-------------------|---|
| Mage Statistics   | to vLAN List VLAN Groups                          |
| iApps             | * × Search Create                                 |
| S DNS             | ✓ ▲ Name  |
| SSL Orchestrator  | □ ha_vlan         69         1.2           Delete |
| Local Traffic     |   |
| Acceleration      |   |
| Device Management |   |
| Security          |   |
| Retwork 1         |   |
| Interfaces        |   |
| Routes 💮          |   |
| Self IPs          |   |
| Packet Filters    |   |
| Trunks            |   |
| Tunnels           |   |
| Route Domains 🕞   |   |
| VLANs 2           |   |
| Service Policies  | VLAN Groups 🕙 💮                                   |

Navigate to: Network >> VLANs : VLAN List

Create a new vlan according to the following table.

| Setting   | Value          |
|-----------|----------------|
| Name      | site1_waf_vlan |
| Tag       | 50             |
| Interface | 1.1 - Untagged |

| Hostname: asm1.site1.example.com Dai<br>IP Address: 10.1.10.14 Tim | e: Sep 13, 2017 User: <b>admin</b><br>e: 11:03 PM (CDT) Role: Administrator Pa |
|--|--|
| ONLINE (ACTIVE)<br>Standalone                                      |  |
| Main Help About  | Network » VLANs : VLAN List » New VLAN   |
| Magazine Statistics  |  |
| iAnne  | General Properties   |
| Цо тарра   | Name site1_waf_vlan  |
| S DNS  | Description  |
| SSL Orchestrator   | Tag 50   |
| Local Traffic  | Resources  |
| Acceleration   | Interface: 1.2 V<br>Tagging: Untagged V  |
| Device Management  |  |
| Security   | Interfaces (integgod)  |
| Network  | Edit Delete  |
| Interfaces   |  |
| Routes 📀   | Source Check   |
| Self IPs 📀   | MTU 1500   |
|  | 1000   |

https://asm1.site1.example.com/tmui/Control/jspmap/tmui/locallb/network/vlan/create.jsp https://asm2.site1.example.com/tmui/Control/jspmap/tmui/locallb/network/vlan/create.jsp TMSH command for both asm1.site1 and asm2.site1:

## TMSH

tmsh create net vlan site1\_waf\_vlan { interfaces add { 1.1 { } } tag 50 }

2.

Note: It is required to complete the following task on both asm1.site2 asm2.site2

Navigate to: Network >> VLANs : VLAN List

| Main     | Help About       | Network » VLA | Ns : VLAN List |        |             |                     |      |
|----------|------------------|---------------|----------------|--------|-------------|---------------------|------|
| Mag Star | tistics          | 🔅 👻 VLAN List | VLAN Groups    |        |             |                     |      |
| iAp      | ps               | *             | ×              | Search |             | Create              |      |
| S DN:    | s                | Name          |                |        | Application | Tag Untagged Interf | face |
| 🔓 ssi    | L Orchestrator   | Delete        |                |        |             | 69 1.2              |      |
| Loc      | cal Traffic      |               |                |        |             |                     |      |
| ᢙ Acc    | celeration       |               |                |        |             |                     |      |
| Dev      | vice Management  |               |                |        |             |                     |      |
| 🕥 Sec    | curity           |               |                |        |             |                     |      |
| 📄 Net    | twork            |               |                |        |             |                     |      |
| I        | Interfaces       |               |                |        |             |                     |      |
| F        | Routes 💮         |               |                |        |             |                     |      |
| ş        | Self IPs         | <b>\</b>      |                |        |             |                     |      |
| F        | Packet Filters   | <b>\</b>      |                |        |             |                     |      |
| 1        | Trunks >         |               |                |        |             |                     |      |
| 1        | Tunnels >        |               |                |        |             |                     |      |
| F        | Route Domains 🕞  |               |                |        |             |                     |      |
| N        | VLANs 2          | VLAN List     | •              |        |             |                     |      |
| 5        | Service Policies | VLAN Groups   | <b>(+)</b>     |        |             |                     |      |
|          |                  |               |                |        |             |                     |      |

Create a new vlan according to the following table.

| Setting   | Value          |
|-----------|----------------|
| Name      | site2_waf_vlan |
| Тад       | 60             |
| Interface | 1.1 - Untagged |

https://asm1.site2.example.com/tmui/Control/jspmap/tmui/locallb/network/vlan/create.jsp https://asm2.site2.example.com/tmui/Control/jspmap/tmui/locallb/network/vlan/create.jsp TMSH command for both asm1.site2 and asm2.site2:

### TMSH

tmsh create net vlan site2\_waf\_vlan { interfaces add { 1.1 { } } tag 60 }

#### 1.1.1.2 SELFIP's



Create an IP address on each WAF instance

Note: It is required to complete the following task on asm1.site1 asm2.site1 asm1.site2 and asm2.site2

Navigate to: Network >> Self IPs

| Hostname:<br>IP Address: | asm1.site1.example.com<br>10.1.10.14 | Date:<br>Time: | Sep 13, 2017<br>11:13 PM (CDT) | User:<br>Role: | <b>admin</b><br>Administra | ator        |      |            |               | Pa            |
|--------------------------|--------------------------------------|----------------|--------------------------------|----------------|----------------------------|-------------|------|------------|---------------|---------------|
| 6                        | ONLINE (ACTIVE)<br>Standalone        |                |                                |                |                            |             |      |            |               |               |
| Main                     | Help About                           |                | Network » Self                 | IPs            |                            |             |      |            |               |               |
| Magazina Statisti        | cs                                   |                | 🔅 🚽 Self IP Lis                | t              |                            |             |      |            |               |               |
| iApps                    |                                      |                | *                              |                |                            | ×           | Sea  | irch       |               | Create        |
| 🌎 dns                    |                                      |                | Vame 🖉                         |                |                            | Application | tion | IP Address | Netmask       | VLAN / Tunnel |
| SSI OF                   | chestrator                           |                | ha_selfip                      |                |                            |             |      | 10.1.69.14 | 255.255.255.0 | ha_vlan       |
| Local T                  | raffic                               |                | Delete                         |                |                            |             |      |            |               |               |
| Device Management        |                                      |                |                                |                |                            |             |      |            |               |               |
| Securit                  | У                                    |                |                                |                |                            |             |      |            |               |               |
| Retwor                   | k 🕇                                  |                |                                |                |                            |             |      |            |               |               |
| Inter                    | faces                                | •              |                                |                |                            |             |      |            |               |               |
| Rout                     | ies 🔄                                | )              |                                |                |                            |             |      |            |               |               |
| Self                     | IPs                                  | )              |                                |                |                            |             |      |            |               |               |

1. asm1.site1

Create a new selfip on asm1.site1 according to the following table.

| Setting     | Value            |
|-------------|------------------|
| Name        | site1_waf_selfip |
| IP Address  | 10.1.50.14       |
| Netmask     | 255.255.255.0    |
| VLAN/Tunnel | site1_waf_vlan   |

https://asm1.site1.example.com/tmui/Control/jspmap/tmui/locallb/network/self\_ip/create.jsp

TMSH command for **asm1.site1**:

## TMSH

tmsh create net self site1\_waf\_selfip { address 10.1.50.14/24 vlan site1\_waf\_vlan }

2. asm2.site1

Create a new selfip on **asm2.site1** according to the following table.

| Setting     | Value            |
|-------------|------------------|
| Name        | site1_waf_selfip |
| IP Address  | 10.1.50.15       |
| Netmask     | 255.255.255.0    |
| VLAN/Tunnel | site1_waf_vlan   |

https://asm2.site1.example.com/tmui/Control/jspmap/tmui/locallb/network/self\_ip/create.jsp

TMSH command for asm2.site1:

#### TMSH

tmsh create net self site1\_waf\_selfip { address 10.1.50.15/24 vlan site1\_waf\_vlan }

#### 3. asm1.site2

Create a new selfip on **asm1.site2** according to the following table.

| Setting     | Value            |
|-------------|------------------|
| Name        | site2_waf_selfip |
| IP Address  | 10.1.60.24       |
| Netmask     | 255.255.255.0    |
| VLAN/Tunnel | site2_waf_vlan   |

https://asm1.site2.example.com/tmui/Control/jspmap/tmui/locallb/network/self\_ip/create.jsp

#### TMSH

tmsh create net self site2\_waf\_selfip { address 10.1.60.24/24 vlan site2\_waf\_vlan }

#### 4. asm2.site2

Create a new selfip on **asm2.site2** according to the following table.

| Setting     | Value            |
|-------------|------------------|
| Name        | site2_waf_selfip |
| IP Address  | 10.1.60.25       |
| Netmask     | 255.255.255.0    |
| VLAN/Tunnel | site2_waf_vlan   |

https://asm2.site2.example.com/tmui/Control/jspmap/tmui/locallb/network/self\_ip/create.jsp

#### TMSH

tmsh create net self site2\_waf\_selfip { address 10.1.60.25/24 vlan site2\_waf\_vlan }

### 1.1.1.3 Default Route

Create a default gateway on each WAF

Navigate to: Network >> Routes

| Hostname:<br>IP Address: | asm1.site1.example.com<br>10.1.10.14 | Date: Sep 14<br>Time: 9:20 A | 4, 2017 Use<br>M (CDT) Role | r: <b>admin</b><br>:: Administrator |             |             |         |              | Pa  |
|--------------------------|--------------------------------------|------------------------------|-----------------------------|-------------------------------------|-------------|-------------|---------|--------------|-----|
| 6                        | ONLINE (ACTIVE)<br>Standalone        |                              |                             |                                     |             | ×           |         |              |     |
| Main                     | Help About                           | Netw                         | ork » Routes                |                                     |             |             |         |              |     |
| Mage Statis              | tics                                 | .⇔                           | Route List                  |                                     |             |             |         |              |     |
| iApps                    |                                      |                              |                             |                                     |             |             |         | 3 Ad         | dd  |
| S DNS                    |                                      |                              | Name                        | ÷ /                                 | Application | Destination | Netmask | Route Jomain | Res |
| 6                        | rohastrator                          | No re                        | cords to display.           |                                     |             |             |         |              |     |
|                          | Traffic                              | Delet                        | e                           |                                     |             |             | /       |              |     |
| Accel                    | eration                              |                              |                             |                                     |             |             |         |              |     |
| E Devic                  | e Management                         |                              |                             |                                     |             |             |         |              |     |
| Secur                    | ity                                  |                              |                             |                                     |             |             |         |              |     |
| e Netwo                  | ork 1                                |                              |                             |                                     |             |             |         |              |     |
| Inte                     | erfaces                              | •                            |                             |                                     |             |             |         |              |     |
| Ro                       | utes 🚄 🕑                             | )                            |                             |                                     |             |             |         |              |     |
| Sel                      | f IPs 🔄                              | )                            |                             |                                     |             |             |         |              |     |
| Par                      | ·kot Filtore                         |                              |                             |                                     |             |             |         |              |     |

1. Create a default gateway according to the table below.

## Note: It is required to complete the following task on both asm1.site1 asm2.site1

| Setting         | Value         |
|-----------------|---------------|
| Name            | default_route |
| Destination     | 0.0.0.0       |
| Netmask         | 0.0.0.0       |
| Gateway Address | 10.1.50.1     |

| Hostname: asm1.site1.example.com Dat<br>IP Address: 10.1.10.14 Tim | e: Sep 14, 2017 User: admin<br>e: 9:24 AM (CDT) Role: Administra | tor Pa               |
|--|--|----------------------|
| ONLINE (ACTIVE)<br>Standalone                                      |  |                      |
| Main Help About  | Network » Routes » New Rout                                      | ie                   |
| Statistics   | Properties   |                      |
| iApps  | Name   | default_route        |
| S DNS  | Description  |                      |
| SSL Orchestrator   | Destination  | 0.0.0.0              |
| Local Traffic  | Netmask  | 0.0.0.0              |
| Acceleration   | Resource<br>Gateway Address                                      | IP Address 10.1.50.1 |
| Device Management  | мти  | 1500                 |
| Security   | Cancel Repeat Finished   |                      |
| Network  |  |                      |
| Interfaces   |  | -                    |
| Routes 🕒   |  |                      |
| Self IPs 主   |  | N                    |
| Packat Eiltare   |  | ht                   |

https://asm1.site1.example.com/tmui/Control/jspmap/tmui/locallb/network/route/create.jsp https://asm2.site1.example.com/tmui/Control/jspmap/tmui/locallb/network/route/create.jsp TMSH command for asm1.site1 and asm2.site1:

#### TMSH

tmsh create net route default\_route { gw 10.1.50.1 network default }

2. Create a default gateway according to the table below.

#### Note: It is required to complete the following task on both asm1.site1 asm2.site1

| Setting         | Value         |
|-----------------|---------------|
| Name            | default_route |
| Destination     | 0.0.0.0       |
| Netmask         | 0.0.0.0       |
| Gateway Address | 10.1.60.1     |

https://asm1.site2.example.com/tmui/Control/jspmap/tmui/locallb/network/route/create.jsp https://asm2.site2.example.com/tmui/Control/jspmap/tmui/locallb/network/route/create.jsp TMSH command for asm1.site2 and asm2.site2:

## TMSH

tmsh create net route default\_route { gw 10.1.60.1 network default }

### 1.1.1.4 Results

On the Jumpbox select the Putty icon on the desktop, and open asm1.site1.example.com





- 1. From asm1.site1 ping the gateway
  - ping 10.1.50.1
- 2. From asm1.site1 ping bigip1.site1 and bigip2.site1
  - ping 10.1.50.2
  - ping 10.1.50.3
- 3. From asm1.site2 ping the gateway
  - ping 10.1.60.1
- 4. From asm1.site2 ping bigip1.site2 and bigip2.site2
  - ping 10.1.60.2
  - ping 10.1.60.3

## 1.1.2 Cluster

Create a trust relationship across all WAF devices



## 1.1.2.1 ConfigSync IP

HA vlan and IP address have already been provisioned on each WAF device.

Log into each WAF and configure the system to use the IP address on the "ha\_vlan" as the "Local Address" for ConfigSync.

Navigate to: Device Management >> Devices >> asm1.site1.example.com

| M          | ain        | Help       | About | Device Management » Devices » asm1.site1.example.com |                    |          |           |                  |           |  |  |
|------------|------------|------------|-------|--|--------------------|----------|-----------|------------------|-----------|--|--|
| M-         | Statistics | ;          |       | .⇔.≁   | Properties         | ConfigSy | nc        | Failover Network | Mirroring |  |  |
| <b>I</b>   | iApps      |            |       | Config   | Sync Configuration | I        |           |                  |           |  |  |
| <b>S</b>   | DNS        |            |       | Local  | Address            | 1        | D.1.69.14 | (ha_vlan) 🗸      | I         |  |  |
|            | SSL Orcl   | nestrator  |       | Upda   | te                 |          |           |                  |           |  |  |
|            | Local Tra  | affic      |       |  |                    |          |           |                  |           |  |  |
|            | Accelera   | tion       |       |  |                    |          |           |                  |           |  |  |
|            | Device M   | lanagement |       |  |                    |          |           |                  |           |  |  |
|            | Overvi     | ew         |       |  |                    |          |           |                  |           |  |  |
|            | Device     | es         |       |  |                    |          |           |                  |           |  |  |
|            | Device     | Groups     | ÷     |  |                    |          |           |                  |           |  |  |
|            | Device     | e Trust    | ) - F |  |                    |          |           |                  |           |  |  |
|            | Traffic    | Groups     | ÷     |  |                    |          |           |                  |           |  |  |
| $\bigcirc$ | Security   |            |       |  |                    |          |           |                  |           |  |  |
|            | Network    |            |       |  |                    |          |           |                  |           |  |  |
|            | System     |            |       |  |                    |          |           |                  |           |  |  |

#### Repeat the above step for all WAF devices

https://asm1.site1.example.com/tmui/Control/jspmap/tmui/devmgmt/device/configsync.jsp?name= %2FCommon%2Fasm1.site1.example.com

https://asm2.site1.example.com/tmui/Control/jspmap/tmui/devmgmt/device/configsync.jsp?name= %2FCommon%2Fasm2.site1.example.com

https://asm1.site2.example.com/tmui/Control/jspmap/tmui/devmgmt/device/configsync.jsp?name= %2FCommon%2Fasm1.site2.example.com

https://asm2.site2.example.com/tmui/Control/jspmap/tmui/devmgmt/device/configsync.jsp?name= %2FCommon%2Fasm2.site2.example.com

TMSH command for asm1.site1:

#### TMSH

tmsh modify cm device asm1.site1.example.com configsync-ip 10.1.69.14

TMSH command for asm2.site1:

#### TMSH

tmsh modify cm device asm2.site1.example.com configsync-ip 10.1.69.15

TMSH command for asm1.site2:

#### TMSH

tmsh modify cm device asm1.site2.example.com configsync-ip 10.1.69.24

TMSH command for asm2.site2:

#### TMSH

tmsh modify cm device asm2.site2.example.com configsync-ip 10.1.69.25

#### 1.1.2.2 Trust Members

The following task only needs to be completed from asm1.site1

#### Navigate to: Device Management >> Device Trust : Device Trust Members

https://asm1.site1.example.com/tmui/Control/jspmap/tmui/devmgmt/device\_trust/create.jsp



From the asm1.site1 UI repeate the steps for adding trust with asm2.site1 asm1.site2 and asm2.site2

| Hostname               | Device IP Address |
|------------------------|-------------------|
| asm2.site1.example.com | 10.1.10.15        |
| asm1.site2.example.com | 10.1.10.24        |
| asm2.site2.example.com | 10.1.10.25        |

| Main    | Help         | About | Device Management » Device Trust |   |  |  |  |  |  |  |
|---------|--------------|-------|----------------------------------|---|--|--|--|--|--|--|
| Statis  | tics         |       | Retrieve Device Credentials (S   | Step 1 of 3)  |  |  |  |  |  |  |
| iApps   |              |       | Device Type                      | Peer  |  |  |  |  |  |  |
| 😚 dns   |              |       | Device IP Address                | 10.1.10.15  |  |  |  |  |  |  |
| 🔓 SSL C | rchestrator  |       | Administrator Username           | admin   |  |  |  |  |  |  |
| Local   | Traffic      |       | Administrator Password           | *****   |  |  |  |  |  |  |
| 0       |              |       | Verify Device Certificate (Step  | 2 of 3)   |  |  |  |  |  |  |
| Accel   | eration      |       | Subject                          | /C=US/ST=WA/L=Seattle/O=F5<br>Networks/OU=IT/CN=asm2.site1.example.com/emailAddress=roo |  |  |  |  |  |  |
| E Devic | e Management |       | Management IP Address            | 10.1.10.15  |  |  |  |  |  |  |
| Ov      | erview       |       | Expiration                       | I Sun Aug 27 14:30:28 CST 2027  |  |  |  |  |  |  |
| De      | /ices        |       | Serial Number                    | 0e67cf04  |  |  |  |  |  |  |
| De      | /ice Groups  | ÷     | Signed                           | Yes   |  |  |  |  |  |  |
| De      | /ice Trust   | Þ     | SHA-1                            | 736c1726ae1ce4da7f312a38b4be9807c317f003  |  |  |  |  |  |  |
| Tra     | ffic Groups  | ÷     | MD5                              | f9665ba229ac3a87704f683bba59ec40  |  |  |  |  |  |  |
| Socur   | ity          |       | Add Device (Step 3 of 3)         |   |  |  |  |  |  |  |
| Jecu    | ity          |       | Name                             | asm2.site1.example.com  |  |  |  |  |  |  |
| Netwo   | ork          |       | Cancel Add Device                |   |  |  |  |  |  |  |
| Syste   | m            |       |                                  |   |  |  |  |  |  |  |
|         |              |       |                                  |   |  |  |  |  |  |  |

| Main               | Help       | About | Devi   | ce Management » 🛙     | evice Trust : Devic | e Trust Members        |                                 |                   |
|--------------------|------------|-------|--------|-----------------------|---------------------|------------------------|---------------------------------|-------------------|
| Magazina Statistic | CS         |       | * -    | Local Domain          |                     | Device Trust Members   |                                 |                   |
| iApps              |            |       | Peer a | and Subordinate Dev   | ices                |                        |                                 | Add               |
| S DNS              |            |       |        | Name                  | Device Type         | + Hostname             | Serial Number                   | MAC Address       |
| SSL Or             | chestrator |       |        | asm1.site2.example.co | om Peer             | asm1.site2.example.com | 564dadcc-a795-99fc-24afead600c3 | 2c:c2:60:53:92:4f |
| _                  |            |       |        | asm2.site1.example.co | om Peer             | asm2.site1.example.com | 564dadcc-a795-99fc-24afead600c3 | 2c:c2:60:1f:ef:92 |
| Local T            | raffic     |       |        | asm2.site2.example.co | om Peer             | asm2.site2.example.com | 564dadcc-a795-99fc-24afead600c3 | 2c:c2:60:55:ca:b3 |
| Acceler            | ration     |       | Dele   | te                    |                     |                        |                                 |                   |
| Device             | Management |       |        |                       |                     |                        |                                 |                   |
| Over               | view       |       |        |                       |                     |                        |                                 |                   |
| Devi               | ces        |       |        |                       |                     |                        |                                 |                   |
| Devi               | ce Groups  | ()    |        |                       |                     |                        |                                 |                   |
| Devi               | ce Trust   | +     |        |                       |                     |                        |                                 |                   |
| Traff              | ic Groups  | ÷     |        |                       |                     |                        |                                 |                   |
| Securit            | у          |       |        |                       |                     |                        |                                 |                   |
| Retwor             | k          |       |        |                       |                     |                        |                                 |                   |
| System             |            |       |        |                       |                     |                        |                                 |                   |
|                    |            |       |        |                       |                     |                        |                                 |                   |
|                    |            |       |        |                       |                     |                        |                                 |                   |

## 1.1.2.3 Changes Pending

1. From asm1.site1 click the "Changes Pending" link:

| Hostname: asm1.site1.example.com Date IP Address: 10.1.10.14 Time | te: Sep 7, 2017 User: a<br>ne: 11:33 AM (CDT) Role: A | <b>dmin</b><br>dministrator |                        | Partition: Commor      |
|---|---|-----------------------------|------------------------|------------------------|
| Changes Pending   | —-ci  | ick                         |                        |                        |
| Main Help About   | Device Management » D                                 | evice Trust : Devic         | e Trust Members        |                        |
| Mage Statistics   | 🔅 🚽 Local Domain                                      |                             | Device Trust Members   |                        |
| iApps   | Peer and Subordinate Devi                             | ces                         |                        |                        |
| S DNS   | ✓ ♦ Name  | Device Type                 | Hostname               | Serial Number          |
| SSI Orchostrator  | asm1.site2.example.co                                 | m Peer                      | asm1.site2.example.com | 564dadcc-a795-99fc-24a |
| SSL Of Chestrator   | asm2.site1.example.co                                 | m Peer                      | asm2.site1.example.com | 564dadcc-a795-99fc-24a |
| Local Traffic   | asm2.site2.example.co                                 | m Peer                      | asm2.site2.example.com | 564dadcc-a795-99fc-24a |
| Acceleration  | Delete  |                             |                        |                        |
| Device Management   |   |                             |                        |                        |
| Overview  |   |                             |                        |                        |
| Devices   |   |                             |                        |                        |
| Device Groups 🛞   |   |                             |                        |                        |
| Device Trust  |   |                             |                        |                        |
| Traffic Groups  |   |                             |                        |                        |
| Security  |   |                             |                        |                        |

2. Click "Sync"

| S DNS             | Sync Issues :   |  |
|-------------------|---|--|
| SSL Orchestrator  | datasync-global-dg ○ Changes Pending  | a 4 Devices Sync-Only Group Manu   |
| Local Traffic     | Changes Pending   |  |
| Acceleration      | 4 devices with 4 different configurations   | 3  |
| Device Management | asm2.site1.example.com made last cor<br>asm1.site2.example.com made last cor                                      | nfiguration change on Tue Aug 29 10:35:52 2017<br>nfiguration change on Tue Aug 29 10:36:02 2017 |
| Overview          | This device made last configuration cha   | ange on Tue Aug 29 10:36:09 2017   |
| Devices           | asm2.site2.example.com made last cor  | figuration change on Tue Aug 29 10:44:19 2017  |
| Device Groups 📀   | Recommended action: Synchronize as  | m2.site2.example.com to group datasync-global-d <u>c</u>   |
| Device Trust      | Devices:  |  |
| Traffic Groups 📀  |   |  |
| Converte          |   |  |
| Security          | asm2.site2.example.com  | O In Sync  |
| Network           | o 🐨 asm1.site1.example.com (Self)   | Does not have the last synced configuration +  |
| System            | o 🐨 asm1.site2.example.com  | Does not have the last synced configuration :  |
|                   | o 🐨 asm2.site1.example.com  | Does not have the last synced configuration  |
|                   | Sync Options:<br>Push the selected device configuration to the selected device configuration to the selected Sync | hick "Sync"  |

After initial synchronization devices will go "OFFLINE" for a few minutes.

#### 1.1.2.4 Device Groups

#### The following task only needds to be completed from asm1.site1

Create a sync-only group that contains all four ASM devices

Navigate to: Device Management >> Device Groups

| Hostname: asm1.site1.example.com Da<br>IP Address: 10.1.10.14 Tim | te: Sep 14, 2017 User: <b>admin</b><br>ne: 3:19 PM (CDT) Role: Administrator |             |
|---|--|-------------|
| ONLINE (ACTIVE) Standalone  |  |             |
| Main Help About   | Device Management » Device Groups  |             |
| Statistics  | 🔅 👻 Device Group List  |             |
| iApps   | * × Search   | 3<br>Create |
| S DNS   | Group Name   | 🗢 Type 🛛 🗢  |
| SSL Orchestrator  | datasync-global-dg (Includes Self)  Delete                                   | Sync-Only N |
| Local Traffic   |  |             |
| Acceleration  |  |             |
| Device Management   |  |             |
| Overview  |  |             |
| Devices   |  |             |
| Device Groups 2 📀 🕕   |  |             |
| Device Trust  |  |             |
| Traffic Groups 🕞  |  |             |
| Security  |  |             |

Create the device group according to the following table:

| Setting                | Value                      |
|------------------------|----------------------------|
| Name                   | example.com_waf_sync-group |
| Group Type             | Sync-Only                  |
| Members                | Add all four WAF devices   |
| Sync Type              | Automatic with Full Sync   |
| Save on Automatic Sync | Checked                    |

| Hostname: asm1.site1.example.com Dat<br>IP Address: 10.1.10.14 Tim | te: Sep 7, 2017 User: <b>admin</b><br>te: 11:45 AM (CDT) Role: Adminis | trator Partition   |
|--|--|--|
| In Sync  |  |  |
| Main Help About  | Device Management » Device   | Groups » New Device Group  |
| Statistics   | General Properties   |  |
| iApps  | Name   | example.com_waf_sync-group ×                                     |
| S DNS  | Group Type   | Sync-Only  |
| SSL Orchestrator   | Description  |  |
| Local Traffic  | Configuration: Advanced 🗸  |  |
| Acceleration   | Members  | Includes Available   |
| Device Management  |  | asm2.site1.example.com >> asm2.site1.example.com                 |
| Overview   | Sync Type  | Automatic with Full Sync   |
| Devices  | Save on Automatic Sync   | Save the configuration to file on the remote devices after an au |
| Device Groups 📀  |  | -  |
| Device Trust   | Cancel Repeat Finished   |  |
| Traffic Groups   |  |  |
| ( Security   |  |  |

https://asm1.site1.example.com/tmui/Control/jspmap/tmui/devmgmt/devicegroups/create.jsp

TMSH command for asm1.site1:

## TMSH

tmsh create cm device-group example.com\_waf\_sync-group { auto-sync enabled devices add { asm1.site1.example.com { } asm1.site2.example.com { } asm2.site1.example.com { } asm2.site2.example.com { } full-load-on-sync true save-on-auto-sync true }

#### 1.1.2.5 Sync... Again

1. From asm1.site1 click the "Not All Devices Synced" link:

| Hostname: asm1.site1.example.com Dat<br>IP Address: 10.1.10.14 Tim | e: Sep 7, 2017 User: admin<br>e: 11:56 AM (CDT) Role: Adminis | strator   |  |  |  |  |
|--|---|---|--|--|--|--|
| ONLINE (ACTIVE) Not All Devices Synced                             |   | -Click  |  |  |  |  |
| Main Help About  | Device Management » Device                                    | Groups » example.com_waf_sync-group   |  |  |  |  |
| Statistics   | 🔅 👻 Properties  |   |  |  |  |  |
| iApps  | General Properties  |   |  |  |  |  |
| S DNS  | Name  | example.com_waf_sync-group  |  |  |  |  |
|  | Group Type  | Sync-Only   |  |  |  |  |
| SSL Orchestrator   | Description   |   |  |  |  |  |
| Local Traffic  | Configuration: Advanced                                       |   |  |  |  |  |
| Acceleration   |   | Includes Available  |  |  |  |  |
| Device Management  | Members   | /Common<br>asm1.site1.example.com<br>asm2.site1.example.com<br>asm2.site1.example.com |  |  |  |  |
| Overview   |   | asm2.site2.example.com  |  |  |  |  |
| Devices  | Sync Type   | Automatic with Full Sync  |  |  |  |  |
| Device Groups 📀  | Save on Automatic Sync  | Save the configuration to file on the remote devices after an a                       |  |  |  |  |
| Device Trust   | Undata   Dalata   |   |  |  |  |  |
| Traffic Groups   | Opdate Delete   |   |  |  |  |  |
| ( Security   |   |   |  |  |  |  |

2. Click "Sync"

The label may show "AWaiting Initial Sync"

TMSH command for asm1.site1:

## TMSH

tmsh run /cm config-sync force-full-load-push to-group example.com\_waf\_sync-group

## Be Patient. Sometimes initial sync takes a minute.

https://support.f5.com/csp/article/K14856

## 1.1.3 Shared Objects



Some configuration objects are common across all devices.

Common objects will replicate across the cluster.

## 1.1.3.1 Sync Folder

Create the sync folder.

This is a cli only task to be completed on asm1.site1

1. On the Jumpbox select the Putty icon on the desktop, and open asm1.site1.example.com

2. Run the following command.

TMSH command for asm1.site1:

## TMSH

tmsh create sys folder shared device-group example.com\_waf\_sync-group traffic-group none



## 1.1.3.2 HTTP Profile

The HTTP profile may be the same across all WAF devices.

Navigate to: Local Traffic >> Profiles : Services : HTTP

| Hostname: asm1.site1.example.com D<br>IP Address: 10.1.10.14 | ate: Sep 14, 2017 User: a<br>me: 4:01 PM (CDT) Role: A | admin<br>Administrator |                                     |
|--|--|------------------------|-------------------------------------|
| In Sync  |  | HTTP OT                |                                     |
| Main Help About  | Local Traffic » Profiles                               | Web Acceleration (+)   |                                     |
| Mage Statistics  | 😙 Services   | FTP (+)                | rersistence Protocol <del>v</del> S |
|  | Analytics 👻 M  | TFTP (+)               | *                                   |
| iApps  |  | DNS 🔶                  |                                     |
| S DNS  | 4  | RTSP 💮                 | 5<br>Create                         |
|  | A Name   | ICAP 🔶                 | ⇒ An                                |
| SSL Orchestrater   | i http   | Request Adapt 🕘        | + ) (b)                             |
| Local Traffic  | i http-explicit  | Response Adapt 💮       | -                                   |
| Notwork Map  | http-transparent                                       | Diameter 💮             |                                     |
| Virtual Convora  | Delete   | DHCPv4 🔶               |                                     |
| Delision   |  | DHCPv6 🕘               |                                     |
| Policies   |  | RADIUS 🕘               |                                     |
| Promies 2  | Services 3   | SIP 🔶                  |                                     |
| Cipners  |  | SMTP 🔶                 |                                     |
| iRules >   | Persistence (+)  | SMTPS (+)              |                                     |
| Pools  | Protocol   | Client LDAP (+)        |                                     |
| Nodes  | SSL  | Server LDAP (+)        |                                     |
| Monitors   | Authentication >                                       | iSession (+)           |                                     |

https://asm1.site1.example.com/tmui/Control/jspmap/tmui/locallb/profile/http/create.jsp

Create an HTTP profile according to the table below.

| Setting | Value                           |
|---------|---------------------------------|
| Name    | shared/example.com_http_profile |

| Ma         | in Help             | About     | Local Traffic » Profiles : Services : HTTP » New HTTP Profile |                   |  |  |  |
|------------|---------------------|-----------|---|-------------------|--|--|--|
| <u>^</u> s | tatistics           |           | General Properties  |                   |  |  |  |
| _⊜ i∕      | Apps                |           | Name  | shared/example.cc |  |  |  |
| S 0        | NS                  |           | Proxy Mode  | Reverse           |  |  |  |
| 🔓 s        | SL Orchestrator     |           | Parent Profile  | http 🗸            |  |  |  |
| ra L       | ocal Traffic        |           | Settings  |                   |  |  |  |
| - 480      |                     |           | Basic Auth Realm  |                   |  |  |  |
|            | Network Map         |           | Fallback Host   |                   |  |  |  |
|            | Virtual Servers     | • •       | Fallback on Error Codes                                       |                   |  |  |  |
|            | Policies            | •         |   |                   |  |  |  |
|            | Profiles            | •         | Request Header Erase  |                   |  |  |  |
|            | Ciphers             | •         | Request Header Insert   |                   |  |  |  |
|            | iRules              | ÷         | Response Headers Allowed                                      |                   |  |  |  |
|            | Pools               | •         | Request Chunking  | Preserve V        |  |  |  |
|            | Nodes               | •         | Response Chunking   | Selective         |  |  |  |
|            | Monitors            | $(\cdot)$ |   |                   |  |  |  |
|            | Traffic Class       | ÷         |   |                   |  |  |  |
|            | Address Translation | ı →       | Redirect Rewrite  | None              |  |  |  |
|            |                     |           | Encrypt Cookies   |                   |  |  |  |
| A          | cceleration         |           | Cookie Encryption Passphrase                                  |                   |  |  |  |
|            |                     |           | Confirm Cookie Encryption                                     |                   |  |  |  |

## TMSH command for asm1.site1:

## TMSH

tmsh create ltm profile http shared/example.com\_http\_profile

## 1.1.3.3 TCP Profile

TCP profiles are the same across WAF's in all sites.

Navigate to: Local Traffic >> Profiles : Protocol : TCP

| Main     | Help               | About |   | Local Traffic » Profiles : Protocol : TCP |                                    |         |            |   |             |               |         |             |          |
|----------|--------------------|-------|---|---|------------------------------------|---------|------------|---|-------------|---------------|---------|-------------|----------|
| Maga Sta | atistics           |       |   | <b>*</b> -                                | Services                           |         | - Content  |   | -           | Persistence   | Protoco | ol 👻 s      | 88       |
| iA,      | pps                |       |   | Authe                                     | entication 👻                       | Ana     | alytics    | - | Messa       | ige Routing 👻 | Other   | -           |          |
| S DN     | IS                 |       |   | *   |                                    |         |            | × | Search      |               |         |             |          |
| 🔓 ss     | L Orchestrator     | /     |   | ÷   | Name                               |         |            |   |             |               |         | Application | 4        |
| C Lo     | cal Traffic        |       |   | i a                                       | pm-forwarding-c<br>pm-forwarding-s | lient-f | cp<br>-tcp |   |             |               |         |             | tc<br>tc |
|          | Network Map        |       |   | f5  | 5-tcp-lan                          |         |            |   |             |               |         |             | tc       |
|          | Virtual Servers    | •     |   | f5  | 5-tcp-mobile                       |         |            |   |             |               |         |             | tc       |
|          | Policies           | Þ     |   | f5  | 5-tcp-progressive                  | )       |            |   |             |               |         |             | tc       |
|          | Profiles           | Þ     | E | Service                                   | s.                                 | •       |            |   |             |               |         |             | tc       |
|          | Ciphe s            | •     |   | Content                                   | t                                  | ).e     | d          |   |             |               |         |             | tc       |
|          | iRujes             | •     |   | Persiste                                  | ence 📀                             | ) ;p    |            |   |             |               |         |             | tc       |
|          | Fools              |       |   | Protoco                                   | bl                                 | •       | Fast L4    |   | ÷           |               |         |             | 1)<br>tr |
|          | Nodes              |       | 3 | SSL                                       |                                    | •       | Fast HTTP  |   | ÷           |               |         |             |          |
| /        | Monitors           | ۲     | ÷ | Authent                                   | tication                           |         | ТСР        |   | •           |               |         |             |          |
|          | Traffic Class      | ÷     |   | Analytic                                  | s                                  | 9       | UDP        |   | ÷           |               |         |             |          |
|          | Address Translatio | n →   |   | Messag                                    | ge Routing                         | •       | SCTP       |   | ÷           |               |         |             |          |
|          |                    |       |   | Other                                     |                                    | •       | Any IP     |   | $( \cdot )$ |               |         |             |          |
| (🧭) Ac   | celeration         |       |   |   |                                    |         |            |   |             |               |         |             |          |
| 0 -      |                    |       |   |   |                                    |         |            |   |             |               |         |             |          |

Create a TCP profile according to the table below.

| Setting | Value                          |
|---------|--------------------------------|
| Name    | shared/example.com_tcp_profile |
| Main Help About  |                 | Local Traffic » Profiles : Protocol : TCP » New TCP Profile |                            |                           |  |
|--|-----------------|---|----------------------------|---------------------------|--|
| Mag S  | tatistics       |   |                            |                           |  |
| i Anne   |                 |   | General Properties         |                           |  |
| To the second se |                 |   | Name                       | shared/example ×          |  |
| S DNS  |                 |   | Parent Profile             | tcp                       |  |
| SSL Orchestrator   |                 |   | Timer Management           |                           |  |
| Local Traffic  |                 |   | Close Wait                 | Specify 🔽 5 seconds       |  |
|  |                 | _   | Fin Wait 1                 | Specify 5 seconds         |  |
| Network Map  |                 | Fin Wait 2  | Specify V 300 seconds      |                           |  |
|  | Virtual Servers |   | I dia Tima and             |                           |  |
|  | Policies        | ×.  | Idie I meout               | Specify                   |  |
|  | Profiles        | ×   | Keep Alive Interval        | Specify 1800 seconds      |  |
|  | Ciphers         | ×   | Minimum RTO                | 1000 milliseconds         |  |
|  | iRules          | •   | Reset On Timeout           | Enabled                   |  |
|  | Pools           | •   | Time Wait                  | Specify 2000 milliseconds |  |
|  | Nodes           | ×.  | Time Wait Recycle          | I Enabled                 |  |
| Monitors (+)   |                 | Zero Window Timeout   | Specify 20000 milliseconds |                           |  |
|  | Traffic Class   | ÷   |                            |                           |  |
| Address Translation  |                 | Memory Management   |                            |                           |  |
|  |                 | Auto Proxy Buffer   |                            |                           |  |
| Acceleration   |                 | Auto Receive Window   |                            |                           |  |
|  |                 | Auto Send Buffer  |                            |                           |  |

TMSH command for asm1.site1:

## TMSH

tmsh create ltm profile tcp shared/example.com\_tcp\_profile defaults-from f5-tcp-lan

## 1.1.3.4 Health Monitor

Create a common health monitor

Navigate to: Local Traffic >> Monitors >> New Monitor...

| Hostname: asm1.site1.example.com Dat<br>IP Address: 10.1.10.14 Tim | e: Sep 14, 2017 User: <b>admin</b><br>e: 4:09 PM (CDT) Role: Administrator |
|--|--|
| In Sync  |  |
| Main Help About  | Local Traffic » Monitors   |
| Mage Statistics  | 🔅 🚽 Monitor List   |
| iApps  | * Search Create  |
| 😚 dns  | ✓     ▲ Name     ♦ Ap  |
| SSL Orchestrator   | gateway_icmp   |
| Docal Traffic  | http_head_f5   |
| Network Map  | https  |
| Virtual Servers  | 443  |
| Policies   | ttps_head_f5   |
| Profiles   |  |
| Ciphers  |  |
| iRules   |  |
| Pools  | i smp_oca  |
| Nodes  |  |
|  |  |
|  |  |

Create a health monitor on asm1.site1 according to the following table.

| Setting     | Value                            |
|-------------|----------------------------------|
| Name        | shared/example.com_https_monitor |
| Туре        | HTTPS                            |
| Send String | GET /login.php\r\n               |

| Hostname: asm1.site1.example.com<br>IP Address: 10.1.10.14 | m Date: Sep 14, 2017<br>Time: 4:14 PM (CDT) | User: <b>admin</b><br>Role: Administrator |
|--|---|---|
| ONLINE (ACTIVE)<br>In Sync                                 |   |   |
| Main Help Ab   | bout Local Traffic »                        | Monitors » New Monitor                    |
| Main Statistics  |   |   |
| i Anns   | General Properti                            | ties                                      |
|  | Name  | shared/example.com_https_monitor          |
| S DNS  | Description                                 |   |
| SSL Orchestrator   | Туре  |   |
|  | Parent Monitor                              | https 🔽                                   |
|  | Configuration:                              | Advanced V                                |
| Network Map  |   | 5 seconds                                 |
| Virtual Servers  |   |   |
| Policies   | Up Interval                                 | Disabled                                  |
| Profiles   | Time Until Up                               | 0 seconds                                 |
| Ciphers  | Timeout                                     | 16 seconds                                |
| iRules   | Manual Resume                               | e O Yes O No                              |
| Pools  |   | GET /login.php\r\n                        |
| Nodes  | Send String                                 |   |
| Monitors   | •   |   |
|  |   |   |

### TMSH command for asm1.site1:

```
tmsh create ltm monitor https shared/example.com_https_monitor send "GET /login.

→php\r\n"
```

https://support.f5.com/csp/article/K13397

## 1.1.3.5 Pools

Create a pool with a single member

Navigate to: Local Traffic >> Pools : Pool List

https://asm1.site1.example.com/tmui/Control/jspmap/tmui/locallb/pool/create.jsp

| Hostname: asm1.site1.example.com Date<br>IP Address: 10.1.10.14 Tim | e: Sep 14, 2017 User: <b>admin</b><br>e: 4:57 PM (CDT) Role: Administrator |
|---|--|
| In Sync   |  |
| Main Help About   | Local Traffic » Pools : Pool List  |
| Mage Statistics   | Pool List Statistics 🗵   |
| iApps   | * × Search Create  |
| S DNS   | Status Aname   |
| SSL Orchestrator  | No records to display. Delete  |
| Coral Traffic   |  |
| Network Map   |  |
| Virtual Servers   |  |
| Policies  |  |
| Profiles  |  |
| Ciphers   |  |
| iRules  |  |
| Pools 2 >   | Pool List 3  |
| Nodes Nodes   | Statistics   |
| Monitors 🕞  |  |

1. Create a pool on asm1.site1 according to the following table.

| Setting         | Value                                  |
|-----------------|--|
| Name            | shared/site1_adc_https_pool            |
| Health Monitors | shared/example.com_https_monitor       |
| New Members     | Node Name: shared/site1_adc_https_node |
| New Members     | Address: 10.1.50.100                   |
| Service Port    | 443                                    |

| Hostname: asm1.site1.example.com Da<br>IP Address: 10.1.10.14 Tin | te: Sep 14, 2017 User: admin<br>ne: 5:07 PM (CDT) Role: Administr | ator Partition: Common   |
|---|---|--|
| In Sync   |   |  |
| Main Help About   | Local Traffic » Pools : Pool Lis                                  | st » New Pool  |
| Statistics  | Configuration: Basic  |  |
| iApps   | Name  | shared/example.com_https_pool  |
| S DNS   | Description   |  |
| SSL Orchestrator  | Health Monitors   | Active Available           Active         Available           /Common/shared         < |
| Network Map   |   | L dup  |
| Virtual Servers >   | Resources   |  |
| Policies  | Load Balancing Method   | Round Robin  |
| Profiles  | Priority Group Activation   | Disabled   |
| Ciphers   |   | New Node      New FQDN Node      Node List   |
| iRules  |   | Node Name: shared/site1_adc_https_node (Optional)                                      |
| Pools >   |   | Address: 10.1.50.100 ×   |
| Nodes   |   | Service Port: 443 HTTPS  |
| Monitors 📀  | New Members   | R:1 P 0 C:0 site1 adc https node 10.1.50.100 :443                                      |
| Traffic Class   |   |  |
| Address Translation   |   |  |
| Acceleration  |   | Edit Delete  |

### TMSH command for asm1.site1

## TMSH

tmsh create ltm pool shared/site1\_adc\_https\_pool monitor shared/example.com\_https\_monitor members add { shared/site1\_adc\_https\_node:443 { address 10.1.50.100 } }

2. Create a pool on asm1.site1 according to the following table.

| Setting         | Value                                  |
|-----------------|--|
| Name            | shared/site2_adc_https_pool            |
| Health Monitors | shared/example.com_https_monitor       |
| New Members     | Node Name: shared/site2_adc_https_node |
| New Members     | Address: 10.1.60.100                   |
| Service Port    | 443                                    |

### TMSH command for asm1.site1

## TMSH

tmsh create ltm pool shared/site2\_adc\_https\_pool monitor shared/example.com\_https\_monitor members add { shared/site2\_adc\_https\_node:443 { address 10.1.60.100 } }

# 1.1.4 Virtuals

|                |                  | www.example.com |
|----------------|------------------|-----------------|
|                |                  |                 |
| Site1          |                  |                 |
| E              | xternal_vip: 203 | .0.113.9:443    |
| Load Balancer  |                  | ·····           |
| site1_waf_vlan | app              | 1_vlan          |
| 10.1.50.0/24   |                  | <u> </u>        |
|                |                  | 6 6 6           |
|                |                  |                 |
|                | 102              |                 |
|                |                  |                 |
|                |                  |                 |
|                |                  |                 |

An LTM VIP needs to be created in order to accept traffic from the ADC.

Navigate to: Local Traffic >> Virtual Servers : Virtual Server List >> New Virtual Server

| Main Help About     | Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server |                          |  |
|---------------------|--|--------------------------|--|
| Mage Statistics     |  |                          |  |
|                     | General Properties   |                          |  |
| TApps               | Name   | waf1_virtual             |  |
| S DNS               | Description  |                          |  |
| SSL Orchestrator    | Туре   | Standard                 |  |
| Contraffic          | Source Address   |                          |  |
|                     | Destination Address/Mask   | 10.1.50.101              |  |
| Virtual Servers     | Service Port   | 443 HTTPS 🔽              |  |
| Delision            | Notify Status to Virtual Address   |                          |  |
|                     | State  | Enabled V                |  |
| Profiles            |  |                          |  |
| Ciphers             | Configuration: Advanced  |                          |  |
| iRules              | Protocol   | TCP 🔽                    |  |
| Pools               | Protocol Profile (Client)  | example.com_tcp_profile  |  |
| Nodes               | Protocol Profile (Server)  | (Use Client Profile)     |  |
| Monitors            | HTTP Profile   | example.com_http_profile |  |
| Traffic Class (+)   | HTTP Proxy Connect Profile   | None                     |  |
| Address Translation | Traffic Acceleration Profile   | None                     |  |
| Acceleration        | FTP Profile  | None                     |  |
| Device Management   | RTSP Profile   | None                     |  |
| Security            | SOCKS Profile  | None                     |  |
| Jocumy              | Stream Profile   | None                     |  |
| Network             | XML Profile  | None                     |  |
| System              | MQTT   |                          |  |

Create VIPS on all four WAF devices according to the follwing tables

1. asm1.site1

| Setting                    | Value                            |
|----------------------------|----------------------------------|
| Name                       | site1_waf1_virtual               |
| Destination Address/Mask   | 10.1.50.101                      |
| Service Port               | 443                              |
| Protocol Profile (Client)  | shared/example.com_tcp_profile   |
| HTTP Profile               | shared/example.com_http_profile  |
| SSL Profile (Client)       | clientssl                        |
| SSL Profile (Server)       | serverssl                        |
| Source Address Translation | Auto Map                         |
| Default Pool               | pool shared/site1_adc_https_pool |

TMSH command for asm1.site1:

#### 2. asm2.site1

| Setting                    | Value                            |
|----------------------------|----------------------------------|
| Name                       | site1_waf2_virtual               |
| Destination Address/Mask   | 10.1.50.102                      |
| Service Port               | 443                              |
| Protocol Profile (Client)  | shared/example.com_tcp_profile   |
| HTTP Profile               | shared/example.com_http_profile  |
| SSL Profile (Client)       | clientssl                        |
| SSL Profile (Server)       | serverssl                        |
| Source Address Translation | Auto Map                         |
| Default Pool               | pool shared/site1_adc_https_pool |

### TMSH command for asm2.site1:

#### 3. asm1.site2

| Value                            |
|----------------------------------|
| site2_waf1_virtual               |
| 10.1.60.101                      |
| 443                              |
| shared/example.com_tcp_profile   |
| shared/example.com_http_profile  |
| clientssl                        |
| serverssl                        |
| Auto Map                         |
| pool shared/site2_adc_https_pool |
|                                  |

#### TMSH command for asm1.site2:

### 4. asm2.site2

| Setting                    | Value                            |
|----------------------------|----------------------------------|
| Name                       | site2_waf1_virtual               |
| Destination Address/Mask   | 10.1.60.102                      |
| Service Port               | 443                              |
| Protocol Profile (Client)  | shared/example.com_tcp_profile   |
| HTTP Profile               | shared/example.com_http_profile  |
| SSL Profile (Client)       | clientssl                        |
| SSL Profile (Server)       | serverssl                        |
| Source Address Translation | Auto Map                         |
| Default Pool               | pool shared/site2_adc_https_pool |

TMSH command for asm2.site2:

https://support.f5.com/kb/en-us/products/big-ip\_asm/manuals/product/asm-implementations-11-1-0/4. html#conceptid

# **1.1.5 Security Policy**

### 1.1.5.1 Sync

Configure global policy synchronization on asam1..site1 only

Navigate to: Security >> Options : Application Security : Synchronization : Application Security Synchronization

Modify "Device Group" to enable "example.com\_waf\_sync-group"



### 1.1.5.2 Parent Child

Finally.... Let's create a policy.

### Navigate to: Security >> Application Security : Security Policies : Policies List

Create a parent policy according to the following table

| Setting         | Value                     |
|-----------------|---------------------------|
| Policy Name     | example.com_parent_policy |
| Policy Type     | Parent                    |
| Policy Template | Rapid Deployment Policy   |



### https://asm1.site1.example.com/dms/policy/policies\_ng.php?create\_policy=1

Create a child policy according to the following table

| Setting         | Value                   |
|-----------------|-------------------------|
| Policy Name     | www.example.com_policy  |
| Policy Type     | Security                |
| Policy Template | Rapid Deployment Policy |
| Virtual Server  | site1_waf2_virtual      |



## 1.1.5.3 Associate Policy

Log into asm2.site1 asm1.site2 and asm2.site2 and associate the security policy to the VIPS. Navigate to: Local Traffic >> Virtual Servers : Virtual Server List >> site1\_waf2\_virtual Click Security and set "Application Security Policy" "Enabled" "www.example.com" Repeat steps for all ASM devices.

| Hostname: asm1.site1.example.com C<br>IP Address: 10.1.10.14 T | ate: Sep 14, 2017 User: admin<br>ime: 10:10 PM (CDT) Role: Admin | istrator                          |                                |
|--|--|-----------------------------------|--------------------------------|
| ONLINE (ACTIVE)<br>In Sync                                     |  |                                   |                                |
| Main Help About  | Local Traffic » Virtual Server                                   | s : Virtual Server List » site1_v | /at1_virtual                   |
| Statistics   | Properties Res   | ources Security                   |                                |
| iApps  | Policy Settings  | (                                 | e l                            |
| S DNS  | Destination  | 10.1.50.101:443                   |                                |
| SSI Orchestrator   | Service  | HTTPS                             |                                |
| 33E Orchestidio  | Application Security Policy                                      | Enabled Policy: www.ex            | ample.com                      |
| Local Traffic  | Service Policy   | None                              | 3                              |
| Network Map  | IP Intelligence  | Disabled 🔽                        |                                |
| Virtual Servers  | DoS Protection Profile   | Disabled 🗸                        |                                |
| Policie  |  | Enabled V                         |                                |
| Profiles >   |  | Selected                          | Available                      |
| Ciphers  | Log Profile  | Log all requests                  | Common<br>Log illegal requests |
| iRules   |  | >>                                | global-network<br>local-dos    |
| Pools  |  |                                   |                                |
| Nodes  | Update   |                                   |                                |
| Monitors (+)   |  |                                   |                                |
|  |  |                                   |                                |

https://asm2.site1.example.com/tmui/Control/jspmap/tmui/locallb/virtual\_server/security.jsp?name=/Common/site1\_waf2\_virtual

https://asm1.site2.example.com/tmui/Control/jspmap/tmui/locallb/virtual\_server/security.jsp?name=/Common/site2\_waf1\_virtual

https://asm2.site2.example.com/tmui/Control/jspmap/tmui/locallb/virtual\_server/security.jsp?name=/Common/site2\_waf2\_virtual

# 1.1.6 Cut-Over





Change the ADC load balancing configuration so that traffic goes through the WAF before the application server.

Make the following changes on both bigip1.site1 and bigip1.site2.

Navigate to: Local Traffic >> Virtual Servers : Virtual Server List >> isp2\_site2\_www.example.com\_tcp\_https\_virtual

Select "Resources" and associate the "site1\_waf\_https\_pool"

| Main          | Help             | About             | Local   | Traffic » Virtual S    | ervers : | Virtual Serv | er List » is | p2_site2_ | www.example | .com_tcp_http |
|---------------|------------------|-------------------|---------|------------------------|----------|--------------|--------------|-----------|-------------|---------------|
| Magaza Statis | tics             |                   | ÷ -     | Properties             | Resou    | rces         | Security     | -         | Statistics  |               |
| iAnns         |                  |                   |         |                        | 2        |              |              |           |             |               |
| Log mpps      |                  |                   | Load B  | Balancing              |          |              |              |           |             |               |
| 📔 Wizar       | ds               |                   | Defau   | ilt Pool               |          | site2_waf_h  | ttps_pool    | ~         |             |               |
| 😚 dns         |                  |                   | Defau   | It Persistence Profile | e        | None         | <b>_</b>     |           |             |               |
| 6             |                  |                   | Fallba  | ack Persistence Profi  | le       | None         | ~            |           |             |               |
| SSL (         | rcnestrator      |                   | Updat   | te                     |          |              |              |           |             |               |
| Local         | Traffic          |                   |         | _                      |          |              |              |           |             |               |
| Ne            | twork Map        |                   | iRules  |                        |          |              |              |           |             |               |
| Vir           | tual Servers     |                   | Name    |                        |          |              |              |           |             |               |
| F             | olicies          | •                 | No rec  | cords to display.      |          |              |              |           |             |               |
| F             | rofiles          |                   | Policie | 5                      |          |              |              |           |             |               |
| 0             | phers            |                   | Name    |                        |          |              |              |           |             |               |
| il            | Rules            |                   | No rec  | cords to display.      |          |              |              |           |             |               |
| F             | ools             | ÷                 |         |                        |          |              |              |           |             |               |
| 1             | lodes            | ÷                 |         |                        |          |              |              |           |             |               |
| Mo            | nitors           | ÷                 |         |                        |          |              |              |           |             |               |
| Tra           | ffic Class       | $( \Rightarrow )$ |         |                        |          |              |              |           |             |               |
| Ad            | dress Translatio | n →               |         |                        |          |              |              |           |             |               |
| <u></u>       |                  |                   |         |                        |          |              |              |           |             |               |

https://bigip1.site1.example.com/tmui/Control/jspmap/tmui/locallb/virtual\_server/properties.jsp?name=/Common/isp1\_site1\_www.example.com\_tcp\_https\_virtual

https://bigip1.site2.example.com/tmui/Control/jspmap/tmui/locallb/virtual\_server/properties.jsp?name=/Common/isp2\_site2\_www.example.com\_tcp\_https\_virtual



# 1.2 Policy Tuning

WAF policies and

Four dedicated WAF instances are deployed across two datacenters.

Each WAF device has already been licensed, and a base configuration including hostname, and DNS settings.

The dedicated WAF instances will be load balanced by the HA pair of F5 LTM's.

In this module we will complete the Layer 2 and Layer 3 connectivity.

# 1.3 Hack and Defend

Four dedicated WAF instances are deployed across two datacenters.

Each WAF device has already been licensed, and a base configuration including hostname, and DNS settings.

The dedicated WAF instances will be load balanced by the HA pair of F5 LTM's.

2 DNS

# 2.1 Availability

# 2.1.1 Network Map













# 2.1.2 System

A BIG-IP System needs to be prepared before creating a GSLB configuration. Administrative tasks including SNMP/DNS/NTP settings have already been completed. The task of creating a "Logging Profile" is the beginning of this class. Create a log publisher and a DNS logging profile and then associate the two objects. The DNS logging profile will then be associated to a DNS listener in a later task. For more information on DNS logging, please refer to the link below.

1. Create a "Log Publisher"



| Hostname: gtm1.site1.example.com Dat<br>IP Address: 10.1.10.13 Tim | e: Jul 20, 2017 User:<br>e: 12:39 PM (CDT) Role: | <b>admin</b><br>Administrator       | Р          |
|--|--|-------------------------------------|------------|
| ONLINE (ACTIVE) Standalone   |  |                                     |            |
| Main Help About  | System » Logs : Confi                            | guration : Log Publishers           |            |
| Market Statistics  | System   | Captured Transactions Packet Filter | GSLB Audit |
| iApps  |  | Click "Create"                      | Create     |
| S DNS  | 🖌 🗢 Name   |                                     | 5          |
| SSI Orchestrator   | default-ipsec-log-put                            | blisher                             |            |
| 33L Ofciestitutor  | local-db-publisher                               |                                     |            |
| Acceleration   | sys-db-access-publis                             | sher                                |            |
| Device Management  | sys-sso-access-publ                              | lisher                              |            |
|  | Delete   |                                     |            |
| Network  |  |                                     |            |
| System   |  |                                     |            |
| Configuration  |  |                                     |            |
| File Management  |  |                                     |            |
| Certificate Management   |  |                                     |            |
| Disk Management  |  |                                     |            |
| Software Management  |  |                                     |            |
| License  | / 1 \  |                                     |            |
| Resource Provisioning  |  |                                     |            |
| Platform   |  |                                     |            |
| High Availability  |  |                                     |            |
| Archives 🛞 🕨   |  | _                                   |            |
| Services   | System   |                                     |            |
| Preferences  | Captured Transactions                            |                                     |            |
| sFlow  | Packe Filter                                     | Options                             |            |
| SNMP >   | Local Traffic                                    | Remote Logging                      |            |
| Crypto Offioadin   | GSLB   | Log Filters 📀                       |            |
| Users  | Audit 3  | L 4 estinations                     |            |
| Logs   | Configuration >                                  | Log Publishers 💽                    |            |
| Logs 2   | Configuration                                    | Log Publishers 📀                    | Lub        |

Create a local syslog publisher according to the table below:

| Field        | Value                  |
|--------------|------------------------|
| Name         | local-syslog-publisher |
| Destinations | local-syslog           |

| Hostname: gtm1.site1.example.com Da<br>IP Address: 10.1.10.13 Tin | te: Jul 20, 2017 User: <b>admin</b><br>ne: 12:43 PM (CDT) Role: Administrator P |
|---|---|
| ONLINE (ACTIVE) Standalone  |   |
| Main Help About   | System » Logs : Configuration : Log Publishers                                  |
| Mage Statistics   |   |
| iApps   | Name local-syslog-publisher   |
| S DNS   | Description   |
| SSL Orchestrator  | Log Destinations  |
| Acceleration  | Selected Available  |
| Device Management   | Destinations  |
| Network   |   |
| System  | Cancel Repeat Finished  |
| Configuration   |   |
| File Management   |   |
| Certificate Management  |   |
| Disk Management   |   |
| Software Management   |   |

## TMSH command for both gtm1.site1 and gtm1.site2:

## TMSH

tmsh create sys log-config publisher local-syslog-publisher { destinations replace-all-with { localsyslog { } } }

### 2. Create a "Logging Profile"

Note: It is required to complete the following task on both gtm1.site1 and gtm1.site2

| Hostname: gtm1.site1.example.com Dat<br>IP Address: 10.1.10.13 Tim | e: Jul 20, 2017<br>e: 12:49 PM (CDT) | User: <b>admin</b><br>Role: Administrator |                  |                   |
|--|--------------------------------------|---|------------------|-------------------|
| ONLINE (ACTIVE)     Standalone                                     |                                      |   |                  |                   |
| Main Help About  | DNS » Delivery :                     | : Profiles : Other : DN                   | S Logging        |                   |
| Mage Statistics  | DNS                                  | Protocol                                  | ✓ Other ✓        |                   |
| iApps  | ŀ                                    |   | × Click "Create" | 5 Create          |
| S DNS  | Vame                                 |   |                  | \$ Lo             |
| Delivery   | Listeners                            | >   |                  |                   |
| GSLB 2   | Profiles                             | DNS                                       | $(\Rightarrow)$  |                   |
| Zones  | Load Balancing                       | Protocol                                  |                  |                   |
| Caches >   | iRules                               | Other                                     | DNS Logging      | $\odot$           |
| Settings   | Translation                          | 3   | 4 Persistence    | $\bigcirc$        |
| SSI Orchostrato  | Nameservers                          | ,   | Statistics       | $( \Rightarrow )$ |
| SSE Orchestrate  | Keys                                 | •   |                  |                   |
| Acceleration   |                                      |   |                  |                   |
| Device Management  |                                      |   |                  |                   |
| Network  |                                      |   |                  |                   |
| System   |                                      |   |                  |                   |

Create a new DNS logging profile as shown in the table below.

| Field            | Value                       |
|------------------|-----------------------------|
| Name             | example_dns_logging_profile |
| Log Publisher    | local-syslog-publisher      |
| Log Responses    | enabled                     |
| Include Query ID | enabled                     |

| Hostname: gtm1.site1.example.com Date<br>IP Address: 10.1.10.13 Time | :: Jul 20, 2017 User: admin<br>e: 12:52 PM (CDT) Role: Administ | rator                       |
|--|---|-----------------------------|
| Standalone   |   |                             |
| Main Help About  | DNS » Delivery : Profiles : Othe                                | er : DNS Logging » New      |
| Magazine Statistics  |   |                             |
|  | General Properties  |                             |
| iApps  | Name  | example_dns_logging_profile |
| S DNS  | Description   | [                           |
| Delivery   | Configuration   |                             |
| GSLB   | Log Publisher   | local-syslog-publisher      |
| Zones  | Log Queries   | Enabled                     |
| Caches   | Log Responses   | Enabled                     |
| Settings   |   |                             |
| 0  | Log Fields  |                             |
| SSL Orchestrator   | Include Complete Answer   | Enabled                     |
|  | Include Query ID  | Enabled                     |
|  | Include Source  | ✓ Enabled                   |
| Device Management  | Include Timestamp   | I Enabled                   |
| Network  | Include View  | Enabled                     |
| System   | Cancel Repeat Finished  |                             |

### TMSH command for both gtm1.site1 and gtm1.site2:

### TMSH

tmsh create ltm profile dns-logging example\_dns\_logging\_profile enable-response-logging yes include-query-id yes log-publisher local-syslog-publisher

# 2.1.3 Settings

Configure a Sync-Group between our BIG-IP DNS servers. DNS-related configurations will replicate and be in a consistent state between both BIG-IP DNS servers at all times. Please see the article below for more information on BIG-IP DNS synchronization.

Note: This enables Config Sync on gtm1.site1 only. Config Sync for gtm1.site2 will be enabled at a later step.

| Hosticame: gtm1.site1.example.com Dat<br>P Address: 10.1.10.13 | e: Jul 20, 2017 User: ad<br>e: 12:19 PM (CDT) Role: Ad | <b>min</b><br>Pai   |  |  |  |  |
|--|--|---------------------|--|--|--|--|
| ONLINE (ACTIVE)<br>Standalone                                  |  |                     |  |  |  |  |
| Main Help About  | DNS » Settings : GSLB : (                              | General             |  |  |  |  |
| Magazina Statistics  | 🚓 🗸 Delivery 🔻   | GSLB - Zones Caches |  |  |  |  |
| iApps  | Configuration Synchronizat                             | ion                 |  |  |  |  |
| S DNS  | Synchronize  |                     |  |  |  |  |
| Delivery   | Group Name   | EXAMPLE_group       |  |  |  |  |
| GSLB   | Time Tolerance   | 10 seconds          |  |  |  |  |
| Zones  | Synchronize DNS Zone File                              | s 🔽 🗲 🗕             |  |  |  |  |
| Caches >   | Configuration Save                                     |                     |  |  |  |  |
| Settings →   | Delivery >   | ☑ Enabled           |  |  |  |  |
| B ssi orah   | GSLB   | General             |  |  |  |  |
| SSL Orchistrator   | Zones  | Load Balancing      |  |  |  |  |
| Acceleration   | Acceleration Carnes Metrics Collection                 |                     |  |  |  |  |
| Auto-Discover  |  |                     |  |  |  |  |
| Device Management  | Request Interval                                       | 30 seconds          |  |  |  |  |
| Retwork  | Monitoring   |                     |  |  |  |  |
| System   | Heartbeat Interval                                     | 10 seconds          |  |  |  |  |

Configure the global settings for GSLB according to the following table:

| Field                      | Value         |
|----------------------------|---------------|
| Synchronize                | checked       |
| Group Name                 | EXAMPLE_group |
| Synchronize DNS Zone Files | checked       |

The above work may alternatively be completed using the command line. Using Putty log into gtm1.site1 and issue the following command.

### TMSH

tmsh modify gtm global-settings general synchronization yes synchronization-group-name EXAM-PLE\_group synchronize-zone-files yes

# 2.1.4 Listeners

A listener object is a specialized BIG-IP DNS virtual server that is configured to respond to DNS queries. Without a listener, the BIG-IP DNS server has no open socket to 'listen' for queries.

Create both a TCP and UDP listener. UDP is the standard for DNS name resolution, and TCP is used when a DNS response greater than 4096 bytes in size is required as well as for zone transfers.



### 2.1.4.1 DNS Profile

Configure a DNS profile to associate with the listener we have just created. The DNS profile is where we define how to handle the DNS traffic received by the listener, this includes DNS specific features such as DNSSEC, DNS Express and many others. For more information on DNS profiles, please refer to the link below.

Note: It is required to complete the following task on both gtm1.site1 and gtm1.site2

| Hostname: gtm1.site1.example.com Da<br>IP Address: 10.1.10.13 Tit | ate: Jul 20, 2017<br>me: 12:57 PM (CDT) | User: <b>admin</b><br>Role: Administrator |                 |        |
|---|---|---|-----------------|--------|
| ONLINE (ACTIVE) Standalone  |   |   |                 |        |
| Main Help About   | DNS » Delivery :                        | Profiles : DNS                            |                 |        |
| Statistics  | t‡r ▼ DNS                               | Protocol                                  | Other     Other | ato"   |
| iApps   | ř                                       |   | × Search        | Create |
| 😚 dns   | ✓ ▲ Name                                |   |                 | 4 ÷ Ar |
| Delivery 1  | Listeners                               | •   |                 |        |
| GSLB  | Profiles                                | DNS                                       | Θ               |        |
| Zones   | 2 load Balancing                        | 3 otocol                                  | •               |        |
| Caches  | iRules                                  | Other                                     |                 |        |
| Settings  | Translation                             | •   |                 |        |
| E SSI Orahadrate  | Nameservers                             | •   |                 |        |
| SSL OICHESTRON  | Keys                                    | •   |                 |        |
| Acceleration  |   |   |                 |        |
| Device Management   |   |   |                 | c      |
| Network   |   |   |                 | _      |
| System  |   |   |                 |        |

Create a new DNS profile as shown in the following table.

| Field                      | Value                        |
|----------------------------|------------------------------|
| Name                       | example.com_dns_profile      |
| DNSSEC                     | Disabled                     |
| DNS Express                | Disabled                     |
| Unhandled Query Action     | Drop                         |
| Use BIND Server on Big-IP  | Disabled                     |
| Logging                    | Enabled                      |
| Logging Profile            | example_dns_logging_profile  |
| AVR statistics Sample Rate | Enabled, 1/1 queries sampled |

| Main Help About   | DNS » Delivery : Profiles : DN | S » Properties : example.com_dns_profile |         |
|-------------------|--------------------------------|--|---------|
| Array Statistics  | 🔅 🚽 Properties                 |  |         |
| iAnne             |                                |  |         |
| Co netro          | General Properties             |  |         |
| S DNS             | Name                           | example.com_dns_profile                  |         |
| Delivery          | Partition / Path               | Common                                   |         |
| GSLB →            | Parent Profile                 | dns 🔽                                    |         |
| Zones >           | Denial of Service Protection   | Ci                                       | ustom 🗌 |
| Caches            | Rapid Response Mode            | Disabled                                 |         |
| Settings          | Rapid Response Last Action     | Drop                                     |         |
| Acceleration      | Hardware Acceleration          |  |         |
| Device Management | Protocol Validation            | Disabled                                 |         |
|                   | Response Cache                 | Disabled                                 |         |
| Network           | DNS Features                   |  |         |
| System            | DNSSEC                         |  | → 🛛     |
|                   | GSLB                           | Enabled V                                |         |
|                   | DNS Express                    |  | → 🗹     |
|                   | DNS Cache                      | Disabled 🔽                               |         |
|                   | DNS Cache Name                 | Select                                   |         |
|                   | DNS IPv6 to IPv4               | Disabled V                               |         |
|                   | Unhandled Query Actions        | Drop                                     | → 🛛     |
|                   | Use BIND Server on BIG-IP      |  | →       |
|                   | DNS Traffic                    |  |         |
|                   | Zone Transfer                  | Disabled 🔽                               |         |
|                   | DNS Security                   | Disabled 🔽                               |         |
|                   | DNS Security Profile Name      | Select                                   |         |
|                   | Process Recursion Desired      | Enabled 🔽                                |         |
|                   | Logging and Reporting          |  |         |
|                   | Logging                        |  |         |
|                   | Logging Profile                | example_dns_logging_profile              | V       |
|                   | AVR Statistics Sample Rate     | Enabled 1/ 1 queries sampled             | → 2     |

TMSH command for both gtm1.site1 and gtm1.site2:

### TMSH

tmsh create ltm profile dns example.com\_dns\_profile use-local-bind no unhandled-query-action drop logprofile example\_dns\_logging\_profile enable-logging yes avr-dnsstat-sample-rate 1 enable-dns-express no enable-dnssec no

### 2.1.4.2 UDP Profile

Next, we are going to define a UDP profile. A UDP profile will instruct the BIG-IP DNS listener on how to handle UDP traffic. The DNS profile we created earlier instructs the BIG-IP DNS on how to process the

layer 7 data inside of the UDP packets, but not how to handle the UDP protocol itself. For more information on UDP profiles, please refer to the link below.

| Note: | It is rec | uired to | complete | the follo | owing t | task on | both | gtm1. | site1 | and g | gtm1. | .site2 |
|-------|-----------|----------|----------|-----------|---------|---------|------|-------|-------|-------|-------|--------|
|       |           |          |          |           | · · · · |         |      | ~     |       |       | -     |        |

| Hostname: gtm1.site1.example.com Da<br>IP Address: 10.1.10.13 Tin | te: Jul 20, 2017 User: a<br>ne: 1:11 PM (CDT) Role: a | <b>admin</b><br>Administrator |                |
|---|---|-------------------------------|----------------|
| ONLINE (ACTIVE) Standalone  |   |                               |                |
| Main Help About   | DNS » Delivery : Profil                               | es : Protocol : UDP           | Click "Create" |
| Mage Statistics   | DNS   | Protocol - Other              |                |
| iApps   | *   | × Search                      | 5 Create       |
| S DNS   | ✓ ♦ Name  |                               | ÷.             |
| Delivery 💦  | Listeners   |                               |                |
| GSLB  | Profiles •  | DNS 📀                         |                |
| Zones   | 2 Load Balancing                                      | Protocol                      | UDP 💿          |
| Caches  | iRules  | <sup>3</sup> Other 4          | тср            |
| Settings  | ranslation  |                               |                |
| E SSI Orchestrator  | Nameservers   |                               |                |
| SSE Orchestrator  | Keys >  |                               |                |
| Acceleration  |   |                               |                |
| Device Management   |   |                               |                |
| Retwork   |   |                               |                |
| System  |   |                               |                |

Create a new UDP profile as shown in the following table:

| Field          | Value                       |
|----------------|-----------------------------|
| Name           | example.com_udp-dns_profile |
| Parent Profile | udp_gtm_dns                 |

### **Reference Architecture Documentation**

| Hostname: gtm1.site1.example.com Da<br>IP Address: 10.1.10.13 Tir | te: Jul 26, 2018 User: admin<br>ne: 8:17 AM (EDT) Role: Administr | ator Partition: Common        | Log out   |
|---|---|-------------------------------|-----------|
| ONLINE (ACTIVE)<br>Standalone                                     |   |                               | 1         |
| Main Help About   | DNS » Delivery : Profiles : Pro                                   | tocol : UDP » New UDP Profile |           |
| Statistics  | 0   |                               |           |
| iApps   | Name  | example.com_udp-dns_profile   |           |
| 😚 dns   | Parent Profile  | udp_gtm_dns                   |           |
| Delivery  | Settings  |                               | Custom 🗌  |
| GSLB  | Proxy Maximum Segment   |                               |           |
| Zones   | Idle Timeout  | Specify 🖌 5                   | seconds 🗌 |
| Caches  | IP ToS  | Specify 🗸 0                   |           |
| Settings  | Link QoS  | Specify 🗸 0                   |           |
| Acceleration  | Datagram LB   | Enabled                       |           |
|   | Allow No Payload  |                               |           |
| Device Management   | TTL Mode  | Proxy 🗸                       |           |
| Network   | Don't Fragment Mode   | PMTU 🔽                        |           |
| System  | Max Buffer Bytes  | 655350                        |           |
|   | Max Buffer Packets  | 0                             |           |

TMSH command for both gtm1.site1 and gtm1.site2:

### TMSH

tmsh create ltm profile udp example.com\_udp-dns\_profile defaults-from udp\_gtm\_dns

### 2.1.4.3 TCP Profile

Similarly, we will need to define a TCP profile. A TCP profile will instruct the BIG-IP DNS listener on how to handle TCP traffic. For more information on TCP profiles, please refer to the link below.

Note: It is required to complete the following task on both gtm1.site1 and gtm1.site2

| Hostname: gtm1.site1.example.com Da<br>IP Address: 10.1.10.13 Ti | ate: Jul 20, 2017<br>me: 1:19 PM (CDT) | User: <b>admin</b><br>Role: Administrator |            | Partition: Common        |
|--|--|---|------------|--------------------------|
| ONLINE (ACTIVE) Standalone                                       |  |   |            |                          |
| Main Help About  | DNS » Delivery                         | : Profiles : Protocol : T(                | CP         |                          |
| Statistics   | DNS                                    | Protocol                                  | • Click "C | reate"                   |
| iApps  | <b>h</b>                               | \$  | Search     | Create                   |
| S DNS  | I                                      |   |            | Application     Parent F |
| Delivery 1   | Listeners                              | ⊧t-tcp                                    |            | tcp-legacy               |
| GSLB   | Profiles                               | DNS                                       | ÷          | tcp-legacy               |
| Zones >  | <sup>2</sup> oad Balancing             | Protocol                                  | ► UDP      | (+) tcp                  |
| Caches   | iRules                                 | 3 Other                                   | ТСР        | • tcp                    |
| Settings   | Translation                            |   | - 4        | tcp                      |
| Gauge  | Nameservers                            | ed  |            | tcp-legacy               |
| SSL Orchestrator   | Keys                                   | ⊧p  |            | tcp-wan-op               |
| Acceleration   | 🖾 tcp                                  |   |            | (none)                   |
| Douico Managoment  | tcp-lan-optim                          | nized                                     |            | tcp-legacy               |
|  | tcp-legacy                             |   |            | tcp                      |
| Retwork  | tcp-mobile-o                           | ptimized                                  |            | tcp-legacy               |
| Ta System  | tcp-wan-opti                           | mized                                     |            | tcp-legacy               |

Create a new TCP profile as shown in the following table.

| Field          | Value                       |
|----------------|-----------------------------|
| Name           | example.com_tcp-dns_profile |
| Parent Profile | f5-tcp-wan                  |

| Hostnam<br>IP Addre | e: gtm1.site1.example.com<br>ss: 10.1.10.13 | Date: Jul 20, 2017 U<br>Time: 1:23 PM (CDT) F | lser: <b>admin</b><br>Role: Administrator |                           | Partition: Common |
|---------------------|---|---|---|---------------------------|-------------------|
| 6                   | ONLINE (ACTIVE)<br>Standalone               |   |   |                           |                   |
| Main                | Help About                                  | DNS » Delivery :                              | Profiles : Protocol                       | : TCP » New TCP Profile   |                   |
| Mag Stat            | tistics                                     |   |   |                           |                   |
| iAn                 | ns  | General Properties                            |   |                           |                   |
| Log mp              | ha  | Name  | ex  | ample.com_tcp-dns_profile |                   |
| S DN                | S   | Parent Profile                                |   | tcp-wan                   | $\overline{}$     |
| C                   | Delivery                                    | Timer Management                              |   |                           |                   |
| 0                   | GSLB  | Close Wait                                    | Spe                                       | cify 🔽 5                  | seconds           |
| Z                   | Zones                                       | Fin Wait 1                                    | Spe                                       | cify 🔽 5                  | seconds           |
| (                   | Caches                                      | Fin Wait 2                                    | Spe                                       | cify 🔽 300                | seconds           |
|                     | Settings                                    | Idle Timeout                                  | Spe                                       | cify 🗸 300                | seconds           |
| SSL                 | Orchestrator                                | Keep Alive Interval                           | Spe                                       | cify 🔽 1800               | seconds           |
| 🔗 Acc               | celeration                                  | Minimum RTO                                   | 500                                       | ) milliseconds            |                   |
| Dev                 | rice Management                             | Reset On Timeout                              | ⊡ E                                       | nabled                    |                   |
|                     |   | Time Wait                                     | Spe                                       | cify 🔽 2000               | milliseconds      |
| Net                 | work  | Time Scroll v                                 | vav.down                                  | to find the "Fir          | ish" button       |
| Svs                 | tem   | Zero Window Time                              | out Spe                                   | cify 20000                | milliseconds      |

TMSH Command for both gtm1.site and gtm1.site2:

## TMSH

tmsh create ltm profile tcp example.com\_tcp-dns\_profile defaults-from f5-tcp-wan

## 2.1.4.4 UDP IP Address

We will now begin to put the pieces together. In this task, we will integrate the logging, DNS and UDP profiles we created earlier with an IP address. The IP address configured on the BIG-IP DNS will listen for queries and process them in accordance with the associated profiles.

### Note: It is required to complete the following task on both gtm1.site1 and gtm1.site2
| Hostname: gtm1.site1.example.com Dat<br>IP Address: 10.1.10.13 Tim | e: Jul 20, 2017 User: a<br>le: 1:29 PM (CDT) Role: A | i <b>dmin</b><br>Administrator | Partition: Common |
|--|--|--------------------------------|-------------------|
| ONLINE (ACTIVE)<br>Standalone                                      |  |                                |                   |
| Main Help About  | DNS » Delivery : Listen                              | ers : Listener List            | Click "Create"    |
| Magazine Statistics  | 🔅 👻 Listener List                                    | Statistics 🗵                   |                   |
| iApps  | ¢  | × Search                       | Create            |
| 😚 dns  | State 🗢 Name   |                                | ▲ Destination ♦ F |
| Delivery   | Listeners  | Listener List 📀                |                   |
| GSLB   | Profiles   | Statistics 🗵                   |                   |
| Zones  | Load Balancing >                                     |                                |                   |
| Caches   | iRules >   |                                |                   |
| Settings   | Translation >  |                                |                   |
| SSI Orchonor   | Nameservers  |                                |                   |
| SSE OTCHERINGTON   | Keys >   |                                |                   |
| Acceleration   |  |                                |                   |
| Device Management  |  |                                |                   |
| Network  |  |                                |                   |
| System   |  |                                |                   |

Create a UDP listener according to the following table:

| Field       |         | gtm1.site1                         | gtm1.site2                                      |        |
|-------------|---------|------------------------------------|---|--------|
| Name        |         | isp1_site1_ns1.example.com_udp_53_ | vi <b>ispa</b> l_site2_ns2.example.com_udp_53_v | virtua |
| Destination |         | 203.0.113.8                        | 198.51.100.40                                   |        |
| Protocol    | Profile | example.com_udp-dns_profile        | example.com_udp-dns_profile                     |        |
| (Client)    |         |                                    |   |        |
| DNS Profile |         | example.com_dns_profile            | example.com_dns_profile                         | ]      |

| Hostname gtm1.site1.example.com Dat<br>IP Address: 10.1.10.13                            | e: Jul 20, 2017 User: admin<br>e: 1:32 PM (CDT) Role: Administra | ator Partition: Common                    |  |  |
|--|--|---|--|--|
| CONLINE (ACTIVE)<br>Standalone<br>Be su  | re to create 20  | 3.0.113.8 on gtm1.SITE1                   |  |  |
| Main         Help         About         DNS » Delivery : Listeners : Listener List » New |  |   |  |  |
| Statistics   | General  |   |  |  |
| iApps  | Name   | isp1_site1_ns1.example.com_udp_53_virtual |  |  |
| S DNS  | Description  |   |  |  |
| Delivery   | State  | Enabled V                                 |  |  |
| GSLB   | Listener: Advanced V   |   |  |  |
| Zones  |  | Type: • Host O Network                    |  |  |
| Caches   | Destination  | Address: 203.0.113.8                      |  |  |
| Settings   | Service Port   | DNS S3                                    |  |  |
| SSL Orchestrator   | VLAN Traffic   | All VLANs 🔽                               |  |  |
| Acceleration   | Source Address Translation                                       | None                                      |  |  |
|  | Address Translation  | Enabled                                   |  |  |
| Device Management  | Port Translation   | Enabled                                   |  |  |
| Retwork  | Route Advertisement  | Enabled                                   |  |  |
|  | Auto Last Hop  | Default                                   |  |  |
| System   | Last Hop Pool  | None                                      |  |  |
|  | Service: Advanced V  |   |  |  |
|  | Protocol   |   |  |  |
|  | Protocol Profile (Client)  | example.com_udp-dns_profile               |  |  |
|  | Protocol Profile (Server)  | (Use Client Profile)                      |  |  |
|  | DNS Profile  | example.com_dns_profile                   |  |  |

Make sure you create the IP addresses on the correct devices.

| Hostname gtm1.site2.example.com Date<br>IP Address: 10.1.10.23 | : Jul 20, 2017 User: admin<br>E: 1:32 PM (CDT) Role: Administra | tor Partition: Common                     |
|--|---|---|
| Main Help About  | O <b>Create 198.5</b><br>DNS » Delivery : Listeners : Lis       | 1.100.40 on gtm1.SITE2                    |
| Statistics   | 0l  |   |
| iApps  | Name  | isp1_site2_ns2.example.com_udp_53_virtual |
| S DNS  | Description   |   |
| Delivery   | State   | Enabled V                                 |
| GSLB   | Listener: Advanced V  |   |
| Zones  | Destination   | Type: O Host O Network                    |
| Caches   |   | Address: 198.51.100.40                    |
| Settings   | Service Port  | DNS 53                                    |
| SSL Orchestrator   | VLAN Traffic  | All VLANS 🔽                               |
| Acceleration   | Source Address Translation                                      | None                                      |
|  | Address Translation   | Enabled                                   |
| Device Management  | Port Translation  | Enabled                                   |
| Network  | Route Advertisement   | Enabled                                   |
|  | Auto Last Hop   | Default 🔽                                 |
| System   | Last Hop Pool   | None                                      |
|  | Service: Advanced   |   |
|  | Protocol  |   |
|  | Protocol Profile (Client)                                       | example.com_udp-dns_profile               |
|  | Protocol Profile (Server)                                       | (Use Client Profile)                      |
|  | DNS Profile   | example.com_dns_profile                   |

gtm1.site1 TMSH command:

#### TMSH

tmsh create gtm listener isp1\_site1\_ns1.example.com\_udp\_53\_virtual address 203.0.113.8 ip-protocol udp mask 255.255.255.255 port 53 profiles add { example.com\_dns\_profile example.com\_udp-dns\_profile }

gtm1.site2 TMSH command:

#### TMSH

tmsh create gtm listener isp1\_site2\_ns2.example.com\_udp\_53\_virtual address 198.51.100.40 ip-protocol udp mask 255.255.255.255 port 53 profiles add { example.com\_dns\_profile example.com\_udp-dns\_profile

}

https://support.f5.com/csp/article/K14923

#### 2.1.4.5 TCP IP Address

The IP address we configured in the previous task is not sufficient on its own in most cases. We need to also configure an IP address that is associated with a TCP profile to ensure that the BIG-IP DNS can process incoming TCP requests in addition to UDP.

Note: It is required to complete the following task on both gtm1.site and gtm1.site2

| Hostname: gtm1.site1.example.com Da<br>IP Address: 10.1.10.13 Tir<br>ONLINE (ACTIVE)<br>Standalone | te: Jul 20, 2017 User:<br>ne: 1:29 PM (CDT) Role: | <b>admin</b><br>Administrator    | Partition: Common |
|--|---|----------------------------------|-------------------|
| Main Help About  | DNS » Delivery : Lister<br>☆  → Listener List     | eners : Listener List Statistics | Click "Create"    |
| iApps  | *   | × Search                         | Create            |
| S DNS  | State 🗢 Name                                      |                                  | ▲ Destination 💠 F |
| Delivery   | Listeners   | Listener List 💽                  |                   |
| GSLB   | Profiles  | Statistics                       |                   |
| Zones  | Load Balancing                                    | •                                |                   |
| Caches   | iRules  | Þ                                |                   |
| Settings   | Translation                                       | Þ                                |                   |
| 6 martin   | Nameservers                                       | Þ                                |                   |
| SSL Orchestrator   | Keys  | Þ                                |                   |
| Acceleration   |   |                                  |                   |
| Device Management  |   |                                  |                   |
| Network  |   |                                  |                   |
| System   |   |                                  |                   |

Create a TCP listener.

| Field       |         | gtm1.site1                          | gtm1.site2                                      |       |
|-------------|---------|-------------------------------------|---|-------|
| Name        |         | isp1_site1_ns1.example.com_tcp_53_v | irt <b>spat</b> _site2_ns2.example.com_tcp_53_v | irtua |
| Destination |         | 203.0.113.8                         | 198.51.100.40                                   |       |
| Protocol    | Profile | example.com_tcp-dns_profile         | example.com_tcp-dns_profile                     | 1     |
| (Client)    |         |                                     |   |       |
| DNS Profile |         | example.com_dns_profile             | example.com_dns_profile                         |       |

| Hostname gtm1.site1.example.com Date<br>IP Addres: 10.1.10.13 Tim | e: Jul 20, 2017 User: admin<br>e: 2:18 PM (CDT) Role: Administ | trator Partition: Common                         |
|---|--|--|
| Standalone Be SUI   | e to create 20   | 3.0.113.8 on gtm1.SITE1                          |
| Main Help About   | DNS » Delivery : Listeners : L                                 | istener List » New                               |
| Statistics  | General  |  |
| iApps   | Name   | isp1_site1_ns1.example.com_udp_53                |
| 😚 dns   | Description  |  |
| Delivery  | State  | Enabled V  |
| GSLB  | Listener: Advanced 🗸   |  |
| Zones >> Caches >>  | Destination  | Type:  Type: Host O Network Address: 203.0.113.8 |
| Settings  | Service Port   | DNS 🔽 53   |
| SSL Orchestrator  | VLAN Traffic   |  |
|   | Source Address Translation                                     | None   |
| Acceleration  | Address Translation  | Enabled  |
| Device Management   | Port Translation   | Enabled  |
| Retwork   | Route Advertisement  | Enabled  |
| E Sustem  | Auto Last Hop  | Default Be sure to select "ICP"                  |
| System  | Last Hop Pool  | None   |
|   | Service: Advanced  |  |
|   | Protocol   | TCP  |
|   | Protocol Profile (Client)                                      | example.com_tcp-dns_profile                      |
|   | Protocol Profile (Server)                                      | (Use Client Profile)                             |
|   | DNS Profile  | example.com_dns_profile                          |
|   | Load Balancing   |  |
|   | Default Pool   | None   |
|   | Default Persistence Profile                                    | None   |
|   | Fallback Persistence Profile                                   | None   |

Be sure to create the 198.51.100.40 address on gtm1.site2

| Hostname gtm1.site2.example.com Dat<br>IP Addres: 10.1.10.23 Tim | e: Jul 20, 2017 User: <b>admin</b><br>e: 2:18 PM (CDT) Role: Administr | rator Partition: Common                        |
|--|--|--|
| CONLINE (ACTIVE)<br>Standalone<br>Be sure                        | to create 198.   | 51.100.40 on gtm1.SITE2                        |
| Main Help About  | DNS » Delivery : Listeners : L   | istener List » New                             |
| Statistics   | General  |  |
| iApps  | Name   | isp1_site2_ns2.example.com_udp_53              |
| 😚 dns  | Description  |  |
| Delivery   | State  | Enabled V                                      |
| GSLB   | Listener: Advanced   |  |
| Zones Caches   | Destination  | Type: Host O Network<br>Address: 198.51.100.40 |
| Settings   | Service Port   | DNS 🔽 53                                       |
| SSL Orchestrator   | VLAN Traffic   | All VLANs 🔽                                    |
|  | Source Address Translation   | None   |
|  | Address Translation  | Enabled  |
| Device Management  | Port Translation   | Enabled  |
| Retwork  | Route Advertisement  | Enabled  |
|  | Auto Last Hop  | Default Be sure to select "TCP"                |
| System   | Last Hop Pool  | None   |
|  | Service: Advanced V  |  |
|  | Protocol   | TCP  |
|  | Protocol Profile (Client)  | example.com_tcp-dns_profile                    |
|  | Protocol Profile (Server)  | (Use Client Profile)                           |
|  | DNS Profile  | example.com_dns_profile                        |
|  | Load Balancing   |  |
|  | Default Pool   | None   |
|  | Default Persistence Profile  | None   |
|  | Fallback Persistence Profile   | None   |

gtm1.site1 TMSH command:

#### TMSH

tmsh create gtm listener isp1\_site1\_ns1.example.com\_tcp\_53\_virtual address 203.0.113.8 ip-protocol tcp mask 255.255.255.255 port 53 profiles add { example.com\_dns\_profile example.com\_tcp-dns\_profile }

gtm1.site2 TMSH command:

#### TMSH

tmsh create gtm listener isp1\_site2\_ns2.example.com\_tcp\_53\_virtual address 198.51.100.40 ip-protocol tcp mask 255.255.255.255 port 53 profiles add { example.com\_dns\_profile example.com\_tcp-dns\_profile }

## 2.1.5 Data Centers

#### 2.1.5.1 Servers

#### 2.1.5.1.1 gtm1.SITE1

The first server we will create is that of gtm1.site1. It is required that we add both gtm1.site1 and gtm1.site2 to establish confgiuration synchronization between them.

| Field           | Value                                |
|-----------------|--------------------------------------|
| Name            | gtm1.site1_server                    |
| Data Center     | site1_datacenter                     |
| Devices Add:    | gtm1.site1.example.com : 203.0.113.7 |
| Health Monitors | bigip                                |

#### 1. Fill in the Name and Datacenter

| Hostname: gtm1.site1.example.com Date:<br>IP Address: 10.1.10.13 Time: | Jul 20, 2017 User: admir<br>2:29 PM (CDT) Role: Admir | n<br>nistrator             | Parti    |
|--|---|----------------------------|----------|
| CONLINE (ACTIVE)<br>Standalone   |   |                            |          |
| Main Help About  | DNS » GSLB : Servers : Se                             | rver List » New Server     |          |
| Statistics   | Conoral Properties                                    |                            |          |
| iApps  | Name  | gtm1.site1_server          |          |
| S DNS  | Product   | BIG-IP System              |          |
| Delivery   | Data Center   | → site1_datacenter         |          |
| GSLB   | Prober Preference                                     | Inherit From Data Center 🗸 |          |
| Zones  | Prober Fallback                                       | Inherit From Data Center 🗸 |          |
| Caches   | State   | Enabled 🔽                  |          |
| Settings   | Devices   | - Click-"Ad                | d"       |
| SSL Orchestrator   | Add   |                            | <b>.</b> |
| Acceleration   |   | Device Name                | Address  |
| Device Management  | BIG-IP<br>System<br>Devices                           | In table                   |          |
| Network  |   |                            |          |
| System   | Edit Delete   |                            |          |

2. Click the "Add" button to define IP addresses

| Hostname: gtm1.site1.example.com<br>IP Address: 10.1.10.13 | Date: Jul 20, 2017<br>Time: 2:36 PM (CDT) | User: <b>admin</b><br>Role: Administrator |                                   | Parti      |
|--|---|---|-----------------------------------|------------|
| ONLINE (ACTIVE)<br>Standalone                              |   |   |                                   |            |
| Main Help About  | DNS » GSLI                                | B : Servers : Server List                 | » New Server                      |            |
| Ma Statistics  |   | Ad  | d BIG-IP System Device            |            |
| iApps  | General Prope                             | Dev                                       | vice Name: gtm1.site1.example.com |            |
| S DNS  | Product                                   | Add<br>Tra                                | Instation:                        | (Optional) |
| Delivery   | Click"A                                   |   | k: Auto-Select 🗸                  |            |
| GSLB   | Prober Prefer                             | ence A                                    | Add 3                             |            |
| Zones  | Prober Fallba                             | ck 201                                    | 3.0.113.7                         |            |
| Caches   | > State                                   |   |                                   |            |
| Settings   | •   |   |                                   |            |
| e  | Devices                                   | D   | elete                             |            |
| SSL Orchestrator   | Ac  | bt  | 0                                 | K Cancel   |
| Acceleration   | BIG-IP                                    | D€<br>o data available in table           |                                   |            |
| Device Management  | System                                    |   |                                   |            |
| Network  | Levices                                   |   | Click"OK"                         |            |
| System   | Ec  |   |                                   |            |

3. Complete the form and associate the "bigip" "Health Monitor"

| Hostname: gtm1.site1.example.com Dat<br>IP Address: 10.1.10.13 Tin      | te: Jul 20, 2017 User: admin<br>ne: 2:43 PM (CDT) Role: Adminis  | strator Parti  |
|---|--|--|
| ONLINE (ACTIVE)<br>Standalone   |  |  |
| Main Help About   | DNS » GSLB : Servers : Serv  | ver List » New Server  |
| Statistics  | General Properties   |  |
| iApps   | Name   | gtm1.site1_server  |
| 😚 dns   | Product  | BIG-IP System  |
| Delivery  | Data Center  | site1_datacenter   |
| GSLB  | Prober Preference  | Inherit From Data Center   |
| Zones   | Prober Fallback  | Inherit From Data Center   |
| Caches  | State  | Enabled  |
| Settings  | Devices  |  |
| SSL Orchestrator   Acceleration   Device Management   Network   Vetwork | Add<br>BIG-II<br>System<br>Devices<br>Edit Delete<br>Configuration: Advanced<br>Health Monitors<br>Availability Requirements<br>Limit Settings<br>iQuery Options | Device Name       Address         .com       203.0.113.7         Selected       Available         //Common       gtp         bigip       <         >>       //Common         gtp       http         http          Bits:       Disabled          Packets:       Disabled          Current Connections:       Disabled          Service Check        Path         Path       ✓ |

#### TMSH

tmsh create gtm server gtm1.site1\_server datacenter site1\_datacenter devices add { gtm1.site1.example.com { addresses add { 203.0.113.7 } } } monitor bigip product bigip

# 2.1.5.1.2 gtm1.SITE2

Continue the same configuration for gtm1.site2.

| Hostname: gtm1.site1.example.com Da<br>IP Address: 10.1.10.13 Ti | ite: Jul 20, 2017 User: admi<br>ne: 2:47 PM (CDT) Role: Admi | <b>n</b><br>inistrator     |             |                  | P         |
|--|--|----------------------------|-------------|------------------|-----------|
| ONLINE (ACTIVE) Standalone                                       |  |                            |             |                  |           |
| Main Help About  | DNS » GSLB : Servers : Se                                    | erver List                 |             |                  |           |
| Mage Statistics  | 🚓 👻 Server List 🛛 T  | rusted Server Certificates | Statistics  |                  |           |
| iApps  | ŕ  | × Search                   |             | Cre              | eate      |
| S DNS  | Status 🔺 Name  | Device                     | es Address  | Dota Center      | Virtual : |
| Delivery   | gtm1.site1_s   | server 1                   | 203.0.113.7 | site1_datacenter | 0         |
| GSLB   | Enable Disable Delete.                                       |                            |             |                  |           |
| Zones  | CI   | ick/"Croate".te            | dofino a    | tm1 cito?        |           |
| Caches   |  | ICK-Create-II              | denne g     | un r.sitez       | 9         |
| Settings   |  |                            |             |                  |           |
| SSL Orchestrator   |  |                            |             |                  |           |
| Acceleration   |  |                            |             |                  |           |
| Device Management  |  |                            |             |                  |           |
| Retwork  |  |                            |             |                  |           |
| System   |  |                            |             |                  |           |

| Field           | Value                                  |
|-----------------|--|
| Name            | gtm1.site2_server                      |
| Data Center     | site2_datacenter                       |
| Devices Add:    | gtm1.site2.example.com : 198.51.100.39 |
| Health Monitors | bigip                                  |

1. Fill in the Name and Datacenter

| Hostname: gtm1.site1.example.com Date<br>IP Address: 10.1.10.13 Time | e: Jul 20, 2017<br>e: 3:18 PM (CE | User:<br>(T) Role: | <b>admin</b><br>Administrato |                            | Parti   |
|--|-----------------------------------|--------------------|------------------------------|----------------------------|---------|
| ONLINE (ACTIVE)<br>Standalone  | DNS G                             | CI D · Convor      | s · Copyor I                 | iet Now Sociar             |         |
| Main Help About  | DNS » G                           | SLD: Server        | s : Server L                 | list » New Server          |         |
| Stausues   | General Pro                       | operties           |                              |                            |         |
| iApps  | Name 🔹                            |                    |                              | gtm1.site2_server          |         |
| 😚 dns  | Product                           |                    |                              | BIG-IP System              |         |
| Delivery   | Data Cen                          | ter                |                              | site2_datacenter           |         |
| GSLB →   | Prober Pre                        | eference           |                              | Inherit From Data Center 🗸 |         |
| Zones  | Prober Fa                         | lback              |                              | Inherit From Data Center 🗸 |         |
| Caches   | State                             |                    |                              | Enabled 🗸                  |         |
| Settings   | Devices                           |                    |                              |                            |         |
| SSL Orchestrator   | Devices                           | Add                |                              |                            |         |
|  |                                   |                    | Devi                         | ice Name                   | Address |
| Acceleration   | BIG-IP                            | No data avai       | lable in tabl                | e                          |         |
| Device Management  | System<br>Devices                 |                    |                              |                            |         |
| Retwork  |                                   |                    |                              |                            |         |
| System   |                                   | Edit Delete        |                              |                            |         |

2. Click the "Add" button to define IP addresses

| Hostname: gtm1.site1.example.com Dat<br>IP Address: 10.1.10.13 Tim | e: Jul 20, 2017 User: <b>admin</b><br>e: 3:30 PM (CDT) Role: Administrator  | Parti |
|--|---|-------|
| ONLINE (ACTIVE) Standalone   |   |       |
| Main Help About  | DNS » GSLB : Servers : Server List » New Server   |       |
| Ma Statistics  | Add BIG-IP System Device  |       |
| iApps  | General Properties         Service Name: gtm1.site2.example.com           Name         Address:         198.51,100.39 |       |
| S DNS  | Product Translation: (Option  | al)   |
| Delivery   | Click Add Link: Auto-Select   |       |
| GSLB >   | Prober Preference Add   |       |
| Zones >  | Prober Fallback 298.51.100.39   | _     |
| Caches   | State   |       |
| Settings   | Devises   |       |
| SSL Orchestrator   | Add   |       |
|  | De OK Cancel  |       |
| ( Acceleration   | No data available in table  |       |
| Device Management  | System<br>Devices   |       |
| Network  |   |       |
| System   | Edit Delete   |       |

3. Complete the form and associate the "bigip" "Health Monitor"

| Hos<br>IP A | tname:<br>ddress: | gtm1.site1.exa<br>10.1.10.13 | mple.com | Date:<br>Time: | Jul 20, 2017<br>3:37 PM (CD | User: <b>adm</b> i<br>)T) Role: Adm | <b>in</b><br>inistrator |                                   |                                     |  |         | Parti |
|-------------|-------------------|------------------------------|----------|----------------|-----------------------------|-------------------------------------|-------------------------|-----------------------------------|-------------------------------------|--|---------|-------|
| (           | 5                 | ONLINE (AC                   | CTIVE)   |                |                             |                                     |                         |                                   |                                     |  |         |       |
| N           | Aain              | Help                         | About    |                | DNS » G                     | SLB : Servers : S                   | erver Lis               | t » New Serve                     | r                                   |  |         |       |
| <b>~</b>    | Statisti          | ics                          |          |                | General Pro                 | operties                            |                         |                                   |                                     |  |         |       |
|             | iApps             |                              |          |                | Name                        |                                     | g                       | tm1.site2_serve                   | r                                   |  |         |       |
| 5           | DNS               |                              |          |                | Product                     |                                     | В                       | IG-IP System                      | ~                                   |  |         |       |
|             | Deli              | very                         |          | •              | Data Cen                    | ter                                 | si                      | te2_datacenter                    | $\checkmark$                        |  |         |       |
|             | GSL               | B                            |          | •              | Prober Pre                  | eference                            | In                      | herit From Data                   | Center 🗸                            |  |         |       |
|             | Zone              | es                           |          | •              | Prober Fa                   | llback                              | In                      | herit From Data                   | Center 🗸                            |  |         |       |
|             | Cac               | hes                          |          | •              | State                       |                                     | E                       | nabled 🗸                          |                                     |  |         |       |
|             | Sett              | ings                         |          | •              | Devices                     |                                     |                         |                                   |                                     |  |         |       |
| 6           | SSL OI            | chestrator                   |          |                |                             | Add                                 | Devic                   | e Name                            |                                     | l l  | Address | 1     |
|             | Accele            | ration                       |          |                | BIGJE                       | gtm1.site2.examp                    | le.com                  |                                   |                                     | 198.51.100.39  | Э       |       |
|             | Device            | Managemen                    | t        |                | System<br>Devices           |                                     |                         |                                   |                                     |  |         |       |
|             | Networ            | ſk                           |          |                |                             |                                     |                         |                                   |                                     |  |         |       |
| 0           | System            | 1                            |          |                |                             | Edit Delete                         |                         |                                   |                                     |  |         |       |
|             |                   |                              |          |                | Configurat                  | on: Advanced 🗸                      | 1                       |                                   |                                     |  |         |       |
|             |                   |                              |          |                | Health Mo                   | nitors                              | → <sup>//C(</sup>       | Selected<br>ommon<br>igip         | <<                                  | Available<br>/Common<br>gateway_icm<br>gtp<br>http<br>http_head_f5 | p ^     |       |
|             |                   |                              |          |                | Availability                | Requirements                        | All                     | Health Monitors                   | $\checkmark$                        |  |         |       |
|             |                   |                              |          |                | Limit Setti                 | ngs                                 | Bits<br>Pac<br>Cur      | 3:<br>ckets:<br>rrent Connection: | Disabled<br>Disabled<br>s: Disabled |  |         |       |
|             |                   |                              |          |                | iQuery Op                   | tions                               | Ser<br>Pat<br>SN        | vice Check 🖌<br>th 🖌<br>MP 🖌      |                                     |  |         |       |
|             |                   |                              |          |                |                             |                                     |                         |                                   |                                     |  |         |       |

#### TMSH

tmsh create gtm server gtm1.site2\_server datacenter site2\_datacenter devices add { gtm1.site2.example.com { addresses add { 198.51.100.39 } } } monitor bigip product bigip

#### 2.1.5.1.3 site1\_ha-pair

We will now add both BIG-IP clusters to our list of servers. Doing so, allows the BIG-IP DNS to perform monitoring of each cluster to evaluate their capability to process traffic.

In this configuration we will enable both virtual server discovery and link discovery. Virtual server discovery allows BIG-IP DNS to find the list of all virtual servers that are created on each BIG-IP cluster, you will see the benefit of this later. Link discovery allows BIG-IP DNS to automatically add and monitor the upstream link that the BIG-IP LTM cluster is dependent on for Internet access; this can be then used to evaluate failover decision.

| Hostnan<br>IP Addre | ne: gtm1.site1.example.com<br>ess: 10.1.10.13 | Date:<br>Time: | Jul 20, 2017<br>3:49 PM (CDT) | User:<br>Role: | <b>admin</b><br>Administrator |              |               |                  |         |
|---------------------|---|----------------|-------------------------------|----------------|-------------------------------|--------------|---------------|------------------|---------|
| ß                   | ONLINE (ACTIVE)<br>Standalone                 |                |                               |                |                               |              |               |                  |         |
| Main                | Help About                                    |                | DNS » GSLB                    | : Servers      | : Server List                 |              |               |                  |         |
| Mage Sta            | tistics                                       |                | 🔅 👻 Server L                  | ist            | Trusted Server                | Certificates | Statistics    |                  |         |
| iAp                 | ops   |                | *                             |                |                               | Search       |               | C                | reate   |
| 😚 dn                | \$  |                | Status                        | ▲ Name         | )                             | Devices      | Address       | Data Center      | Virtual |
|                     | Deliverv                                      |                |                               | gtm1.sit       | e1_server                     | 1            | 203.0.113.7   | ate1_datacenter  | 0       |
|                     | GSI B   |                |                               | gtm1.sit       | e2_server                     | 1            | 198.51.100.39 | site2_datacenter | 0       |
|                     | Zones   | -<br>-         | Enable Disal                  | ble De         | lete                          |              |               |                  |         |
|                     | Caches  | •              |                               |                |                               | /            |               |                  |         |
|                     | Settings                                      | •              |                               |                | Cli                           | ck "Cre      | ate"          |                  |         |
| 🛱 ss                | L Orchestrator                                |                |                               |                |                               |              |               |                  |         |
| Acc                 | celeration                                    |                |                               |                |                               |              |               |                  |         |
| E Der               | vice Management                               |                |                               |                |                               |              |               |                  |         |
| e Net               | twork   |                |                               |                |                               |              |               |                  |         |
| Sys                 | stem  |                |                               |                |                               |              |               |                  |         |

| Field                    | Value                                  |
|--------------------------|--|
| Name                     | site1_ha-pair                          |
| Data Center              | site1_datacenter                       |
| Devices Add:             | bigip1.site1.example.com : 203.0.113.5 |
| Devices Add:             | bigip2.site1.example.com : 203.0.113.6 |
| Health Monitors          | bigip                                  |
| Virtual Server Discovery | Enabled                                |
| Link Discovery           | Enabled                                |

1. Fill in the Name and Datacenter

| Hostname: gtm1.site1.example.com Da<br>IP Address: 10.1.10.13 Tir  | ate: Jul 20, 2017<br>me: 3:58 PM (CDT) | User: <b>admin</b><br>Role: Administra | itor                       | Parti   |
|--|--|--|----------------------------|---------|
| ONLINE (ACTIVE)       Standalone       Main       Help       About | DNS » GSL                              | B : Servers : Server                   | List » New Server          |         |
| Statistics   | General Prop                           | erties                                 |                            |         |
| iApps  | Name 💻                                 |  | site1_ha-pair              |         |
| 😚 dns  | Product                                |  | BIG-IP System              |         |
| Delivery   | Data Center                            | $\rightarrow$                          | site1_datacenter           |         |
| GSLB →   | Prober Prefe                           | rence                                  | Inherit From Data Center 🗸 |         |
| Zones  | Prober Fallba                          | ack                                    | Inherit From Data Center 🗸 |         |
| Caches   | State                                  |  | Enabled 🗸                  |         |
| Settings   | Deviese                                |  |                            |         |
| SSL Orchestrator   | A                                      | dd 🔶                                   | Click "Add"                |         |
| Acceleration   |  | De                                     | vice Name                  | Address |
| Device Management  | BIG-IP<br>System<br>Devices            | o data available in ta                 | DIE                        |         |
| Retwork  |  |  |                            |         |
| System   | E                                      | dit Delete                             |                            |         |

2. Click the "Add" button to define IP addresses

| Hostname: gtm1.site1.example.com Da<br>IP Address: 10.1.10.13 Tir | ate: Jul 20, 2017 User: <b>admin</b><br>me: 4:33 PM (CDT) Role: Administrat | or Pa                    |
|---|---|--------------------------|
| ONLINE (ACTIVE) Standalone  |   |                          |
| Main Help About   | DNS » GSLB : Servers : Server I   | List » New Server        |
| Ma Statistics   |   | Add BIG-IP System Device |
| iApps   | General Properties  | Address: 203.0.113.5     |
| S DNS   | Product   | Translation: (Optional)  |
| Delivery  | Data Center   | Link: Auto-Select        |
| GSLB  | Prober Preference   | Add 2                    |
| Zones   | Click "Add"   | 203.0.113.5              |
| Caches  | State   |                          |
| Settings  | Devices   | Delete                   |
| SSL Orchestrator  | Add   | 3 OK Cancel              |
| Acceleration  | De<br>No data available in tab  |                          |
| Device Management   | BIG-IP<br>System<br>Devices   | Click"OK"                |
| Network   |   |                          |
| 📳 System  | Edit Delete   |                          |

3. Click "Add" again to define the other BIG-IP in the HA pair.

| Hostname: gtm1.site1.example.com Date<br>IP Address: 10.1.10.13 Time | :: Jul 20, 2017 User: admin<br>e: 4:38 PM (CDT) Role: Administra | tor Par                  |
|--|--|--------------------------|
| Standalone   |  |                          |
| Main Help About  | DNS » GSLB : Servers : Server                                    | List » New Server        |
| Statistics   | Constal Properties   |                          |
| iApps  | Name   | site1_ha-pair            |
| S DNS  | Product  | BIG-IP System            |
| Delivery   | Data Center  | site1_datacenter         |
| GSLB   | Prober Preference  | Inherit From Data Center |
| Zones  | Prober Fallback  | Inherit From Data Center |
| Caches   | State  | Enabled V                |
| Settings   | Devices  | Click "Add"again         |
| SSL Orchestrator   | Add  | 0                        |
| Acceleration   | bigip1.site1.example.c   | om 203.0.113.5           |
| Device Management  | BIG-IF<br>System<br>Devices                                      |                          |
| Retwork  |  |                          |
| System   | Edit Delete  |                          |

4. Click the "Add" button to define IP addresses

| Hostname: gtm1.site1.example.com Date:<br>IP Address: 10.1.10.13 Time: | Jul 20, 2017 User: <b>admin</b><br>4:53 PM (CDT) Role: Administrato | r Par                                 |
|--|---|---------------------------------------|
| ONLINE (ACTIVE) Standalone   |   |                                       |
| Main Help About  | DNS » GSLB : Servers : Server I                                     | ist » New Server                      |
| Arrow Statistics   |   | Add BIG-IP System Device              |
| iApps  | General Properties  | Device Name: bigip2.site1.example.com |
| S DNS  | Product   | Translation: (Optional)               |
| Delivery   |   | Link: Auto-Select                     |
| GSLB   | Prober Prélérence   | Add                                   |
| Zones >  | Prober Fallback   | 203.0.113.6                           |
| Caches   | State   |                                       |
| Settings   |   |                                       |
| SSL Orchestrator   | Add   | OK Cancel                             |
| Acceleration   | bigip1.site1.example.com  | n 2000.113.5                          |
| Device Management  |   | Click"OK"                             |
| System   |   |                                       |

5. Complete the form and associate the "bigip" "Health Monitor"

| Hos<br>IP A | tname: gtm1.site1.example.com<br>address: 10.1.10.13 | Date:<br>Time: | Jul 20, 2017<br>5:00 PM (CC | 7 User: <b>admin</b><br>DT) Role: Administral | tor   | Par         |
|-------------|--|----------------|-----------------------------|---|---|-------------|
| (           | ONLINE (ACTIVE)<br>Standalone                        |                |                             |   |   |             |
| N           | Main Help About                                      |                | DNS » G                     | SLB : Servers : Server                        | List » New Server   |             |
| <b>~</b>    | Statistics   |                |                             |   |   |             |
|             | iAnns  |                | General Pr                  | roperties                                     |   |             |
| 193         | n thing  |                | Name                        |   | site1_ha-pair   |             |
| 5           | DNS  |                | Product                     |   | BIG-IP System   |             |
|             | Delivery   | •              | Data Cer                    | nter  | site1_datacenter  |             |
|             | GSLB   | •              | Prober Pro                  | eference                                      | Inherit From Data Center  |             |
|             | Zones  | •              | Prober Fa                   | allback                                       | Inherit From Data Center  |             |
|             | Caches   | •              | State                       |   | Enabled V   |             |
|             | Settings   | •              | Dovicos                     |   |   |             |
| 6           | SSL Orchestrator                                     |                |                             | Add Two.d                                     | evices belong to this H   | IA-Pair     |
|             | Acceleration   |                |                             | bigip1.site1.example.co                       | om 203.0.11   | 13.5        |
|             | Device Management                                    |                | BIG-IF<br>Syster            | bigip2.site1.example.co                       | om 203.0.11   | 13.6        |
|             | Network  |                | Devices                     |   |   |             |
|             | System   |                |                             | Edit Delete                                   |   |             |
| A           | dd the "bigip" He                                    | alti           | Moni                        | Advanced V                                    |   |             |
|             |  |                | Health Mo                   |   | Selected     Availa       /Common     /Common       bigip     <       bigip     <       >>     /Provide       >>     /Provide       All Health Monitors | able<br>cmp |
|             |  |                | Availability                | yrtequirements                                |   |             |

6. Make sure to enable both "Virtual Server" and "Link" discovery

#### Resource

| Resources                        |  |  |  |  |  |  |  |  |  |
|----------------------------------|--|--|--|--|--|--|--|--|--|
| Virtual Server Discovery Enabled |  |  |  |  |  |  |  |  |  |
| Link Discovery Enabled           |  |  |  |  |  |  |  |  |  |
| Cancel Repeat Finished           |  |  |  |  |  |  |  |  |  |

### TMSH

 $\label{eq:comparameter} tmsh \ create \ gtm \ server \ site1\_ha-pair \ datacenter \ site1\_datacenter \ devices \ add \ \{ \ bigip1.site1.example.com \ \{ \ addresses \ add \ \{ \ 203.0.113.6 \ \{ \ \} \ \} \ \} \ bigip2.site1.example.com \ \{ \ addresses \ add \ \{ \ 203.0.113.6 \ \{ \ \} \ \} \ \} \ link-discovery \ enabled \ monitor \ bigip \ product \ bigip \ virtual-server-discovery \ enabled \ monitor \ bigip \ product \ bigip \ virtual-server-discovery \ enabled \ monitor \ bigip \ virtual-server-discovery \ enabled \ wirtual-server-discovery \ wirtual-server-discovery$ 

#### 2.1.5.1.4 site2\_ha-pair

Contiue the same configuration for the BIG-IP cluster in site 2.



| Field                    | Value                                    |
|--------------------------|--|
| Name                     | site2_ha-pair                            |
| Data Center              | site2_datacenter                         |
| Device Add:              | bigip1.site2.example.com : 198.51.100.37 |
| Device Add:              | bigip2.site2.example.com : 198.51.100.38 |
| Health Monitors          | bigip                                    |
| Virtual Server Discovery | Enabled                                  |
| Link Discovery           | Enabled                                  |

1. Fill in the Name and Datacenter

| Hostname: gtm1.site1.example.com Date<br>IP Address: 10.1.10.13 Time | : Jul 20, 2017 User: <b>admin</b><br>: 5:52 PM (CDT) Role: Administrat | lor                        |
|--|--|----------------------------|
| CONLINE (ACTIVE)<br>Standalone                                       |  |                            |
| Main Help About  | DNS » GSLB : Servers : Server  | List » New Server          |
| Mage Statistics  |  |                            |
|  | General Properties   |                            |
| IApps  | Name   | site2_ha_pair              |
| S DNS  | Product  | BIG-IP System              |
| Delivery   | Data Center 🛑 🔶  | site2_datacenter           |
| GSLB   | Prober Preference  | Inherit From Data Center   |
| Zones  | Prober Fallback  | Inherit From Data Center   |
| Caches   | State  | Enabled V                  |
| Settings   | Devices  | Click "Add"                |
| SSL Orchestrator   |  | Add                        |
|  |  | Device Name                |
| Acceleration   |  | No data available in table |
| Device Management  | BIG-IP System Devices  |                            |
| Retwork  |  |                            |
| System   |  | Edit Delete                |

2. Click the "Add" button to define IP addresses

| Hostname: gtm1.site1.example.com Date:<br>IP Address: 10.1.10.13 Time: | Jul 20, 2017<br>5:56 PM (CDT) | User: <b>admin</b><br>Role: Administrator                          | Partition: Common |
|--|-------------------------------|--|-------------------|
| ONLINE (ACTIVE) Standalone   |                               |  |                   |
| Main Help About  | DNS » GSLB:                   | Servers : Server List » New Server                                 |                   |
| Statistics   | General Propertie             | es Device Name: bigip1.site2.example.com<br>Address: 198.51.100.37 | ]                 |
| S DNS  | Product                       | Translation:   | (Optional)        |
| Delivery   | Data Center                   |  |                   |
| GSLB Clic  | k"Add"-                       | Add  |                   |
| Zones  | Prober Fallback               | 130.51.100.57  |                   |
| Caches   | State                         |  |                   |
| Settings   | Devices                       | Delete   |                   |
| SSL Orchestrator   | Add                           |  | OK Cancel         |
| Acceleration   | No da                         | Device Name (ddr   | ress              |
| Device Management  | BIG-IP<br>System<br>Devices   | Click"OK"  |                   |
| Network  |                               |  |                   |
| System   | Edit                          |  |                   |

3. Click "Add" again to define the other BIG-IP in the HA pair.

| Hostname: gtm1.site1.example.com Date<br>IP Address: 10.1.10.13 Time | : Jul 20, 2017 User: admin<br>: 6:13 PM (CDT) Role: Adminis | trator Partition: Common |
|--|---|--------------------------|
| Standalone   |   |                          |
| Main Help About  | DNS » GSLB : Servers : Serv                                 | er List » New Server     |
| Statistics   | Concert Descertion  |                          |
| iApps  |   |                          |
|  | Name  | site2_na_pair            |
| S DNS  | Product   | BIG-IP System            |
| Delivery   | Data Center   | site2_datacenter         |
| GSLB   | Prober Preference   | Inherit From Data Center |
| Zones  | Prober Fallback   | Inherit From Data Center |
| Caches   | State   | Enabled V                |
| Settings >   |   |                          |
| e  | Devices   | Click "Add"              |
| SSL Orchestrator   | Add   |                          |
| Acceleration   | bigin1 site2 exemple  | Device Name Autress      |
| _  | BIG-IP  | 196.51.100.57            |
| Device Management  | System<br>Devices   |                          |
| Network  |   |                          |
| हिंगे System   | Edit Delete   |                          |

4. Click the "Add" button to define IP addresses

| Hostname: gtm1.site1.example.com<br>IP Address: 10.1.10.13 | Date: Jul 20, 2017<br>Time: 6:22 PM (CD] | User: <b>admin</b><br>T) Role: Administra | tor                              | Partition: Common       |
|--|--|---|----------------------------------|-------------------------|
| ONLINE (ACTIVE) Standalone                                 |  |   |                                  |                         |
| Main Help About  | DNS » GS                                 | LB : Servers : Server                     | List » New Server                |                         |
| Statistics   | General Pro                              | perties Devi                              | e Name: bigip2.site2.example.com |                         |
| iApps  | Name =                                   | Addr                                      | ess: 198.51.100.38               |                         |
| S DNS  | Product                                  | Tran                                      | slation:                         | (Optional)              |
| Delivery   | Click"Ad                                 | 2   | Auto-Select                      |                         |
| GSLB   |  | Ad Ad                                     | 51 100 29                        |                         |
| Zones  | Prober Fall                              | back                                      | 51.100.56                        |                         |
| Caches   | State                                    |   |                                  |                         |
| Settings   | Devices                                  | De  | ete                              |                         |
| SSL Orchestrator   |  | Add                                       |                                  | 3 OK Cancel             |
| Acceleration   |  | Di<br>bigip1.site2.example.c              | om 1                             | Address<br>98,51,110,37 |
| Device Management  | BIG-IP<br>System<br>Devices              |   | (                                | lick"OK"                |
| Retwork  |  |   |                                  |                         |
| System   |  | Edit Delete                               |                                  |                         |

5. Complete the form and associate the "bigip" "Health Monitor"

| Hostname: gtm1.site1.example.com Da<br>IP Address: 10.1.10.13 Tir | ite: Jul 20, 2017<br>ne: 7:55 PM (CD | User: <b>admin</b><br>)T) Role: Administra | itor                     | Partition: Comm   | ion |
|---|--------------------------------------|--|--------------------------|---|-----|
| ONLINE (ACTIVE)<br>Standalone                                     |                                      |  |                          |   |     |
| Main Help About   | DNS » G                              | SLB : Servers : Server                     | List » New Server        |   |     |
| Statistics  | General Pro                          | operties                                   |                          |   |     |
| iApps   | Name                                 |  | site2_ha_pair            |   |     |
| 😚 dns   | Product                              |  | BIG-IP System            | ~   |     |
| Delivery  | Data Cen                             | ter  | site2_datacenter         |   |     |
| GSLB >  | Prober Pre                           | eference                                   | Inherit From Data Center |   |     |
| Zones   | Prober Fa                            | llback                                     | Inherit From Data Center |   |     |
| Caches  | State                                |  | Enabled 🔽                |   |     |
| Settings  | Devices                              |  |                          |   |     |
| SSL Orchestrator  |                                      | Add  |                          |   |     |
| Acceleration  |                                      | bigip1.site2.example.co                    | om                       | 198.51,100.37   |     |
| Device Management   | BIG-IP<br>System                     | bigip2.site2.example.c                     | om                       | 198.51.100.38   |     |
|   | Devices                              |  |                          |   |     |
| Network   |                                      | Edit Doloto                                |                          |   | _   |
| System  |                                      |  |                          |   | _   |
|   | Configurati                          | ion: Advanced                              |                          |   |     |
|   | Health Mo                            | nitors                                     | Selected                 | Available<br>/Common<br>gateway_icmp<br>gtp<br>http_head_f5 |     |
|   | Availability                         | Requirements                               | All Health Monitors      |   |     |

#### 6. Make sure to enable both "Virtual Server" and "Link" discovery

| tesources                |         |  |  |  |  |  |  |  |
|--------------------------|---------|--|--|--|--|--|--|--|
| Virtual Server Discovery | Enabled |  |  |  |  |  |  |  |
| Link Discovery           | Enabled |  |  |  |  |  |  |  |
| Cancel Repeat Finished   |         |  |  |  |  |  |  |  |

#### TMSH

tmsh create gtm server site2\_ha-pair datacenter site2\_datacenter devices add { bigip1.site2.example.com { addresses add { 198.51.100.37 { } } } bigip2.site2.example.com { addresses add { 198.51.100.38 { } } } link-discovery enabled monitor bigip product bigip virtual-server-discovery enabled

Server objects represent a system such as an application delivery controller which host a service. A server can be a BIG-IP system, a third party ADC or a third-party host server such as a web or database server. In this task we will create a server on gtm1.site1 referencing gtm1.site2, which is required for config synchronization.

When we create a BIG-IP server with auto-discovery enabled (which we will do), BIG-IP DNS will discover all of the virtual servers defined on the BIG-IP LTM. For more information on Servers, please refer to the link below.



Click the create button and continue to define objects

| Hostname: gtm1.site1.example.com Date<br>IP Address: 10.1.10.13 Time | : Jul 20, 2017 User: <b>a</b><br>:: 2:00 PM (CDT) Role: A | dmin<br>dministrator        |                       | Partition: Common |  |  |  |  |
|--|---|-----------------------------|-----------------------|-------------------|--|--|--|--|
| Standalone   |   |                             |                       |                   |  |  |  |  |
| Main Help About  | DNS » GSLB : Servers                                      | : Server List               |                       |                   |  |  |  |  |
| Statistics   | 🚓 👻 Server List   | Trusted Server Certificates | Statistics 🔎          |                   |  |  |  |  |
| iApps  | *   | Search                      |                       | Create            |  |  |  |  |
|  |   | Davison                     |                       | Vitual Convers    |  |  |  |  |
| DNS  | Ve status - Name  | Devices                     | Address © Data Center | litual Servers    |  |  |  |  |
| Delivery   | No records to display.                                    |                             |                       |                   |  |  |  |  |
| GSLB   | Enable Disable Dele                                       | ete                         |                       |                   |  |  |  |  |
| Zones  |   |                             |                       |                   |  |  |  |  |
| Caches   | Clic  | k-"Create" to d             | efine.atm1.sit        | e1                |  |  |  |  |
| Settings >   | <u> </u>  |                             |                       |                   |  |  |  |  |
| SSL Orchestrator   |   |                             |                       |                   |  |  |  |  |
| Acceleration   |   |                             |                       |                   |  |  |  |  |
| Device Management  |   |                             |                       |                   |  |  |  |  |
| Retwork  |   |                             |                       |                   |  |  |  |  |
| System   |   |                             |                       |                   |  |  |  |  |

### 2.1.5.2 Device Trust

A group of F5 DNS servers must exchange keys to establish a trusted mechanism for HA communications and Config Sync. In this task we will establish device trust between gtm1.site1 and gtm1.site2. For more information on device trust, please refer to the link below.

| Hostna<br>IP Add | ame: <b>gtm1.site1.examp</b><br>Iress: 10.1.10.13 | <b>le.com</b> Dat | te: Jul 20, 2017 User: admin<br>ne: 8:05 PM (CDT) Role: Administrator |          |                          |          |          | Partition: Com               | mon                |                 |     |
|------------------|---|-------------------|---|----------|--------------------------|----------|----------|------------------------------|--------------------|-----------------|-----|
| R                | ONLINE (ACT)<br>Standalone                        | VE)               | DNS   | SI B     | : Servers : 1            | Server I | ist      |                              |                    |                 |     |
| Ma s             | tatistics   |                   | * -   | Server L | ist                      | Trusted  | Server C | ertificates Sta              | atistics 🔎         |                 |     |
| i/               | Apps  |                   | *   |          |                          |          |          | Search                       |                    |                 |     |
| 🕥 р              | NS  |                   |   | Status   | <ul> <li>Name</li> </ul> |          | Devices  | Address                      | Data Center        | Virtual Servers | Pr  |
|                  | Delivery  | ۰.                |   |          | gtm1.site1_              | _server  | 1        | 203.0.113.7                  | site1_datacenter   | 0               | BI  |
|                  | GSLB  | •                 |   |          | gtm1.site2_              | server   | 1        | 198.51.100.3                 | 9 site2_datacenter | 0               | BI  |
|                  | Zones   | +                 |   |          | site1_ha-pa              | air      | 2        | 203.0.113.5<br>203.0.113.6   | site1_datacenter   | 0               | BI¢ |
|                  | Caches  | ×                 |   |          | site2_ha_p               | air      | 2        | 198.51.100.3<br>198.51.100.3 | 7 site2_datacenter | 0               | BIG |
|                  | Settings  | +                 | Enabl   | e Disal  | ble Delete               | ə İ      |          |                              |                    |                 | -   |
| 🔓 s              | SL Orchestrator                                   |                   | T   | iree (   | other s                  | erve     | ers n    | eed to "                     | establish (        | trust"          |     |
| 🦳 A              | cceleration                                       |                   |   |          |                          |          |          |                              |                    |                 |     |
| a d              | evice Management                                  |                   |   |          |                          |          |          |                              |                    |                 |     |
| <u>_</u> N       | etwork  |                   |   |          |                          |          |          |                              |                    |                 |     |
| 8 P S            | ystem   |                   |   |          |                          |          |          |                              |                    |                 |     |

1. Launch Putty and login to gtm1.SITE1

Run the following command, and when prompted for a password use "default"

# TMSH

bigip\_add



2. Observe the exchanged certificates

| Hostname: gtm1.site1.example.com<br>IP Address: 10.1.10.13 | n Date: .<br>Time: : | Jun 25, 2017<br>3:36 PM (CDT) | User: <b>admi</b><br>Role: Admi  | n<br>inistrator                              |                                    |
|--|----------------------|-------------------------------|--|--|------------------------------------|
| ONLINE (ACTIVE)<br>Standalone                              |                      |                               |  |  |                                    |
| Main Help Ab   | out                  | DNS » GSLB: S                 | Servers : Tr   | usted Server Certificates                    |                                    |
| Mage Statistics  |                      | 🔅 🚽 Server List               | t T  | rusted Server Certificates                   | Statistics 🔎                       |
| iApps  | (                    | General Propertie             | s  |  |                                    |
| S DNS  |                      | Name                          |  | server                                       |                                    |
| Delivery   |                      | Partition / Path              |  |  |                                    |
| GSLB   | → V                  | Vide IPs                      | •  | gtm1.site2.example.o<br>bigip2.site1.example | com, MyCompany<br>.com, MyCompany  |
| Zones  | +                    | Pools                         | ÷  | bigip1.site2.example<br>bigip2.site2.example | .com, MyCompany<br>.com, MyCompany |
| Caches   |                      | iRules                        | <ul> <li>Image: Image: Ima</li></ul> | gim i.site i.example.                        | com, myCompany                     |
| Settings   | ) - D                | Data Centers                  | ×.   |  |                                    |
| £  | 7                    | Servers                       | <u>ک</u> (   | Server List 💮                                |                                    |
| SSL Orchestrator   |                      | Links                         |  | Trusted Server                               |                                    |
| Acceleration   |                      | Prober Pools                  |  | Certificates                                 | GMT                                |
| _  |                      | Ionitors                      | (+) <b>(</b>   | Statistics                                   |                                    |
| Device Management  | Т                    | opology                       | <u> </u>   | 234963207                                    |                                    |
|  |                      | 0,0003)                       |  | Common Name: atr                             | n1 site? evample.com               |

3. Observe the server status

| Hos<br>IP A | stname:<br>Address: | gtm1.site1.example.com<br>10.1.10.13 | Date:<br>Time: | Jul 26,<br>3:44 P | , 2018<br>M (EDT)          | User: a<br>Role: A | <b>dmin</b><br>dministrato | NF .     |                        |          |                  | Partition: Co   | ommor |
|-------------|---------------------|--------------------------------------|----------------|-------------------|----------------------------|--------------------|----------------------------|----------|------------------------|----------|------------------|-----------------|-------|
| (           | 5                   | ONLINE (ACTIVE)<br>Standalone        |                |                   |                            |                    |                            |          |                        |          |                  |                 |       |
| N           | Main                | Help About                           |                | DNS               | » GSLB                     | Servers :          | Server L                   | .ist     |                        |          |                  |                 |       |
| <b>~</b>    | Statis              | tics                                 |                | ₩ -               | Server L                   | ist                | Trusted                    | Server C | ertificates            | Stati    | stics 🗷          |                 |       |
|             | iApps               |                                      |                | k                 |                            |                    |                            | ×        | Search                 |          |                  |                 |       |
| 53          | DNS                 |                                      |                |                   | <ul> <li>Status</li> </ul> | ▲ Name             |                            | Devices  | Address                |          | Data Center      | Virtual Servers | s Pro |
|             | Del                 | ivery                                | •              |                   | •                          | gtm1.site          | 1_server                   | 1        | 203.0.113              | .7       | site1_datacenter | 0               | BIC   |
|             | GS                  | LB                                   | •              |                   | 0                          | gtm1.site          | 2_server                   | 1        | 198.51.10              | 0.39     | site2_datacenter | 0               | BIC   |
|             | Zor                 | nes                                  | •              |                   | •                          | site1_ha-          | pair                       | 2        | 203.0.113<br>203.0.113 | .5<br>.6 | site1_datacenter | 3               | BIC   |
|             | Ca                  | ches                                 | •              |                   | •                          | site2_ha-          | pair                       | 2        | 198.51.10              | 0.37     | site2_datacenter | 2               | BIC   |
|             | Set                 | tings                                | •              | Enat              | ole Disal                  | ble Dele           | ete                        |          |                        |          |                  |                 |       |
|             | Accel               | eration                              |                | G                 | re                         | en                 | G                          | re       | en                     |          | Gree             | n !!            |       |
|             | Devic               | e Management                         |                |                   |                            |                    |                            |          |                        |          |                  |                 |       |
|             | Netwo               | ork                                  |                |                   |                            |                    |                            |          |                        |          |                  |                 |       |
|             | Syste               | m                                    |                |                   |                            |                    |                            |          |                        |          |                  |                 |       |
|             |                     |                                      |                |                   |                            |                    |                            |          |                        |          |                  |                 |       |

Note: If your server list is not green, do not proceed to the next step. Please confirm that the device trust is complete and troubleshoot the issue.

#### 2.1.5.3 Sync Group

After the BIG-IP DNS server in the site 2 data center is joined to the sync group, an administrator may make changes on any of the F5 DNS servers, and changes will be automatically replicated across all F5 DNS servers.

From the Jumpbox Launch Putty and log in to gtm1.site2

In the Putty terminal logged into gtm1.site2 run the command "gtm\_add 203.0.113.7", and enter the password "default" when prompted.

Select "y" to allow the bigip-ip to join the mesh.

Note: A word of caution. Running this command will PULL configuration from the remote BIG-IP DNS and overwrite the local DNS configuration.



#### TMSH

gtm\_add 203.0.113.7

Datacenters are logical groupings of services or applications that are typically located within the same physical location such as a Data Center. The Data Center configuration will allow BIG-IP DNS to understand the location of your services for the purposes of high availability. For more information on Data Centers,

please refer to the link below.

Perform configuration changes on gtm1.site1. The reason for this is that by the end of this lab we will demonstrate how BIG-IP DNS Synchronization works to ensure configuration consistency is maintained between both BIG-IP DNS devices. Once Synchronization is established, gtm1.site2 will receive a copy of these new configurations.

Note: The tasks in this section are to be only completed on gtm1.site1

| Hostname: gtm1.site1.example.com Date<br>IP Address: 10.1.10.13 Tim | e: Jul 20, 2017 User: <b>admin</b><br>e: 1:45 PM (CDT) Role: Administrator | Partition: Common |  |  |  |
|---|--|-------------------|--|--|--|
| CONLINE (ACTIVE) Standalone   |  |                   |  |  |  |
| Main Help About   | DNS » GSLB : Data Centers : Data Center List                               |                   |  |  |  |
| Statistics  | Data Center List Statistics Data Center List                               | ate"              |  |  |  |
| iApps   | * Search   | Create            |  |  |  |
| S DNS   | Availability      Aname     Location Links                                 |                   |  |  |  |
| Delivery  | No records to display.   |                   |  |  |  |
| GSLB  | Wide IPs   |                   |  |  |  |
| Zones   | Pools >  |                   |  |  |  |
| Caches  | iRules 🛞   |                   |  |  |  |
| Settings  | Data Centers 💦 Data Center List 💽  |                   |  |  |  |
| SSL Orchestra or  | 2 Servers 3 Statistics 2   |                   |  |  |  |
| Acceleration  | Prober Pools   |                   |  |  |  |
| Device Management   | Monitors 📀   |                   |  |  |  |
| Device management   | Topology >   |                   |  |  |  |
| Network   | Distributed Applications >   |                   |  |  |  |
| System  |  |                   |  |  |  |

Create two data centers according to the table below:

| Field | Value            |
|-------|------------------|
| Name  | site1_datacenter |
| Name  | site2_datacenter |

| Hostname: gtm1.site1.example.co<br>IP Address: 10.1.10.13 | om Date:<br>Time: | Jul 20, 2017 Us<br>1:48 PM (CDT) Ro | er: <b>admin</b><br>de: Administrator |                          | Partition: Common |
|---|-------------------|-------------------------------------|---------------------------------------|--------------------------|-------------------|
| ONLINE (ACTIVE)<br>Standalone                             |                   |                                     |                                       |                          |                   |
| Main Help A   | bout              | DNS » GSLB : Data                   | a Centers : Dat                       | a Center List            |                   |
| Statistics  |                   | Conoral Proportion                  |                                       |                          |                   |
| iApps   |                   | Name                                | [                                     | site1_datacenter         | _                 |
| S DNS   |                   | Description                         | [                                     |                          |                   |
| Delivery  | •                 | Location                            | [                                     |                          |                   |
| GSLB  | •                 | Contact                             | [                                     |                          |                   |
| Zones   | ÷                 | Prober Preference                   | [                                     | Inside Data Center 🔽     |                   |
| Caches  |                   | Prober Fallback                     | [                                     | Any Available            |                   |
| Settings  | •                 | State                               | [                                     | Enabled 🔽                |                   |
| SSL Orchestrator  |                   | Cancel Repeat                       | Finished                              |                          |                   |
| Acceleration  |                   |                                     |                                       |                          |                   |
| Device Management   |                   | Repeat th                           | nis step                              | to create "site2_datacer | iter"             |
| Network   |                   |                                     |                                       |                          |                   |
| System  |                   |                                     |                                       |                          |                   |

TMSH command for only site1.gtm1:

### TMSH

tmsh create gtm datacenter site1\_datacenter

### TMSH

tmsh create gtm datacenter site2\_datacenter

# 2.1.6 Pools

Pools are a grouping of related virtual servers. Pools will typically reference virtual servers on BIG-IP LTM systems. The pool we create below will be later referenced by a Wide-IP (FQDN). For more information on pools, please refer to the link below.

| Hos<br>IP A | stname:<br>Address: | gtm1.site1.exan<br>10.1.10.13 | nple.com | Date:<br>Time: | Jul 26,<br>3:58 Pl | 2018<br>M (EDT)            | Partition:  | Common     |          | Log out          |
|-------------|---------------------|-------------------------------|----------|----------------|--------------------|----------------------------|-------------|------------|----------|------------------|
| (           | 5                   | ONLINE (AC<br>Standalone      | TIVE)    |                |                    |                            |             |            |          |                  |
| N           | Main                | Help                          | About    |                | DNS                | » GSLB                     | : Pools : P | ool List   |          |                  |
| M           | Statisti            | CS                            |          |                | ☆ -                | Pool Lis                   | t           | Statistics |          |                  |
| 3           | iApps               |                               |          |                | )*                 |                            |             |            | × Search | Create           |
| <b>5</b>    | DNS                 |                               |          |                |                    | <ul> <li>Status</li> </ul> | Name        | Type       | Members  | Partition / Path |
|             | Deliv               | very                          |          | ×.             | No re              | cords to di                | isplay.     |            |          |                  |
|             | GSL                 | B 🚺                           | 4        | F I            | Wide IF            | °s                         | , ) , j     | te         |          |                  |
|             | Zone                | es                            |          |                | Pools              | ;                          |             | Pool List  | 0        |                  |
|             | Cach                | nes                           |          | /              | iRule              | s                          | $\odot$     | Statistics | (        | 7                |
|             | Setti               | ngs                           |          | •              | Data O             | enters                     | F           |            |          |                  |
|             | Accolo              | ration                        | //       |                | Serve              | ers                        | Þ           |            |          |                  |
|             | Accelei             |                               |          |                | Links              |                            | F           |            |          |                  |
|             | Device              | Management                    | t        |                | Probe              | er Pools                   | Þ           |            |          |                  |
|             |                     |                               |          |                |                    |                            |             |            |          |                  |

| Field  | Value  |
|--------|--|
| Name   | www.example.com_pool                         |
| Туре   | A  |
| member | isp1_site1_www.example.com_tcp_https_virtual |
| member | isp2_site2_www.example.com_tcp_https_virtual |

| IP Ac    | name: gtm1.site1.example.com<br>kdress: 10.1.10.13 | Date:<br>Time | : Jul 26, 2018<br>: 4:11 PM (EDT) | User: <b>admin</b><br>Role: Administra   | rator Partition: Common V  |  |  |  |  |  |  |
|----------|--|---------------|-----------------------------------|--|--|--|--|--|--|--|--|
|          | ONLINE (ACTIVE) Standalone                         |               |                                   |  |  |  |  |  |  |  |  |
| M        | ain Help About                                     |               | DNS » GSLB                        | : Pools : Pool Lis   | ist » New Pool   |  |  |  |  |  |  |
| <b>~</b> | Statistics   |               | General Properties                |  |  |  |  |  |  |  |  |
| iApps    |  |               | Name                              |  | www.example.com_pool ×   |  |  |  |  |  |  |
| <b>S</b> | DNS  |               | State                             |  | Enabled  |  |  |  |  |  |  |
|          | Delivery   | ÷             |                                   |  |  |  |  |  |  |  |  |
|          | GSLB   | ÷             | Configuration                     |  | Delested Auslable  |  |  |  |  |  |  |
|          | Zones  | •             | Health Monitors                   |  | Available //Common   |  |  |  |  |  |  |
|          | Caches   | •             |                                   |  | gateway_icmp   |  |  |  |  |  |  |
|          | Settings   | ->            |                                   |  | http_head_f5   |  |  |  |  |  |  |
|          | Acceleration                                       |               |                                   |  | Up Down  |  |  |  |  |  |  |
|          | Acceleration                                       |               | Availability Req                  | uirements  | All Health Monitors  |  |  |  |  |  |  |
|          | Device Management                                  |               |                                   |  | Bits: Disabled   |  |  |  |  |  |  |
| Network  |  |               | Limit Settings                    |  | Packets: Disabled V<br>Current Connections: Disabled V   |  |  |  |  |  |  |
|          | System   |               | Manual Resum                      | e  |  |  |  |  |  |  |  |
|          |  |               | TTL                               |  | 30   |  |  |  |  |  |  |
|          |  |               | Dynamic Ratio                     |  |  |  |  |  |  |  |  |
|          |  |               | Maximum Answers Returned          |  | 1  |  |  |  |  |  |  |
|          |  |               | Verify Member                     | Availability   |  |  |  |  |  |  |  |
|          |  |               | Members                           |  | Select two LTM VIP's and click "Add"   |  |  |  |  |  |  |
|          |  |               | Load<br>Balancing<br>Method       | Preferred: Round<br>Alternate: Round<br>Fallback: Return                                   | nd Robin   Ind Robin Ind R |  |  |  |  |  |  |
|          |  |               | Fallback IP                       | 0.0.0.0  |  |  |  |  |  |  |  |
|          |  |               | Member List                       | Virtual Server: S<br>Ratio: 1<br>Add<br>//Common/isp1_<br>//Common/isp2_s<br>Delete Up Dow | Select 1 site1_www.example.com_tcp_https_virtual (/Common/site1_ha-pair) - 203.0.113.9:443, Ratio(1) site2_www.example.com_tcp_https_virtual (/Common/site2_ha-pair) - 198.51.100.41:443, Ratio(1) wm  |  |  |  |  |  |  |

TMSH command to run on only gtm1.site1:

#### TMSH

tmsh create gtm pool а www.example.com\_pool { members add { site1\_hapair:/Common/isp1\_site1\_www.example.com\_tcp\_https\_virtual { member-order } site2 ha-0 pair:/Common/isp2\_site2\_www.example.com\_tcp\_https\_virtual { member-order 1 } } }

### 2.1.7 FQDN

F5 refers to an FQDN as a "wide-ip", or "wip". The Wide IP maps a FQDN (fully qualified domain name) to one or more pools of virtual servers. For more information on Wide IPs, please refer to the link below.
| Hosti<br>IP Ac | name: <b>gtn</b><br>ddress: 10. | n <b>1.site1.example</b><br>1.10.13 | e.com Da<br>Til | ite: Jun 25, 2017<br>me: 8:49 PM (CDT) | User: <b>a</b><br>) Role: A | dmin<br>Administrator |          |  |
|----------------|---------------------------------|-------------------------------------|-----------------|--|-----------------------------|-----------------------|----------|--|
|                |                                 | ONLINE (ACTIVI<br>Standalone        | E)              |  |                             |                       |          |  |
| M              | ain                             | Help                                | About           | DNS » GSI                              | LB : Wide IPs               | : Wide IP List        |          |  |
| -              | Statistics                      |                                     |                 | 🕁 🚽 Wide                               | IP List                     | Statistics            |          |  |
| i 🔊            | iApps                           |                                     |                 | <b>k</b>                               |                             |                       | × Search |  |
| <b>S</b>       | DNS                             |                                     |                 | 💌 💌 Stat                               | us 🔺 Name                   |                       |          |  |
|                | Deliver                         | у                                   | +               |  | www.gslt                    | o.example.com         |          |  |
|                | GSLB                            |                                     | -               | Wide IPs                               | <b>_</b> +                  | Wide IP List          | •        |  |
|                | Zones                           |                                     |                 | Pools                                  | ×                           | Statistics            |          |  |
|                | Caches                          |                                     |                 | IRules                                 | $( \Rightarrow )$           |                       |          |  |
|                | Setting                         | s                                   |                 | Data Centers                           | Þ                           |                       |          |  |
| 6              | SSL Orch                        | ostrator                            |                 | Servers                                | Þ                           |                       |          |  |
|                | 33L OICH                        | estrator                            |                 | Links                                  | Þ                           |                       |          |  |
|                | Accelerat                       | ion                                 |                 | Prober Pools                           | s ⊧                         |                       |          |  |
|                | Device Ma                       | anagement                           |                 | Monitors                               | (+)                         |                       |          |  |
|                | Dorroo m                        | anagonioni                          |                 | Topology                               | Þ                           |                       |          |  |
|                | Network                         |                                     |                 | Distributed Ap                         | plications >                |                       |          |  |
| 00             | System                          |                                     |                 |  |                             |                       |          |  |

# Create an F5 "wide IP" according to the following table:

| Field   | Value                |
|---|----------------------|
| Name  | www.example.com      |
| Туре  | A                    |
| Alias List                                    | www.gslb.example.com |
| Load-Balancing Decision Log - Pool Selection  | Checked              |
| Load-Balancing Decision Log - Pool Traversal  | Checked              |
| Load-Balancing Decision Log - Pool Member Se- | Checked              |
| lection                                       |                      |
| Load-Balancing Decision Log - Pool Member     | Checked              |
| Traversal                                     |                      |
| Pool  | www.example.com_pool |

| Hostname: gtm1.site1.example.com Date<br>IP Address: 10.1.10.13 Tim | e: Jul 29, 2018 User: admin<br>e: 4:13 PM (EDT) Role: Administr | ator Partition: Common V   |
|---|---|--|
| ONLINE (ACTIVE)<br>Standalone                                       |   |  |
| Main Help About   | DNS » GSLB : Wide IPs : Wide                                    | PList » New  |
| Statistics  |   | _  |
| iApps   | General Properties: Advanced                                    |  |
|   | Name  | www.example.com  |
| S DNS   | Туре  |  |
| Delivery  | Description   |  |
| GSLB >  |   | Alias: www.gslb.example.com  |
| Caches  |   | www.gslb.example.com   |
| Settings  | Alias List  | L  |
|   |   |  |
| Acceleration  |   | Delete   |
| Device Management   | State   | Enabled  |
| Retwork   | Minimal Response  | Enabled V  |
|   | Return Code On Failure  | Disabled 🔽   |
| System  | Load-Balancing Decision Log                                     | <ul> <li>Pool Selection</li> <li>Pool Traversal</li> <li>Pool Member Selection</li> <li>Pool Member Traversal</li> </ul> |
|   | iRules  |  |
|   |   | Selected Available   |
| For trouble   | shooting  | <<<br>>>   |
| hathoses  | Eliance   | Up Down  |
| verbose   | logging   |  |
|   | iBulo List  | Selected Available   |
|   | ikule List  | Up Down  |
|   | Pools   |  |
|   | Load Balancing Method   | Round Robin  |
|   | Persistence   | Disabled V   |
| 108   |   | Pool Select Chapter 2. DNS<br>Ratio 1  |

TMSH command to run on only gtm1.site1:

### TMSH

tmsh create gtm wideip a www.example.com { pools add { www.example.com\_pool } aliases add
{ www.gslb.example.com } load-balancing-decision-log-verbosity { pool-member-selection pool-membertraversal pool-selection pool-traversal } }

#### Results

Use the "dig" command to query directly to the GTM to test the configuration. DIG will bypass locally configured DNS servers when specifying an "@203.0.113.8" argument.

From the Jumpbox use "dig" from the CMD prompt. The first command below will query 203.0.113.8 for the A record of www.example.com, then query @203.0.113.8 for www.gslb.example.com.

### Note: Your result may differ from below





| tname: gtm1.site1.example.com<br>ddress: 10.1.10.13 | Date:<br>Time:   | Jul 29, 2018<br>11:21 PM (EDT)   | User: <b>adr</b><br>Role: Adr   | nin<br>ninistrator   |  |   |  |   |  |   | Par   | tition:   |
|---|--|--|---|--|--|---|--|---|--|---|---|---|
| ONLINE (ACTIVE) Standalone                          |  |  |   |  |  |   |  |   |  |   |   |   |
| lain Help About                                     |  | Statistics »   | Module Statist  | ics : DN   | \$ : G \$  | LB  |  |   |  |   |   |   |
| Statistics  |  | 🔅 👻 Traffic  | Summary <del>-</del>  | DNS  |  | -   | Subsc  | riber Man   | agement  | Netv  | vork  |   |
| Dashboard   | æ  |  |   |  |  |   |  |   |  |   |   |   |
| Module Statistics                                   | •  | Display Option   | 15  |  |  |   |  |   |  |   |   |   |
| Analytics   | •  | Statistics Type  | а   | Wi   | de IPs   |   |  | ~   |  |   |   |   |
| Performance   | •  | Data Format  |   | No   | rmaliz   | ed 🗸  |  |   |  |   |   |   |
| iApps   |  | Auto Refresh   |   | Dis  | sabled   |   | Refrest  | ı   |  |   |   |   |
| DNS   |  | Status   | Wide IP   |  | Туре   | Partition   | n / Path   | Details   | Pools  | Re<br>Total   | quests<br>Resolved  | Re  |
| Acceleration  |  | 🗆 🥥 v  | ww.example.co   | om   | A  | Commo   | 'n   | View  | /iew   | 44  | 44  | 0   |
| Device Management                                   |  | Reset  |   |  |  | /   |  |   | ۰.   |   |   |   |
| Network   |  | For  | mo  | re   |  | de  | ta   | hile  |  | li  | ck  |   |
| System  |  |  |   |  |  |   |  |   |  |   |   |   |
|   |  |  |   |  |  |   |  |   |  |   |   |   |
|   |  |  |   |  |  |   |  |   |  |   |   |   |
|   | thame: gtm1.site1.example.com<br>ddress: 10.1.10.13<br>Standalone<br>Standalone<br>About<br>Statistics<br>Dashboard<br>Module Statistics<br>Analytics<br>Performance<br>Acceleration<br>Device Management<br>Network<br>System | tname: gtm1.site1.example.com Date:   ddress: 10.1.10.13 Time:     Standalone     lain Help   About     Statistics     Dashboard   Module Statistics   Dashboard   Module Statistics   Performance     Analytics   Performance     Acceleration   Device Management     Network     System | tname: gtm1.site1.example.com<br>ddress: 10.1.10.13   ONLINE (ACTIVE)<br>Standalone   Analytics Performance  IAuto Refresh  Acceleration  Network System   Date: Jul 29, 2018 Time: 11:21 PM (EDT)     Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)     Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)   Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)    Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)   Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)   Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)   Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)   Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)   Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)   Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)   Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)   Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)   Statistics >  Date: Jul 29, 2018 Time: 11:21 PM (EDT)   Statistics >  Date: Jul 29, 2018 Time: Jul 29, 2018 Tim | Iname: gtm1.site1.example.com Date: Jul 29, 2018 User: adm   Iddress: 10.1.10.13 Time: 111.21 PM (EDT) Role: Adm   Image: Statistics Image: Statistics Image: Statistics Image: Statistics Image: Statistics   Image: Dashboard Image: Statistics Image: Statistics Image: Statistics Image: Statistics   Image: Dashboard Image: Statistics Image: Statistics Image: Statistics Image: Statistics   Image: Dashboard Image: Statistics Image: Statistics Image: Statistics Image: Statistics   Image: Add Image: Statistics Image: Statistics Image: Statistics Image: Statistics   Image: Add Image: Statistics Image: Statistics Image: Statistics Image: Statistics   Image: Add Image: Statistics Image: Statistics Image: Statistics Image: Statistics   Image: Add Image: Statistics Image: Statistics Image: Statistics Image: Statistics   Image: Add Image: Statistics Image: Statistics Image: Statistics Image: Statistics   Image: Add Image: Statistics Image: Statistics Image: Statistics Image: Statistics   Image: Add Image: Statistics Image: Statistics Image: Statistics Image: Statistics   Image: Add Image: Statistics Image: Statistics Image: Statistics Image: Statistics   Image: Add Image: Statistics Image: Statistics Image: Statistics <td< th=""><th>thame: gtm1.site1.example.com   ddress: 10.1.10.13   Time: 11.21 PM (EDT)   ONLINE (ACTIVE)   Standalone     Statistics   Dashboard   Module Statistics   Module Statistics   Module Statistics   Performance   NS   Acceleration   Device Management   Network   System     Date:   Jute:   Jut</th><th>thame: gtm1.site1.example.com   ddress: 10.1.10.13     ONLINE (ACTIVE)   Statistics     Iain Help     About     Statistics     Dashboard   Module Statistics     Dashboard   Module Statistics   Parformance   Analytics   Performance   IApps     Das   Acceleration   Network     System     Desc. Jul 29, 2018   Time: 11:21 PM (EDT)   Value Statistics:   DNS   Acceleration   Network     For more of a statistic /th><th>thame: gtm1 site1.example.com   ddress: 10.1.10.13     Time: 11.21 PM (EDT)   Constraints   Constraints   Constraints     Constraints Constraints Constrai</th><th>thame: gtm1.site1.example.com<br/>ddress: 10.1.10.13   Date: Jul 29, 2018<br/>Time: 11:21 PM (EDT)  Def: Administrator  DINLINE (ACTIVE)<br/>Standatone   Statistics → Module Statistics : DNS : GSLB  Cashboard  Module Statistics  Dashboard  Module Statistics  Dashboard  Display Options  Statistics Type Display Options  Statistics Type Data Format  Network  System  Display Options  For more detted  For Management  For Management</th><th>thame: gtm1.site1 example.com   ddress: 10.1.10.13</th><th>Interner: gdrm1.aike1.example.com   ddress: 10.1.10.13     CNLINE (ACTIVE)   Statistics     Dashboard   Module Statistics   Dashboard   Module Statistics   Data Format   Normalized   Acceleration   Device Management   Network   System    For moore details of our partition / Path Details Pools</th><th>trame gtrt 1 stel example.com<br/>ddress 10.1.0.13 The: 11.21 PM (EDT) Role: Administrator<br/>CNLINE (ACTIVE)<br/>Standaione<br/>Statistics Statistics &gt; Module Statistics : DNS : GSLB<br/>statistics Statistics &gt; Module Statistics : DNS : GSLB<br/>statistics &gt; Module Statistics : DNS · Subscriber Management Netw<br/>Dashboard<br/>Module Statistics &gt;<br/>Performance &gt;<br/>Acceleration<br/>Network<br/>System<br/>System</th><th>Interner     gint/statel example.com     Date:     Jul 29, 2018     User administrator     Par       ONLINE (ACTIVE)     Statistics     Image: 11:21 PM (EDT)     Role:     Administrator     Par       Statistics     Image: 11:21 PM (EDT)     Statistics : DNS : GSLB     Image: 11:21 PM (EDT)     Statistics : DNS : GSLB       Dashboard     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Statistics     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Statistics     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Statistics     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Statistics     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21</th></td<> | thame: gtm1.site1.example.com   ddress: 10.1.10.13   Time: 11.21 PM (EDT)   ONLINE (ACTIVE)   Standalone     Statistics   Dashboard   Module Statistics   Module Statistics   Module Statistics   Performance   NS   Acceleration   Device Management   Network   System     Date:   Jute:   Jut | thame: gtm1.site1.example.com   ddress: 10.1.10.13     ONLINE (ACTIVE)   Statistics     Iain Help     About     Statistics     Dashboard   Module Statistics     Dashboard   Module Statistics   Parformance   Analytics   Performance   IApps     Das   Acceleration   Network     System     Desc. Jul 29, 2018   Time: 11:21 PM (EDT)   Value Statistics:   DNS   Acceleration   Network     For more of a statistic | thame: gtm1 site1.example.com   ddress: 10.1.10.13     Time: 11.21 PM (EDT)   Constraints   Constraints   Constraints     Constraints Constraints Constrai | thame: gtm1.site1.example.com<br>ddress: 10.1.10.13   Date: Jul 29, 2018<br>Time: 11:21 PM (EDT)  Def: Administrator  DINLINE (ACTIVE)<br>Standatone   Statistics → Module Statistics : DNS : GSLB  Cashboard  Module Statistics  Dashboard  Module Statistics  Dashboard  Display Options  Statistics Type Display Options  Statistics Type Data Format  Network  System  Display Options  For more detted  For Management   thame: gtm1.site1 example.com   ddress: 10.1.10.13 | Interner: gdrm1.aike1.example.com   ddress: 10.1.10.13     CNLINE (ACTIVE)   Statistics     Dashboard   Module Statistics   Dashboard   Module Statistics   Data Format   Normalized   Acceleration   Device Management   Network   System    For moore details of our partition / Path Details Pools | trame gtrt 1 stel example.com<br>ddress 10.1.0.13 The: 11.21 PM (EDT) Role: Administrator<br>CNLINE (ACTIVE)<br>Standaione<br>Statistics Statistics > Module Statistics : DNS : GSLB<br>statistics Statistics > Module Statistics : DNS : GSLB<br>statistics > Module Statistics : DNS · Subscriber Management Netw<br>Dashboard<br>Module Statistics ><br>Performance ><br>Acceleration<br>Network<br>System<br>System | Interner     gint/statel example.com     Date:     Jul 29, 2018     User administrator     Par       ONLINE (ACTIVE)     Statistics     Image: 11:21 PM (EDT)     Role:     Administrator     Par       Statistics     Image: 11:21 PM (EDT)     Statistics : DNS : GSLB     Image: 11:21 PM (EDT)     Statistics : DNS : GSLB       Dashboard     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Statistics     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Statistics     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Statistics     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Statistics     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)       Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 PM (EDT)     Image: 11:21 |

# TMSH

tmsh show gtm wideip A www.example.com detail

| g <sup>2</sup> gtm1.SITE1   |
|---|
| [root8gtm1:Active:Standalone] config # tmsh show gtm wideip A www.example.com detail                |
|   |
| Gtm::WideIp::A www.example.com  |
| Status  |
| Availability : available  |
| State : enabled   |
| Reason : Available  |
| Requests  |
| Total 44<br>Persisted 0   |
| Resolved 44   |
| Dropped O   |
| Load Balancing  |
| Preferred 44  |
| Alternate O   |
| CNAME Resolutions 0   |
| Returned from DNS 0   |
| Returned to DNS O   |
|   |
|   |
| Gtm::Pool::A www.example.com_pool   |
|   |
| Status<br>Availability : available  |
| State : enabled   |
| Reason : Available  |
| Load Balancing  |
| Preferred 44  |
| Alternate O   |
| Returned from DNS 0   |
| Returned to DNS 0   |
| Dropped O   |
|   |
| Gtm::Pool Member: www.example.com_pool:A isp1_site1_www.example.com_tcp_https_virtual:site1_ha-pair |
| Status  |
| Availability : available  |
| State : enabled   |
| Reaboli . Available   |
| Load Balancing  |
| Preferred 35  |
| Fallback 0  |
|   |
| Gtm::Virtual Server: isp1_site1_www.example.com_tcp_https_virtual                                   |
| Status  |
| Availability : available  |
| State : enabled<br>Peason : Monitor /Common/bigin from 203 0 113 5 : UP                             |
| Destination : 203.0.113.9:443   |
| Up Time : 10:18   |
| Link Name 203.0.113.1   |
|   |
| Global  |
| Connections 0   |
| Virtual Server Score 1  |
| Throughput In Out   |
| Bits/sec 0 0  |
| Packets/sec 0 0   |
|   |
| Gtm::Pool Member: www.example.com_pool:& isp2_site2_www.example.com_tcp_https_virturd:site2_ho-paid |
| Status  |
| Availability : available  |
| State : enabled   |

### TMSH

tail -f /var/log/ltm

| rent nitration in the second s |
|--|
| rootdatm1.betive.Standalonel config # tail _f _n 12 /var/log/ltm   |
| Jul 30 00:19:49 gtml info thmm[1966]: 2018-07-30 00:19:49 gtml.sitel.example.com gid 991 from 198  |
| $51,100,68$ # $64119$ : view none: query: www.gslb.example.com IN $\lambda$ + (203.0.113.880)  |
| Jul 30 00:19:49 gtml info tmm[1966]: 2018-07-30 00:19:49 gtml.sitel.example.com gid 991 from 198   |
| 51.100.68#64119 [www.gslb.example.com A] [round robin selected pool (www.example.com pool)] [poo   |
| 1 member check succeeded (isp1 site1 www.example.com tcp https virtual:203.0.113.9) - pool member  |
| state is available (green) [ round robin selected pool member (ispl sitel www.example.com tcp ht   |
| tps virtual:203.0.113.9)]  |
| Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com gid 991 to 198.5  |
| 1.100.68#64119: [NOERROR gr,aa,rd] response: www.gslb.example.com. 30 IN & 203.0.113.9;  |
| Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com gid 372 from 198  |
| .51.100.68#64120: view none: query: www.gslb.example.com IN & + (203.0.113.8%0)  |
| Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 from 198  |
| .51.100.68#64120 [www.gslb.example.com A] [round robin selected pool (www.example.com pool)] [poo  |
| l member check succeeded (isp1 site1_www.example.com tcp_https_virtual:203.0.113.9) - pool member  |
| state is available (green)] [round robin selected pool member (isp1_site1_www.example.com_tcp_ht   |
| tps_virtual:203.0.113.9)]  |
| Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 to 198.5  |
| 1.100.68#64120: [NOERROR qr,aa,rd] response: www.gslb.example.com. 30 IN & 203.0.113.9;  |
| Jul 30 00:23:44 gtm1 info tmm[11966]: 2018-07-30 00:23:43 gtm1.site1.example.com qid 261 from 203  |
| .0.113.68#64121: view none: query: www.example.com IN & + (203.0.113.8%0)  |
| Jul 30 00:23:44 gtm1 info tmm[11966]: 2018-07-30 00:23:43 gtm1.site1.example.com qid 261 from 203  |
| .0.113.68#64121 [www.example.com A] [round robin selected pool (www.example.com_pool)] [pool memb  |
| er check succeeded (isp2_site2_www.example.com_tcp_https_virtual:198.51.100.41) - pool member sta  |
| te is available (green)] [round robin selected pool member (isp2_site2_www.example.com_tcp_https_  |
| virtual:198.51.100.41)]  |
| Jul 30 00:23:44 gtml info tmm[11966]: 2018-07-30 00:23:43 gtml.sitel.example.com qid 261 to 203.0  |
| .113.68#64121: [NOERROR qr,aa,rd] response: www.example.com. 30 IN & 198.51.100.41;  |
| Jul 30 00:23:50 gtml info tmm[11966]: 2018-07-30 00:23:50 gtml.sitel.example.com qid 97 from 203.  |
| 0.113.68#64122: view none: query: www.example.com IN A + (203.0.113.8%0)   |
| Jul 30 00:23:50 gtml info tmm[11966]: 2018-07-30 00:23:50 gtml.sitel.example.com qid 97 from 203.  |
| U.113.68#64122 [www.example.com A] [round robin selected pool (www.example.com_pool)] [pool membe  |
| r check succeeded (1spl_sitel_www.example.com_tcp_https_virtual:203.0.113.9) - pool member state   |
| is available (green)] [round robin selected pool member (ispl_sitel_www.example.com_tcp_https_vir  |
|  |
| Jul 30 00:23:50 gtml into tmm[11966]: 2018-07-30 00:23:50 gtml.sitel.example.com qid 97 to 203.0.  |

# 2.1.8 Delegation

Delegate a subdomain of example.com to the BIG-IP DNS. Delegation is a means to 'defer' or assign management of a portion of your DNS namespace to another DNS server. When the DNS server receives a query for the delegated subdomain it will either recursively resolve the CNAME target, or respond with a referral.

Login to the local DNS server (this should already be open) from the jumpbox, and open the DNS management UI:



### 2.1.8.1 A Records

An A record is the most common DNS query. In this type of query, 'A' refers to an IP address - the cleint is asking for the IP address of the domain name being queried. Create two A records, one for each BIG-IP DNS server.

1. Expand the sub-menus to expose EXAMPLE.COM in the "Forward Lookup Zones"



2. Right click on EXAMPLE.COM and select "New Host (A or AAAA)"

| 2                    | 👼 DC01 - 10.1.70.200 - Remote Desktop Connection  |   |  |   | _ 🗆 ×  |
|----------------------|---|---|--|---|--|
| Postman              | Å   |   | DNS Manager  |   | - • ×  |
| Internet<br>Explorer | File Action View Help   | d | ick on EX  |   | l and  |
| dig_www-ex           | <ul> <li>✓ Forw to ookup Zonessites</li> <li>▷ Trudes DEMUPLE.CC</li> <li>△ EN</li> <li>Update Server Date File</li> <li>▷ Reload</li> <li>2</li> </ul> |   | Select "N  | ew Host"  |  |
| 5001                 | New Host (Å or AAAA)       New Alias (CNAME)       New Alias (CNAME)       New Mail Exchanger (MD)       New Domain                                     |   |  |   |  |
| agility_pub-key      | b     New Delegation       b     Other New Records       b     DNSSEC       b     Rever:  | , | er) Start of Authority<br>er) Name Server (NS)<br>er) Host (A)<br>Host (A) | (SOA) [637], dc01.example.com<br>dc01.example.com.<br>10.1.70.200<br>10.1.71.100<br>10.1.70.200 | n., static<br>static<br>7/30/2018 8:<br>7/30/2018 7: |
| agility_prv_key      | p ⊆ Trust View<br>p ⊆ Condi View<br>p ⊡ Globa<br>Delete<br>Refresh  | • | Host (A)<br>Host (A)<br>Host (A)   | 10.1.70.200<br>10.1.10.60<br>10.1.71.21<br>203.0.113.9  | static<br>static<br>static                           |
| PuTTY (64-bit)       | Export List  Create a new host  |   | ш  |   | >  |
| Notepad++            |   |   |  | • 🏲 🤤   | 9:41 AM<br>7/30/2018                                 |
| 🔊 Start 🛛 🔏          | 🎉 🧬 🧊 📼 夷 DC01 - 10.1.70.200 - Re   |   |  | * 🖓 🖗   | 🗐 👍 9:41 AM 🚦  |

3. Create two new A records for the new BIGP-IP nameservers.

| Field | Value         |
|-------|---------------|
| ns1   | 203.0.113.8   |
| ns2   | 198.51.100.40 |



Create ns2.example.com

| I            | DE01 - 10.1.70.200 - Remote   | Deskton Connection  |                           |                  |
|--------------|---|---|---------------------------|------------------|
|              |   | DNS Mana  | ager                      |                  |
| BIG-IP Edge  | File Action View Help   | New Host X  | ger                       |                  |
| Client       | (+ -> 2 🗊 🗙 🖾 Q   | Name (uses parent domain name if blank):                                    |                           |                  |
|              | 🚊 DNS   | ns2   | Data                      | Time:            |
| agility_pub  | ⊿ ☐ DC01 ⊿ ☐ Forward Lookup Zon b 📆 _msdcs.EXAMPLE  | Fully qualified domain name (FQDN):<br>ns2.EXAMPLE.COM.                     |                           |                  |
|              | A 📑 EXAMPLE.COM   | IP address:   |                           |                  |
| 2            | ▷ [] _msdcs   | 198.51.100.40   |                           |                  |
| agility_prv  | psites  | Create associated pointer (PTR) record                                      |                           |                  |
| æ            | ▷ □ _udp▷ □ branch01▷ □ DomainDnsZc   | Allow any authenticated user to update DNS records with the same owner name |                           |                  |
| PuTTY (64-bi | ▷ PorestUns∠on ▷ □ mgmt   |   | [152], dc01.example.com., | static<br>static |
|              | ▷ ite1  |   | ns1.branch01.example.com. | static           |
| <u>.</u>     | Reverse Lookup Zone   | Add Host Done   | 10.1.70.200               | 6/26/            |
| Notepad++    | Trust Points  |   | 10.1.71.100               | 6/26/            |
|              | Conditional Forwarde  | rs dc01 Host (A)  | 10.1.70.200               | static           |
|              |   | ns1 Host (A)  | 203.0.113.9               | static           |
| <b>*</b>     | < III   |   | 20510:115:0               |                  |
|              |   | - JI  |                           |                  |
|              |   |   |                           |                  |
| // Start     | <i>(i)</i> (ii) (iii) ( | DC01 - 10.1.70.200 - Re   |                           |                  |

### 2.1.8.2 Sub Domain

Configure the delegation of gslb.example.com to ns1 and ns2, the A records which were created in the previous step.

1. Expand "Forward Lookup Zones", and right click on "EXAMPLE.com

| dent - 10.1.70.200 - Remote Desktop Connection   |  |  |  |
|--|--|--|--|
| Å.   | DNS Mar  | nager  |  |
| File Action View Help  |  |  |  |
| ◆ → ≥ 📰 🗙 🗈 @ 🖻 🗾 🚛 🗄 🗆 🛱  |  |  |  |
| DNS DC01 Forward Lookep Zones Forward Lookep Zones Judgets Server Data File Judgets Serv | Type<br>Start of Authority (SOA)<br>Name Server (NS)<br>Name Server (NS)<br>Host (A)<br>Host (A)<br>Host (A)<br>Host (A)<br>Host (A) | Data<br>[152], dc01.example.com.,<br>dc01.example.com.<br>ns1.branch01.example.com.<br>10.1.70.200<br>10.1.71.100<br>10.1.70.200<br>203.0.113.8<br>198.51.100.40 | Static<br>static<br>static<br>5/26/2017 12:00:00 /<br>6/26/2017 12:00:00 /<br>static |
| Create a new delegated DNS domain.   |  |  |  |
|  |  |  |  |

2. Create the "gslb" subdomain.



3. Step through the Delegation Wizard. Add "ns1.example.com - 203.0.113.8"

|              | File Action View | v Help  |                      |               |                     |
|--------------|------------------|---|----------------------|---------------|---------------------|
| 1            | Þ 🄿 🖄 📰          | X 🖬 🍳 🗟 🛛 🖬 🕷   | 1                    |               |                     |
| Explo ; ww   | 🚉 DNS            | Name  | Туре                 | Data          | Т                   |
|              | ⊿ ]              | New Delegation  | Wizard               | x             |                     |
|              | Name S <u>e</u>  | rvers   |                      |               |                     |
| dig_www ; ;  | You              | Nev   | v Name Server Record | x             |                     |
| , ; ;<br>C:\ | Spec             | Enter the name of a DNS server that is a<br>Server fully qualified domain name (FOD | N); <b>Do not</b>    | click "Resolv | e"                  |
| DCC          | Nam              | ns1.example.com   |                      | Resolve       | _                   |
|              | Sei              | IP Addresses of this NS record:   |                      |               |                     |
|              |                  | IP Address  | Validated            | Delete        | om., s <sup>.</sup> |
| agility_p    |                  | <click add="" address="" an="" here="" ip="" to=""></click>                         |                      | Un            | 5 7                 |
|              | 5                |   |                      |               | 7                   |
| đ            |                  |   |                      | Down          | 5                   |
| agility_p    |                  | Click here to a   | dd the IP addr       | ess           | 2.                  |
|              |                  |   |                      |               |                     |
|              |                  |   |                      |               |                     |
| PuTTY (      | <                |   |                      | OK Cancel     |                     |
|              |                  |   |                      |               |                     |
|              |                  |   |                      |               |                     |
| Notepa       |                  |   |                      | • 🖻           | P 🕼                 |
|              |                  |   |                      |               |                     |
| 灯 Start 🥖 g  | 🧬 🛛 🙀 🐼 Com      | mand Prompt 🛛 🛼 DC01 - 10.1   | .70.200              |               |                     |

Repeat to add ns2.example.com

| - 10.1.70.200 - Remote De  | sktop Connection  |   |  |  |  |  |  |
|--|---|---|--|--|--|--|--|
|  |   | DNS Manager   |  |  |  |  |  |
| ction View Help  |   | New Delegation Wizard   |  |  |  |  |  |
| 2 🖬 🗙 🗎 Q 🗟  | Name  | Name Servers<br>You can select one or more name servers to host the delegated zone.   |  |  |  |  |  |
| CO1 Forward Lookup Zones CO1 Forward Lookup Zones CAMPLE.COM CAMPL | <ul> <li>msdcs</li> <li>sites</li> <li>tcp</li> <li>udp</li> <li>branch01</li> <li>DomainDnsZones</li> <li>ForestDnsZones</li> <li>mgmt</li> <li>site1</li> <li>site2</li> <li>(same as parent folder)</li> <li>ns1</li> </ul> | Specify the names and IP addresses of the DNS servers you want to have host the delegated zone.          Name servers:         Server Fully Qualified Domain Name (FQDN)         IP Address         ns1.example.com.         Add         Edit         Remove            Add         Edit         Remove |  |  |  |  |  |
| III >  | ns2   | Host (A) 198.51.100.40  |  |  |  |  |  |
| 2  | <b>2</b>  |   |  |  |  |  |  |

4. Also add "ns2.example.com - 198.51.100.40"



5. Make sure both ns1.example.com and ns2.example.com are added

| 0.1.70.200 - Remote De   | sktop Connection   |   |    |  |  |  |  |  |
|--|--|---|----|--|--|--|--|--|
| DNS Mapager  |  |   |    |  |  |  |  |  |
| on View Help   |  | New Delegation Wizard   |    |  |  |  |  |  |
| a 📰 🗙 📰 a 🖻  | Name   | Name Servers<br>You can select one or more name servers to host the delegated zone.   |    |  |  |  |  |  |
| >1         Forward Lookup Zones         _msdcs.EXAMPLE.COM         > | <ul> <li>_msdcs</li> <li>_sites</li> <li>_tcp</li> <li>_udp</li> <li>branch01</li> <li>DomainDnsZones</li> <li>ForestDnsZones</li> <li>mgmt</li> <li>site1</li> <li>site2</li> <li>(same as parent folder)</li> </ul> | Specify the names and IP addresses of the DNS servers you want to have host the delegated zone.          Name servers:         Server Fully Qualified Domain Name (FQDN)       IP Address         ns1.example.com.       [203.0.113.8]         ns2.example.com.       [198.51.100.40] |    |  |  |  |  |  |
| Trust Points<br>Conditional Forwarders                               | dc01   | < Back Next > Cano  | el |  |  |  |  |  |
| GIODAI LOGS  | ns2  | Host (A) 198.51.100.40  |    |  |  |  |  |  |
| III >  |  | 1   |    |  |  |  |  |  |
|  |  |   | •  |  |  |  |  |  |

6. Click "Finish"



### 2.1.8.3 CNAME

A CNAME (Canonical name record) functions as an alias for another domain name. Create a CNAME for "www" an as alias to www.gslb.example.com. When configured, this will result in a query for www.example.com to be directed to the name www.gslb.example.com where a subsequent A record query will be resolved.

1. Make sure "Forward Lookup Zones" and "EXAMPLE.COM" is expanded. Right click on "www", and select delete.



2. Right click on "EXAMPLE.COM", and select "New Alias (CNAME)"



3. Add "www - www.gslb.example.com"

| 👼 DC01 - 10.1.70.200 - Remote De  | sktop Connection  |                                 |                                   |                  |
|---|-------------------|---------------------------------|-----------------------------------|------------------|
| Å   |                   | DN                              | IS Manager                        |                  |
| File         Action         View         Help   |                   | ČI.                             |                                   |                  |
| a dns   | Name              | Type                            | Data                              | Timestamp        |
| ⊿ 📋 DC01  | 🛐 _msdcs          |                                 |                                   |                  |
| Forward Lookup Zones Signature Control Contr        | <pre></pre>       | New R                           | esource Record                    | ×                |
| A DEVAMPLE.COM  | 🚞 _udp            |                                 |                                   |                  |
| ⊳ <sub>[⊆]</sub> _msacs   | branch01          | Alias (CNAME)                   |                                   |                  |
| ⊳ <u> </u>  | DomainDnsZon      | Alias name (uses parent domain  | n if left blank):                 |                  |
| ⊳ 🧰 _udp  | mamt              | www                             |                                   |                  |
| ▷ Dranch01  | site1             | Fully qualified domain name (EC | DN):                              |                  |
| DomainDrszones  | 🚞 site2           | www.EXAMPLE.COM.                |                                   |                  |
| ⊳ 🧰 mgmt  | 🗊 gslb            |                                 |                                   |                  |
| ▷ ite1  | 📋 (same as parent | Full quarted domain marce (FC   | (UN) for target nost:             | c                |
| site2   | (same as parent   |                                 | Dr                                | owse             |
| E SID Solution Sol | (same as parent   |                                 | P exemple ee                      | /2017 12:00:00 A |
| Trust Points  | Client01          | WWW.GSL                         | D.example.co                      | 2017 12:00:00 A  |
| Conditional Forwarders  | 🔲 dc01            | Allow any authenticated use     | er to update all DNS records with | the same         |
| Global Logs   | ns1               | name. This setting applies o    | nly to DNS records for a new nan  | ne.              |
|   | lans2             |                                 |                                   |                  |
|   |                   |                                 |                                   |                  |
|   |                   |                                 |                                   |                  |
|   |                   |                                 | OK                                | Cancel           |
|   | I                 |                                 |                                   |                  |
|   |                   |                                 |                                   |                  |
| <   |                   |                                 |                                   |                  |
|   | 6                 |                                 |                                   |                  |
|   | Å                 |                                 |                                   |                  |

#### 2.1.8.4 Results

From the Jumpbox use "dig" from the CMD prompt

Do not specifing an IP address to the dig command, DNS requests will use the locally configured DNS server (the DC01 server).

The results will be similar to that of the image below. The first request for the CNAME www.example.com was resolved to a CNAME of www.gslb.example.com, and the DNS server also inserts the resolved CNAME to 203.0.113.9; the IP address of gtm1.site1. A subsequent DNS query resolved to 198.51.100.41 which follow the round-robin algorithm configured on the pool.





| Ho<br>IP | stname: gtm1.site1.example.com<br>Address: 10.1.10.13 | Date:<br>Time: | Jul 2<br>11:21  | 9, 2018<br>1 PM (EC | User: adr<br>DT) Role: Ad | <b>nin</b><br>ministra | itor      |                |              |         |       | Part     | tition: |
|----------|---|----------------|-----------------|---------------------|---------------------------|------------------------|-----------|----------------|--------------|---------|-------|----------|---------|
|          | ONLINE (ACTIVE) Standalone                            |                |                 |                     |                           |                        |           |                |              |         |       |          |         |
|          | Main Help About                                       |                | Stat            | tistics >           | » Module Statis           | tics : C               | ONS : GSL | В              |              |         |       |          |         |
| m_       | Statistics  |                | \$              | ➡ Trafi             | fic Summary 🔫             | DNS                    | 3         | ▼ Sul          | oscriber Man | agement | Netw  | ork      |         |
|          | Dashboard   | e.             |                 |                     |                           |                        |           |                |              |         |       |          |         |
|          | Module Statistics                                     | •              | Disp            | lay Opti            | ions                      |                        |           |                |              |         |       |          |         |
|          | Analytics   | •              | Statistics Type |                     |                           |                        | Wide IPs  |                |              |         |       |          |         |
|          | Performance   | •              | Dat             | ta Forma            | at                        | I                      | Normalize | ed 🔽           |              |         |       |          |         |
|          | iApps   |                | Aut             | o Refres            | sh                        |                        | Disabled  | Refr<br>Search | esh          |         | Re    | quests   |         |
| 53       | DNS   |                |                 | Status              | ▲ Wide IP                 |                        | Туре      | Partition / P  | ath Details  | Pools   | Total | Resolved | Re      |
| ?        | Acceleration  |                |                 | ot l                | www.example.c             | om                     | A         | Common         | View         | ∕iew    | 44    | 44       | 0       |
| 3        | Device Management                                     |                | 1163            | Ser                 |                           |                        |           |                |              | -       |       |          |         |
|          | Network   |                | F               | 0                   | r mo                      | )r                     | e         | let            | ail          | 5 6     |       | ck       |         |
| 8 🕈      | System  |                | -               |                     |                           |                        |           |                |              |         |       |          |         |
|          |   |                |                 |                     |                           |                        |           |                |              |         |       |          |         |
|          |   |                |                 |                     |                           |                        |           |                |              |         |       |          |         |

Note: Geographically redundant Web service by using BIG-IP DNS have been configured. Great job!

# TMSH

tmsh show gtm wideip A www.example.com detail

| g <sup>2</sup> gtm1.SITE1   |
|---|
| [root8gtm1:Active:Standalone] config # tmsh show gtm wideip A www.example.com detail                |
|   |
| Gtm::WideIp::A www.example.com  |
| Status  |
| Availability : available  |
| State : enabled   |
| Reason : Available  |
| Requests  |
| Total 44<br>Persisted 0   |
| Resolved 44   |
| Dropped O   |
| Load Balancing  |
| Preferred 44  |
| Alternate O   |
| CNAME Resolutions 0   |
| Returned from DNS 0   |
| Returned to DNS O   |
|   |
|   |
| Gtm::Pool::A www.example.com_pool   |
|   |
| Status<br>Availability : available  |
| State : enabled   |
| Reason : Available  |
| Load Balancing  |
| Preferred 44  |
| Alternate O   |
| Returned from DNS 0   |
| Returned to DNS 0   |
| Dropped O   |
|   |
| Gtm::Pool Member: www.example.com_pool:A isp1_site1_www.example.com_tcp_https_virtual:site1_ha-pair |
| Status  |
| Availability : available  |
| State : enabled   |
| Reaboli . Available   |
| Load Balancing  |
| Preferred 35  |
| Fallback 0  |
|   |
| Gtm::Virtual Server: isp1_site1_www.example.com_tcp_https_virtual                                   |
| Status  |
| Availability : available  |
| State : enabled<br>Peason : Monitor /Common/bigin from 203 0 113 5 : UP                             |
| Destination : 203.0.113.9:443   |
| Up Time : 10:18   |
| Link Name 203.0.113.1   |
|   |
| Global  |
| Connections 0   |
| Virtual Server Score 1  |
| Throughput In Out   |
| Bits/sec 0 0  |
| Packets/sec 0 0   |
|   |
| Gtm::Pool Member: www.example.com_pool:& isp2_site2_www.example.com_tcp_https_virturd:site2_ho-paid |
| Status  |
| Availability : available  |
| State : enabled   |

### TMSH

tail -f /var/log/ltm

| atm1.SITE1  |
|---|
| Front@stm1.%stive.Standalonel_config # tail_f _n 12 /var/log/ltm                                  |
| Jul 30 00:19:49 gtml info tmm[1966]: 2018-07-30 00:19:49 gtml.sitel.example.com gid 991 from 198  |
| .51.100.68#64119: view none: guery: www.gslb.example.com IN & + (203.0.113.8%0)                   |
| Jul 30 00:19:49 gtml info tmm[11966]: 2018-07-30 00:19:49 gtml.sitel.example.com gid 991 from 198 |
| .51.100.68#64119 [www.gslb.example.com A] [round robin selected pool (www.example.com pool)] [poo |
| 1 member check succeeded (isp1 site1 www.example.com tcp https virtual:203.0.113.9) - pool member |
| state is available (green)] [round robin selected pool member (isp1 site1 www.example.com tcp ht  |
| tps virtual:203.0.113.9)]   |
| Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com qid 991 to 198.5 |
| 1.100.68#64119: [NOERROR qr,aa,rd] response: www.gslb.example.com. 30 IN & 203.0.113.9;           |
| Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 from 198 |
| .51.100.68#64120: view none: query: www.gslb.example.com IN & + (203.0.113.8%0)                   |
| Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 from 198 |
| .51.100.68#64120 [www.gslb.example.com A] [round robin selected pool (www.example.com pool)] [poo |
| l member check succeeded (isp1 site1_www.example.com tcp_https virtual:203.0.113.9) - pool member |
| state is available (green)] [round robin selected pool member (isp1_site1_www.example.com_tcp_ht  |
| tps_virtual:203.0.113.9)]   |
| Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 to 198.5 |
| 1.100.68#64120: [NOERROR qr,aa,rd] response: www.gslb.example.com. 30 IN & 203.0.113.9;           |
| Jul 30 00:23:44 gtm1 info tmm[11966]: 2018-07-30 00:23:43 gtm1.site1.example.com qid 261 from 203 |
| .0.113.68#64121: view none: query: www.example.com IN & + (203.0.113.8%0)                         |
| Jul 30 00:23:44 gtm1 info tmm[11966]: 2018-07-30 00:23:43 gtm1.site1.example.com qid 261 from 203 |
| .0.113.68#64121 [www.example.com A] [round robin selected pool (www.example.com_pool)] [pool memb |
| er check succeeded (isp2_site2_www.example.com_tcp_https_virtual:198.51.100.41) - pool member sta |
| te is available (green)] [round robin selected pool member (isp2_site2_www.example.com_tcp_https_ |
| virtual:198.51.100.41)]   |
| Jul 30 00:23:44 gtml info tmm[11966]: 2018-07-30 00:23:43 gtml.sitel.example.com qid 261 to 203.0 |
| .113.68#64121: [NOERROR qr,aa,rd] response: www.example.com. 30 IN & 198.51.100.41;               |
| Jul 30 00:23:50 gtml info tmm[11966]: 2018-07-30 00:23:50 gtml.sitel.example.com qid 97 from 203. |
| 0.113.68#64122: view none: query: www.example.com IN & + (203.0.113.8%0)                          |
| Jul 30 00:23:50 gtml info tmm[11966]: 2018-07-30 00:23:50 gtml.sitel.example.com qid 97 from 203. |
| 0.113.68#64122 [www.example.com &] [round robin selected pool (www.example.com_pool)] [pool membe |
| r check succeeded (ispl_sitel_www.example.com_tcp_https_virtual:203.0.113.9) - pool member state  |
| is available (green)] [round robin selected pool member (ispl_sitel_www.eXample.com_tcp_https_vir |
| tual:203.0.113.9)]  |
| Jul 30 00:23:50 gtml info tmm[11966]: 2018-07-30 00:23:50 gtml.sitel.example.com qid 97 to 203.0. |

# 2.1.9 Failure Condition

Having followed the excercises up to this point will have resulted in the creation of an active/active disaster recovery topology. An alternating response is received when querying www.example.com. From the command prompt in the Jumpbox type "dig www.example.com". Repeat dig commands and observe the TTL counting down.

| 2               |   |  |
|-----------------|---|--|
| agility_prv     |   |  |
| _               |   |  |
|                 | i; MSG SIZE roud: 72  |  |
| PuTTY (64-bit)  |   |  |
|                 | C:\Users\user.EXAMPLE>dig www.example.com   |  |
| 0++             | ; <<>> DiG 9.3.2 <<>> www.example.com<br>;; global options: printcmd                              |  |
|                 | ;; Got answer:<br>;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 838                         |  |
| Notepau++       | ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0                           |  |
|                 | ;; QUESTION SECTION:<br>;www.example.com. IN A  |  |
| - 🔁             | , HNSWER SECTION:   |  |
| Mozilla Firefox | www.example.com. 3600 IN CNAME www.gslb.example.com.<br>www.gslb.example.com. 30 IN A 203.0.113.9 |  |
|                 | ;; Query time: ji Note  |  |
|                 | ;; SERVER: 1011.70.207453(10.1.70.200)<br>;; WHEN: Sun Jun 25 21:37:31 2017                       |  |
| Coordo          | , Not SILE FLOW. 2  |  |
| Chrome          | C:\Users\user.EXP iPLE>dig www.example.com_   |  |
| _               |   |  |
| s 💽             |   |  |
| Recycle Bin     |   |  |
|                 |   |  |
|                 |   |  |
|                 |   |  |
| Start 🖉 🖉 BI    | IG-IP® - gtm1.site2.ex 📴 🖸 👩 🗰 Command Prompt 💋 🍢 DC01 - 10.1.70.200 - Re                         |  |

Log into both the Active and the Standby ADC device in SITE1 and disable all interfaces. https://bigip1.site1.example.com/tmui/Control/jspmap/tmui/locallb/network/interface/list.jsp https://bigip2.site1.example.com/tmui/Control/jspmap/tmui/locallb/network/interface/list.jsp

| Hos<br>IP A | tname:<br>\ddress: | bigip1.site1.exa<br>10.1.10.11 | mple.com        | Date: /<br>Time: 1 | Aug 9,<br>10:40 F | 2018<br>PM (EDT | User<br>) Role: | admin<br>Administrator |      |   |            |
|-------------|--------------------|--------------------------------|-----------------|--------------------|-------------------|-----------------|-----------------|------------------------|------|---|------------|
| ſ           | 5                  | ONLINE (AC<br>In Sync          | TIVE)           |                    |                   |                 |                 |                        |      |   |            |
| N           | lain               | Help                           | About           |                    | Netwo             | rk» I           | nterfaces :     | Interface List         |      |   |            |
| 6           | SSL O              | rchestrator                    |                 | 18                 | ¢ -               | Interfa         | ce List         | Interface Mirroring    | LLDP |   | Statistics |
| ^           | Statist            | tics                           |                 |                    |                   |                 |                 |                        | ]    |   |            |
| -           | iApps              |                                |                 | Ī                  | <b>~</b>          | Status          | ▲ Name          |                        |      |   |            |
| 2-2         | Local              | Traffie                        |                 | Ē                  | <b>7</b> U        | P               | 1.1             |                        |      |   |            |
| -UL         | Local              | Trame                          |                 | E                  | <b>7</b> UI       | Þ               | 1.2             |                        |      |   |            |
|             | Device             | e Management                   | :               | 6                  | <b>7</b> UI       | Þ               | 1.3             |                        |      |   |            |
|             | Notwo              | rk                             |                 | 6                  | <b>7</b> UI       | Þ               | 1.4             |                        |      |   |            |
|             | Netwo              |                                |                 | 6                  | <b>7</b> UI       | P               | 1.5             |                        |      |   |            |
|             | hte                | rfaces                         |                 |                    | <b>7</b> UI       | >               | 1.6             |                        |      |   |            |
|             | Rou                | ıtes                           | $(\Rightarrow)$ |                    | Enable            | Dis             | able            |                        |      |   |            |
|             | Self               | fIPs                           | $(\Rightarrow)$ |                    |                   |                 |                 |                        |      |   |            |
|             | Pad                | ket Filters                    |                 | Þ                  |                   |                 | lia             |                        | aabl |   |            |
|             | Tru                | nks                            |                 | Þ                  |                   |                 |                 |                        | Japi | 9 |            |
|             |                    |                                |                 |                    |                   |                 |                 |                        |      |   |            |

TMSH command to run on bigip1.site1 and bigip2.site1 to simulate a network failure

# TMSH

tmsh modify interface all disabled

Log into gtm1.site1 and observe the status of "Server" objects:

| Hostname: gtm1.site1.example.com<br>IP Address: 10.1.10.13 | Date:<br>Time: | Aug 9, 2018<br>11:01 PM (EDT) | User:<br>Role:           | <b>admin</b><br>Administrator |              |
|--|----------------|-------------------------------|--------------------------|-------------------------------|--------------|
| ONLINE (ACTIVE)<br>Standalone                              |                |                               |                          |                               |              |
| Main Help About  |                | DNS » GSLB                    | Servers                  | : Server List                 |              |
| Magazine Statistics  |                | 🔅 🗸 Server L                  | ist                      | Trusted Server Certificates   | Statistics 🗾 |
| iApps  |                | *                             |                          | Search                        |              |
| S DNS  |                | 🖌 💌 Status                    | <ul> <li>Name</li> </ul> |                               | Devices A    |
| Delivery   | •              |                               | gtm1.site                | 1_server                      | 1 20         |
| GSLB   | •              |                               | gtm1.site                | 2_server                      | 1 19         |
| Zones  | •              |                               | site1_ha                 | pair                          | 2 20<br>20   |
| Caches   | F              |                               | site2_ha                 | ir ir                         | 2 19         |
| Settings   | •              | Enable Disat                  | ole Del                  | ete                           |              |
| Acceleration   |                |                               |                          |                               |              |
| Device Management  |                | Site                          | LH                       | A pair is                     | Down         |
| Retwork  |                |                               |                          |                               |              |

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/server/list.jsp

# TMSH

tmsh show gtm server



Log into bigip1.site1 and bigip2.site1 and enable all interfaces

https://bigip1.site1.example.com/tmui/Control/jspmap/tmui/locallb/network/interface/list.jsp

https://bigip2.site1.example.com/tmui/Control/jspmap/tmui/locallb/network/interface/list.jsp

#### TMSH

tmsh modify interface all enabled

### 2.1.10 Rest API

#### 2.1.10.1 Authenticate

From the Jumpbox using the Postman application navigate to the "API" section under the Collections on the left.

Note: Config Sync has been enabled in previous lab tasks. All of the iControlREST configuration changes will be performed only on gtm1.site1 and changes will automatically synchronized to gtm1.site2

1. Reveal the navigation panel in Postman



2. Click on "Authenticate and Obtain Token from gtm1.site1".



3. Click on the "Send" button in the top right.

| Get GTM F Create a \ | example.com_environment | t  | · «    | •   | ۵    |
|----------------------|-------------------------|----|--------|-----|------|
|                      |                         | Ex | amples | (0) | •    |
|                      | Params Send             | •) | Save   | 2   | Ŧ    |
|                      |                         |    | Cookie | s C | Iode |

4. Open the respone body and observe the received token. The token value is dynamic and your result will not be the same as illustrated below. The token received will be used for all subsequent authenticated actions with the BIG-IP DNS.

| POST  | https://{{gtm1.site1}}/mgmt/shared/authn/login   |
|---|--|
| Pretty  | Raw Preview JSON -   |
| 1 • {<br>2<br>3 •<br>4<br>5<br>6<br>7 •<br>8<br>9<br>10<br>11<br>12 •<br>13<br>14<br>15<br>16<br>17<br>18<br>19<br>20<br>21<br>22 | <pre>"username": "admin",<br/>"loginReference": {<br/>"link": "https://localhost/mgmt/cm/system/authn/providers/local/login"<br/>},<br/>"loginProviderName": "local",<br/>"token": [<br/>"token": "IK54KQEQECEBAS3UHUAOMOW5XV",<br/>"name": "IK54KQEQECEBAS3UHUAOMOW5XV",<br/>"userName": "dofmin",<br/>"userName": "dofmin",<br/>"authProviderName": "local",<br/>"user": {<br/>"link": "https://localhost/mgmt/shared/authz/users/admin"<br/>},<br/>"groupReferences": [],<br/>"timeout": 1200,<br/>"startTime": "2018-08-07T11:40:20.671-0400",<br/>"address": "10.1.10.100",<br/>"partition": "[All]",<br/>"generation": 1,<br/>"lastUpdateMicros": 1533656420670671,<br/>"expirationMicros": 1533657620671000,<br/>"timeout": "</pre> |
| 24<br>25  | "selfLink": "https://localhost/mgmt/shared/authz/tokens/IK54KQEQECEBAS3UHUAOMOW5XV" },   |

#### 2.1.10.2 POST

Authentication tokens have been acquired in the previous step, and will be used to create new BIG-IP DNS configurations. A new FTP service will be created, which includes the automated creation of a new pool and a Wide-IP.

Using the Postman application, select the "API" collection, and navigate to each of the next 4 requests and click Send for each.



Once complete, login to gtm1.site1 via Web interface and look for the new configuration elements to confirm that they were successfully created. Do the same on gtm1.site2.

#### 2.1.10.3 Results

Now lets test the new service we created. The related configuration on the BIG-IP LTM and on the Microsoft DNS server are already complete for you. Open up FileZilla from your client workstation and connect to the DNS service ftp.example.com. This is a CNAME for ftp.gslb.example.com.

#### Note: Use FTP credentials admin/admin

| 🔁 admin@ftp.example.com - FileZilla   |
|---|
| File Edit View Transfer Server Bookmarks Help New version available!        |
| H - 🖹 🗂 🗮 😂 🎼 😂 🛼 🔛 🔳 🍳 🦘 🦚   |
| Host: [ftp.example.com Username: admin Password: ••••• Port: Quickconnect • |
| Status: Resolving address of ftp.example.com                                |
| Status: Connecting to 203.0.113.9:21  |
| Status: Connection established, waiting for welcome message                 |
| Status: Insecure server, it does not support FTP over TLS.                  |
| Status: Logged in   |
| Status: Retrieving directory listing  |
| Status: Calculating timezone offset of server                               |
| Status: Timezone offset of server is 0 seconds.                             |
| Status: Directory listing of "/home/admin" successful                       |
|   |

You've just successfully created a new highly available service on BIG-IP DNS all with only a few very simple API commands.

### 2.1.10.4 Active/Standby

Create a brand new configuration element that is relevant to a disaster recovery design, where site 2 is converted to a standby site.

In order to make site2 a standby site, modify the load balancing method of each of its pools from "Preferred" to "Global Availability". Demonstrate the behavior using the dig command on the Jumpbox. For more information on GSLB load balancing please refer to the link below.

Open Postman and send both of the patch commands below.



Login to the web interface of both gtm1.site1 and gtm1.site2 to witness the change. Confirm with dig that the load balancing method is working as intended, what has changed? You should now be seeing a consistent DNS respone when querying either ftp.example.com or www.example.com instead of the round robin behavior.

### 2.1.10.5 API Extras (Optional)

In Postman, feel free to browse the other collections and experiment with additional REST commands.

Note: Please note that some of the commands in the collections may not be working. Challenge yourself and fix one or two !



F5 supports many APIs (Application Programmable Interfaces) including TMSH, WebUI, iControlREST, iControlLX and SNMP to name a few. In this task, the example company will deploy an additional service for FTP which requires geographic high availability. Postman will be used to execute configuration changes on the BIG-IP, which uses the iControlREST interface.

Note: We are using Postman for demonstration purposes. All of the REST commands could also be issued via curl if desired.

| update_do Rervrie kin            |                              |                                 |                              |                        |
|----------------------------------|------------------------------|---------------------------------|------------------------------|------------------------|
| Postman<br>File Edit View Help   |                              |                                 |                              |                        |
| Internet<br>Explorer             | Runner 📭 🖬                   | example.com_workspace           | 🔹 🌲 Invite 🧿 🕚               | 2 4                    |
| filezilla.exe -<br>Shortcut      | pen th                       |                                 | stera Ve<br>stma             | <sup>com_e</sup>       |
| POST - https://                  | //{{etm1.site1}}/memt/tm/etm |                                 | Params                       |                        |
| Command Prompt                   | APP                          | licatio                         |                              |                        |
| 🔁 FileZilla                      |                              |                                 |                              |                        |
| PuTTY (64-bit)                   | Documents                    |                                 |                              |                        |
| C Google Chrome                  |                              |                                 |                              |                        |
| 💀 Remote Desktop Connection 🔹 🕨  | Downloads                    | quest is not inheriting any aut | orization beloer at the more | ent S                  |
| Postman                          | Recent Items +               | the p                           | arent's authorization helper | ,                      |
| Votepad+                         | Computer                     |                                 |                              |                        |
| Notepad  CuteFTP 9               | Control Panel                |                                 |                              |                        |
| BIG-IP Edge Client               | Devices and Printers         |                                 |                              |                        |
| Snipping Tool                    | Default Programs             |                                 |                              | -                      |
| · · · · ·                        | Administrative Tools         |                                 |                              |                        |
|                                  | Run                          |                                 |                              |                        |
| All Programs                     | Windows Security             | Canal builters to ant           | Build                        | Bro                    |
| Is 1 rosrams and files           | Log off                      |                                 | 0010                         |                        |
| Start 🦙 🤕 Rest API — Reference A | C:\Windows\system32\c        | 💋 Postman                       | gtm1.SITE1                   | Buser@docker:~/example |

# 2.1.11 Congratulations

You have successfully completed the 'Data Center Availability Services Using BIG-IP DNS' lab.



- Students will configure F5 DNS servers to support GSLB (Global Services Load Balancing) on a single device in site1.
- Join an additional F5 DNS server in site2 to the GSLB cluster.
- An Internal group of DNS servers is authoritative for the zone example.com and contains a static A record for "www.example.com", which resolves to 203.0.113.9.
- Students will add glue records and delegate gslb.example.com to the F5 GSLB DNS servers.
- Convert the A record "www.example.com" to be a CNAME record pointing to www.gslb.example.com.
- · Students will create an additional GSLB service using iControl REST
- · Modify the DNS load balancing method from active/active to active/standby

By the end of the lab students will have configured F5 GSLB DNS servers to alternately resolve www.example.com to 203.0.113.9 and 198.51.100.41. At the end of the lab, students will then have an opportunity to simulate a real-life failure scenario and observe how BIG-IP DNS responds to mitigate the service outage.

# 2.2 Security

The lab environment consists of a Lan of workstations in a remote location with internal DNS servers behind an F5 firewall.
The F5 device is directly connected to the internet.



Students will work with the following concepts as part of a group of lab exercises.

- 1. Transparent Cache
- 2. Hidden Master
- 3. DNSSec
- 4. Validating Resolver
- 5. RPZ
- 6. URL Categorization

# 2.2.1 Transparent Cache

#### 2.2.1.1 Monitors

A DNS application specific health monitor provides intelligence in the steering DNS queries towards the fastest responding DNS server.



Navigate to: Delivery : Load Balancing : Monitors

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 18, 2017<br>Time: 1:30 PM (CDT) | User: <b>admin</b><br>Role: Administrator | Partition: Commo |
|---|---|---|------------------|
| Standalone  |   |   |                  |
| Main Help About   | DNS » Delivery : Load                     | Balancing : Monitors                      |                  |
| Mage Statistics   | 🔅 👻 Monitor List                          |   |                  |
| iApps   | r   | × Search                                  | Create           |
| S DNS   | ✓ ▲ Name                                  |   | Application      |
| Delivery 🔒 💦 🔸  | Listeners                                 |   | Gatew            |
| GSLB  | Profiles                                  |   | HTTP             |
| Zones   | Load Balancing                            | Pools                                     | HTTP             |
| Caches  | iRules                                    | Nodes                                     | HTTP:            |
| Cattings  | Translation                               | Monitore                                  | HTTP:            |
| Setungs   | Translation                               | Monitors                                  | HTTPS            |
| SSL Orch and in   | Nameservers                               |   | ICMP             |
|   | Keys                                      |   | Inband           |
| Local Traffic   | real_server                               |   | Real S           |
| Acceleration  | 🔲 snmp_dca                                |   | SNMP             |
| _   | C tcp                                     |   | TCP              |
| Device Management   | tcp_echo                                  |   | TCP E            |
| Network   | tcp_half_open                             |   | TCP H            |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/monitor/list.jsp

Create a monitor according to the following table:

| Field      | Value                   |
|------------|-------------------------|
| Name       | example.com_dns_monitor |
| Туре       | DNS                     |
| Query Name | www.example.com         |

| General Properties      |                         |
|-------------------------|-------------------------|
| Name                    | example.com_dns_monitor |
| Description             |                         |
| Туре                    | DNS                     |
| Parent Monitor          | dns 🗸                   |
| Configuration: Advanced |                         |
| Interval                | 5 seconds               |
| Up Interval             | Disabled                |
| Time Until Up           | 0 seconds               |
| Timeout                 | 16 seconds              |
| Manual Resume           | ⊖ Yes   No              |
| Reverse                 | ⊖ Yes 	● No             |
| Alias Address           | * All Addresses         |
| Alias Service Port      |                         |
| Query Name              | www.example.com         |
| Query Type              | a 🔽                     |
| Answer Section Contains | Query Type 🗸            |
| Accept RCODE            | No Error 🗸              |
| Receive String          |                         |
| Adaptive                |                         |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/monitor/create.jsp

## TMSH

tmsh create ltm monitor dns example.com\_dns\_monitor defaults-from dns qname www.example.com

## 2.2.1.2 Load Balancing

Augment and scale an existing DNS infrastructure by Load Balancing DNS queries across a pool of DNS servers.

Navigate to: Delivery : Load Balancing : Pools : Pool List

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 18, 2017<br>Time: 1:22 PM (CDT) | User: <b>admin</b><br>Role: Administrator |            |        |
|---|---|---|------------|--------|
| ONLINE (ACTIVE) Standalone  |   |   |            |        |
| Main Help About   | DNS » Delivery : Load                     | Balancing : Pools : Pool List             |            |        |
| Statistics  | 🚓 👻 Pool List                             | Statistics 🗾                              |            |        |
| iApps   | *   | × Search                                  |            | Create |
| S DNS   | Status 🔺 Name                             |   |            | \$ Des |
| Delivery  | Listeners >                               | ateway_pool                               |            |        |
| GSLB  | Profiles                                  |   |            |        |
| Zones   | 2 Load Balancing                          | <sup>3</sup> Pools ▶                      | Pool List  | (+)    |
| Caches  | iRules                                    | Nodes >                                   | Statistics |        |
| Settings  | Translation >                             | Monitors 💮                                |            |        |
| E cel Carbonat  | Nameservers                               |   |            |        |
| SSL Orchestrator  | Keys >                                    |   |            |        |
| Local Traffic   |   |   |            |        |
| Acceleration  |   |   |            |        |
| Device Management   |   |   |            |        |
| Network   |   |   |            |        |

Create a pool according to the following table:

| Field           | Value                          |
|-----------------|--------------------------------|
| Name            | branch01_dns_pool              |
| Health Monitors | example.com_dns_monitor        |
| 1. Node Name    | dc01.branch01.example.com_node |
| 1. Address      | 10.1.70.200                    |
| 1. Service Port | 53                             |
| 2. Node Name    | dc02.branch01.example.com_node |
| 2. Address      | 10.1.70.210                    |
| 2. Service Port | 53                             |

| Configuration: Advanced   |  |
|---------------------------|--|
| Name                      | branch01_dns_pool  |
| Description               |  |
| Health Monitors           | Active Available //Common example.com_dns_monitor <  |
| Availability Requirement  | All Health Monitor(s)  |
| Allow SNAT                | Yes  |
| Allow NAT                 | Yes  |
| Action On Service Down    | None   |
| Slow Ramp Time            | 10 seconds   |
| IP ToS to Client          | Pass Through   |
| IP ToS to Server          | Pass Through   |
| Link QoS to Client        | Pass Through   |
| Link QoS to Server        | Pass Through   |
| Reselect Tries            | 0  |
| Enable Request Queueing   | No Y   |
| Request Queue Depth       | 0  |
| Request Queue Timeout     | 0 ms   |
| IP Encapsulation          | None 🔽   |
| Resources                 |  |
| Load Balancing Method     | Round Robin  |
| Priority Group Activation | Disabled   |
| New Members               | New Node O New FQDN Node O Node List Node Name: dc02.branch01.example.com_node (Optional) Address: 10.1.70.210 Service Port: 53 Select Add R:1 P:0 C:0 dc01.branch01.example.com_node 10.1.70.200 :53 R:1 P:0 C:0 dc02.branch01.example.com_node 10.1.70.210 :53 |
|                           | Edit Delete  |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/pool/create.jsp

### TMSH

tmsh create ltm pool branch01\_dns\_pool members add { dc01.branch01.example.com\_node:53 { address 10.1.70.200 } dc02.branch01.example.com\_node:53 { address 10.1.70.210 } } monitor exam-

### 2.2.1.3 Results

1. Navigate to: DNS >> Delivery : Load Balancing : Pools : Pool List

Click to select the branch01\_dns\_pool, and then click "Members"

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 18, 2017<br>Time: 3:41 PM (CDT) | User: <b>admin</b><br>Role: Administrator |  |
|---|---|---|--|
| ONLINE (ACTIVE)<br>Standalone                                     |   |   |  |
| Main Help About   | DNS » Delivery : Loa                      | oad Balancing : Pools : Pool List         |  |
| Mage Statistics   | 🔅 🗸 Pool List                             | Statistics                                |  |
| iApps   | ł   | × Search                                  |  |
| 😚 dns   | Status 🔺 Nar                              | ame                                       |  |
| Deliver, 1  | Listeners                                 | ▶ _dns_pool                               |  |
| GSLB  | Profiles                                  | ateway_pool                               |  |
| Zones   | oad Balancing                             | 3 pole 4 Pool List                        |  |
| Cash  | iDulas                                    |   |  |
| Cachis  | IRules                                    | Nodes Statistics                          |  |
| Settings  | ranslation                                | Monitors (+)                              |  |
| E SSI John Fator  | Namervers                                 | 5   |  |
| SSL TCD stran   | Keys                                      |   |  |
| Local Traffic   |   |   |  |
| Acceleration  |   |   |  |
| Device Management   |   |   |  |
| Retwork   |   |   |  |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/pool/list.jsp

2. Click to select "branch01\_dns\_pool", and then select "Members"

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 18, 2017 U<br>Time: 3:47 PM (CDT) R | lser: <b>admin</b><br>tole: Administrator  |
|---|---|--|
| ONLINE (ACTIVE) Standalone  |   |  |
| Main Help About   | DNS » Delivery : Load B                       | alancing : Pools : Pool List » Properties : branch01_dns_pool                              |
| Mage Statistics   | 🔅 👻 Properties                                | Members Statistics   |
| iApps   | General Properties                            |  |
| S DNS   | Name  | branch01_dns_pool  |
| Delivery >  | Partition / Path                              | Common   |
| GSLB  | Descriptic                                    |  |
| Zones   | Availoility                                   | Available (Enabled) - The pool is available  |
| Caches C  |   | embers"  |
| Settings  |   | Active Available   |
| SSL Orchestrator  | Health Monitors                               | /Common<br>example.com_dns_monitor<br>>> //Common<br>gateway_icmp<br>http_head_f5<br>https |
| Local Traffic   | Availability Requirement                      | All Health Monitor(s)  |
| Acceleration  | Allow SNAT                                    | Yes V  |
| Device Management   | Allow NAT                                     | Yes  |
| Network   | Action On Service Down                        | None   |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/pool/resources.jsp?name=/Common/branch01\_dns\_pool

3. Notice the health status of the existing DNS infrastructure.

| Hostn<br>IP Ad | ame: router01.branch01.example.com<br>dress: 10.1.10.31 | Date:<br>Time: | Jul 18, 20<br>4:54 PM (0 | 17 I<br>CDT) I | User: ;<br>Role: / | admin<br>Administrator |          |                             |           |       |        |    |
|----------------|---|----------------|--------------------------|----------------|--------------------|------------------------|----------|-----------------------------|-----------|-------|--------|----|
| ſ              | ONLINE (ACTIVE)<br>Standalone                           |                |                          |                |                    |                        |          |                             |           |       |        |    |
| Ma             | in Help About   | DNS            | » Delive                 | ry : Load E    | Balanc             | ing : Pools : P        | ool List | » Members                   | : branch0 | 1_dns | _pool  |    |
| M_ 9           | Statistics  | .⇔             | Properti                 | 25             | Меп                | ıbers                  | Statisti | :s 🛛                        |           |       |        |    |
| <b>i</b>       | Apps  | Load F         | alancing                 |                |                    |                        |          |                             |           |       |        |    |
|                | DNS   | Load           | Balancing                | Method         |                    | Round Robin            | n        |                             |           |       |        | _  |
|                |   | Eodd           | Balanting                | meaned         |                    |                        |          |                             |           |       |        |    |
|                | Delivery  | Priori         | y Group A                | Activation     |                    | Disabled               | $\sim$   |                             |           |       |        |    |
|                | GSLB  | Upda           | te                       |                |                    |                        |          |                             |           |       |        |    |
|                | Zones Notice  | that           | heal                     | th mo          | onit               | tors ma                | rke      | d one a                     | serve     | r d   | own    |    |
|                | Caches >  | Curren         | t Membe                  | rs             |                    |                        |          |                             |           |       |        |    |
|                | Settings >  |                | Status                   | A Member       | er                 |                        |          | <ul> <li>Address</li> </ul> | Service   | Port  |        | \$ |
| -              |   |                | 0                        | dc01.brar      | nch01.             | example.com_n          | ode:53   | 10.1.70.200                 | 53        |       |        | Nc |
| 6              | SSL Orchestrator  |                | •                        | dc02.brar      | nch01.             | example.com_n          | ode:53   | 10.1.70.210                 | 53        |       |        | No |
| lijî l         | ocal Traffic  | Enab           | e Disa                   | ble Ford       | e Offli            | ne Remove              | 1        |                             |           |       |        |    |
| <b>&gt;</b>    | Acceleration  | N              | layb                     | e tha          | <b>t's</b>         | why us                 | ers      | are co                      | mpla      | ini   | ng. It | 5  |
|                | Device Management                                       | 5              | eem                      | <u>s tha</u>   | ta                 | local D                | NS :     | server                      | is fa     | ilin  | g.     |    |
|                | letwork   |                |                          |                |                    |                        |          |                             |           |       |        |    |
|                |   |                |                          |                |                    |                        |          |                             |           |       |        |    |

# TMSH

tmsh show ltm pool branch01\_dns\_pool detail



In this module we will prepare the objects required to build a transparent cache.

In the next exercise a DNS profile will reference the cache and a Listener will forward traffic to a healthy backend DNS server



Enabling a transparent cache on the BIG-IP will offload some DNS queries from being sent to the internal DNS servers.



Log into the gateway device router01.brancho1 in the branch office

#### Navigate to DNS >> Caches : Cache List

Create a transparent cache

| Field         | Value             |
|---------------|-------------------|
| Name          | transparent_cache |
| Resolver Type | Transparent       |

| Hostname:<br>IP Address: | router01.branch<br>10.1.10.31 | 01.example.com | Date: Jun 20, 2017<br>Time: 9:38 PM (CDT) | User: admir<br>Role: Admir | n<br>nistrator    |       |
|--------------------------|-------------------------------|----------------|---|----------------------------|-------------------|-------|
| 6                        | ONLINE (AC                    | rive)          |   |                            |                   |       |
| Main                     | Help                          | About          | DNS » Caches : Cache                      | e List » Ne                | w                 |       |
| Magaza Statist           | ics                           |                |   |                            |                   |       |
| _                        |                               |                | General Properties                        |                            |                   |       |
| iApps                    |                               |                | Name                                      |                            | transparent_cache |       |
| 🌍 dns                    |                               |                | Resolver Type                             |                            | Transparent (None |       |
| Deli                     | very                          | Þ              | DNS Cache                                 |                            |                   |       |
| Zon                      | es                            | ×              | Message Cache Size                        |                            | 1048576           | bytes |
| Cac                      | hes                           |                | Cache List 📀                              | Size                       | 10485760          | bvtes |
| Jett                     | ings                          |                | Statistics                                |                            | Enabled           | _,    |
| SS SS                    | rchestrator                   |                | RRSet Rotate                              | Γ                          | none 🔽            |       |
| Local 1                  | Fraffic                       |                | Cancel Repeat Fir                         | ished                      |                   |       |
| Accele                   | ration                        |                |   |                            |                   |       |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/create.jsp

TMSH command for router01.branch01:

## TMSH

tmsh create ltm dns cache transparent transparent\_cache

## 2.2.2 Listeners

A listener object is an specialized virtual server that is configured to respond to DNS queries.

We will be creating both TCP and UDP based listeners that have the same IP address of the existing DNS server.

Note: the Workstation is configured to use 10.1.70.200 and 10.1.70.210 for DNS.

After this module students will have enabled the BIG-IP to intercept and cache DNS requests.



#### 2.2.2.1 Log Profile

Configure DNS query and response logging.

1. Create a "Log Publisher" for local syslog.

Navigate to: System >> Logs : Configuration : Log Publishers

| Hostna<br>IP Add | ime: gtm1.site1.example.com<br>ress: 10.1.10.13 | Date:<br>Time: | Jul 20, 2017<br>12:39 PM (CDT) | User: a<br>Role: a | admin<br>Administrator |         |              |                      | P      |
|------------------|---|----------------|--------------------------------|--------------------|------------------------|---------|--------------|----------------------|--------|
| ſ                | ONLINE (ACTIVE)<br>Standalone                   |                |                                |                    |                        |         |              |                      |        |
| Mai              | n Help About                                    |                | System » Logs                  | : Config           | uration : Log Publis   | shers   |              |                      |        |
| 1 S              | tatistics                                       |                | 🔅 👻 System                     | _                  | Captured Transacti     | ions P  | acket Filter | GSLB                 | Audit  |
| iA               | pps   |                |                                |                    | Click "C               | reat    | e"           | $\rightarrow$        | Create |
| 5 D              | NS  |                | Vame 🕈                         |                    |                        |         |              | 5                    |        |
| 6.               | SI Orchestrator                                 |                | default-ipsec                  | -log-publ          | isher                  |         |              |                      |        |
|                  | SE OTCHESUAIO                                   |                | local-db-pub                   | lisher             |                        |         |              |                      |        |
| A                | cceleration                                     |                | sys-db-acce                    | ss-publist         | her                    |         |              |                      |        |
|                  | evice Management                                |                | sys-sso-acco                   | ess-publis         | sher                   |         |              |                      |        |
| - 0              | erice munugement                                |                | Delete                         |                    |                        |         |              |                      |        |
| <u></u> N        | etwork  |                |                                |                    |                        |         |              |                      |        |
| 8 🛉 S            | ystem   |                |                                |                    |                        |         |              |                      |        |
|                  | Configuration                                   |                |                                |                    |                        |         |              |                      |        |
|                  | Eile Management                                 | -<br>-         |                                |                    |                        |         |              |                      |        |
|                  | Certificate Management                          |                |                                |                    |                        |         |              |                      |        |
|                  | Disk Management                                 |                | <b>`</b>                       |                    |                        |         |              |                      |        |
|                  | Software Management                             | -              | ĺπ –                           |                    |                        |         |              |                      |        |
|                  | License   | -/             |                                |                    |                        |         |              |                      |        |
|                  | Resource Provisioning                           | 1              |                                |                    |                        |         |              |                      |        |
|                  | Platform  | /              |                                |                    |                        |         |              |                      |        |
|                  | High Availability                               | 5              | +                              |                    |                        |         |              |                      |        |
|                  | Archives  | 2              | $+ \lambda$                    |                    |                        |         |              |                      |        |
|                  | Services  |                | System                         |                    |                        |         |              |                      |        |
|                  | Preferences                                     | -1             | Captured Transact              | ins                |                        |         |              |                      |        |
|                  | sElow   | -              | Packe Filter                   |                    | Options                |         |              |                      |        |
|                  | SNMP  | -              | Local Traffic                  |                    | Remote Logging         |         |              |                      |        |
|                  | Crypto Offloading                               | -              | GSLB                           |                    | Log Filters            | ÷       |              |                      |        |
|                  | Users   | -              | Audit                          | •                  | L 4 stinations         | ÷       |              |                      |        |
|                  |   |                | Configuration                  | •                  | Log Publishers         | $\odot$ |              |                      |        |
|                  | Logs  |                |                                |                    |                        |         |              | Laborary Colored and |        |

Create a local syslog publisher as shown in the table below:

| Field        | Value                  |
|--------------|------------------------|
| Name         | local-syslog-publisher |
| Destinations | local-syslog           |

| Hostname: gtm1.site1.example.com Da<br>IP Address: 10.1.10.13 Tin | e: Jul 20, 2017 User: <b>admin</b><br>ne: 12:43 PM (CDT) Role: Administrator P |
|---|--|
| ONLINE (ACTIVE) Standalone  |  |
| Main Help About   | System » Logs : Configuration : Log Publishers                                 |
| Magazine Statistics   |  |
| iApps   | Name         Iocal-syslog-publisher  |
| S DNS   | Description  |
| SSL Orchestrator  | Log Destinations   |
| Acceleration  | Selected Available   |
| Device Management   | Destinations   |
| Network   |  |
| System  | Cancel Repeat Finished   |
| Configuration   |  |
| File Management   |  |
| Certificate Management  |  |
| Disk Management   |  |
| Software Management   |  |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/system/log/create\_publisher.jsp

## TMSH

tmsh create sys log-config publisher local-syslog-publisher { destinations add { local-syslog { } } }

2. Create a "Logging Profile"

Navigate to DNS >> Delivery : Profiles : Other : DNS Logging

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 19, 2017<br>Time: 12:09 PM (CDT) | User: <b>admin</b><br>Role: Administrator |               |
|---|--|---|---------------|
| ONLINE (ACTIVE)<br>Standalone                                     |  | CI  | ick"Create"   |
| Main Help About   | DNS » Delivery : Profil                    | es : Other : DNS Logging Protocol    Othe |               |
| Stausues  | ·  |   |               |
| iApps   | *  | × Search                                  | Create        |
| 🔁 Wizards   | 💌 🗢 Name                                   |   |               |
|   | No records to display.                     |   |               |
| () DNS  | Delete                                     |   |               |
| Delivery 🔶 🕨 🕨  | Listeners                                  |   |               |
| GSLB >  | Profiles •                                 | DNS 🔶                                     |               |
| Zones   | Load Balancing 🔋 🕨                         | Protocol >                                |               |
| Caches  | iRules                                     | Other                                     | DNS Logging 📀 |
| Settings  | Translation                                |   | Persistence 💮 |
| G SSI Ontertainty   | Nameservers                                |   | Statistics 🕞  |
| SSL Orchestrator  | Keys 🕨                                     |   |               |
| Local Traffic   |  |   |               |
| Traffic Intelligence  |  |   |               |
| Acceleration  |  |   |               |

Create a DNS logging profile as shown in the table below:

| Field            | Value                       |
|------------------|-----------------------------|
| Name             | example_dns_logging_profile |
| Log Publisher    | local-syslog-publisher      |
| Log Responses    | enabled                     |
| Include Query ID | enabled                     |

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 19, 2017 User: a<br>Time: 12:14 PM (CDT) Role: A | admin<br>Administrator      |
|---|--|-----------------------------|
| Standalone  |  |                             |
| Main Help About   | DNS » Delivery : Profiles : Oth                            | er : DNS Logging » New      |
| Mage Statistics   |  |                             |
| _   | General Properties   |                             |
| iApps   | Name 🗾   | example_dns_logging_profile |
| 📔 Wizards   | Description  |                             |
| S DNS   | Configuration  |                             |
| Delivery  | Log Publisher  | local-syslog-publisher      |
| GSLB  | Log Queries  | ☑ Enabled                   |
| Zones >   | Log Responses  | C Enabled                   |
| Caches  | Log Fields   |                             |
| Settings  | Include Complete Answer                                    | Enabled                     |
|   | Include Query ID   | 🗹 Enabled                   |
| SSL Orchestrator  | Include Source   | Enabled                     |
| Local Traffic   | Include Timestamp  | Enabled                     |
| Traffic Intelligence  | Include View   | Enabled                     |
| Acceleration  | Cancel Repeat Finished                                     |                             |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/locallb/profile/dns\_log/create.jsp

## TMSH

tmsh create ltm profile dns-logging example\_dns\_logging\_profile enable-response-logging yes include-query-id yes log-publisher local-syslog-publisher

#### 2.2.2.2 DNS Profile

A DNS profile will control which features are enabled as part of processing a query.

Navigate to: DNS >> Delivery : Profiles : DNS

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 19, 2017<br>Time: 12:19 PM (CDT) | User: <b>admin</b><br>Role: Administrator |
|---|--|---|
| Standalone  |  |   |
| Main Help About   | DNS » Delivery : Profil                    | es : DNS                                  |
| Market Statistics   | ⇔ v DNS                                    | Protocol - Other                          |
| iApps   | ŀ.   | × Search Create                           |
| 🔁 Wizards   | Name                                       |   |
|   | iii dns                                    |   |
|   | Delete                                     |   |
| Delivery >  | Listeners                                  |   |
| GSLB  | Profiles                                   |   |
| Zones   | Load Balancing                             | Protocol                                  |
| Caches  | iRules                                     | Other                                     |
| Settings >  | Translation >                              |   |
|   | Nameservers >                              |   |
| SSL Orchestrator  | Keys >                                     |   |
| Local Traffic   |  |   |
| Traffic Intelligence  |  |   |
| Acceleration  |  |   |

Create a DNS profile as shown in the table below.

| Field                      | Value                        |
|----------------------------|------------------------------|
| Name                       | example.com_dns_profile      |
| DNS Cache                  | Enabled                      |
| DNS Cache Name             | transparent_cache            |
| Use BIND Server on Big-IP  | Disabled                     |
| Logging                    | Enabled                      |
| Logging Profile            | example_dns_logging_profile  |
| AVR statistics Sample Rate | Enabled, 1/1 queries sampled |

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 25, 2017 User:<br>Time: 11:40 PM (CDT) Role: | admin Partition: Common V Log o | ut           |
|---|--|---------------------------------|--------------|
| ONLINE (ACTIVE) Standalone  |  |                                 |              |
| Main Help About   | DNS » Delivery : Profiles : DN                         | S » New DNS Profile             |              |
| Statistics  | General Properties                                     |                                 |              |
| iApps   | Name   | example.com_dns_                |              |
| Wizards   | Parent Profile   | dns                             |              |
| 😚 dns   | Denial of Service Protection                           | Custom                          |              |
| Delivery  | Rapid Response Mode                                    | Disabled                        |              |
| GSLB  | Rapid Response Last Action                             | Drop                            |              |
| Zones   | Hardware Acceleration                                  |                                 |              |
| Caches  | Protocol Validation                                    | Disabled 🗸                      |              |
| Settings  | Response Cache   | Disabled                        |              |
| SSL Orchestrator  | DNS Features   |                                 |              |
| Local Traffic   | DNSSEC   | Enabled 🔽                       |              |
|   | GSLB   | Enabled 🔽                       |              |
|   | DNS Express  | Enabled 🗸                       |              |
| Acceleration  | DNS Cache  | Enabled                         |              |
| Access  | DNS Cache Name   | transparent_cache               | $\checkmark$ |
| Device Management   | DNS IPv6 to IPv4                                       | Disabled 🔽                      |              |
|   | Unhandled Query Actions                                | Allow                           |              |
| Network   | Use BIND Server on BIG-IP                              | Disabled V                      | V            |
| System  | DNS Traffic  |                                 |              |
|   | Zone Transfer  | Disabled                        |              |
|   | DNS Security   | Disabled                        |              |
|   | DNS Security Profile Name                              | Select                          |              |
|   | Process Recursion Desired                              | Enabled V                       |              |
|   | Logging and Reporting                                  |                                 |              |
|   | Logging  | Enabled V                       | •            |
|   | Logging Profile  | example_dns_logging_profile     | 1            |
|   | AVR Statistics Sample Rate                             | Enabled 1/ 1 queries sampled    |              |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/locallb/profile/dns/create.jsp

## TMSH

tmsh create ltm profile dns example.com\_dns\_profile { avr-dnsstat-sample-rate 1 cache transparent\_cache defaults-from dns enable-cache yes enable-logging yes log-profile example\_dns\_logging\_profile use-local-bind no }

## 2.2.2.3 UDP Profile

A UDP profile controls the way the platform processes UDP traffic.

#### Navigate to: DNS >> Delivery : Profiles : Protocol : UDP

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31  | Date: Jul 19, 2017<br>Time: 12:27 PM (CDT) | User: <b>admin</b><br>Role: Administrator |               |
|--|--|---|---------------|
| ONLINE (ACTIVE) Standalone   |  |   |               |
| Main Help About  | DNS » Delivery : Profi                     | les : Protocol : UDP                      |               |
| Statistics   | 🔅 👻 DNS                                    | Protocol - Other                          | Click"Create" |
| iApps  | *  | × Search                                  | Create        |
| 🔁 Wizards  | ✓ \$ Name                                  |   |               |
|  | iii udp                                    |   |               |
| <b>b</b> iii <b>b</b> ii <b>b</b> i <b>b</b> i | udp_decrement_ttl                          |   |               |
| Delivery 1 🕨   | Listeners                                  |   |               |
| GSLB   | 2 Profiles                                 | DNS 💮                                     |               |
| Zones  | Load Balancing                             | <sup>3</sup> Protocol                     |               |
| Caches   | iRules                                     | Other >                                   | тср 💮         |
| Settings   | Translation                                |   |               |
|  | Nameservers                                |   |               |
| SSE Orchestrato  | Keys                                       |   |               |
| Local Traffic  |  |   |               |
| Traffic Intelligence   |  |   |               |
| Acceleration   |  |   |               |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/profile/udp/list.jsp

Create a UDP profile as shown in the following table.

| Field          | Value                       |
|----------------|-----------------------------|
| Name           | example.com_udp-dns_profile |
| Parent Profile | udp_gtm_dns                 |

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 19, 2017 Us<br>Time: 12:32 PM (CDT) Ro | er: <b>admin</b><br>le: Administrator |
|---|--|---------------------------------------|
| Standalone  |  |                                       |
| Main Help About   | DNS » Delivery : Profiles :                      | Protocol : UDP » New UDP Profile      |
| Mage Statistics   |  |                                       |
| iApps   | Name   | example.com_udp-                      |
| i Wizards   | Parent Profile                                   | udp_gtm_dns                           |
| 😚 dns   | Settings   |                                       |
| Delivery  | Proxy Maximum Segment                            |                                       |
| GSLB →  | Idle Timeout                                     | Specify 5 seconds                     |
| Zones   | IP ToS   | Specify V                             |
| Caches  | Link QoS   | Specify 🔽 0                           |
| Settings  | Datagram LB                                      | Enabled                               |
| SEL Orchestrator  | Allow No Payload                                 |                                       |
| SSL Orchestrator  | TTL Mode   | Proxy 🗸                               |
| Local Traffic   | Don't Fragment Mode                              | PMTU 🔽                                |
| Traffic Intelligence  | Cancel Repeat Finished                           | 1                                     |
| Acceleration  |  |                                       |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/profile/udp/create.jsp

## TMSH

tmsh create ltm profile udp example.com\_udp-dns\_profile defaults-from udp\_gtm\_dns

## 2.2.2.4 TCP Profile

A TCP profile controls the way the platform processes TCP traffic.

Navigate to: DNS >> Delivery : Profiles : Protocol : TCP

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 19, 2017<br>Time: 12:34 PM (CDT) | User: <b>admin</b><br>Role: Administrator |     |        |
|---|--|---|-----|--------|
| ONLINE (ACTIVE)<br>Standalone                                     |  |   |     |        |
| Main Help About   | DNS » Delivery : Profil                    | es : Protocol : TCP                       |     | eate"  |
| Mage Statistics   | DNS  | Protocol - Othe                           |     |        |
| iApps   | *  | × Search                                  |     | Create |
| 🔁 Wizards   | 🖌 🕈 Name                                   |   |     |        |
|   | apm-forwarding-clier                       | it-tcp                                    |     |        |
| UN3   | apm-forwarding-serv                        | er-tcp                                    |     |        |
| Delivery >  | Listeners                                  | s_profile                                 |     |        |
| GSLB  | Profiles •                                 | DNS 💮                                     |     |        |
| Zones   | Load Balancing                             | Protocol >                                | UDP | (+)    |
| Caches  | inules                                     | Other                                     | ТСР | •      |
| Setti   | ranslation >                               |   |     |        |
| 8   | Nameservers                                | ed  |     |        |
| SSL Orchestrator  | Keys >                                     | -tcp-lan_profile                          |     |        |
| Contraffic  |  | ср  |     |        |
|   | iii tcp                                    |   |     |        |
| Traffic Intelligence  | tcp-lan-optimized                          |   |     |        |
|   | tcp-legacy                                 |   |     |        |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/profile/tcp/list.jsp

Create a TCP profile as shown in the following table.

| Field          | Value                       |
|----------------|-----------------------------|
| Name           | example.com_tcp-dns_profile |
| Parent Profile | f5-tcp-lan                  |

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 12, 2017 User: admin Par<br>Time: 7:45 PM (CDT) Role: Administrator Par |                              |  |
|---|---|------------------------------|--|
| ONLINE (ACTIVE)<br>Standalone                                     |   |                              |  |
| Main Help About   | Local Traffic » Profiles : Prot   | ocol : TCP » New TCP Profile |  |
| Statistics  |   |                              |  |
|   | General Properties  |                              |  |
| IApps   | Name  | example.com_tcp-(            |  |
| S DNS   | Parent Profile  | f5-tcp-lan                   |  |
| SSL Orchestrator  | Timer Management  |                              |  |
|   | Close Wait  | Specify 🗹 5 seconds          |  |
| Notwork Man   | Fin Wait 1  | Specify 5 seconds            |  |
| Virtual Servers   | Fin Wait 2  | Specify 🔽 300 seconds        |  |
| Policies  | Idle Timeout  | Specify 300 seconds          |  |
| Profiles  | Keep Alive Interval   | Specify                      |  |
| Ciphers   | Minimum RTO   | 200 milliseconds             |  |
| iRules  | Reset On Timeout  | Enabled                      |  |
| Pools   | Time Wait   | Specify 2000 milliseconds    |  |
| Nodes   | Time Wait Recycle   | Enabled                      |  |
| Monitors  | Zero Window Timeout   | Specify 20000 milliseconds   |  |
| Traffic Class 🕞   |   |                              |  |
| Address Translation   | Memory Management   | -                            |  |
|   | Auto Proxy Buffer   |                              |  |
| Acceleration  | Auto Receive Window   |                              |  |
| Device Management   | Auto Send Buffer  |                              |  |
|   | Proxy Buffer High   | 65535 bytes                  |  |
| Network   | Proxy Buffer Low  | 32768 bytes                  |  |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/profile/tcp/create.jsp

#### TMSH

tmsh create ltm profile tcp example.com\_tcp-dns\_profile defaults-from f5-tcp-lan

### 2.2.2.5 DNS Servers

Create a monitor and a pool for the Internal DNS servers.

Navigate to: DNS >> Delivery : Load Balancing : Monitors

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: May 17, 2018<br>Time: 2:56 PM (CDT) | User: <b>admin</b><br>Role: Administrator |  |  |
|---|---|---|--|--|
| Firewall: Consistent<br>ONLINE (ACTIVE)<br>Standalone             |   |   |  |  |
| Main Help About   | DNS » Delivery : Loa                      | ad Balancing : Monitors                   |  |  |
| Mage Statistics   | 🔅 👻 Monitor List                          | Click "Create"                            |  |  |
| iApps   | ŀ   | × Search Create                           |  |  |
| Wizards   | ✓ ▲ Name                                  |   |  |  |
|   | example.com_dns_monitor                   |   |  |  |
| DNS   | gateway_icmp                              |   |  |  |
| Delivery >  | Listeners                                 | •   |  |  |
| GSLB  | Profiles                                  | •   |  |  |
| Zones   | Load Balancing                            | > Pools >                                 |  |  |
| Caches  | iRules                                    | Nodes                                     |  |  |
| Settings  | Trapolation                               | Monitors 📀                                |  |  |
| e   | Nameservers                               | •   |  |  |
| SSL Orchestrator  | Keys                                      | >   |  |  |
| Local Traffic   | i real_server                             |   |  |  |
|   | Snmp_dca                                  |   |  |  |
| Traffic Intelligence  | tcp                                       |   |  |  |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/monitor/create.jsp

Create a DNS monitor according to the table below:

| Field      | Value                   |
|------------|-------------------------|
| Name       | example.com_dns_monitor |
| Туре       | DNS                     |
| Query Name | www.example.com         |

| Host<br>IP Ad | name: router01.branch01.example.com ddress: 10.1.10.31  | Date: May 17, 2018 User:<br>Time: 4:12 PM (CDT) Role: | admin<br>Administrator        |
|---------------|---|---|-------------------------------|
|               | 5 Firewall: Consistent<br>ONLINE (ACTIVE)<br>Standalone |   |                               |
| M             | lain Help About   | DNS » Delivery : Load Balan                           | cing : Monitors » New Monitor |
| 5             | Statistics  |   |                               |
|               | iApps   | General Properties                                    |                               |
|               |   | Name  | example.com_dns_monitor       |
| 1             | Wizards   | Description   |                               |
| 3             | DNS   | Туре  | DNS                           |
|               | Delivery >  | Parent Monitor  | dns                           |
|               | GSLB >  | Configuration: Advanced                               |                               |
|               | Zones >   | Interval  | 5 seconds                     |
|               | Caches >  | Up Interval   | Disabled                      |
|               | Settings >  | Time Until Up   | 0 seconds                     |
| 6             | SSL Orchestrator  | Timeout   | 16 seconds                    |
| 2-2           | Local Traffic   | Manual Resume   | O Yes ℗ No                    |
| -00           | Local frame   | Reverse   | ○ Yes <sup>®</sup> No         |
| 2             | Traffic Intelligence                                    | Transparent   | ○ Yes ● No                    |
|               | Acceleration  | Alias Address   | * All Addresses               |
| 9             | Subseriber Management                                   | Alias Service Port                                    | * All Ports 🗸                 |
| 2             | subscriber management                                   | Query Name  | www.example.com               |
| <b>)</b> ]    | Access  | Query Type  | av                            |
|               | Device Management                                       | Answer Section Contains                               | Query Type                    |
| ~             | Security  | Accept RCODE  | No Error                      |
|               |   | Receive String  |                               |
|               | Network   | Adaptive  | Enabled                       |
| <b>7</b>      | System  | Cancel Repeat Finished                                |                               |

# TMSH

tmsh create ltm monitor dns example.com\_dns\_monitors qname www.example.com

Navigate to: DNS >> Delivery : Load Balancing : Pools : Pool List

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: May 15, 2018 User: admin<br>Time: 10:01 PM (CDT) Role: Administrator |
|---|--|
| Firewall: Consistent<br>ONLINE (ACTIVE)<br>Standalone             |  |
| Main Help About   | DNS » Delivery : Load Balancing : Pools : Pool List                        |
| Statistics  | 🔅 🗸 Pool List Statistics 🗩   |
| iApps   | * × Search Create  |
| Wizards   | V Status A Name  |
| S DNS   | branch01_dns_pool     default_gateway_pool                                 |
| Delivery >  | Listeners  |
| G B >   | Profiles   |
| Zches   | Load Balancing  Pools  Pool List   |
| Caches  | iRules Nodes Statistics  |
| Settings  | Translation Monitors   |
| G CCL Ownhandtart   | Nameservers  |
| SSL Orchestrator  | Keys   |
| Local Traffic   |  |
| Traffic Intelligence  |  |
| Acceleration  |  |

# https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/pool/list.jsp

Create a DNS pool according to the table below:

| Field           | Value                   |
|-----------------|-------------------------|
| Name            | example.com_dns_pool    |
| Health Monitors | example.com_dns_monitor |
| Node1 Name:     | dc01.example.com_node   |
| Node1 Address:  | 10.1.70.200             |
| Node1 Port:     | 53                      |
| Node2 Name:     | dc02.example.com_node   |
| Node2 Address:  | 10.1.70.210             |
| Node2 Port:     | 53                      |

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: May 15, 2018 User:<br>Time: 10:13 PM (CDT) Role: | admin<br>Administrator   |
|---|--|--|
| Firewall: Consistent<br>ONLINE (ACTIVE)<br>Standalone             |  |  |
| Main Help About   | DNS » Delivery : Load Balan                            | cing : Pools : Pool List » New Pool                            |
| Mage Statistics   | Raeia IV   |  |
| iApps   | Name   |  |
| Minuda  | Name   | example.com_uis_bool   |
| Wizarus   | Description  |  |
| Delivery  | Health Monitors  | Active Available //Common example.com_dns_monitor  <           |
| Zones >   |  |  |
| Caches  | Resources  |  |
| Settings  | Load Balancing Method                                  | Round Robin  |
| e   | Priority Group Activation                              | Disabled   |
| SSL Orchestrator  |  | New Node      New FQDN Node      Node List      FQDN Node List |
| Local Traffic   |  | Node Name: dc02.example.com_node (Optional)                    |
| C Traffic Intelligence  |  | Service Port: 53 Select  |
| Inanic Intelligence   | New Members  | Add  |
| Acceleration  |  | Node Name Address/FQDN Service Port Auto Populate Priority     |
| Subscriber Management   |  | dc01.example.com_node 10.1.70.200 53 0                         |
| ~   |  | dc02.example.com_node 10.1.70.210 53 0                         |
| Access  |  | Edit Doloto  |
| Device Management   | Cancel Repeat Finished                                 |  |
| Security  |  |  |

#### TMSH

tmsh create ltm pool example.com\_dns\_pool members add { dc01.example.com\_node:53 { address 10.1.70.200 } dc02.example.com\_node:53 { address 10.1.70.210 } } monitor example.com\_dns\_monitor

### 2.2.2.6 UDP Listener

A UDP listener is an IP address that will receive DNS queries.

Navigate to: DNS >> Delivery : Listeners : Listener List

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 19, 2017 User: admin<br>Time: 11:43 AM (CDT) Role: Administrator |  |  |
|---|--|--|--|
| ONLINE (ACTIVE) Standalone  |  |  |  |
| Main Help About   | DNS » Delivery : Listeners : Listener List                                 |  |  |
| Magazine Statistics   | 🔅 👻 Listener List Statistics 🗵   |  |  |
| iApps   | * Search Create  |  |  |
| 📔 Wizards   | ✓ ♦ State ♦ Name   |  |  |
|   | No records to display.   |  |  |
|   | Enable Disable Delete  |  |  |
| Delivery >  | Listeners  Listener List  O  |  |  |
| GSLB  | Profiles > Statistics .  |  |  |
| Zones   | Load Balancing   |  |  |
| Caches  | iRules >   |  |  |
| Settings  | Translation  |  |  |
| e manual  | Nameservers  |  |  |
| SSL Orchestrator  | Keys   |  |  |
| Local Traffic   |  |  |  |
| Traffic Intelligence  |  |  |  |
| Acceleration  |  |  |  |

# https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/listener/list.jsp

Create two UDP listeners according to the tables below:

| Field                                 | Value                       |
|---------------------------------------|-----------------------------|
| Name                                  | DC01_udp_53_virtual         |
| Destination Address                   | 10.1.70.200                 |
| Service Port                          | DNS 53                      |
| VLAN and Tunnel Traffic -> Enabled on | branch01_vlan               |
| Protocol                              | UDP                         |
| Protocol Profile (Client)             | example.com_udp-dns_profile |
| DNS Profile                           | example.com_dns_profile     |
| Default Pool                          | example.com_dns_pool        |

| Field                                 | Value                       |
|---------------------------------------|-----------------------------|
| Name                                  | DC02_udp_53_virtual         |
| Destination Address                   | 10.1.70.210                 |
| Service Port                          | DNS 53                      |
| VLAN and Tunnel Traffic -> Enabled on | branch01_vlan               |
| Protocol                              | UDP                         |
| Protocol Profile (Client)             | example.com_udp-dns_profile |
| DNS Profile                           | example.com_dns_profile     |
| Default Pool                          | example.com_dns_pool        |

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 19, 2017 User: a<br>Time: 12:01 PM (CDT) Role: A | <b>dmin</b><br>.dministrator  |  |
|---|--|---|--|
| ONLINE (ACTIVE)<br>Standalone                                     |  |   |  |
| Main Help About   | DNS » Delivery : Listeners : List                          | stener List » New   |  |
| Statistics  | General  |   |  |
| iApps   | Name   | DC01_udp_53_virtual   |  |
| 📔 Wizards   | Description  |   |  |
| S DNS   | State  | Enabled V   |  |
| Delivery  | Listener: Advanced   |   |  |
| GSLB  | Destination  | Type:  Host O Network Address: 10.1.70.200  |  |
| Caches  | Service Port   | DNS <b>&gt;</b> 53  |  |
| Settings >  | VLAN Traffic   | Enabled on  |  |
| SSL Orchestrator  | VLANs and Tunnels  | Selected     Available       /Common     isp1_site1_vlan       branch01_vlan     <       >>     isp2_site1_vlan       isp2_site2_vlan     vailable       socks-tunnel |  |
| Traffic Intelligence  | Source Address Translation                                 | None  |  |
| Acceleration  | Address Translation  | Enabled   |  |
| Access  | Port Translation   | Enabled   |  |
|   | Route Advertisement  |   |  |
| Device Management   | Auto Last Hop  | Default 🔽   |  |
| Retwork   | Last Hop Pool  | None  |  |
| System  | Service: Advanced  |   |  |
|   | Protocol   |   |  |
|   | Protocol Profile (Client)                                  | example.com_udp-dns_profile   |  |
|   | Protocol Profile (Server)                                  | (Use Client Profile)  |  |
|   | DNS Profile  | example.com_dns_profile   |  |
|   | Load Balancing   |   |  |
|   | Default Pool   | branch01_dns_pool   |  |
|   | Default Persistence Profile                                | None  |  |
|   | Fallback Persistence Profile                               | None  |  |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/locallb/virtual\_server/create.jsp

## TMSH

tmsh create gtm listener DC01\_udp\_virtual address 10.1.70.200 port 53 ip-protocol udp pool example.com\_dns\_pool profiles add { example.com\_dns\_profile example.com\_udp-dns\_profile } vlans add { branch01\_vlan } vlans-enabled

### TMSH

tmsh create gtm listener DC02\_udp\_virtual address 10.1.70.210 port 53 ip-protocol udp pool example.com\_dns\_pool profiles add { example.com\_dns\_profile example.com\_udp-dns\_profile } vlans add { branch01\_vlan } vlans-enabled

#### 2.2.2.7 TCP Listeners

A TCP listener is an IP address that will receive DNS queries.

#### Navigate to: DNS >> Delivery : Listeners : Listener List

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 19, 2017<br>Time: 11:43 AM (CDT) | User: <b>admin</b><br>Role: Administrato |        |                    |  |  |  |  |
|---|--|--|--------|--------------------|--|--|--|--|
| Main Help About   | DNS » Delivery : Liste                     | eners : Listener Lis                     | st     | <b>ClickCreate</b> |  |  |  |  |
| Statistics  | 🔅 👻 Listener List                          | Statistics                               |        |                    |  |  |  |  |
| iApps   | *  |  | Search | Create             |  |  |  |  |
| Wizards   | Vo records to display                      |  |        |                    |  |  |  |  |
| S DNS   | Enable Disable De                          | elete                                    |        |                    |  |  |  |  |
| Delivery 🚽 🕨 🕨  | Listeners                                  | Listener List                            | 0      |                    |  |  |  |  |
| GSLB  | Profiles                                   | Statistics                               | 7      |                    |  |  |  |  |
| Zones   | Load Balancing                             |  |        |                    |  |  |  |  |
| Cachee  | iRules                                     |  |        |                    |  |  |  |  |
| Settings  | Translation                                |  |        |                    |  |  |  |  |
| E market  | Nameservers                                |  |        |                    |  |  |  |  |
| SSL Orchestrator  | Keys                                       |  |        |                    |  |  |  |  |
| Local Traffic   |  |  |        |                    |  |  |  |  |
| Traffic Intelligence  |  |  |        |                    |  |  |  |  |
| Acceleration  |  |  |        |                    |  |  |  |  |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/listener/list.jsp Create two TCP listeners according to the table below:

| Field                                 | Value                       |
|---------------------------------------|-----------------------------|
| Name                                  | DC01_tcp_53_virtual         |
| Destination                           | 10.1.70.200                 |
| Service Port                          | DNS 53                      |
| VLAN and Tunnel Traffic -> Enabled on | branch01_vlan               |
| Protocol                              | TCP                         |
| Protocol Profile (Client)             | example.com_tcp-dns_profile |
| DNS Profile                           | example.com_dns_profile     |
| Pool                                  | example.com_dns_pool        |

| Field                                 | Value                       |
|---------------------------------------|-----------------------------|
| Name                                  | DC02_tcp_53_virtual         |
| Destination                           | 10.1.70.210                 |
| Service Port                          | DNS 53                      |
| VLAN and Tunnel Traffic -> Enabled on | branch01_vlan               |
| Protocol                              | TCP                         |
| Protocol Profile (Client)             | example.com_tcp-dns_profile |
| DNS Profile                           | example.com_dns_profile     |
| Pool                                  | example.com_dns_pool        |

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 19, 2017 User: a<br>Time: 12:46 PM (CDT) Role: A | admin<br>Administrator                             |  |  |  |  |  |
|---|--|--|--|--|--|--|--|
| ONLINE (ACTIVE)<br>Standalone                                     |  |  |  |  |  |  |  |
| Main Help About   | DNS » Delivery : Listeners : Lis                           | stener List » New                                  |  |  |  |  |  |
| Statistics  | Conoral  |  |  |  |  |  |  |
| iApps   | Name   | DC01 tcp 53 virtual                                |  |  |  |  |  |
| Wizards   | Description  |  |  |  |  |  |  |
|   | State  |  |  |  |  |  |  |
| <b>DNS</b>  | Advansed V   |  |  |  |  |  |  |
| Delivery  | Listener: Advanced   | Trans Quart Onternat                               |  |  |  |  |  |
| GSLB  | Destination  | Address: 10.1.70.200                               |  |  |  |  |  |
| Caches  | Service Port   | DNS 7 53   |  |  |  |  |  |
| Settings  | VLAN Traffic   | Enabled on   |  |  |  |  |  |
| C   |  | Selected Available                                 |  |  |  |  |  |
| SSL Orchestrator  | VLANs and Tunnels  | /Common<br>branch01_vlan <                         |  |  |  |  |  |
| Local Traffic   |  | >> external_vlan<br>http-tunnel<br>isp1_site1_vlan |  |  |  |  |  |
| Traffic Intelligence  | Source Address Translation                                 | None   |  |  |  |  |  |
| Acceleration  | Address Translation  | Enabled  |  |  |  |  |  |
|   | Port Translation   | Enabled  |  |  |  |  |  |
| Access  | Route Advertisement  | Enabled  |  |  |  |  |  |
| Device Management   | Auto Last Hop  | Default 🔽  |  |  |  |  |  |
| Retwork   | Last Hop Pool  | None   |  |  |  |  |  |
| Suctom  | Service: Advanced V  |  |  |  |  |  |  |
| ST System   | Protocol   |  |  |  |  |  |  |
|   | Protocol Profile (Client)                                  | example.com_tcp-dns_profile                        |  |  |  |  |  |
|   | Protocol Profile (Server)                                  | (Use Client Profile)                               |  |  |  |  |  |
|   | DNS Profile  | example.com_dns_profile                            |  |  |  |  |  |
|   | Load Balancing   |  |  |  |  |  |  |
|   | Default Pool   | branch01_dns_pool                                  |  |  |  |  |  |
|   | Default Persistence Profile                                | None   |  |  |  |  |  |
|   | Fallback Persistence Profile                               | None   |  |  |  |  |  |
|   |  |  |  |  |  |  |  |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/listener/create.jsp

# TMSH

tmsh create gtm listener DC01\_tcp\_virtual address 10.1.70.200 port 53 ip-protocol tcp pool example.com\_dns\_pool profiles add { example.com\_dns\_profile example.com\_tcp-dns\_profile } vlans add { branch01\_vlan } vlans-enabled

#### TMSH

tmsh create gtm listener DC02\_tcp\_virtual address 10.1.70.210 port 53 ip-protocol tcp pool example.com\_dns\_pool profiles add { example.com\_dns\_profile example.com\_tcp-dns\_profile } vlans add { branch01\_vlan } vlans-enabled

https://support.f5.com/kb/en-us/products/big-ip\_ltm/manuals/product/bigip-dns-cache-implementations-11-3-0/2.html

#### 2.2.2.8 Results

1. From the jumpbox open a command prompt, perform several recursive queries to your new listener to test.

Repeat some of the same queries multiple times

```
dig www.f5.com
dig www.wikipedia.org
dig www.ncsu.edu
dig www.example.com
```

2. Viewing Cache Entries

Navigate to: DNS >> Caches : Cache List >> Properties : transparent\_cache

| Hoster and router01.branch01.example.com<br>IP Autorss: 10.1.10.31 | Pate: Jun 27, 2017 User<br>Ime: 12:48 PM (CDT) Role | admin<br>Administrator                      |
|--|---|---|
| ONLINE (ACTIVE) Standalone   |   |   |
| Main Help About  | DNS » Caches : Cache List                           | » Properties : transparent_cache            |
| Mage Statistics  | 🔅 👻 Properties Loc                                  | ar Zones Response Policy Zones Statistics 🗵 |
| iApps  | General Properties                                  | 1   |
| S DNS  | Name  | transparent_cache                           |
| Delivery   | Resolver Type                                       | Transparent (None)                          |
| Zones >  | DNS Cache   | Click Statistics                            |
| Caches   | Message Cache Size                                  | 1048576 × bytes                             |
| Settings >   | Resource Record Cache Size                          | 10485760 bytes                              |
| SSL Orchestrator   | Answer Default Zones                                | Enabled                                     |
|  | RRSet Rotate  | none  |
|  | Update Delete                                       |   |
| Acceleration   |   |   |
| Device Management  |   |   |
| Network  |   |   |
| System   |   |   |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/properties.jsp?name= %2FCommon%2Ftransparent\_cache

Navigate to: Statistics >> Module Statistics : DNS : Caches >> Caches

| Hos<br>IP A | inamon outer01.branch01.example.com<br>ddr. co: 10.1.10.31 | Date:<br>Time:                  | Jun 27, 2017<br>12:50 PM (CDT) | User: admin<br>Role: Admin | istrator   |              |         |           |           |        |       | Partition: Co | ommon 💽 | -  |
|-------------|--|---------------------------------|--------------------------------|----------------------------|------------|--------------|---------|-----------|-----------|--------|-------|---------------|---------|----|
| ſ           | ONLINE (ACTIVE)<br>Standalone                              |                                 |                                |                            |            |              |         |           |           |        |       |               |         |    |
| N           | ain Help About   | Statis                          | tics » Module S                | tatistics : DNS            | :Caches »  | Caches       |         |           |           |        |       |               |         |    |
| M-          | Statistics   | ⇔ -                             |                                | - DNS                      | -          | Local Traffi |         |           |           |        |       |               |         |    |
| -           | Dashboard .=   |                                 |                                |                            |            |              |         |           |           |        |       |               |         |    |
|             | Module Statistics  | Displa                          | y Options                      |                            |            |              |         |           |           |        |       |               |         |    |
|             | Analytics >  | Statis                          | tics Type                      | Ca                         | ches       | $\checkmark$ |         |           |           |        |       |               |         |    |
|             | Performance  | Data                            | Format                         | No                         | rmalized 🔽 |              |         |           |           |        |       |               |         |    |
|             |  | Auto Refresh Disabled V Refresh |                                |                            |            |              |         |           |           |        |       |               |         |    |
| 13          | IApps  | /Comn                           | non/transparent_ca             | ache                       | Search     | Reset Sear   | ch      |           | DNS Quer  | ioe    |       |               | Failur  |    |
| 5           | DNS  |                                 | ▲ Name                         |                            | Partition  | n / Path     | Details | ¢ Queries | Responses | ⇒ Sync | Async | Resolve       | Connect | \$ |
| ß           | SSL Orchestrator   |                                 | transparent_cach               | e                          | Commo      | n n          | View    | 7         | 4         | 4      | 0     | 0             | 0       | 0  |
|             |  | Rese                            | t Clear Cache                  |                            |            | 7            |         |           |           |        |       |               |         |    |
| (1)         | Local Traffic  |                                 |                                |                            |            |              | •       |           |           |        |       |               |         |    |
|             | Acceleration   |                                 |                                |                            |            |              |         |           |           |        |       |               |         |    |
|             | Device Management  |                                 |                                | C                          | lick       |              | W       |           |           |        |       |               |         |    |
|             | Network  |                                 |                                |                            |            |              |         |           |           |        |       |               |         |    |
| 8 9         | System   |                                 |                                |                            |            |              |         |           |           |        |       |               |         |    |

| Date: Jun 27, 2017 User:<br>Time: 12:52 PM (CDT) Role: | admin<br>Administrator   |  |   | Partition: Co  | mmon V Log out  |  |  |  |  |  |
|--|--|--|---|--|---|--|--|--|--|--|
|  |  |  |   |  |   |  |  |  |  |  |
| Statistics » Module Statistics                         | : DNS : Caches » (   | Caches : transparent_cach  | 10  |  |   |  |  |  |  |  |
| 🔅 🗸 Summary  |  |  |   |  |   |  |  |  |  |  |
|  |  |  |   |  |   |  |  |  |  |  |
| Display Options  | Display Options  |  |   |  |   |  |  |  |  |  |
| Data Format  | Normalized V   |  |   |  |   |  |  |  |  |  |
| Auto Refresh   | Disabled 🔽   | Refresh  |   |  |   |  |  |  |  |  |
| << Back Clear Statistics                               |  |  |   |  |   |  |  |  |  |  |
|  |  |  |   |  |   |  |  |  |  |  |
| Query Details  |  |  |   |  |   |  |  |  |  |  |
| Queries  | 7  |  |   |  |   |  |  |  |  |  |
| Responses  | 4  | _  |   |  |   |  |  |  |  |  |
| Synchronous Responses                                  | 4  |  |   |  |   |  |  |  |  |  |
| Asynchronous Responses                                 | 0  |  |   |  |   |  |  |  |  |  |
| Failure Details  |  |  |   |  |   |  |  |  |  |  |
| Resolve  | 0  |  |   |  |   |  |  |  |  |  |
| Connection   | 0  |  |   |  |   |  |  |  |  |  |
| Server   | 0  |  |   |  |   |  |  |  |  |  |
| Send   | 0  |  |   |  |   |  |  |  |  |  |
| Cache Details  |  | Misson   | Incorte   | Undatos  | Evictions   |  |  |  |  |  |
| DNS Message Cache                                      | 4  | 3  | 0   | 0  | 0   |  |  |  |  |  |
| Resource Record Cache                                  | 0  | 15   | 0   | 0  | 0   |  |  |  |  |  |
|  | -  |  | -   | -  | -   |  |  |  |  |  |
| Forwarder Activity                                     |  |  |   |  |   |  |  |  |  |  |
| Queries  | 0  |  |   |  |   |  |  |  |  |  |
| Responses  | 0  |  |   |  |   |  |  |  |  |  |
| Response Policy  |  |  |   |  |   |  |  |  |  |  |
| Rewrites   | 0  |  |   |  |   |  |  |  |  |  |
|  | Une:     22:52 PM (COT)     User:       Time:     12:52 PM (COT)     Role:         Statistics     >> Module Statistics         Statistics     >> Summary         Display Options         Data Format         Auto Refresh         << | Une: 12:52 PM (COT)     User: admin       Time: 12:52 PM (COT)     Role: Administrator   Statistics >> Module Statistics : DNS : Caches >> 1   (************************************ | Unter     June 27, 2017     User admin       Time: 12:52 PM (COT)     Role: Administrator   Statistics >> Module Statistics: DNS : Caches : transporent_cacl     Statistics >> Module Statistics: DNS : Caches : transporent_cacl           (3)     Summary   Display Options Data Format       Auto Refresh     Disabled           Auto Refresh     Disabled           (auery Details         Query Details         Queries     7         Resource Record     0         Failure Details     Misses       DNS Message Cache     4       Resource Record Cache     0       Towarder Activity     0       Queries     0         Responses     0         Responses     0         Responses     0 | Date: Jun 2/, 2017     User: administrator       Time: 12:52 PM (COT)     Role: Administrator   Statistics -> Module Statistics : DNS : Caches -> Caches : transparent_cache        Image: Statistics -> Module Statistics : DNS : Caches -> Cache -> | Date:     User:     administrator       Statistics :     Nodule Statistics :     DNS : Caches ::     ransporent_cache       Statistics :     Nodule Statistics :     DNS :     Caches ::     ransporent_cache       Statistics :     Nodule Statistics :     DNS :     Caches ::     ransporent_cache       Statistics :     Nodule Statistics :     DNS :     Caches ::     ransporent_cache       Statistics :     Nodule Statistics :     No     No       Display Options     Data Format     Nomalized Image: Cache       Outer Details     Display Options     Image: Cache Image: |  |  |  |  |  |

Navigate to: Statistics >> Module Statistics : DNS : Caches >> Caches : transparent\_cache

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/stats\_detail.jsp?name=/Common/transparent\_cache

## TMSH

tmsh show Itm dns cache records rrset cache transparent\_cache

| [root@router01:Active:             | Standa | alone] c | onfig # | tmsh s  | show l | ltm dns | cache | records | rrset | cache | transparent | cache |
|------------------------------------|--------|----------|---------|---------|--------|---------|-------|---------|-------|-------|-------------|-------|
| Ltm::DNS-Cache/Resolver RR Records |        |          |         |         |        |         |       |         |       |       |             |       |
| Owner                              | 111    |          | Class   | rdata   |        |         |       |         |       |       |             |       |
| www.gslb.example.com               | 25     | A        | 11      | 203.0.1 | 113.9  |         |       |         |       |       |             |       |
| www.example.com                    | 3595   | CNAME    | 7.1     | www.gsl | lb.exa | mple.co | om    |         |       |       |             |       |
| www.nesu.                          | 2500   | 24       | IN      | 152.1.2 | 227.24 | 12      |       |         |       |       |             |       |
| www.ncsu.edu                       | 3588   | A        | IN      | 152.1.2 | 227.24 | 13      |       |         |       |       |             |       |
| www.ncsu.edu                       | 3588   | A        | IN      | 152.1.2 | 227.24 | 1       |       |         |       |       |             |       |
| www.ncsu.edu                       | 3588   | A        | IN      | 152.1.2 | 227.24 | 10      |       |         |       |       |             |       |
| Owner TTI                          | . Туре | e Class  | rdata   | L       |        |         |       |         |       |       |             |       |
| www.wikipedia.org 578              | 3 A    | IN       | 198.3   | 5.26.96 |        |         |       |         |       |       |             |       |
| Total records returned (tmm0): 7   |        |          |         |         |        |         |       |         |       |       |             |       |
| [root@router01:Active:             | Standa | alone] c | onfig # |         |        |         |       |         |       |       |             |       |

## TMSH

show Itm dns cache transparent transparent\_cache

3. Clearing Entire Cache
Navigate to **Statistics > Module Statistics > DNS > Caches** Set "Statistics Type" to "Caches". Select the cache and click "Clear Cache" to empty the cache.

# 2.2.3 Hidden Master

The internal DNS servers are authoritative for example.com so we need to slave the zone to the BIG-IP. After this module is complete the BIG-IP will become an authoritative slave.



https://support.f5.com/kb/en-us/products/big-ip\_ltm/manuals/product/dns-services-implementations-11-6-0/2.html#unique\_1658664851

### 2.2.3.1 Name Server

Define the Active Directory server as a nameserver and initiate a zone transfer.

Navigate to DNS » Delivery : Nameservers : Nameserver List

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 12, 2017<br>Time: 10:23 PM (CDT) | User: <b>admin</b><br>Role: Administrator | Partiti                        |
|---|--|---|--------------------------------|
| ONLINE (ACTIVE) Standalone  |  |   |                                |
| Main Help About   | DNS » Delivery : Name                      | servers : Nameserver List                 |                                |
| Mage Statistics   | 🔅 👻 Nameserver List                        | Statistics 💌                              |                                |
| iApps   | k  | × Search                                  |                                |
| 🚯 dns   | ✓ ▲ Name                                   |   | Address      Port      TSIG Ke |
| Delivery 🗼 🕨 🕨  | Listeners                                  |   |                                |
| GSLB  | Profiles >                                 |   |                                |
| Zones   | Load Balancing                             |   |                                |
| Caches  | iRules >                                   |   |                                |
| Settings  | Translation                                |   |                                |
| C cci curturtarta   | Nameservers                                | Nameserver List 📀                         |                                |
| SSL Orchestrator  | Kevs                                       | Statistics                                |                                |
| Local Traffic   |  |   |                                |
| Acceleration  |  |   |                                |
| Device Management   |  |   |                                |
| Network   |  |   |                                |

Create a nameserver according to the following table:

| Field   | Value            |
|---------|------------------|
| Name    | dc01.example.com |
| Address | 10.1.70.200      |

| Hostname: gtm1.site1.example.com Dat<br>IP Address: 10.1.10.13 Tim | e: Jul 21, 2017 User: <b>admin</b><br>e: 1:47 AM (CDT) Role: Administrator |
|--|--|
| Standalone   |  |
| Main Help About  | DNS » Delivery : Nameservers : Nameserver List » New Nameserver            |
| Mage Statistics  |  |
| iAnne  | General Properties   |
| To table   | Name dc01.example.com  |
| S DNS  | Address 10.1.70.200 ×  |
| Delivery   | Service Port 53 Other:   |
| GSLB   | Configuration  |
| Zones >  | Route Domain   |
| Caches   |  |
| Settings >   |  |
| SSL Orchestrator   | Cancel Repeat Finished   |
| Acceleration   |  |
| Device Management  |  |
| Network  |  |
| System   |  |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/nameserver/create.jsp

## TMSH

tmsh create ltm dns nameserver dc01.example.com { address 10.1.70.200 }

### 2.2.3.2 DNS Express

The zone example.com is served from the high performance authoritative resolver.

Navigate to DNS >> Zones : Zones : Zone List

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 12, 2017<br>Time: 10:32 PM (CDT) | User: <b>admin</b><br>Role: Administrator | Partition: Common V |
|---|--|---|---------------------|
| ONLINE (ACTIVE) Standalone  |  |   |                     |
| Main Help About   | DNS » Zones : Zones :                      | Zone List                                 |                     |
| Statistics  | 🔅 🚽 Zone List                              | Statistics 🗾                              |                     |
| iApps   | *  | × Search                                  | Create              |
| 😚 dns   | ✓ A Name                                   |   |                     |
| Delivery  | No records to display.                     |   |                     |
| GSLB  | Delete                                     |   |                     |
| Zones 🔶 🕨   | Zones                                      | Zone List 💽                               |                     |
| Caches  | NSSEC Zones                                | Statistics                                |                     |
| Settings  | ZoneRunne >                                |   |                     |
| SSL Orchestrator  |  |   |                     |
| Local Traffic   |  |   |                     |
| Acceleration  |  |   |                     |
| Device Management   |  |   |                     |
| Network   |  |   |                     |

Create a DNS Express zone according to the following table:

| Field             | Value            |
|-------------------|------------------|
| Name              | example.com      |
| Server            | dc01.example.com |
| Allow NOTIFY From | 10.1.70.200      |

| Hostname: gtm1.site1.example.com Date<br>IP Address: 10.1.10.13 Time | : Jul 21, 2017 User: <b>admin</b><br>:: 1:55 AM (CDT) Role: Administr | ator             |
|--|---|------------------|
| ONLINE (ACTIVE) Standalone   |   |                  |
| Main Help About  | DNS » Zones : Zones : Zone L  | ist » New Zone   |
| Maga Statistics  |   |                  |
| _  | General Properties  |                  |
| iApps  | Name  | example.com      |
| S DNS  | DNS Express   |                  |
| Delivery   | Server  | dc01.example.com |
| GSLB   | Availability  | Unknown          |
| Zones  | State   | Enabled V        |
| Caches   | Notify Action   | Consume          |
| Settings   |   | Address: Add     |
| SSL Orchestrator   | Allow NOTIEY From   |                  |
| Acceleration   |   |                  |
| Device Management  |   | Delete           |
|  | Verify Notify TSIG  |                  |
| Network  | Response Policy   |                  |
| System   | Zone Transfer Clients   |                  |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/zone/create.jsp

### TMSH

tmsh create ltm dns zone example.com { dns-express-allow-notify add { 10.1.70.200 } dns-express-notify-tsig-verify no dns-express-server dc01.example.com }

https://support.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-services-implementations-12-1-0/ 1.html#guid-977cd16a-5d12-4b1e-964c-5d8206f647ed

https://www.unbound.net

#### 2.2.3.3 Results

The BIG-IP will now be an authoratative slave for the example.com zone. This protects the master as well as increases performance utilizing the BIG-DNS delivery engine.

1. Click on the newly created DNS Express zone and make sure it is showing green for 'Available' indicating that the initial AXFR transfer was successful.

| DNS Express  |                                       |  |
|--------------|---------------------------------------|--|
| Server       | dc01.example.com                      |  |
| Availability | Available (Enabled) - Successful AXFR |  |

2. Using putty from the taskbar, log in to router01.branch01.example.com.

Run the following command to see the contents of the DNS Express database:

| dnsxdump | less |
|----------|------|
|          |      |

#### Examine the results



## 2.2.4 DNSSec



https://support.f5.com/kb/en-us/products/big-ip\_ltm/manuals/product/dns-services-implementations-11-6-0/2.html#unique\_1658664851

#### 2.2.4.1 Zone Signing Key

Navigate to: DNS >> Delivery : Keys : DNSSEC Key List

| IP Address: 10.1.10.31     | Date:         Jul 18, 2017         User:         admin         Partition:         Common           Time:         12:27 PM (CDT)         Role:         Administrator         Partition:         Common |
|----------------------------|---|
| ONLINE (ACTIVE) Standalone |   |
| Main Help About            | DNS » Zones : DNSSEC Zones : DNSSEC Zone List   |
| Main Statistics            | DNSSEC Zone List Statistics     Click "Create"  |
| iApps                      | * Search Create   |
| S DNS                      | Status A Name   |
| Delivery 🗼 🕨 🕨             | Listeners >   |
| GSLB                       | Profiles  |
| Zones                      | Load Balancing  |
| Caches                     | iRules >  |
| Settings                   | Translation >   |
| e                          | Nameservers   |
| SSL Orchestrator           | Keys TSIG Key List  |
| Local Traffic              | DNSSEC Key List 💽   |
| Acceleration               |   |
| Device Management          |   |
| Network                    |   |

Create zone signing key according the following table:

| Field          | Value            |
|----------------|------------------|
| Name           | example.com_zsk  |
| Туре           | Zone Signing Key |
| Key Management | Manual           |
| Certificate    | default.crt      |
| Private Key    | default.key      |

| Hustname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 18, 2017 User: ad<br>Time: 1:40 PM (CDT) Role: Ac | lmin<br>Iministrator        |
|---|---|-----------------------------|
| ONLINE (ACTIVE)<br>Standalone                                     |   |                             |
| Main Help About   | DNS » Delivery : Keys : DNSSE                               | C Key List » New DNSSEC Key |
| Magazine Statistics   |   |                             |
| iApps   | General Properties  |                             |
| - 10 mappe  | Name  | example.com_ksk ×           |
| S DNS   | Туре  | Zone Signing Key            |
| Delivery  | State   | Enabled V                   |
| GSLB  | Hardware Security Module                                    | None                        |
| Zones   | Algorithm   | RSA/SHA1                    |
| Caches  | Key Management  | Manual 🔽                    |
| Settings  | Key Settings  |                             |
| SSL Orchestrator  | Certificate   | default.crt                 |
| Local Traffic   | Private Key   | default.key                 |
| Acceleration  | Cancel Repeat Finished                                      |                             |
| Device Management   |   |                             |
| Retwork   |   |                             |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/dnssec\_key/create.jsp

# TMSH

tmsh create ltm dns dnssec key example.com\_zsk key-type zsk certificate-file default.crt key-file default.key

### 2.2.4.2 Key Signing Key

Navigate to: DNS >> Delivery : Keys : DNSSEC Key List

| IP Address: 10.1.10.31     | Date:         Jul 18, 2017         User:         admin         Partition:         Common           Time:         12:27 PM (CDT)         Role:         Administrator         Partition:         Common |
|----------------------------|---|
| ONLINE (ACTIVE) Standalone |   |
| Main Help About            | DNS » Zones : DNSSEC Zones : DNSSEC Zone List   |
| Main Statistics            | DNSSEC Zone List Statistics     Click "Create"  |
| iApps                      | * Search Create   |
| S DNS                      | Status A Name   |
| Delivery 🗼 🕨 🕨             | Listeners >   |
| GSLB                       | Profiles  |
| Zones                      | Load Balancing  |
| Caches                     | iRules >  |
| Settings                   | Translation >   |
| e                          | Nameservers   |
| SSL Orchestrator           | Keys TSIG Key List  |
| Local Traffic              | DNSSEC Key List 💽   |
| Acceleration               |   |
| Device Management          |   |
| Network                    |   |

Create a key signing key according to the following table:

| Field          | Value           |
|----------------|-----------------|
| Name           | example.com_ksk |
| Туре           | Key Signing Key |
| Key Management | Manual          |
| Certificate    | default.crt     |
| Private Key    | default.key     |

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 26, 2017 User:<br>Time: 12:30 AM (CDT) Role: | <b>admin</b><br>Administrator  | Partition: |
|---|--|--------------------------------|------------|
| ONLINE (ACTIVE)<br>Standalone                                     | DNS Dolivony - Kove - DNSS                             | EC Koy List Now DNSSEC Koy     |            |
| Statistics  | General Properties                                     | ACC REY LISL >> NEW DN33CC REY |            |
| iApps   | Name   | example.com_ksk                | _          |
| Wizards   | Туре   | Key Signing Key 🔽              |            |
| 🚱 DNS   | State  | Enabled V                      |            |
| Delivery  | Hardware Security Module                               | None 🔽                         |            |
| GSLB  | Algorithm  | RSA/SHA1                       |            |
| Zones   | Key Management   | Manual 🔽                       |            |
| Caches  | Key Settings   |                                |            |
| Settings  | Certificate  | default.crt                    |            |
| SSL Orchestrator  | Private Key  | default.key                    |            |
| Local Traffic   | Cancel Repeat Finished                                 |                                |            |
| Traffic Intelligence  |  |                                |            |
| Acceleration  |  |                                |            |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/dnssec\_key/create.jsp

TMSH commands for Key Signing key creation:

## TMSH

tmsh create ltm dns dnssec key example.com\_ksk key-type ksk certificate-file default.crt key-file default.key

### 2.2.4.3 Signed Zone

Navigate to: DNS >> Zones : DNSSEC Zones : DNSSEC Zone List

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Common Partition: Common Parti |
|---|--|
| ONLINE (ACTIVE) Standalone  |  |
| Main Help About   | DNS » Zones : DNSSEC Zones : DNSSEC Zone List  |
| Mage Statistics   | Image: Statistic st                  |
| iApps   | * <u>Search</u>  |
| 😚 dns   | Status A Name  |
| Delivery  | No records to display.   |
| GSLB  | Enable Disable Delete  |
| Zones 🗼 🕨 🕨   | Zones >  |
| Caches  | DNSSEC Zones → DNSSEC Zone List ④  |
| Settings  | ZoneRunner > Statistics >  |
| SSL Orchestrator  |  |
| Local Traffic   |  |
|   |  |
| Device Management   |  |
| Retwork   |  |

https://router01.branch01.example.com/tmui/Control/form?\_\_handler=/tmui/dns/dnssec\_zone/list&\_\_ source=delete\_confirm&\_\_linked=false&\_\_fromError=false

Create DNS Express zone signed by DNSSEC

| Field            | Value           |
|------------------|-----------------|
| Name             | example.com     |
| Zone Signing Key | example.com_zsk |
| Key Signing Key  | example.com_ksk |

| Hostname: router01.brand<br>IP Address: 10.1.10.31 | ch01.example.com | Date: Jul 18, 2017<br>Time: 3:18 PM (CDT) | User: adm<br>Role: Adm | i <b>n</b><br>ninistrator |              |                        | Partition: Common |
|--|------------------|---|------------------------|---------------------------|--------------|------------------------|-------------------|
| ONLINE (A<br>Standalone                            | CTIVE)           |   |                        |                           |              |                        |                   |
| Main Help  | About            | DNS » Zones : DNSS                        | EC Zones :             | DNSSEC Zone               | List » New D | NSSEC Zone             |                   |
| Statistics   |                  | General Properties: Ba                    | asic 🔽                 | example.coi               | m            |                        |                   |
| iApps  |                  | Name                                      |                        | example.com               |              |                        |                   |
| S DNS  |                  | State                                     |                        | Enabled 🔽                 |              |                        |                   |
| Delivery   | Þ                | Keys                                      |                        |                           |              |                        |                   |
| GSLB   | •                |   |                        | Active                    |              | Availab                | le                |
| Zones  |                  | Zone Signing Key                          |                        |                           | <<           | /Common<br>example.com | _zsk              |
| Caches   | •                |   |                        |                           | >>           |                        |                   |
| Settings   | •                |   |                        | Active                    |              | Availab                | le                |
| SSL Orchestrator                                   |                  | Key Signing Key                           | [                      |                           | <<           | /Common<br>example.com | _ksk              |
| Local Traffic                                      |                  |   |                        |                           | >>           |                        |                   |
| Acceleration                                       |                  | Cancel Repeat Fi                          | inished                |                           |              |                        |                   |
| Device Managemen                                   | nt               |   |                        |                           |              |                        |                   |
| Retwork  |                  |   |                        |                           |              |                        |                   |

TMSH commands for DNSSEC signed zone creation:

## TMSH

tmsh create ltm dns dnssec zone example.com keys add { example.com\_ksk example.com\_zsk }

### 2.2.4.4 Results

From the CLI on the router01.branch01 BIGIP run tail -f /var/log/ltm From the Workstation CMD prompt run: "dig example.com +dnssec"



# 2.2.5 Validating Resolver

#### 2.2.5.1 Trust Anchors

Create a trust anchor to validate content in a DNS response.

Using Putty, ssh into router01.branch01 and run the following command:

#### TMSH

dig dnskey . | grep 257 > /root/dnskey.txt

dnssec-dsfromkey -f /root/dnskey.txt .

| 🛃 router01   |  |
|--|--|
| [root@router01:Eval:Active:Standalone] config #  |  |
| [root@router01:Eval:Active:Standalone] config # dig dnskey .   grep 257 > /root/dnskey.txt |  |
| [root@router01:Eval:Active:Standalone] config # dnssec-dsfromkey -f /root/dnskey.txt .     |  |
| . IN DS 19036 8 1 B256BD09DC8DD59F0E0F0D8541B8328DD986DF6E                                 |  |
| . IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5         |  |
| . IN DS 20326 8 1 AE1EA5B974D4C858B740BD03E3CED7EBFCBD1724                                 |  |
| . IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D         |  |
| [root@router01:Eval:Active:Standalone] config #  |  |
| [root@router01:Eval:Active:Standalone]   |  |

## Navigate to: DNS >> Caches : Cache List >> validating-resolver\_cache : Trust Anchors

Select the validating-resolver\_cache and click "Trust Anchors"

| Hos<br>IP A | stname: gtm1.site1.example.com<br>Address: 10.1.10.13 | Date<br>Time | : Jul 21, 2017<br>: 1:28 AM (CDT) | User:<br>Role: | <b>admin</b><br>Administrator |                   | Partiti | on: Commor   |
|-------------|---|--------------|-----------------------------------|----------------|-------------------------------|-------------------|---------|--------------|
| (           | ONLINE (ACTIVE)<br>Standalone                         |              |                                   |                |                               |                   |         |              |
| N           | Main Help About                                       |              | DNS » Caches                      | : Cach         | e List                        |                   |         |              |
| M           | Statistics  |              | 🔅 👻 Cache Li                      | st             | Statistics                    |                   |         |              |
|             | iApps   |              | *                                 |                |                               | Search            |         |              |
| 5           | DNS   |              | ✓ ♦ Name                          |                |                               |                   |         | Resolver     |
|             | Delivery  | •            | validating-re                     | solver_        | cache                         |                   |         | Validating F |
|             | GSLB  | •            | Delete                            |                |                               |                   |         |              |
|             | Zones   | •            |                                   |                | <b>C</b> U-L                  |                   |         |              |
|             | Caches  | •            | Cache List                        | •              | CLICK                         | validating-resolv | er_e    | iche.        |
|             | Settings  |              | statistics                        | 2              |                               |                   |         |              |
| 6           | SSL Orchestrator                                      | 1            |                                   |                |                               |                   |         |              |
|             | Acceleration  | /            |                                   |                |                               |                   |         |              |
|             | Device Management                                     |              |                                   |                |                               |                   |         |              |
|             | Network   |              |                                   |                |                               |                   |         |              |
| 84          | System  |              |                                   |                |                               |                   |         |              |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/trust\_anchor/list.jsp?name=

| Hostname: gtm1.site1<br>IP Address: 10.1.10.13 | .example.com       | Date: Jul 21, 20<br>Time: 1:33 AM | )17 User:<br>(CDT) Role: | <b>admin</b><br>Administrator |                        |               |           |
|--|--------------------|-----------------------------------|--------------------------|-------------------------------|------------------------|---------------|-----------|
| Concline<br>Standa                             | E (ACTIVE)<br>Ione |                                   |                          |                               |                        |               |           |
| Main Help                                      | About              | DNS »                             | Caches : Cach            | e List » Trust.               | Anchors : validating-r | esolver_cache |           |
| Ma Statistics                                  |                    | <b>⇔</b> -                        | Properties               | Trust Ancho                   | rs DLV Anchors         | Local Zones   | Forward Z |
| iApps  |                    | Trust An                          | chors                    | /0                            |                        |               | 2 Add     |
| S DNS  |                    | 🗹 Tr                              | ust Anchor               |                               |                        | -             | 1         |
| Delivery                                       |                    | No reco                           | rds to display           |                               |                        |               |           |
| GSLB   |                    | Remov                             | e /                      |                               |                        |               |           |
| Zones  | Clic               | k "Trus                           | st Anch                  | ors"                          |                        | Click "A      | dd"       |
| Caches   |                    | •                                 |                          |                               |                        | ener A        |           |
| Settings                                       |                    | •                                 |                          |                               |                        |               |           |
| SSL Orchestrat                                 | Dr                 |                                   |                          |                               |                        |               |           |
| Acceleration                                   |                    |                                   |                          |                               |                        |               |           |
| Device Manage                                  | nent               |                                   |                          |                               |                        |               |           |
| Network  |                    |                                   |                          |                               |                        |               |           |
| System   |                    |                                   |                          |                               |                        |               |           |

%2FCommon%2Fvalidating-resolver\_cache&tab=dns\_cache\_validating\_config

For each line of output from the preceding command create a "Trust Anchor"

# DNS » Caches : Cache List

| Add Trust Anchor   |  |
|--|--|
| Trust Anchor   | . IN DS 19036 8 1 B256BD09DC8DD59F0E0F0D8541B8328DD986DF6E   |
| Cancel Repeat Finished   |  |
| 🛃 router01   |  |
| <pre>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>210:domain ip-protocol t<br/>rofile ( ) } translate-s<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>[root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:Eval:Acti<br/>]root@routerO1:E</pre> | <pre>ve:Standalone] config #<br/>ve:Standalone] config #<br/>ve:Standalone] config # tmsh create ltm virtual DC02_tcp_53_virt<br/>cp mask 255.255.255.255 profiles add { example.com_dns_profile {<br/>ddress disabled vlans add { branch01_vlan } vlans-enabled pool b<br/>ve:Standalone] config #<br/>ve:Standalone] config #<br/>ve:Standalone] config # tmsh create ltm dns cache validating-res<br/>ones yes<br/>ve:Standalone] config #<br/>ve:Standalone] config #<br/>ve:Standalone] config #<br/>ve:Standalone] config #<br/>ve:Standalone] config #<br/>ve:Standalone] config #<br/>ve:Standalone] config #<br/>dnsec_dsfromkey -f /root/dnskey.t<br/>ve:Standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>ve:Standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>ve:Standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>ve:Standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>ve:Standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>ve:Standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>ve:Standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>ve:Standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>ve:Standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>ve:Standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>ve:Standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>set standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>set standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>set standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>set standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>set standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>set standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>set standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>set standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>set standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>set standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>set standalone] config # dig dnskey .   grep 257 &gt; /root/dnskey.t<br/>set standalone] config # dig dnsk</pre> |
| IN DJ 20020 0 2 LOOD44<br>[root@router01:Eval:Acti   | ve:Standalonel config #  |
| [root@router01:Eval:Acti   | ve:Standalone] config #  |
| [root@router01:Eval:Acti   | ve:Standalone] config # c  |

| 🔅 🚽 Properties      | Trust Anchors    | DLV Anchors       | Local Zones     | Forward Zones    | Response Policy Zones |     |
|---------------------|------------------|-------------------|-----------------|------------------|-----------------------|-----|
| Statistics 🗵        |                  |                   |                 |                  |                       |     |
|                     |                  |                   |                 |                  |                       |     |
| rust Anchors        |                  |                   |                 |                  |                       | Add |
| Trust Anchor        |                  |                   |                 |                  |                       |     |
| . IN DS 19036 8 1 B | 256BD09DC8DD59F  | DE0F0D8541B8328D  | D986DF6E        |                  |                       |     |
| . IN DS 19036 8 2 4 | 9AAC11D7B6F64467 | 02E54A1607371607A | 1A41855200FD2CE | 1CDDE32F24E8FB5  |                       |     |
| . IN DS 20326 8 1 A | E1EA5B974D4C8588 | 3740BD03E3CED7EE  | FCBD1724        |                  |                       |     |
| . IN DS 20326 8 2 E | 06D44B80B8F1D39A | 95C0B0D7C65D0845  | 8E880409BBC6834 | 57104237C7F8EC8E | )                     |     |
| Remove              |                  |                   |                 |                  |                       |     |

1

tmsh modify ltm dns cache validating-resolver validating-resolver\_cache trust-anchors\_ →replace-all-with { ". IN DS 19036 8 1 B256BD09DC8DD59F0E0F0D8541B8328DD986DF6E" ".\_ →IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5" ". → IN DS 20326 8 1 AE1EA5B974D4C858B740BD03E3CED7EBFCBD1724" ". IN DS 20326 8 2\_ →E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D" }

### 2.2.5.2 Modify DNS Profile

In order to activate the new "Validating Resolver", modify the DNS profile example.com\_dns\_profile.

```
Navigate to: DNS >> Delivery : Profiles : DNS
```



Select the profile "example.com\_dns\_profile"

Modify the DNS profile to activate the new validating-resolver\_cache.

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 19, 2017 User: a<br>Time: 1:07 PM (CDT) Role: A | <b>dmin</b><br>.dministrator             |
|---|---|--|
| ONLINE (ACTIVE)<br>Standalone                                     |   |  |
| Main Help About   | DNS » Delivery : Profiles : DN                            | S » Properties : example.com_dns_profile |
| Mage Statistics   | 🔅 👻 Properties  |  |
| iApps   | General Properties  |  |
| 🔁 Wizards   | Name  | example.com_dns_profile                  |
|   | Partition / Path  | Common                                   |
|   | Parent Profile  | dns                                      |
| Delivery  | Denial of Service Protection                              |  |
| GSLB  | Rapid Response Mode                                       | Disabled V                               |
| Control   | Rapid Response Last Action                                |  |
| Settings  |   |  |
| octango   | Hardware Acceleration                                     | Disabled                                 |
| SSL Orchestrator  |   |  |
| Local Traffic   | Response Cacne  |  |
| 0   | DNS Features  | ct the "validating-resolver_cache"       |
| Traffic Intelligence  | DNSSEC  | Enabled 🔽                                |
| Acceleration  | GSLB  | Enabled 💟                                |
| Access  | DNS Express   | Enabled 🗸                                |
|   | DNS Cache   | Enabled V                                |
| Device Management   | DNS Cache Name  | validating-resolver_cache                |
| Retwork   | DNS IPv6 to IPv4  | Disabled 🔽                               |
| System  | Unhandled Query Actions                                   | Allow 🔽                                  |
|   | Use BIND Server on BIG-IP                                 | Disabled V                               |
|   | DNS Traffic   |  |
|   | Zone Transfer   | Disabled                                 |
|   | DNS Security  | Disabled                                 |
|   | DNS Security Profile Name                                 | Select                                   |
|   | Process Recursion Desired                                 | Enabled V                                |
|   | Logging and Reporting                                     |  |
|   | Logging   | Enabled V                                |
|   | Logging Profile   | example_dns_logging_profile              |
|   | AVR Statistics Sample Rate                                | Enabled 1/ 1 queries sampled             |
|   |   | ,,                                       |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/profile/dns/properties.jsp?name=/Common/example.com\_dns\_profile

### TMSH

tmsh modify ltm profile dns example.com\_dns\_profile cache validating-resolver\_cache

#### 2.2.5.3 Results

From the CLI on the router01.branch01 BIGIP run

tail -f /var/log/ltm

From the Workstation CMD prompt run: "dig ghghghghg.com"



From the Workstation CMD prompt run: "dig google.com"



From the Workstation CMD prompt run: "dig dnssec-deployment.org +dnssec"

#### **Reference Architecture Documentation**

| 📾 Command Prompt 📃 🗆 🗙  |   |
|---|---|
| C:\Users\user.EXAMPLE>dig dnssec-deployment.org +dnssec   |   |
| ; <<>> DiG 9.3.2 <<>> dnssec-deployment.org +dnssec<br>;; global options: printcmd<br>;; Got answer:<br>;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1568<br>;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 1   |   |
| ;; OPT PSEUDOSECTION:<br>; EDNS: version: 0, flags: do; udp: 4096<br>;; QUESTION SECTION:<br>;dnssec-deployment.org. IN A   |   |
| ;; ANSWER SECTION:<br>dnssec-deployment.org. 294 IN A 46.43.37.10<br>dnssec-deployment.org. 294 IN RRSIG A 5 2 300 20170801204001 2017071<br>8204001 36518 dnssec-deployment.org. fcsC4invKmAp0c+39rYtx+tWzp9cPb6I/MRVeG9gvn<br>wMXkGNFXuJwU1 +eBsy6NRNW184maIW7vY0bmwJkqsET2okUCcEP00/BzY/RFPHmzBsG5N Bxhg+0Lei<br>MUYp/gHiDXAtGQUMvMgn6Z3oeqD4Ut6FJEcLuyGED0cRYNB yBc=  |   |
| ;; AUTHORITY SECTION:<br>dnssec-deployment.org. 294 IN NS ns1.sea1.afilias-nst.info.<br>dnssec-deployment.org. 294 IN NS ns1.mia1.afilias-nst.info.<br>dnssec-deployment.org. 294 IN NS ns1.yyz1.afilias-nst.info.<br>dnssec-deployment.org. 294 IN NS ns1.hkg1.afilias-nst.info.<br>dnssec-deployment.org. 294 IN NS ns1.ams1.afilias-nst.info.<br>dnssec-deployment.org. 294 IN NS ns1.ams1.afilias-nst.info.<br>dnssec-deployment.org. 294 IN RRSIG NS 5 2 300 20170801204001 201707<br>18204001 36518 dnssec-deployment.org. Jr13JdhS8T+ScKm+ZRpweEMywc1h0LM6T/5032dwp5   | erv   |
| <pre>[ul 19 13:07:46 router01 info tmm[12513]: 2017-07-19 13:07:45 router01.branch01.exam<br/>.16 from 10.1.71.100#65485: view none: query: dnssec-deployment.org IN &amp; + (10.1.70.<br/>[ul 19 13:07:46 router01 info tmm[12513]: 2017-07-19 13:07:45 router01.branch01.exam<br/>.16 to 10.1.71.100#65485: [NOERROR qr,rd,ra] response: dnssec-deployment.org. 300 IN<br/>.0;<br/>[ul 19 13:07:52 router01 info tmm[12513]: 2017-07-19 13:07:52 router01.branch01.exam<br/>.568 from 10.1.71.100#65486: view none: query: dnssec-deployment.org IN &amp; +ED (10.1.<br/>.01 19 13:07:52 router01 info tmm[12513]: 2017-07-19 13:07:52 router01.branch01.exam<br/>.568 to 10.1.71.100#65486: view none: query: dnssec-deployment.org IN &amp; +ED (10.1.<br/>.01 19 13:07:52 router01 info tmm[12513]: 2017-07-19 13:07:52 router01.branch01.exam<br/>.568 to 10.1.71.100#65486: [NOERROR qr,rd,ra,ad] response: dnssec-deployment.org. 29<br/>37.10; dnssec-deployment.org. 294 IN RRSIG &amp; 5 2 300 20170801204001 20170718204001<br/>.02170801204001 20170718204001<br/>.02170801204001_20170718204001</pre> | ple.com qid<br>200%0)<br>ple.com qid<br>A 46.43.37.<br>ple.com qid<br>70.200%0)<br>ple.com qid<br>4 IN A 46.43<br>36518 dnssec<br>4maIU7.YObmw<br>RYNByBc=; |

From the Workstation CMD prompt run: "dig dnssec-failed.org +dnssec"



http://www.internetsociety.org/deploy360/resources/dnssec-test-sites/

Configure a validating resolver cache on the BIG-IP® system to recursively query public DNS servers, validate the identity of the DNS server sending the responses, and then cache the responses.

After completing this lab students will entirely offload DNS queries from internal masters.





Navigate to DNS >> Caches : Cache List

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 16, 2017 User: admin<br>Time: 6:47 PM (CDT) Role: Administrator |
|---|---|
| ONLINE (ACTIVE)<br>Standalone                                     |   |
| Main Help About   | DNS » Caches : Cache List   |
| Statistics  | 🚓 🚽 Cache List Statistics 🗵   |
| iApps   | * × Search  |
| 😚 dns   | ✓ ♦ Name  |
| Delivery  | No records to display.  |
| GSLB  | Delete  |
| Zones   |   |
| Caches  | Cache List 📀  |
| Settings  | Statistics  |
| SSL Orchestrator  |   |
| Local Traffic   |   |
| Acceleration  |   |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/list.jsp

Create a validating resolver cache according to the table below:

| Field                | Value                     |
|----------------------|---------------------------|
| Name                 | validating-resolver_cache |
| Resolver Type        | Validating Resolver       |
| Answer default zones | Checked - Enabled         |

| General Properties         |                           |
|----------------------------|---------------------------|
| Name                       | validating-resolver_cache |
| Resolver Type              | Validating Resolver 🗸     |
| Route Domain Name          | 0 🗸                       |
| DNS Cache                  |                           |
| Message Cache Size         | 1048576 bytes             |
| Resource Record Cache Size | 10485760 bytes            |
| Name Server Cache Count    | 16536 entries             |
| DNSSEC Key Cache Size      | 1048576 bytes             |
| Answer Default Zones       |                           |
| RRSet Rotate               | none 🗸                    |
| DNS Resolver               |                           |
| Use IPv4                   | ☑ Enabled                 |

| Use IPv4   | ✓ Enabled   |
|--|-------------|
| Use IPv6   | ☑ Enabled   |
| Use UDP  | Enabled     |
| Use TCP  | Enabled     |
| Max. Concurrent UDP Flows                          | 8192        |
| Max. Concurrent TCP Flows                          | 20          |
| Max. Concurrent Queries                            | 1024        |
| Unsolicited Reply Threshold                        | 0           |
| Allowed Query Time                                 | 200         |
| Randomize Query Character<br>Case                  | Enabled     |
| Root Hints (Optional: Leave blank<br>for defaults) | IP Address: |
| 2.2. Security                                      | 205         |
|  |             |

# DNSSEC Validator

Profetch Kov

Finabled

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/create.jsp

#### TMSH

tmsh create Itm dns cache validating-resolver validating-resolver\_cache answer-default-zones yes

https://support.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-services-implementations-12-1-0/7.html#guid-d4548549-b4e2-4dae-9ada-3ea00eb84c1f

## 2.2.6 RPZ

Response Policy Zone will be turned on to stop clients from trying to resolve blacklisted domains.



https://support.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-services-implementations-12-1-0/8.html

#### 2.2.6.1 Zone Runner

Customers will subscribe to their RPZ vendor of choice.

Use Zonerunner to create a custom RPZ zone for our lab.

Navigate to DNS >> Zones : ZoneRunner : Zone List

| Hostnan<br>IP Addre | me: router01.branch01.example.co<br>ess: 10.1.10.31 | m | Date: Jul 12, 2017<br>Time: 9:19 PM (CDT) | ) F      | Iser: <b>admin</b><br>Role: Administra | itor         |                   |            | Partition:         | Common    | Log out          | ] |
|---------------------|---|---|---|----------|--|--------------|-------------------|------------|--------------------|-----------|------------------|---|
|                     | ONLINE (ACTIVE) Standalone                          |   |   |          |  |              |                   |            |                    |           |                  |   |
| Main                | Help About  |   | DNS » Zones : Zo                          | neRun    | ner : Zone Lis                         | st           |                   |            |                    |           |                  |   |
| Sta                 | atistics  |   | Resource Re                               | ecord L  | ist Zone List                          |              | View I            | _ist       | named Configuratio | n         |                  |   |
| iAp                 | pps   |   | Find Zones                                |          |  |              |                   |            |                    |           |                  |   |
| S DN                | IS  |   | View Name                                 |          | All                                    | $\checkmark$ |                   |            |                    | ~         |                  |   |
|                     | Delivery  | Þ | Zone Name                                 |          | *                                      |              | 5                 | Bearch Res | et Search          |           |                  |   |
|                     | GSLB  | Þ | -   |          |  |              |                   |            |                    |           | Create           | D |
|                     | Zones   | Þ | Zones                                     | •        |  |              |                   |            | Zone Type          | View Name | Resource Records |   |
|                     | Caches  | F | DNSSEC Zones                              | •        |  |              |                   |            |                    |           |                  |   |
|                     | Settings  | > | ZoneRunner                                | ×        | Resource Re<br>List                    | ecord (      | Ð                 |            |                    |           |                  |   |
| ss ss               | L Orchestrator                                      |   |   | <b>→</b> | Zone List                              | (            | $\mathbf{\Sigma}$ |            |                    |           |                  |   |
|                     | cal Traffic   |   |   |          | View List                              | (            | Ð                 |            |                    |           |                  |   |
| 00                  |   |   |   |          | named Confi                            | guration     |                   |            |                    |           |                  |   |
| Ac                  | celeration  |   |   |          |  |              |                   |            |                    |           |                  |   |
| E De                | vice Management                                     |   |   |          |  |              |                   |            |                    |           |                  |   |
| Net                 | twork   |   |   |          |  |              |                   |            |                    |           |                  |   |
| Sy:                 | stem  |   |   |          |  |              |                   |            |                    |           |                  |   |

# https://router01.branch01.example.com/tmui/Control/jspmap/tmui/globallb/zfd/zone/create.jsp

Create a zone according to the following table:

| Field                 | Value                           |
|-----------------------|---------------------------------|
| View Name             | external                        |
| Zone Name             | rpz.example.com                 |
| Zone Type             | Master                          |
| Zone File Name        | db.external.rpz.example.com     |
| Options               | also-notify { ::1 port 5353; }; |
| TTL                   | 300                             |
| Master Server         | router01.branch01.example.com.  |
| Email Contact         | hostmaster.example.com.         |
| NS Record: TTL        | 300                             |
| NS Record: Nameserver | router01.branch01.example.com.  |
| Create A Record       | Checked - Enabled               |
| A Record: IP Address  | 10.1.71.1                       |

| General Properties      |   |  |  |  |  |
|-------------------------|---|--|--|--|--|
| View Name               | external V  |  |  |  |  |
| Zone Name               | rpz.example.com   |  |  |  |  |
| Zone Type               | Master V NO GOU AL LITE ELLO  |  |  |  |  |
| Configuration           |   |  |  |  |  |
| Records Creation Method | Manual  |  |  |  |  |
| Zone File Name          | db.external.rpz.example.com   |  |  |  |  |
| Options                 | <pre>allow-update { localhost; }; also-notify { ::1 port 5353; }; </pre>  |  |  |  |  |
| Create Reverse Zone     | Enable  |  |  |  |  |
| Records Creation        | Dots at the end   |  |  |  |  |
| SOA Record              | TTL     300       Master Server     router01.branch01.example.com.       Email Contact     hostmaster.example.com.       Serial Number     2017071801       Refresh Interval     10800       Retry Interval     3600       Expire     604800       Negative TTL     86400 |  |  |  |  |
| NS Record               | TTL 300<br>Nameserver router01.branch01.example.com.  |  |  |  |  |
| Create A Record         | ☑ Enable  |  |  |  |  |
| A Record                | IP Address 10.1.71.1  |  |  |  |  |

# Navigate to: DNS >> Zones : ZoneRunner : Resource Record List

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/globallb/zfd/record/create.jsp

| Hos<br>IP A | stname: router01.branch01.example.com<br>Address: 10.1.10.31 | Date: Jul 12, 2017 Use<br>Time: 10:06 PM (CDT) Role | r: <b>admin</b><br>e: Administrator |                          | Partition: Co       |
|-------------|--|---|-------------------------------------|--------------------------|---------------------|
| (           | Standalone   |   |                                     |                          |                     |
| N           | Main Help About  | DNS » Zones : ZoneRunner                            | : Resource Reco                     | ord List                 |                     |
| <b>M</b>    | Statistics   | 🚓 👻 Resource Record List                            | Zone List                           | View List                | named Configuration |
|             | iApps  | Find Records  |                                     |                          |                     |
| $\bigcirc$  | DN\$   | View Name   | All 🔽                               |                          |                     |
|             | Delivery   | Zone Name   | All Zones (Se                       | elect a View to search a | a specific zone) 🔽  |
|             | GSLB >   | Туре  | All                                 | $\checkmark$             |                     |
|             | Zones 🕨  | Name  | *                                   |                          |                     |
|             | Caches   | RDATA   |                                     |                          |                     |
|             | Settings   | Search Reset Search Cr                              | eate                                |                          |                     |
| f           | SSL Orchestrator   |   |                                     |                          |                     |
| 69          | Local Traffic  |   |                                     |                          |                     |
|             | Acceleration   |   |                                     |                          |                     |
|             | Device Management  |   |                                     |                          |                     |

Create a resource record according to the following table:

| Field     | Value                       |
|-----------|-----------------------------|
| View Name | external                    |
| Zone Name | rpz.example.com             |
| Name      | *.guns.com.rpz.example.com. |
| TTL       | 300                         |
| Туре      | CNAME                       |
| CNAME     |                             |

| Record Configuration |                             |
|----------------------|-----------------------------|
| View Name            | external 🗸                  |
| Zone Name            | rpz.example.com. 🗸          |
| Name                 | *.guns.com.rpz.example.com. |
| TTL                  | 300                         |
| Туре                 |                             |
| CNAME                | Period                      |

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 18, 2017<br>Time: 11:29 PM (CDT) | User: <b>admin</b><br>Role: Administrator |                        |                   |
|---|--|---|------------------------|-------------------|
| ONLINE (ACTIVE)<br>Standalone<br>Main Help About                  | DNS » Zones : ZoneRun                      | ner : Resource Record L                   | ist                    |                   |
| Statistics  | 🔅 🚽 Resource Record Li                     | ist Zone List 🛛 🔪                         | /iew List nar          | ned Configuration |
| iApps   | Find Records                               |   |                        |                   |
| S DNS   | View Name                                  | All                                       |                        |                   |
| Delivery  | Zone Name                                  | All Zones (Select                         | a ∨iew to search a spe | cific zone) 🔽     |
| GSLB  | Туре                                       | Ali                                       | 2                      |                   |
| Zones   | Name                                       | *   |                        |                   |
| Caches  | RDATA                                      | *   |                        |                   |
| Settings  | Search Reset Search                        | Create.                                   |                        |                   |
| SSL Orchestrator  |  | <u> </u>                                  | <u>k "Se</u>           | arch"             |
| Local Traffic   | ✓ ▲ Name                                   | View Name                                 | ⇒ Zone N               | lame 🗘            |
|   | suns.com.rpz.examp                         | le.com. external                          | rpz.exam               | ple.com. 30       |
| Acceleration  | rpz.example.com.                           | external                                  | rpz.exam               | ple.com. 30       |
| Device Management   | Delete                                     | external                                  | rpz.exan               | ple.com. 30       |
| Network   |  |   |                        |                   |

### 2.2.6.2 Name Server

Navigate to DNS >> Delivery : Nameservers : Nameserver List

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 12, 2017<br>Time: 10:23 PM (CDT) | User: <b>admin</b><br>Role: Administrator | Partiti |
|---|--|---|---------|
| ONLINE (ACTIVE) Standalone  |  |   |         |
| Main Help About   | DNS » Delivery : Name                      | eservers : Nameserver List                |         |
| Statistics  | 🔅 👻 Nameserver List                        | Statistics 💌                              |         |
| iApps   | ŕ  | × Search                                  |         |
| S DNS   | ✓ A Name                                   |   |         |
| Delivery 🗼 🕨 🕨  | Listeners                                  |   |         |
| GSLB  | Profiles                                   |   |         |
| Zones   | Load Balancing                             |   |         |
| Caches  | iRules                                     |   |         |
| Settings  | Translation >                              |   |         |
|   | Nameservers                                | Nameserver List 📀                         |         |
| SSL Orchestrator  | Kevs                                       | Statistics                                |         |
| Local Traffic   |  |   |         |
| Acceleration  |  |   |         |
| Device Management   |  |   |         |
| Network   |  |   |         |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/nameserver/list.jsp

Create a nameserver according to the following table:

| Field | Value     |
|-------|-----------|
| Name  | localhost |

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 18, 2017 User: a<br>Time: 11:33 PM (CDT) Role: A | <b>udmin</b><br>Administrator      |
|---|--|------------------------------------|
| Standalone  |  |                                    |
| Main Help About   | DNS » Delivery : Nameservers                               | : Nameserver List » New Nameserver |
| Statistics  |  |                                    |
|   | General Properties   |                                    |
| iApps   | Name   | localhost                          |
| S DNS   | Address  | 127.0.0.1                          |
| Delivery  | Service Port   | 53 Other:                          |
| GSLB  | Configuration  |                                    |
| Zones   | Route Domain   |                                    |
| Caches  | TSIG Key   | None                               |
| Settings  |  |                                    |
| SSL Orchestrator  | Cancel Repeat Finished                                     |                                    |
| Local Traffic   |  |                                    |
| Acceleration  |  |                                    |
| Device Management   |  |                                    |
| Network   |  |                                    |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/nameserver/create.jsp

## TMSH

tmsh create ltm dns nameserver localhost { address 127.0.0.1 tsig-key none }

### 2.2.6.3 DNS Express

#### Navigate to DNS >> Zones : Zones : Zone List

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/zone/create.jsp

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 12, 2017<br>Time: 10:32 PM (CDT) | User: <b>admin</b><br>Role: Administrator | Partition: Common V |
|---|--|---|---------------------|
| ONLINE (ACTIVE)<br>Standalone                                     |  |   |                     |
| Main Help About   | DNS » Zones : Zones :                      | : Zone List                               |                     |
| Statistics  | 🔅 👻 Zone List                              | Statistics 💌                              |                     |
| a iApps   |  |   |                     |
| iApps   | *  | × Search                                  | Create              |
| 😚 dns   | ✓ A Name                                   |   |                     |
| Delivery  | No records to display.                     |   |                     |
| GSLB  | Delete                                     |   |                     |
| Zones 🗼 🔸   | Zones                                      | Zone List 💽                               |                     |
| Caches  | NSSEC Zones                                | Statistics                                |                     |
| Settings  | ZoneRunne 🕨                                |   |                     |
| SSL Orchestrator  |  |   |                     |
| Local Traffic   |  |   |                     |
| Acceleration  |  |   |                     |
| Device Management   |  |   |                     |
| Network   |  |   |                     |

Create a DNS Express zone according to the following table:

| Field             | Value           |
|-------------------|-----------------|
| Name              | rpz.example.com |
| Server            | localhost       |
| Allow NOTIFY From | 127.0.0.1       |
| Response Policy   | checked         |

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 18, 2017<br>Time: 11:37 PM (CDT) | User: <b>admin</b><br>Role: Administrator          |  |
|---|--|--|--|
| ONLINE (ACTIVE)<br>Standalone                                     |  |  |  |
| Main Help About   | DNS » Zones : Zones :                      | Zone List » New Zone                               |  |
| Statistics  |  |  |  |
| -   | General Properties                         |  |  |
| IApps   | Name                                       | rpz.example.com                                    |  |
| S DNS   | DNS Express                                |  |  |
| Delivery  | Server                                     | localhost  |  |
| GSLB  | Availability                               | Unknown  |  |
| Zones >   | State                                      | Enabled V  |  |
| Caches  | Notify Action                              | Consume 🗸  |  |
| Settings  |  | Address: 127.0.0.1 × Add                           |  |
| SSL Orchestrator  | Allow NOTIFY From                          |  |  |
| Local Traffic   |  |  |  |
| Acceleration  |  | Delete   |  |
|   | Verify Notify TSIG                         |  |  |
| Device Management   | Response Policy                            |  |  |
| Network   | Zone Transfer Clients                      |  |  |
| System  | Nameservers                                | Active Available Common dc01.example.com localhost |  |
|   | TSIG                                       |  |  |
|   | Server Key                                 | None   |  |

### TMSH

tmsh create ltm dns zone rpz.example.com { dns-express-server localhost response-policy yes dns-express-allow-notify add { 127.0.0.1 } dns-express-notify-tsig-verify no }

#### 2.2.6.4 Local Zone

#### Navigate to: DNS >> Caches : Cache List

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/list.jsp
| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 18, 2017 User: admin<br>Time: 11:40 PM (CDT) Role: Administrator |
|---|--|
| ONLINE (ACTIVE) Standalone  |  |
| Main Help About   | DNS » Caches : Cache List  |
| Statistics  | Cache List Statistics  |
| iApps   | * Search   |
| S DNS   | ✓ ♦ Name   |
| Delivery  | transparent_cache  |
|   | validating-resolver_cache  |
| GSLB  | Delete   |
| Zones   |  |
| Caches  | Cache List 📀   |
| Settings  | Statistics   |
| SSL Orchestrator  |  |
| Local Traffic   |  |
| Acceleration  |  |
| Device Management   |  |
| Network   |  |

Select validating-resolver\_cache, click "Local Zones", and click "Add"

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/local\_zone/list.jsp?name= %2FCommon%2Fvalidating-resolver\_cache&tab=dns\_cache\_config

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 18, 2017<br>Time: 11:45 PM (CDT) | User: <b>admin</b><br>Role: Administrator |                     | Pi          | artition: Common |
|---|--|---|---------------------|-------------|------------------|
| ONLINE (ACTIVE)<br>Standalone                                     |  |   |                     |             |                  |
| Main Help About   | DNS » Caches: Cach                         | e List » Local Zones                      | : validating-resolv | er_cache    |                  |
| Magazina Statistics   | 🔅 👻 Properties                             | Trust Anchors                             | DLV Anchors         | Local Zones | Forward Z        |
| iApps   | Response Policy Zones                      | Statistics 🔎                              |                     | /1          |                  |
| S DNS   | Local Zones                                |   |                     |             | Add              |
| Delivery  | ✓ Name                                     |   |                     |             | 2                |
| GSLB  | No records to display.                     |   | Select "Lo          | ocal Zone   | s"               |
| Zones >   | Delete                                     |   | Then clic           | c"Add"      | ~                |
| Caches  |  |   |                     |             |                  |
| Settings  |  |   |                     |             |                  |
| SSL Orchestrator  |  |   |                     |             |                  |
| Local Traffic   |  |   |                     |             |                  |
| Acceleration  |  |   |                     |             |                  |
| Device Management   |  |   |                     |             |                  |
| Retwork   |  |   |                     |             |                  |

Create a local zone entry according to the following table:

| Field   | Value                              |
|---------|------------------------------------|
| Name    | sorry.example.com                  |
| Туре    | Static                             |
| Records | sorry.example.com. IN A 10.1.71.21 |

| Local Zone |   |
|------------|---|
| Name       | sorry.example.com   |
| Туре       | Static  |
| Records    | sorry.example.com. IN A 10.1.71.21 × Add sorry.example.com. IN A 10.1.71.21 There is a "dot" at the end !! Delete |

TMSH commands for router01.branch01:

(continued from previous page)

### 2.2.6.5 Walled Garden

#### Navigate to: DNS >> Caches : Cache List

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/list.jsp

Click "validating-resolver\_cache"

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 18, 2017 User: admin<br>Time: 11:40 PM (CDT) Role: Administrator |
|---|--|
| ONLINE (ACTIVE) Standalone  |  |
| Main Help About   | DNS » Caches : Cache List  |
| Statistics  | trache List Statistics   |
| iApps   | search   |
| S DNS   | ✓ \$ Name  |
| Delivery  | transparent_cache  |
| GSLB  | validating-resolver_cache  |
| Zones   | Delete Click "validating-resolver cache                                    |
| Caches  | Cache List   |
| Settings  | Statistics   |
| SSL Orchestrator  |  |
| Local Traffic   |  |
| Acceleration  |  |
| Device Management   |  |
| Network   |  |

Select validating-resolver\_cache, click "Response Policy Zones", and then click "Add"

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/rpz/list.jsp?name= %2FCommon%2Fvalidating-resolver\_cache&tab=dns\_cache\_config

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 13, 2017<br>Time: 3:48 PM (CDT) | User: <b>admin</b><br>Role: Administrator |                       | Partition:            | ommon 🔽          | Log out          |
|---|---|---|-----------------------|-----------------------|------------------|------------------|
| Standalone  |   |   |                       |                       |                  |                  |
| Main Help About   | DNS » Caches : Cach                       | he List » Response F                      | Policy Zones : resolv | /er_cache             |                  |                  |
| Mage Statistics   | 🚓 🗸 Properties                            | Local Zones                               | Forward Zones         | Response Policy Zones | Statistics       |                  |
| iApps   | Response Policy Zones                     | 8   | ,                     | 1                     |                  | Add              |
| S DNS   | ✓ ▲ Name                                  |   | ≑ <u>Action</u>       | ♦ Willed Garden ♦ Log | s and Stats Only | Partition / Path |
| Delivery  | No records to display.                    |   |                       | / 0                   | 2/               |                  |
| GSLB  | Delete                                    | Click "Res                                | <u>ponse Po</u> l     | licy Zone"            | Click "          | Add"             |
| Zones   |   |   | _                     | -                     |                  |                  |
| Caches  |   |   |                       |                       |                  |                  |
| Settings  |   |   |                       |                       |                  |                  |
| SSL Orchestrator  |   |   |                       |                       |                  |                  |
| Local Traffic   |   |   |                       |                       |                  |                  |
| Acceleration  |   |   |                       |                       |                  |                  |
| Device Management   |   |   |                       |                       |                  |                  |

Create a local zone entry according to the following table:

| Field         | Value             |
|---------------|-------------------|
| Zone          | rpz.example.com   |
| Action        | Walled Garden     |
| Walled Garden | sorry.example.com |



TMSH commands for router01.branch01:

#### TMSH

tmsh modify ltm dns cache resolver validating-resolver\_cache response-policy-zones add { rpz.example.com { action walled-garden walled-garden sorry.example.com } }

### 2.2.6.6 Results

From a Workstation command prompt run "dig www.guns.com"



Try running additional dig commands to verify that other domains still resolve as expected.

dig www.f5.com

# 2.2.7 URL Categorization

Configure DNS queries filtering based on the category of the requested domain. This will be done with using F5 iRules and built-in categorization database.



### 2.2.7.1 Create an iRule

Navigate to: DNS >> Delivery : iRules : iRules List

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 18, 2017<br>Time: 8:30 PM (CDT) | User: <b>admin</b><br>Role: Administrator |              |
|---|---|---|--------------|
| CONLINE (ACTIVE) Standalone                                       |   |   |              |
| Main Help About   | DNS » Delivery : iRule                    | s : iRule List                            |              |
| Mage Statistics   | 🔅 👻 iRule List                            | Data Group List iFile List                | Statistics 🔎 |
| iApps   | *   | × Search                                  |              |
| S DNS   | Name                                      | Verification                              | \$           |
| Delivery  | Listeners >                               | g None                                    |              |
| GSLB  | Profiles                                  | eSupport_OA_BasicAuth 🖭 F5 Verifie        | d f5         |
| Zones   | Load Balancing                            | eSupport_OA_NtImAuth 🖭 F5 Verifie         | d f5         |
| Caches  | iRules N                                  | iRule List                                | <b>1</b> f5  |
|   |   | F5 Verifie                                | 1 15         |
| Settings  | Iransiation                               | Data Group List + F5 Verifie              | d f5         |
| SSI Orchestrator  | Nameservers                               | iFile List (+) F5 Verifie                 | <b>1</b> f5  |
| JE SE OTCHESTURO  | Keys                                      | Statistics P5 Verifie                     | d f5         |
| Local Traffic   | sys_auth_Idap                             | 🖭 F5 Verifie                              | d f5         |
| Acceleration  | sys_auth_radius                           | ES Verifie                                | d f5         |
| Acceleration  | sys_auth_ssl_cc_ld                        | ap 🖭 F5 Verifie                           | 1 15         |
| Device Management   | sys_auth_ssl_cridp                        | E F5 Verifie                              | 1 15         |
| -   | sys_auth_ssl_ocsp                         | Pa F5 Verifie                             | d f5         |
| Network   |   |   |              |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/rule/list.jsp

Create new iRule, copy the content below and paste it.

| Field | Value               |
|-------|---------------------|
| Name  | DNS-query-filtering |

| when RULE_INIT {   |                         |
|--|-------------------------|
| <i># Set categories to block for DNS hosts</i>             |                         |
| <pre>set static::blocked_categories {</pre>                |                         |
| /Common/Bot_Networks                                       |                         |
| /Common/Spyware  |                         |
| /Common/Malicious_Web_Sites                                |                         |
| /Common/Adult_Content                                      |                         |
| /Common/Sex  |                         |
| }  |                         |
|  |                         |
| # CONFIGURATION  |                         |
| # Check all requests by default                            |                         |
| set static: request check 1                                |                         |
| to the entering of the shad we have NVDOMATN (1)           |                         |
| # II the category returns as blocked, return NXDOMAIN (1)  |                         |
| # Otherwise if (0), return a statically defined IP address |                         |
| <pre>set static::request_return_nxdomain 0</pre>           |                         |
|  | (continues on next page |

(continues on next page)

```
set static::request_redirect_to "10.1.71.21"
  # Toggle for debug logs
  set static::request_debug 1
}
when DNS_REQUEST {
 if { $static::request_check } {
   set lookup_category [getfield [CATEGORY::lookup "http://[DNS::question name]"] "
→" 1]
   if { [lsearch -exact $static::blocked_categories $lookup_category] >= 1 } {
      if { $static::request_debug } {
         log local0. "BLOCKED: Category $lookup_category matching [DNS::question_
→name] is filtered."
      }
      DNS::answer clear
      if { $static::request_return_nxdomain } {
         DNS::header opcode QUERY
         DNS::header rcode NXDOMAIN
      } else {
         if { [DNS::question type] equals "A" } {
            DNS::answer insert "[DNS::question name]. 111 [DNS::question class].

→[DNS::question type] $static::request_redirect_to"

         }
      }
      DNS::return
} else {
   if { $static::request_debug } {
      log local0. "Category $lookup_category matching [DNS::question name] is not.
\hookrightarrow filtered"
      }
    }
  }
}
```

TMSH commands for router01.branch01 (Make sure you use text editor to copy content above and paste it)

## TMSH

tmsh create Itm rule DNS-query-filtering

## 2.2.7.2 iRule assignment

Repeat the following steps for all 4 DNS listeners.

Navigate to: DNS >> Delivery : Listeners : Listener List

|            | name: router01.branch01.example.com<br>Idress: 10.1.10.31 | Date: Jul 18, 2017<br>Time: 8:59 PM (CDT) | User: <b>admin</b><br>Role: Administrator |               |                |    |
|------------|---|---|---|---------------|----------------|----|
|            | ONLINE (ACTIVE) Standalone                                |   |   |               |                |    |
| Ma         | ain Help About  | Local Traffic » iRule                     | es : iRule List                           |               |                |    |
| <b>1</b>   | Statistics  | 🔅 👻 iRule List                            | Data Group List                           | iFile List    | Statistics 🏼 🄊 |    |
| i 💭        | Apps  | *   |   | Search        |                |    |
| <b>(</b> ) | DNS   | ✓ ▲ Name                                  | -   | Verification  |                | ÷  |
|            | Delivery .  | Listeners                                 | Listener List                             | F5 Verified   |                | f5 |
|            | GSLB  | Profiles                                  | Statistics                                | F5 Verified   |                | f5 |
|            | 70000   | Load Palansing                            | soupport_neiper                           | F5 Verified   |                | f5 |
|            | Zones   | Load Balancing                            | Support_main                              | E F5 Verified |                | f5 |
|            | Caches  | iRulés                                    | SAML_BasicAuth                            | F5 Verified   |                | f5 |
|            | Settings  | Translation                               | c   | F5 Verified   |                | f5 |
| S          | COL Orab a starter  | Nameservers                               | ▶ te                                      | F5 Verified   |                | f5 |
|            | SSL Orchestrator  | Keys                                      | •   | E5 Verified   |                | f5 |
|            | Local Traffic   | sys_auth_radius                           |   | F5 Verified   |                | f5 |
|            | hosplaration  | sys_auth_ssl_cc                           | _ldap                                     | F5 Verified   |                | f5 |
| ••••       | Acceleration  | sys_auth_ssl_crl                          | ldp                                       | E F5 Verified |                | f5 |
|            | Device Management   | sys_auth_ssl_oc                           | sp  | F5 Verified   |                | f5 |
|            | 7   | sys_auth_tacacs                           | •   | F5 Verified   |                | f5 |
|            | Vetwork   |   |   |               |                |    |

Navigate to the listener DC01\_udp\_virtual

| DNS » Delivery : Listeners : Listener List |                                 |            |                    |
|--|---------------------------------|------------|--------------------|
| tistener List Statistics                   |                                 |            |                    |
|  |                                 |            |                    |
| * Search                                   |                                 |            | Create             |
| ✓   ♦ State   ♦ Name                       | <ul> <li>Destination</li> </ul> | + Protocol | + Partition / Path |
| Enabled DC01_tcp_virtual                   | 10.1.70.200                     | TCP        | Common             |
| Enabled DC01_udp_virtual                   | 10.1.70.200                     | UDP        | Common             |
| Enabled DC62_tep_virtual                   | 10.1.70.210                     | TCP        | Common             |
| Enabled DC02_udp_virtual                   | 10.1.70.210                     | UDP        | Common             |
| Enable Disable Delete                      |                                 |            |                    |

Navigate to iRules section

| DNS » Delivery : Listeners : Listener List » Properties : DC01_udp_virtual |  |  |  |  |
|--|--|--|--|--|
| 🔅 🚽 Properties Load B  | Balancing Rules Itatistics 💌                       |  |  |  |
|  |  |  |  |  |
| General  |  |  |  |  |
| Name   | DC01_udp_virtual                                   |  |  |  |
| Partition  | Common   |  |  |  |
| Description  |  |  |  |  |
| State  |  |  |  |  |
| Listener: Advanced   |  |  |  |  |
| Destination  | Type:      Host O Network     Address: 10.1.70.200 |  |  |  |
| Service Port   | DNS 53   |  |  |  |
| VLAN Traffic   | Enabled on V                                       |  |  |  |
| VLANs and Tunnels  | Selected     Available       //Common     <        |  |  |  |
| Source Address Translation   | None   |  |  |  |
| Address Translation  | Enabled  |  |  |  |
| Port Translation   | Enabled  |  |  |  |
| Route Advertisement  | Enabled  |  |  |  |

# Navigate to Manage

| DNS » Delivery : Listeners : Listener List » iRules : DC01_udp_virtual |                  |                |        |            |  |        |
|--|------------------|----------------|--------|------------|--|--------|
| <b>#</b> -   | Properties       | Load Balancing | iRules | Statistics |  |        |
|  |                  |                |        |            |  |        |
| Statistic  | cs               |                |        |            |  |        |
| Statist  | ics Profile      | None           | ~      |            |  |        |
| Update   | e                |                |        |            |  |        |
|  | _                |                |        |            |  |        |
| iRules   |                  |                |        |            |  | Manage |
| Name   |                  |                |        |            |  |        |
| No rec   | ords to display. |                |        |            |  |        |
|  |                  |                |        |            |  |        |

https://router01.branch01.example.com/tmui/Control/form?\_\_handler=/tmui/dns/listener/irules&\_\_source=Manage...&\_\_lin Highlight DNS-query-filtering iRule and move it to Selected column

| DNS » Delivery : Listeners : Listener List » Properties : DC01_udp_virtual |             |           |        |  |  |   |
|--|-------------|-----------|--------|--|--|---|
| 🔅 👻 Prope  | erties Load | Balancing | iRules | Statistics   |  |   |
| iRule Management<br>iRules<br>Update                                       |             | Select    | ed //  | Common<br>DNS-query-filtering<br>sys_APM_Excha<br>_sys_APM_Excha | Available<br>ngeSupport_OA_BasicAuth<br>ngeSupport_OA_NtimAuth | Ŷ |
|  |             | Up D      | bown   | _sys_APM_Excha   | ngeSupport_helper  |   |

TMSH commands for router01.branch01

### TMSH

tmsh modify gtm listener all rules { DNS-query-filtering }

#### 2.2.7.3 Results

From the CLI on the router01.branch01 BIGIP run

tail -f /var/log/ltm

From the Workstation command prompt run "dig example.com" and check for the results

#### **Reference Architecture Documentation**

| Command Prompt   |          |         |          |                              |                    |  |
|--|----------|---------|----------|------------------------------|--------------------|--|
| ; <<>> DiG 9.3.2 <<>> example.com<br>; global options: printcmd<br>;; global options: printcmd<br>;; Got answer:<br>;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 116<br>;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1   |          |         |          |                              |                    |  |
| ;; QUESTION SECTION:<br>;example.com.  |          | IN      | A        |                              |                    |  |
| ;; ANSWER SECTION:<br>example.com.   | 600      | IN      | A        | 10.1.70.200                  |                    |  |
| ;; AUTHORITY SECTION:<br>example.com.  | 3600     | IN      | NS       | dc01.example.com.            |                    |  |
| ;; ADDITIONAL SECTION:<br>dc01.example.com.  | 3600     | IN      | A        | 10.1.70.200                  |                    |  |
| ;; Query time: 31 msec<br>;; SERVER: 10.1.70.200#53<10.1.70.200><br>;; WHEN: Tue Jul 18 22:06:35 2017<br>;; MSG SIZE rcvd: 80  |          |         |          |                              |                    |  |
| C:\Users\user.EXAMPLE>   |          |         |          |                              |                    |  |
| Jul 18 22:06:35 router01 info tmm[11519]: 2017-07-18 22:06:34 router01.branch01.example.com<br>qid 116 from 10.1.71.100#49954: view none: query: example.com IN A + (10.1.70.200%0)<br>Jul 18 22:06:35 router01 info tmm3[11519]: Rule /Common/DNS-guery-filtering <dns_request>: C<br/>ategory /Common/Information_Technology matching example.com is not filtered<br/>Jul 18 22:06:35 router01 info tmm11519]: 2017 87-10 22:06:34 router01.branch01.example.com</dns_request> |          |         |          |                              |                    |  |
| qid 116 to 10.1.71.100#  | 49954: [ | NOERROR | qr,aa,rd | l] response: example.com. 60 | O IN A 10.1.70.200 |  |
|  |          |         |          |                              |                    |  |
| Update   | Delete   |         |          |                              |                    |  |

From the Workstation command prompt run "dig porno.com" and check for the results



Navigate to: DNS >> Delivery : iRules : iRules List

| Hostname: router01.branch01.example.com<br>IP Address: 10.1.10.31 | Date: Jul 18, 2017<br>Time: 8:30 PM (CDT) | User: <b>admin</b><br>Role: Administrator |              |
|---|---|---|--------------|
| ONLINE (ACTIVE) Standalone  |   |   |              |
| Main Help About   | DNS » Delivery : iRules                   | s : iRule List                            |              |
| Mage Statistics   | 🚓 👻 iRule List                            | Data Group List iFile List                | Statistics 🔎 |
| iApps   | þ   | × Search                                  |              |
| S DNS   | Name                                      | Verification                              | \$           |
| Delivery >>   | Listeners >                               | g None                                    |              |
| GSLB  | Profiles >                                | eSupport_OA_BasicAuth 🖭 F5 Verified       | d f5-        |
| Zones   | Load Balancing                            | eSupport_OA_NtImAuth 🖭 F5 Verifie         | d f5-        |
| Caches  | iRules >>                                 | Rule List                                 | d f5-        |
| Sattings  | Translation                               | F5 Verifier                               | d f5-        |
| Setungs   |   | F5 Verifie                                | d f5-        |
| SSI Orchestrator  | Nameservers                               | F5 Verifie                                | d 15-        |
|   | Keys                                      | Statistics B5 Verifie                     | d 15-        |
| Local Traffic   | sys_auth_Idap                             | 🗐 F5 Verifie                              | 1 f5-        |
| Acceleration  | sys_auth_radius                           | E F5 Verifie                              | d f5-        |
| - Acceletation  | Sys_auth_ssl_cc_ld                        | ap 📃 F5 Verifie                           | d f5-        |
| Device Management   | sys_auth_ssl_cridp                        | E F5 Verifie                              | d f5-        |
|   | sys_auth_ssl_ocsp                         | 🖭 F5 Verifie                              | d f5-        |
| MEIWOIK   |   |   |              |

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/rule/list.jsp

Click on the DNS-query-filtering iRule and add new filtering category "News\_and\_Media"

| DNS » Delivery : iRules : iRule List » Properties : DNS-query-filtering |   |  |  |  |  |  |
|---|---|--|--|--|--|--|
| to -<br>Properties  | Statistics 🗾  |  |  |  |  |  |
|   |   |  |  |  |  |  |
| Properties  |   |  |  |  |  |  |
| Name  | DNS-query-filtering   |  |  |  |  |  |
| Partition / Path  | Common  |  |  |  |  |  |
| Definition  | <pre>1 * When RULE_INIT { 2     # Set categories to block for DNS hosts 3 * set static::blocked_categories { 4     /Common/Bot_Networks 5     /Common/Spyware 6     /Common/Adult_Content 8     /Common/Adult_Content 8     /Common/News_and_Media 9 11 12 13     # CONFIGURATION 14     # Check all requests by default 15     set static::request_check 1 16     # If the category returns as blocked, return NXDOMAIN (1) 17     # Otherwise if (0), return a statically defined IP address 18     set static::request_return_nxdomain 0 19     set static::request_return_invdomain 0 19     set static::request_debug 1 22  } 23 24 25 * when DNS_REQUEST { 26 *     if { \$static::request check } { 27 28 29 29 20 20 20 20 20 20 20 20 20 20 20 20 20</pre> |  |  |  |  |  |
| Ignore Signature/Checksum   |   |  |  |  |  |  |

From the Workstation command prompt run "dig cnn.com" and check for the results



# 2.2.8 Title

Here's some stuff.











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.