

---

# **DNS Documentation**

**F5 Networks, Inc.**

**Jun 03, 2020**



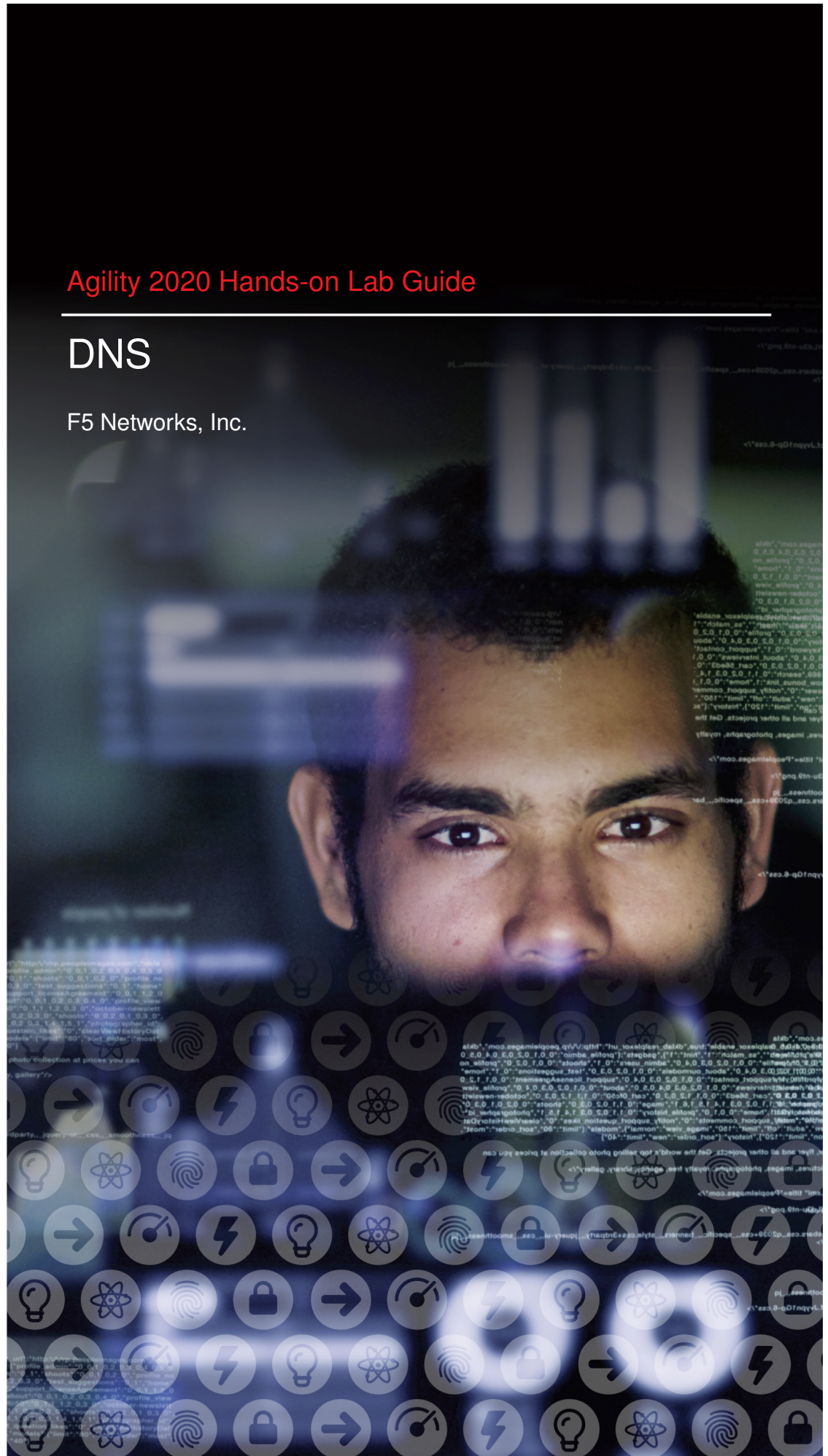




## Agility 2020 Hands-on Lab Guide

# DNS

F5 Networks, Inc.



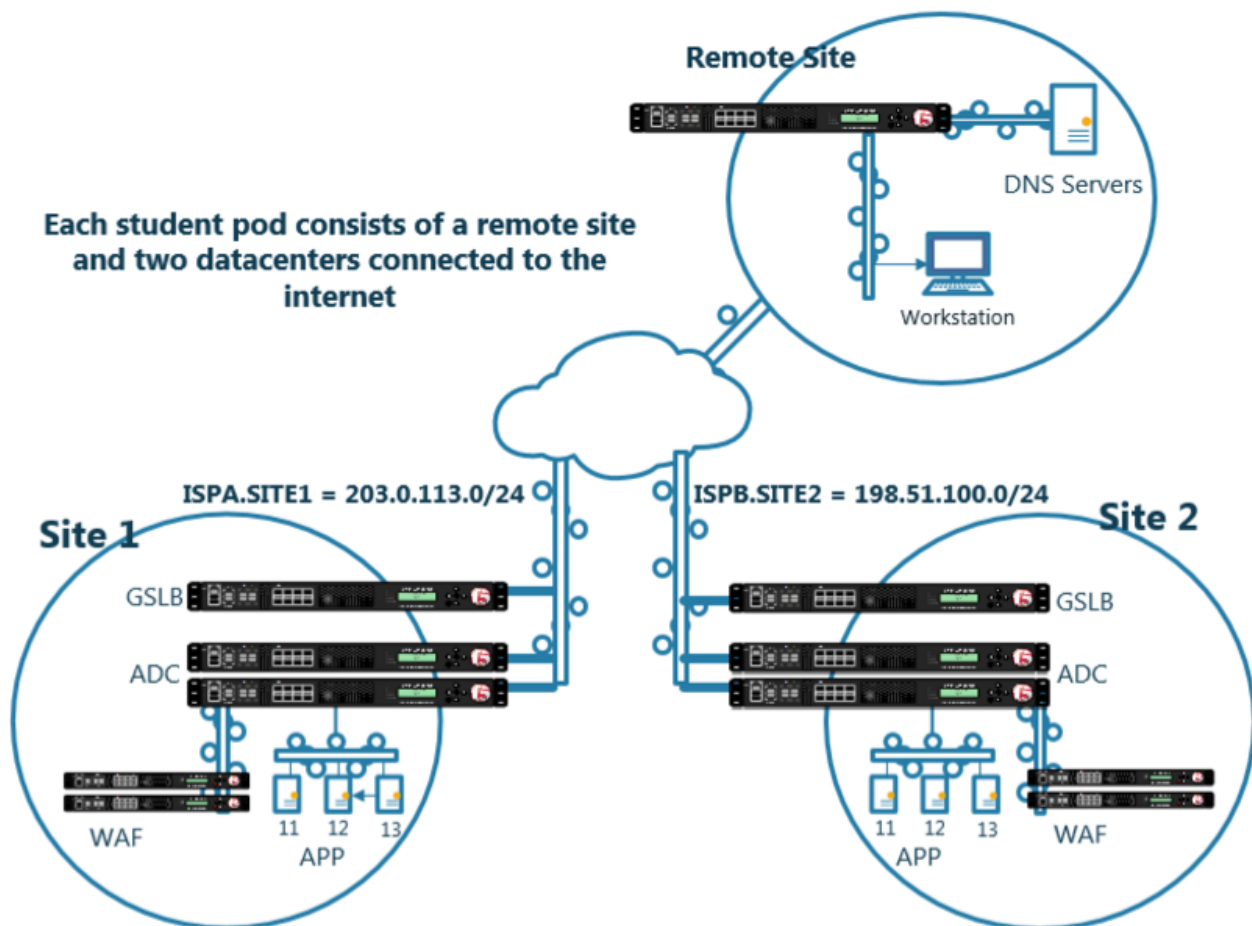


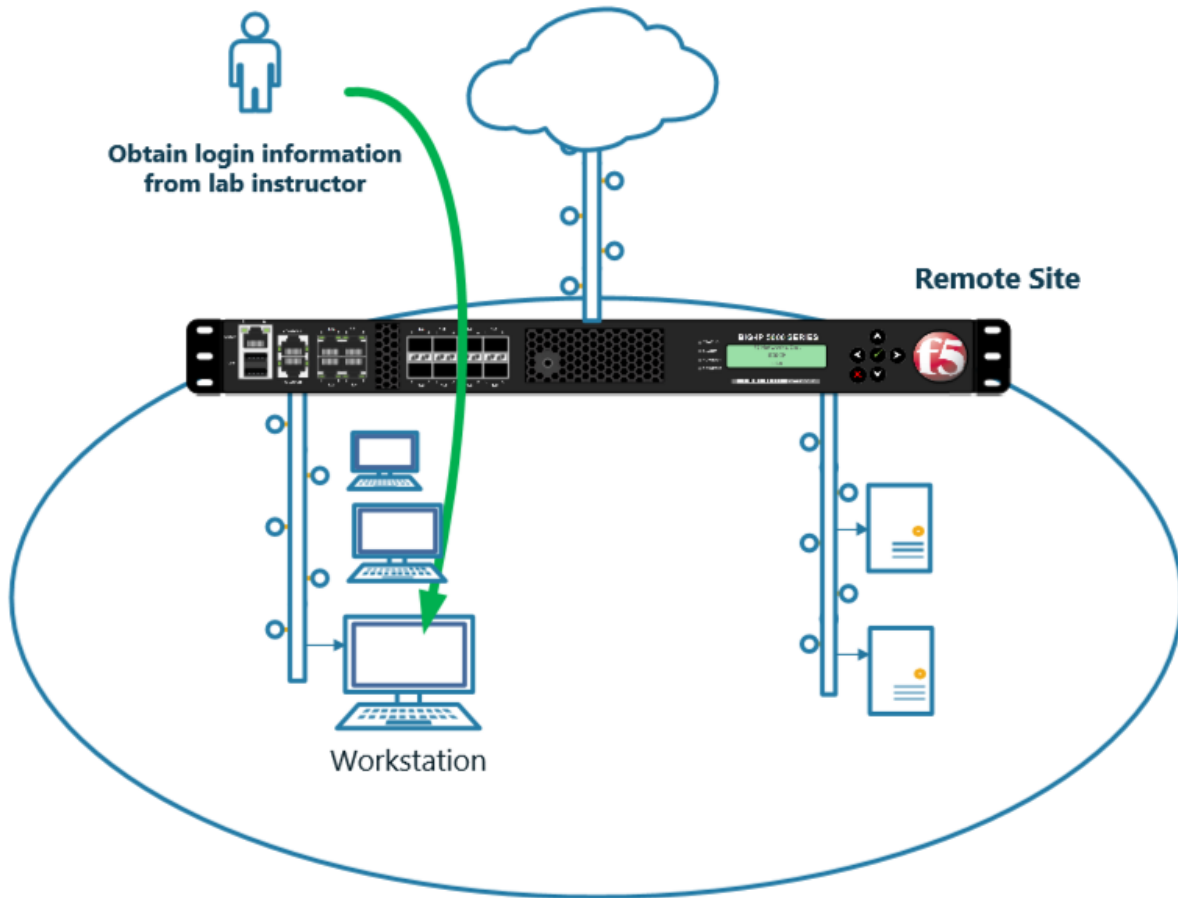
## Contents:

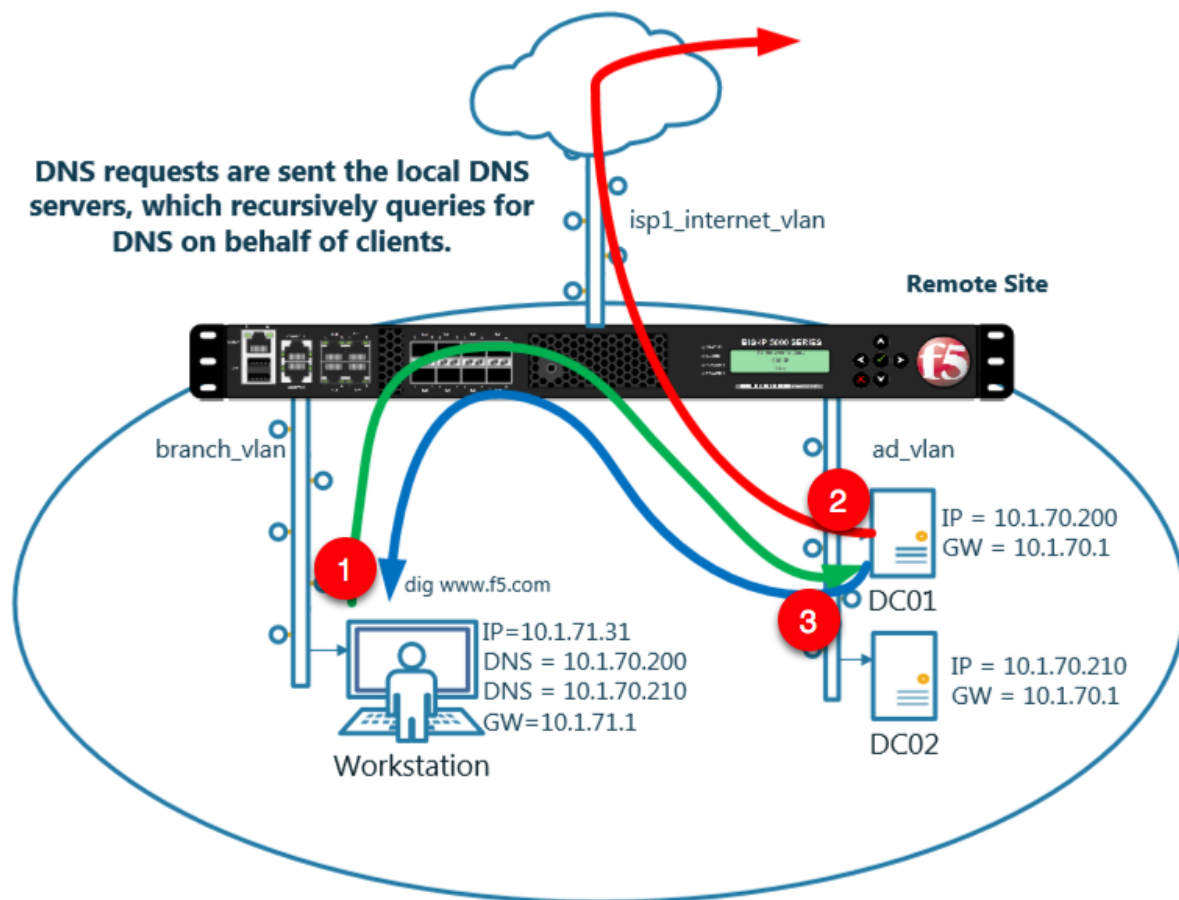
<b>1</b>	<b>Lab Environment</b>	<b>5</b>
<b>2</b>	<b>Class 1 - Intro to GSLB</b>	<b>11</b>
<b>3</b>	<b>Class 2 - Next Generation DNS Services</b>	<b>83</b>
<b>4</b>	<b>Class 3 - Data Center Availability Services Using BIG-IP DNS</b>	<b>143</b>
<b>5</b>	<b>Class 4 - EDNS0 client subnet</b>	<b>235</b>
<b>6</b>	<b>Class 5 - DNS over HTTPS/DNS over TLS</b>	<b>255</b>
<b>7</b>	<b>LAB: F5 DNS Cloud Service &amp; F5 DNS Load Balancer Cloud Service</b>	<b>289</b>
<b>8</b>	<b>Credits</b>	<b>359</b>

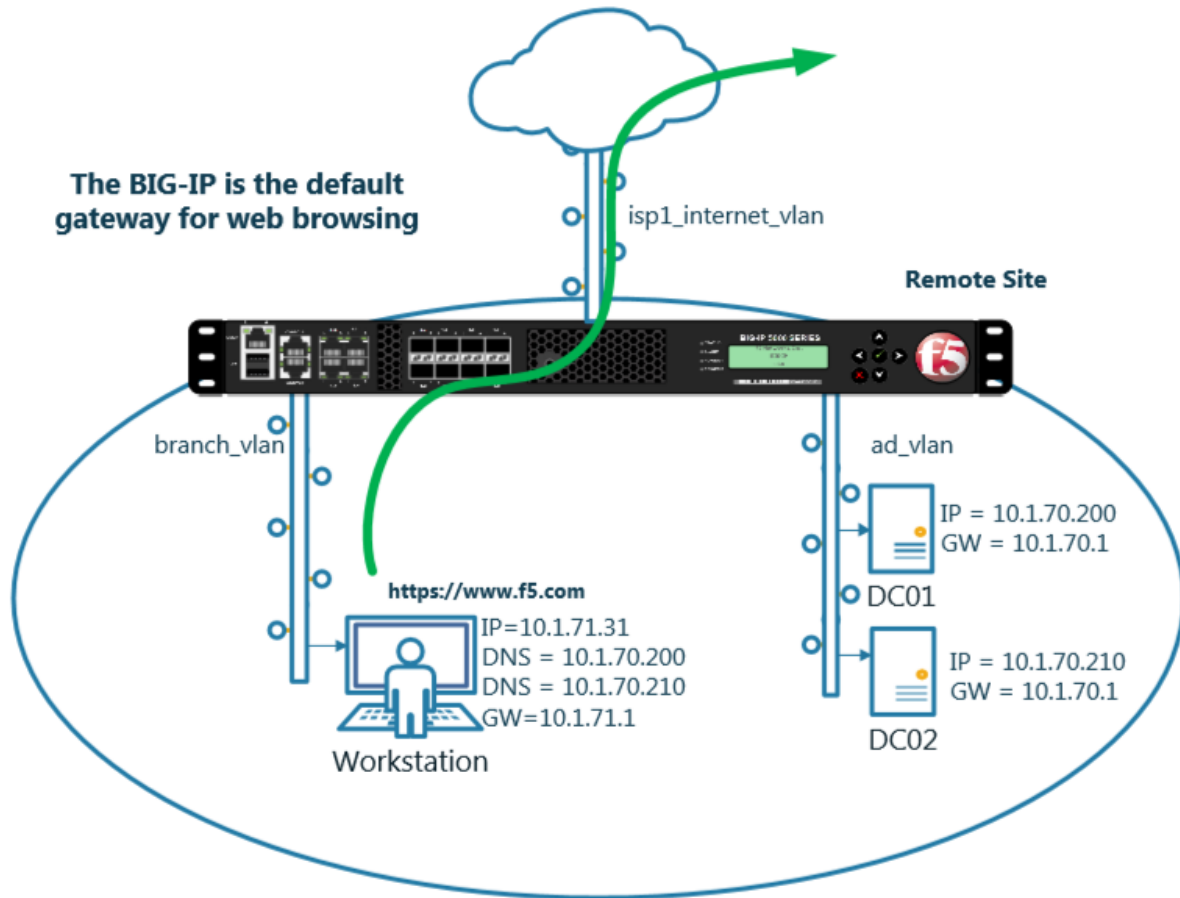


## Lab Environment

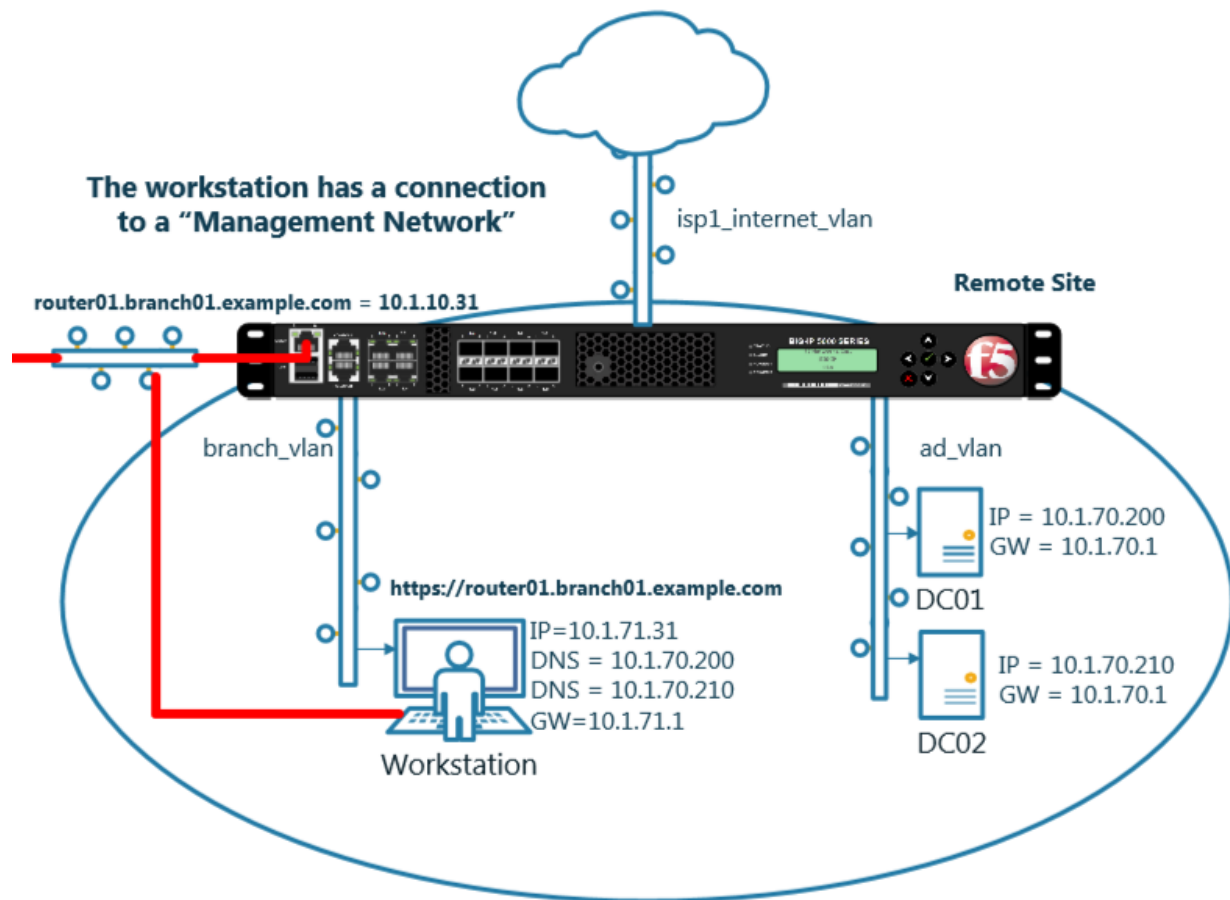


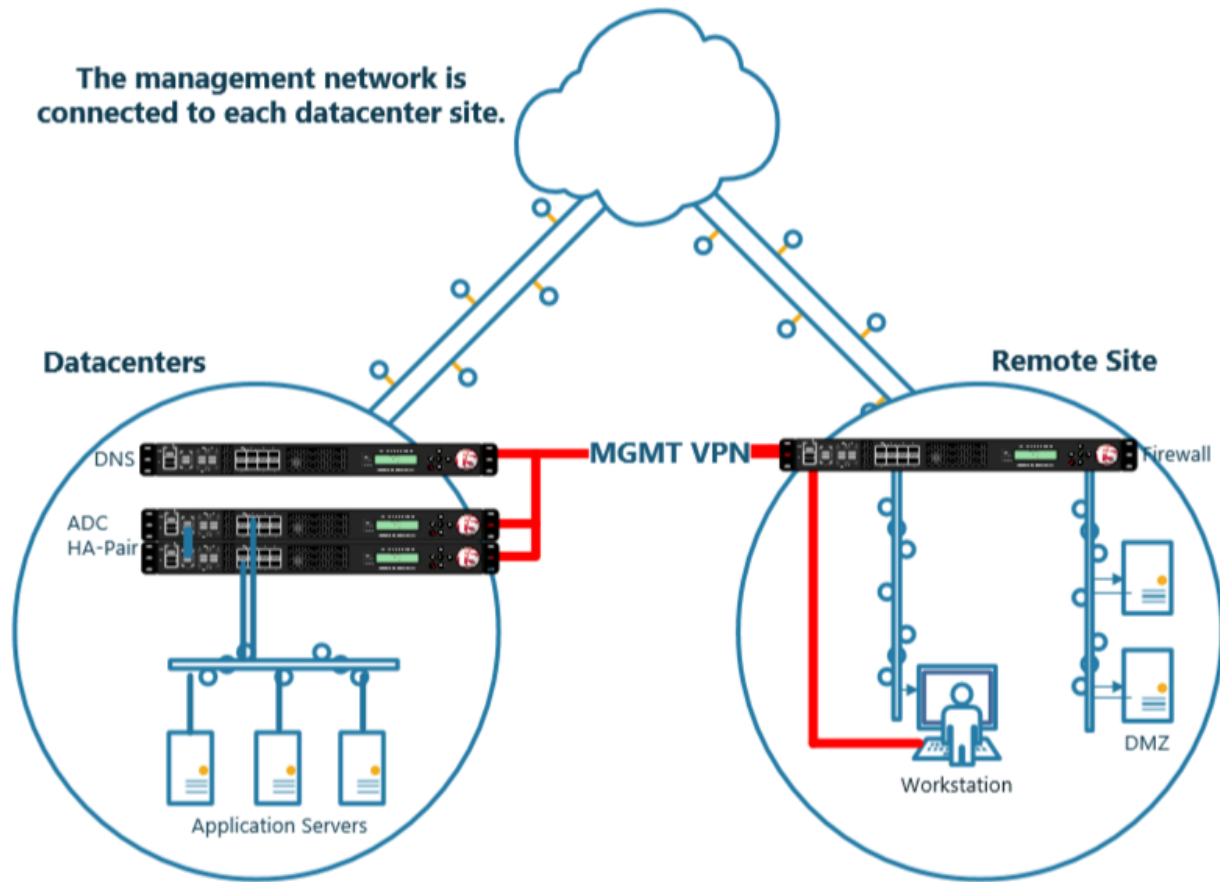








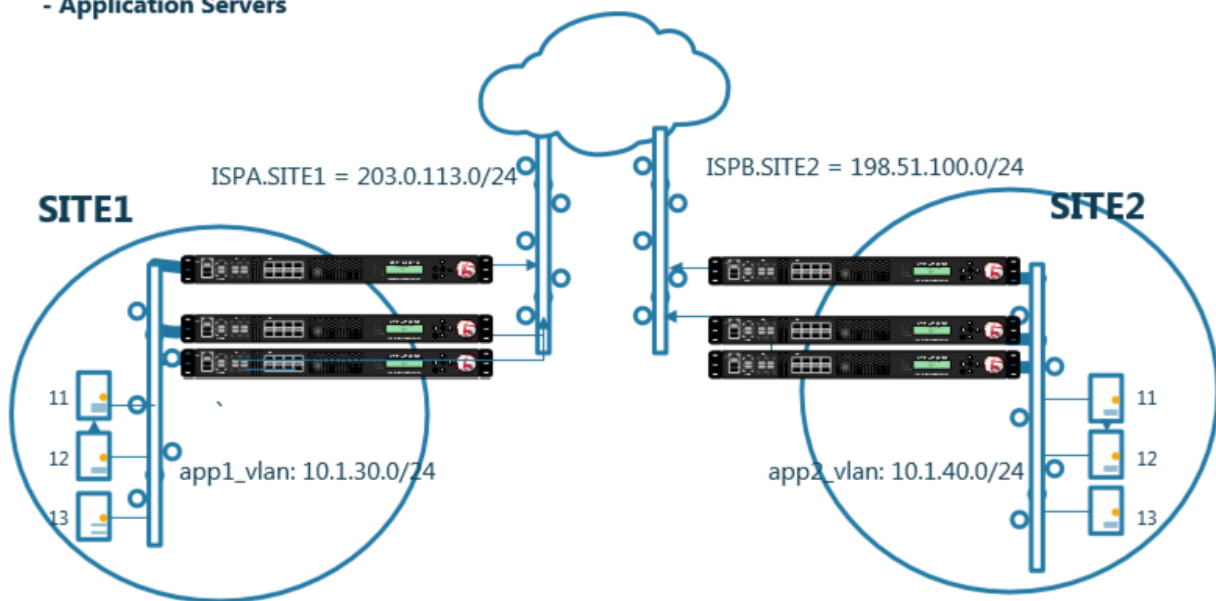




## Class 1 - Intro to GSLB

**EXAMPLE INC. occupies two datacenters. Each datacenter is identically configured with:**

- HA pair of F5 ADC
- Standalone F5 DNS
- Application Servers



- Students will configure F5 DNS servers to support GSLB services 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*.

At 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

## 2.1 Settings

A site specific sync group name will be created, and synchronization will be enabled.

Navigate to: **DNS » Settings : GSLB : General**

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

Setting	Value
Synchronize	checked
Group Name	EXAMPLE_group
Synchronize DNS Zone Files	checked

Host Name: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 12:19 PM (CDT) Role: Administrator

ONLINE (ACTIVE)  
Standalone

Main Help About

DNS » Settings : GSLB : General

Statistics iApps DNS Delivery GSLB Zones Caches Settings SSL Orchestrator Acceleration Device Management Network System

Configuration Synchronization

Synchronize	<input checked="" type="checkbox"/>
Group Name	EXAMPLE_group
Time Tolerance	10 seconds
Synchronize DNS Zone Files	<input checked="" type="checkbox"/>

Configuration Save

Delivery	<input checked="" type="checkbox"/> Enabled
GSLB	General
Zones	Load Balancing
Caches	Metrics Collection

Auto-Discover ☒ Enabled

Request Interval 30 seconds

Monitoring

Heartbeat Interval	10 seconds
--------------------	------------

[https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/settings/gslb/properties\\_general.jsp](https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/settings/gslb/properties_general.jsp)

```
tmsh modify gtm global-settings general synchronization yes synchronization-group-name EXAM-
PLE_group synchronize-zone-files yes
```

<https://support.f5.com/csp/article/K13734>

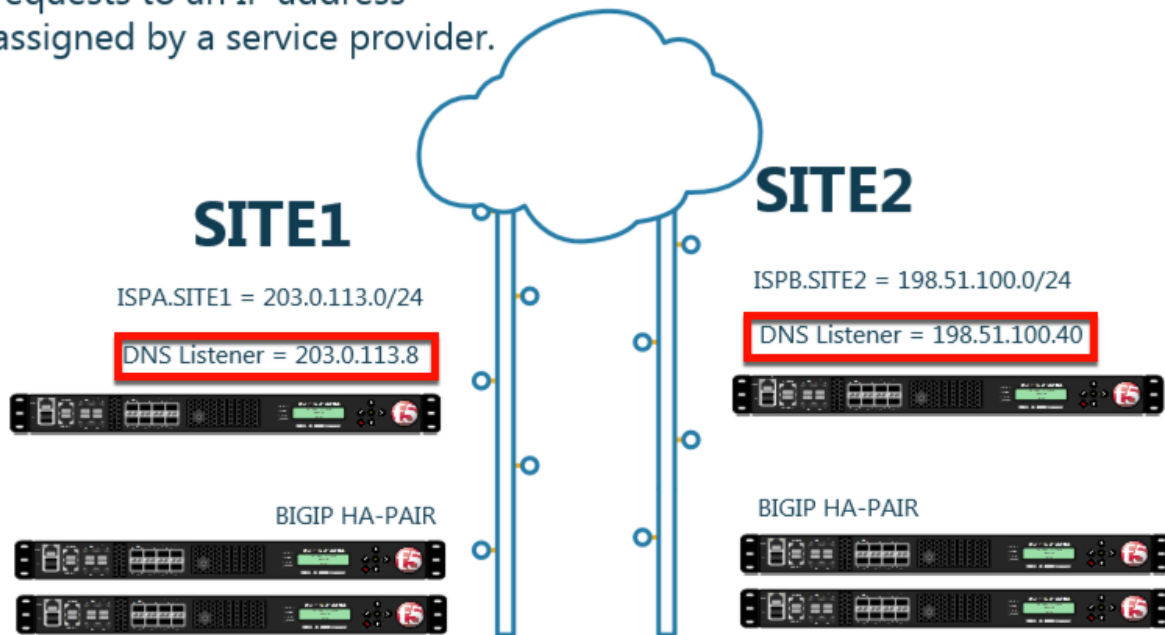
<https://support.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-implementations-12-0-0/4.html>

## 2.2 Listeners

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

We will be creating both TCP and UDP based listeners.

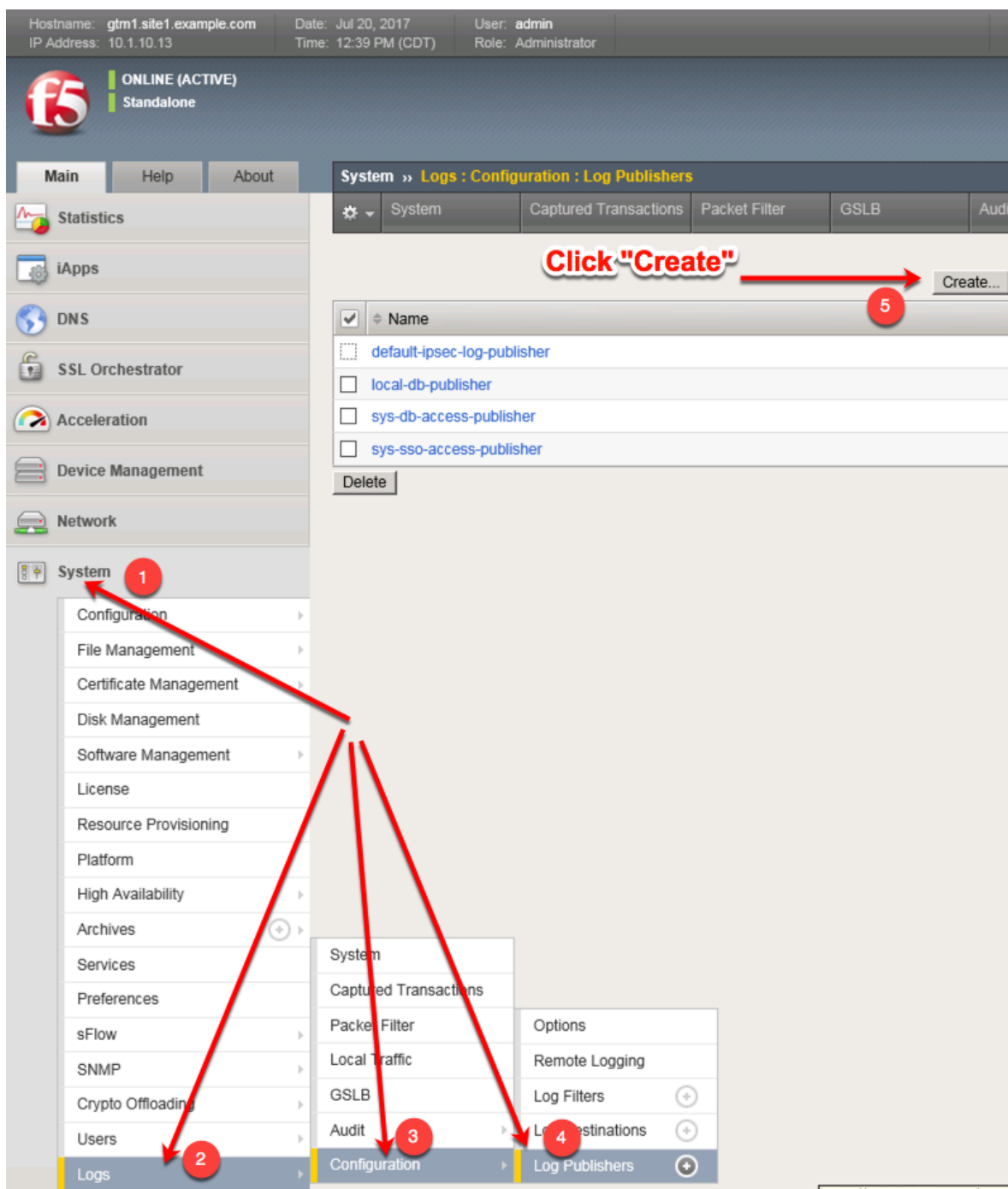
A listener will receive DNS requests to an IP address assigned by a service provider.



### 2.2.1 Logging

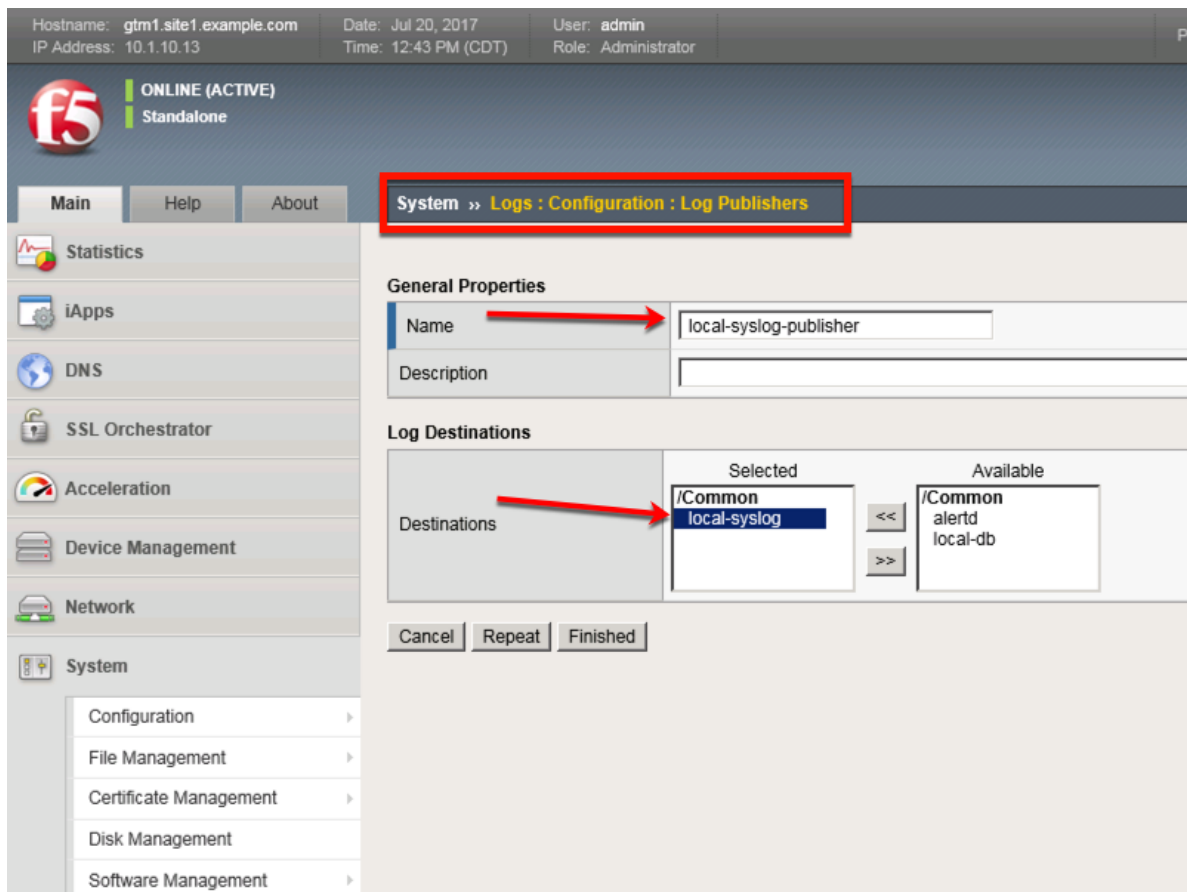
Configure DNS query and response logging. Create a “Log Publisher”, and a “Logging Profile”

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

1. Navigate to: **System » Logs : Configuration : Log Publishers**

Create a local syslog publisher according to the table below:

Setting	Value
Name	local-syslog-publisher
Destinations	local-syslog



[https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/system/log/create\\_publisher.jsp](https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/system/log/create_publisher.jsp)

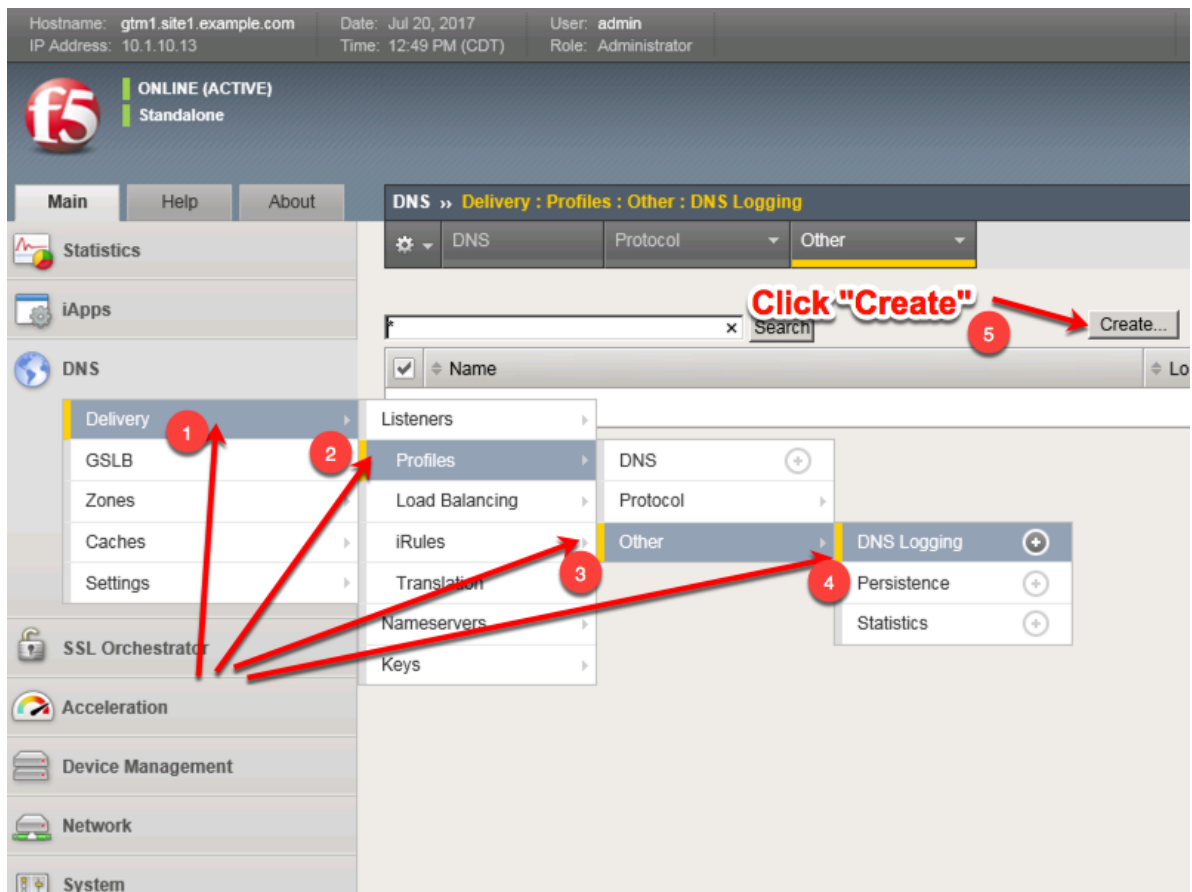
[https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/system/log/create\\_publisher.jsp](https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/system/log/create_publisher.jsp)

On both gtm1.site1 and gtm1.site run the following command:

### TMSH

```
tmsl create sys log-config publisher local-syslog-publisher { destinations { local-syslog { } } }
```

2. Navigate to: **DNS > Delivery > Profiles > Other > DNS Logging: Create**



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

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



Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 12:52 PM (CDT) Role: Administrator

ONLINE (ACTIVE)  
Standalone

Main Help About

DNS >> Delivery : Profiles : Other : DNS Logging >> New...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name example\_dns\_logging\_profile  
Description

**Configuration**

Log Publisher local-syslog-publisher  
Log Queries ☒ Enabled  
Log Responses ☒ Enabled

**Log Fields**

Include Complete Answer ☒ Enabled  
Include Query ID ☒ Enabled  
Include Source ☒ Enabled  
Include Timestamp ☒ Enabled  
Include View ☒ Enabled

Cancel Repeat Finished

[https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/profile/dns\\_log/create.jsp](https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/profile/dns_log/create.jsp)

[https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/dns/profile/dns\\_log/create.jsp](https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/dns/profile/dns_log/create.jsp)

**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
```

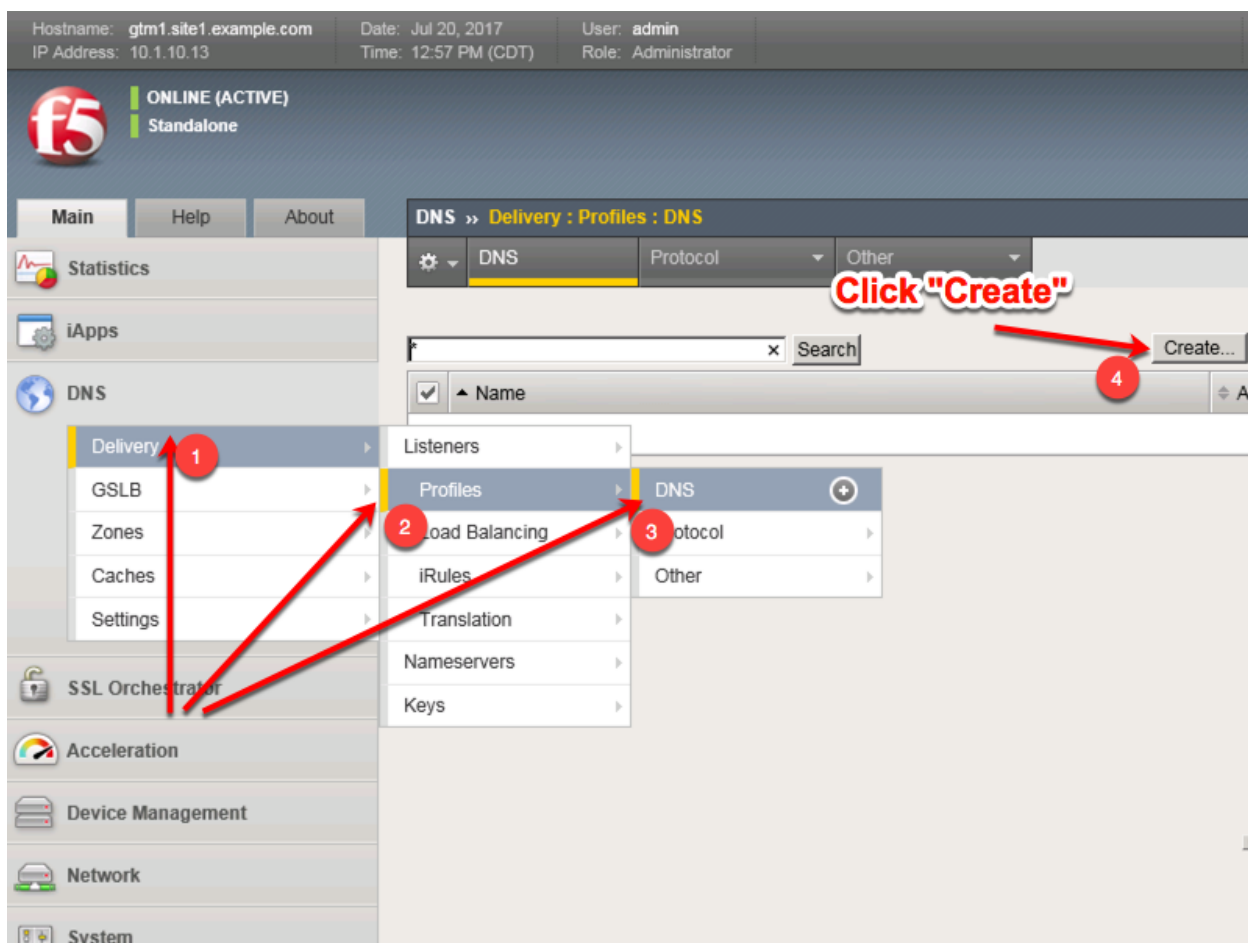
[https://support.f5.com/kb/en-us/products/big-ip\\_ltm/manuals/product/bigip-external-monitoring-implementations-12-0-0/5.html](https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-12-0-0/5.html)

## 2.2.2 DNS Profile

A DNS profile controls the way a listener processes a query.

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

Navigate to: **DNS > Delivery > Profiles > DNS: Create**



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

Setting	Value
Name	example.com_dns_profile
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

**General Properties**

Name	example.com_dns_profile
Partition / Path	Common
Parent Profile	dns

**Denial of Service Protection** Custom ☐

Rapid Response Mode	Disabled	<input type="checkbox"/>
Rapid Response Last Action	Drop	<input type="checkbox"/>

**Hardware Acceleration**

Protocol Validation	Disabled	<input type="checkbox"/>
Response Cache	Disabled	<input type="checkbox"/>

**DNS Features**

DNSSEC	Disabled	<input checked="" type="checkbox"/>
GSLB	Enabled	<input type="checkbox"/>
DNS Express	Disabled	<input checked="" type="checkbox"/>
DNS Cache	Disabled	<input type="checkbox"/>
DNS Cache Name	Select...	<input type="checkbox"/>
DNS IPv6 to IPv4	Disabled	<input type="checkbox"/>
Unhandled Query Actions	Drop	<input checked="" type="checkbox"/>
Use BIND Server on BIG-IP	Disabled	<input checked="" type="checkbox"/>

**DNS Traffic**

Zone Transfer	Disabled	<input type="checkbox"/>
DNS Security	Disabled	<input type="checkbox"/>
DNS Security Profile Name	Select...	<input type="checkbox"/>
Process Recursion Desired	Enabled	<input type="checkbox"/>

**Logging and Reporting**

Logging	Enabled	<input checked="" type="checkbox"/>
Logging Profile	example_dns_logging_profile	<input checked="" type="checkbox"/>
AVR Statistics Sample Rate	<input checked="" type="checkbox"/> Enabled 1/ 1 queries sampled	<input checked="" type="checkbox"/>

<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/profile/dns/create.jsp>

<https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/dns/profile/dns/create.jsp>

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

## TMSH

```
tms create ltm profile dns example.com_dns_profile use-local-bind no unhandled-query-action drop log-profile example_dns_logging_profile enable-logging yes avr-dnsstat-sample-rate 1
```

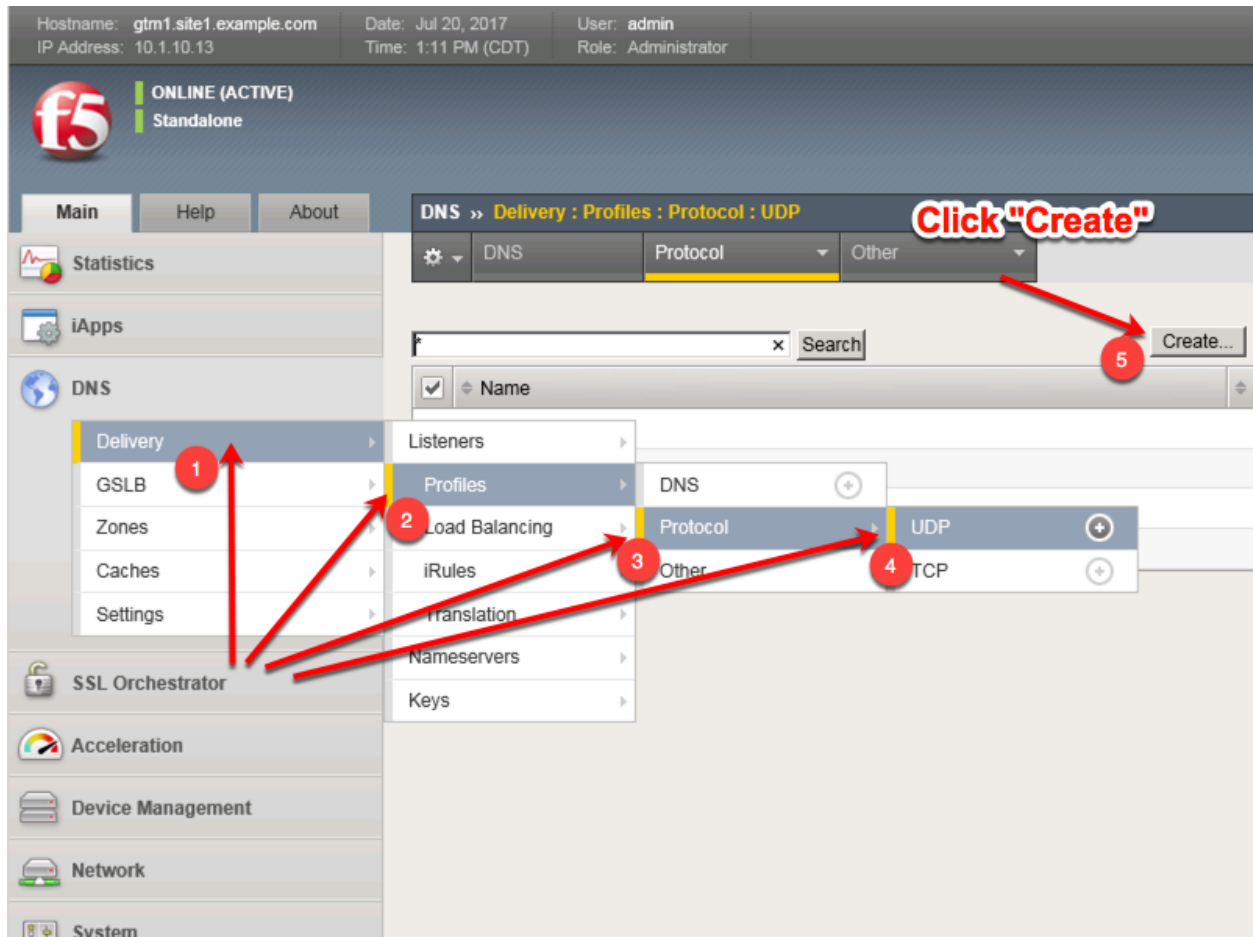
<https://support.f5.com/csp/article/K14510>

## 2.2.3 UDP Profile

A UDP profile is associated with a listener.

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

Navigate to: **DNS » Delivery : Profiles : Protocol : UDP**



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

Setting	Value
Name	example.com_udp-dns_profile
Parent Profile	udp_gtm_dns

Hostname: gtm1.site1.example.com Date: Jul 26, 2018 User: admin  
IP Address: 10.1.10.13 Time: 8:17 AM (EDT) Role: Administrator Partition: Common Log out

**f5** ONLINE (ACTIVE) Standalone

Main Help About

**DNS » Delivery : Profiles : Protocol : UDP » New UDP Profile...**

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name   
Parent Profile

**Settings** Custom ☐

Proxy Maximum Segment	<input type="checkbox"/>	<input type="checkbox"/>
Idle Timeout	Specify... 5 seconds	<input type="checkbox"/>
IP ToS	Specify... 0	<input type="checkbox"/>
Link QoS	Specify... 0	<input type="checkbox"/>
Datagram LB	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Allow No Payload	<input type="checkbox"/>	<input type="checkbox"/>
TTL Mode	Proxy	<input type="checkbox"/>
Don't Fragment Mode	PMTU	<input type="checkbox"/>
Max Buffer Bytes	655350	<input type="checkbox"/>
Max Buffer Packets	0	<input type="checkbox"/>

<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/profile/udp/create.jsp>

<https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/dns/profile/udp/create.jsp>

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

## TMSH

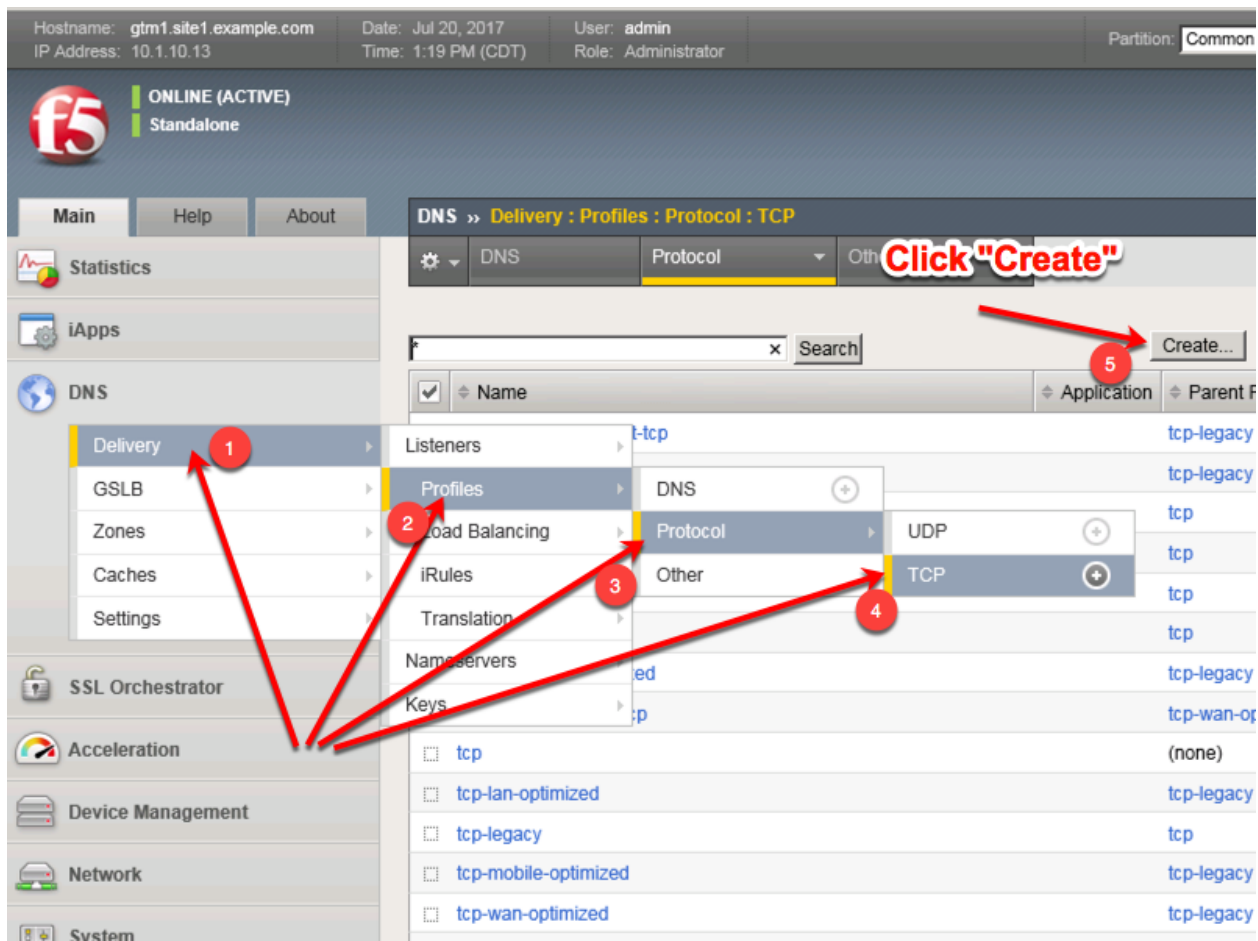
tmsh create ltm profile udp example.com\_udp-dns\_profile defaults-from udp\_gtm\_dns

## 2.2.4 TCP Profile

A TCP profile is associated with a listener.

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

Navigate to: **DNS » Delivery : Profiles : Protocol : TCP**



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

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

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 1:23 PM (CDT) Role: Administrator Partition: Common

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About **DNS » Delivery : Profiles : Protocol : TCP » New TCP Profile...**

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name   
Parent Profile

**Timer Management**

Close Wait	<input type="text" value="Specify..."/> 5	seconds
Fin Wait 1	<input type="text" value="Specify..."/> 5	seconds
Fin Wait 2	<input type="text" value="Specify..."/> 300	seconds
Idle Timeout	<input type="text" value="Specify..."/> 300	seconds
Keep Alive Interval	<input type="text" value="Specify..."/> 1800	seconds
Minimum RTO	<input type="text" value="500"/>	milliseconds
Reset On Timeout	<input checked="" type="checkbox"/> Enabled	
Time Wait	<input type="text" value="Specify..."/> 2000	milliseconds
Time Wait Delay	<input checked="" type="checkbox"/> Enabled	
Zero Window Timeout	<input type="text" value="Specify..."/> 20000	milliseconds

**Scroll way down to find the "Finish" button**

<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/profile/tcp/create.jsp>

<https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/dns/profile/tcp/create.jsp>

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

## TMSH

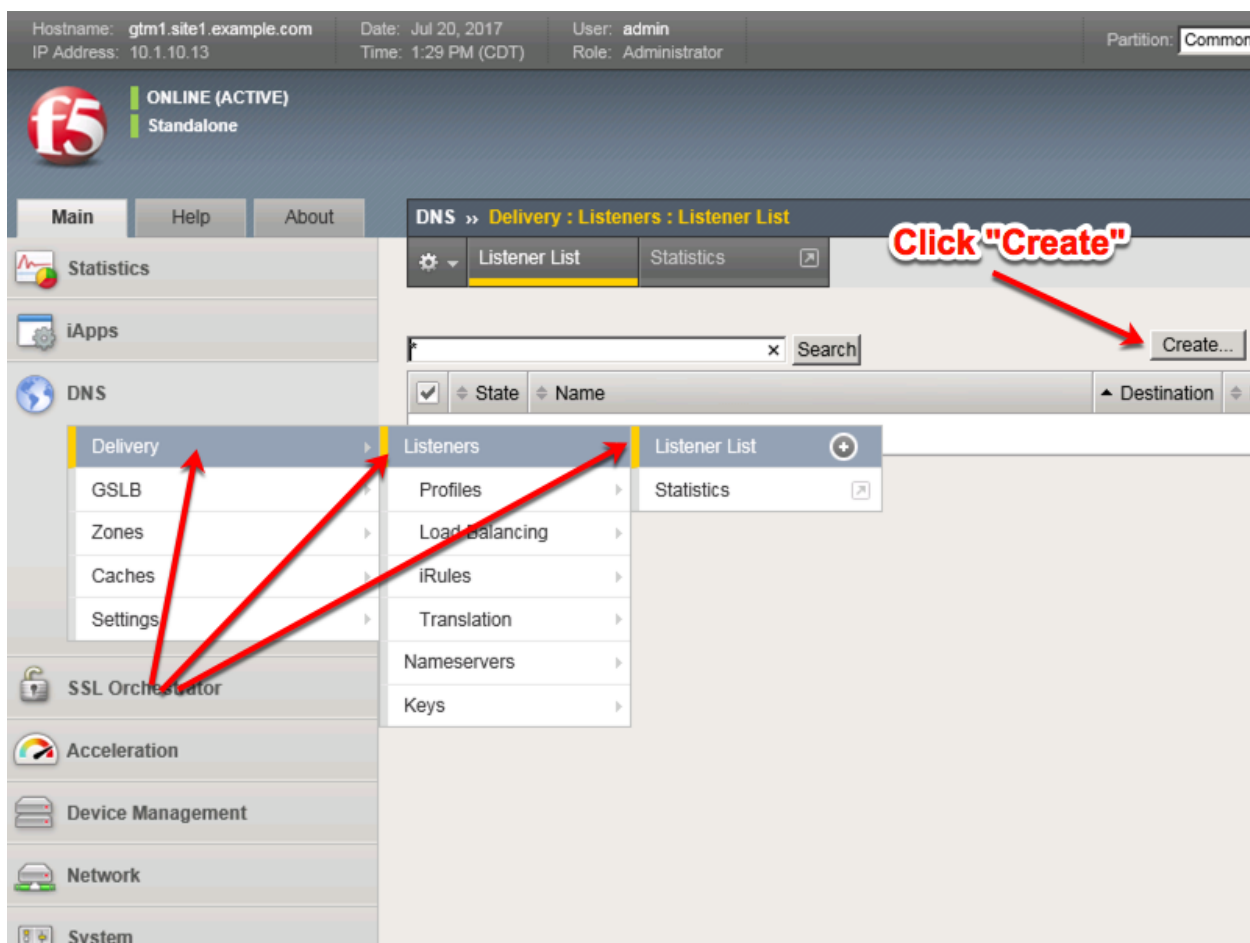
tmsh create ltm profile tcp example.com\_tcp-dns\_profile defaults-from tcp-wan-optimized

## 2.2.5 UDP IP Address

A UDP listener will receive and process DNS queries.

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

Navigate to: **DNS » Delivery : Listeners : Listener List**



Create a UDP listener according to the following table:

Setting	gtm1.site1	gtm1.site2
Name	isp1_site1_ns1.example.com_udp_53_virtual	isp1_site2_ns2.example.com_udp_53_virtual
Destination	203.0.113.8	198.51.100.40
Protocol (Client) Profile	example.com_udp-dns_profile	example.com_udp-dns_profile
DNS Profile	example.com_dns_profile	example.com_dns_profile

<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/listener/create.jsp>

<https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/dns/listener/create.jsp>



Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 1:32 PM (CDT) Role: Administrator Partition: Common

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About **DNS » Delivery : Listeners : Listener List » New...**

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General**

Name: isp1\_site1\_ns1.example.com\_udp\_53  
Description:  
State: Enabled

Listener: Advanced

Destination: Type: ☒ Host ☐ Network  
Address: 203.0.113.8  
Service Port: DNS 53  
VLAN Traffic: All VLANs  
Source Address Translation: None  
Address Translation: ☐ Enabled  
Port Translation: ☐ Enabled  
Route Advertisement: ☐ Enabled  
Auto Last Hop: Default  
Last Hop Pool: None

Service: Advanced

Protocol: UDP  
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 }
```

}

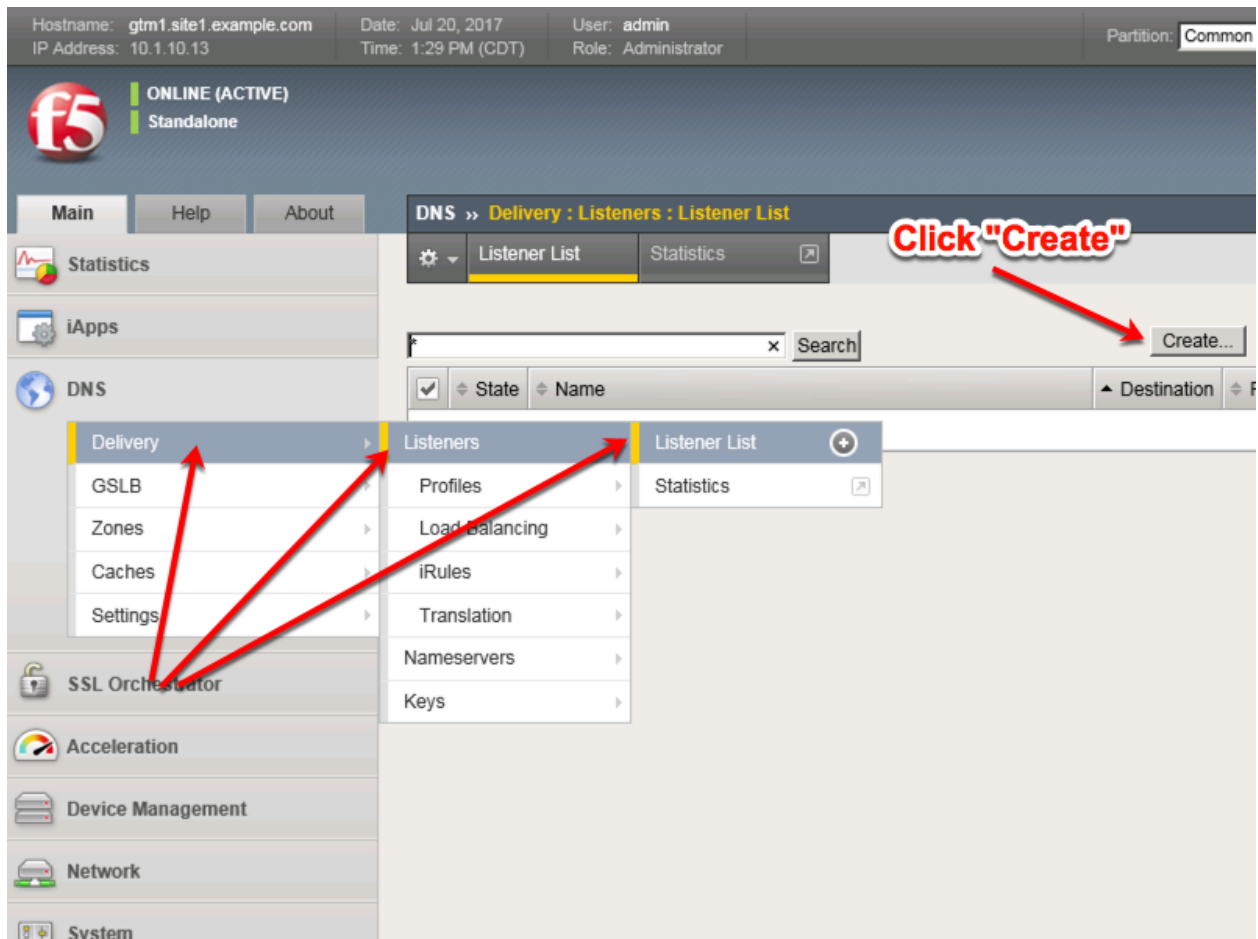
<https://support.f5.com/csp/article/K14923>

## 2.2.6 TCP IP Address

A TCP listener will receive and process DNS queries.

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

Navigate to: **DNS » Delivery : Listeners : Listener List**



Create a TCP listener.

Setting	gtm1.site1	gtm1.site2
Name	isp1_site1_ns1.example.com_tcp_53_virtual	isp1_site2_ns2.example.com_tcp_53_virtual
Destination	203.0.113.8	198.51.100.40
Protocol (Client) Profile	example.com_tcp-dns_profile	example.com_tcp-dns_profile
DNS Profile	example.com_dns_profile	example.com_dns_profile

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 2:18 PM (CDT) Role: Administrator Partition: Common

**f5** ONLINE (ACTIVE) Standalone

Main Help About **DNS » Delivery : Listeners : Listener List » New...**

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General**

Name: isp1\_site1\_ns1.example.com\_udp\_53  
Description:  
State: Enabled

**Listener:** Advanced

Destination: Type: ☒ Host ☐ Network  
Address: 203.0.113.8  
Service Port: DNS 53  
VLAN Traffic: All VLANs  
Source Address Translation: None  
Address Translation: ☐ Enabled  
Port Translation: ☐ Enabled  
Route Advertisement: ☐ Enabled  
Auto Last Hop: Default  
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 select "TCP"**

<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/listener/create.jsp>

<https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/dns/listener/create.jsp>

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

```
tmsl 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 }
```

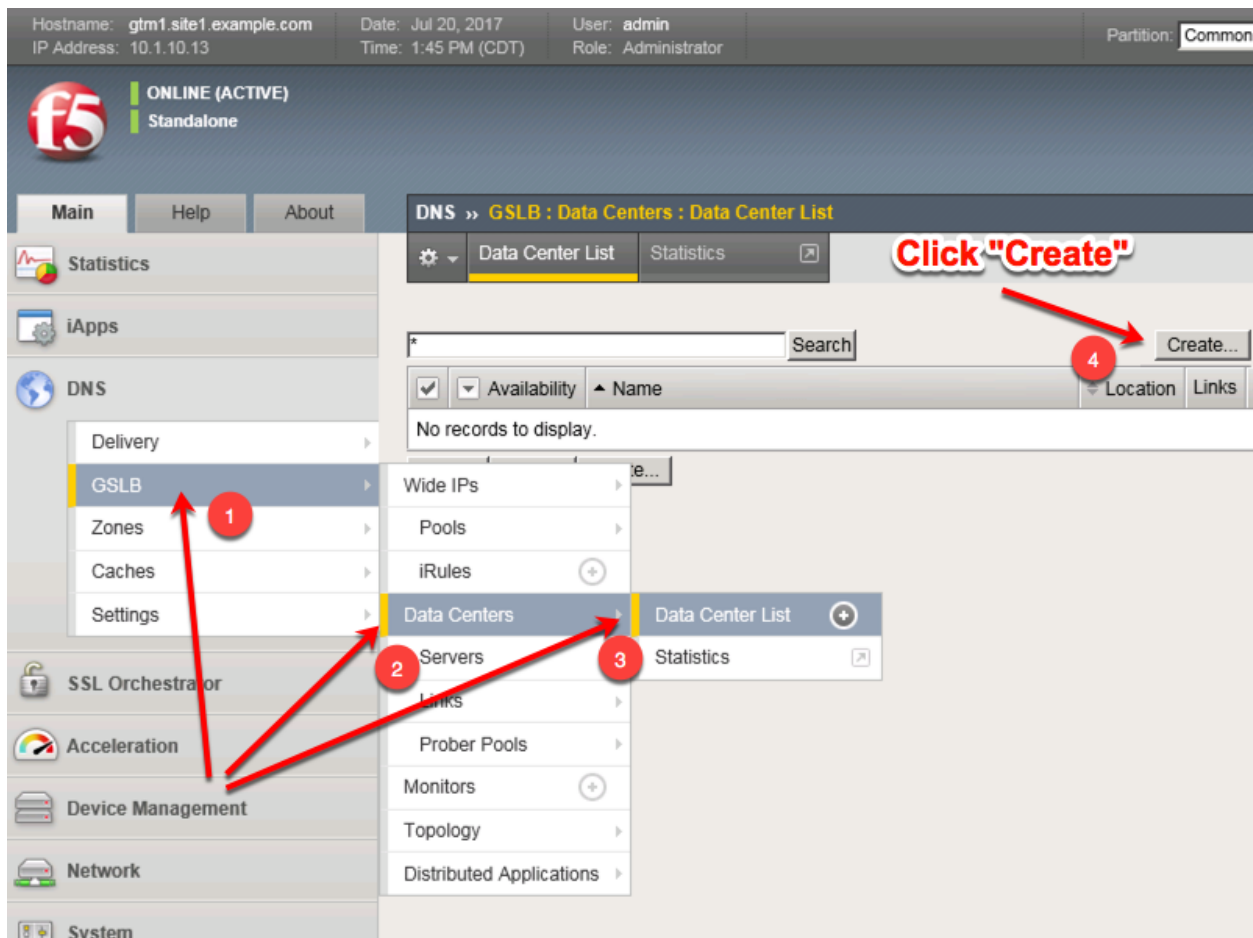
<https://support.f5.com/csp/article/K14923>

## 2.3 Datacenters

Datacenters are logical groupings of devices that share a gateway.

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

Navigate to: **DNS > GSLB > Data Centers > Data Center List: Create**



[https://gtm1.site1.example.com/tmui/Control/jspmap/xsl/gtm\\_dc/list](https://gtm1.site1.example.com/tmui/Control/jspmap/xsl/gtm_dc/list)

Create two data centers according to the table below:

Setting	Value
Name	site1_datacenter
Name	site2_datacenter

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin Partition: Common  
IP Address: 10.1.10.13 Time: 1:48 PM (CDT) Role: Administrator

ONLINE (ACTIVE)  
Standalone

Main Help About DNS » **GSLB : Data Centers : Data Center List**

Statistics iApps DNS Delivery GSLB Zones Caches Settings SSL Orchestrator Acceleration Device Management Network System

**General Properties**

Name	site1_datacenter
Description	
Location	
Contact	
Prober Preference	Inside Data Center
Prober Fallback	Any Available
State	Enabled

Cancel Repeat Finished

**Repeat this step to create "site2\_datacenter"**

[https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/data\\_center/create.jsp](https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/data_center/create.jsp)

TMSH command for only site1.gtm1:

### TMSH

```
tmsh create gtm datacenter site1_datacenter
```

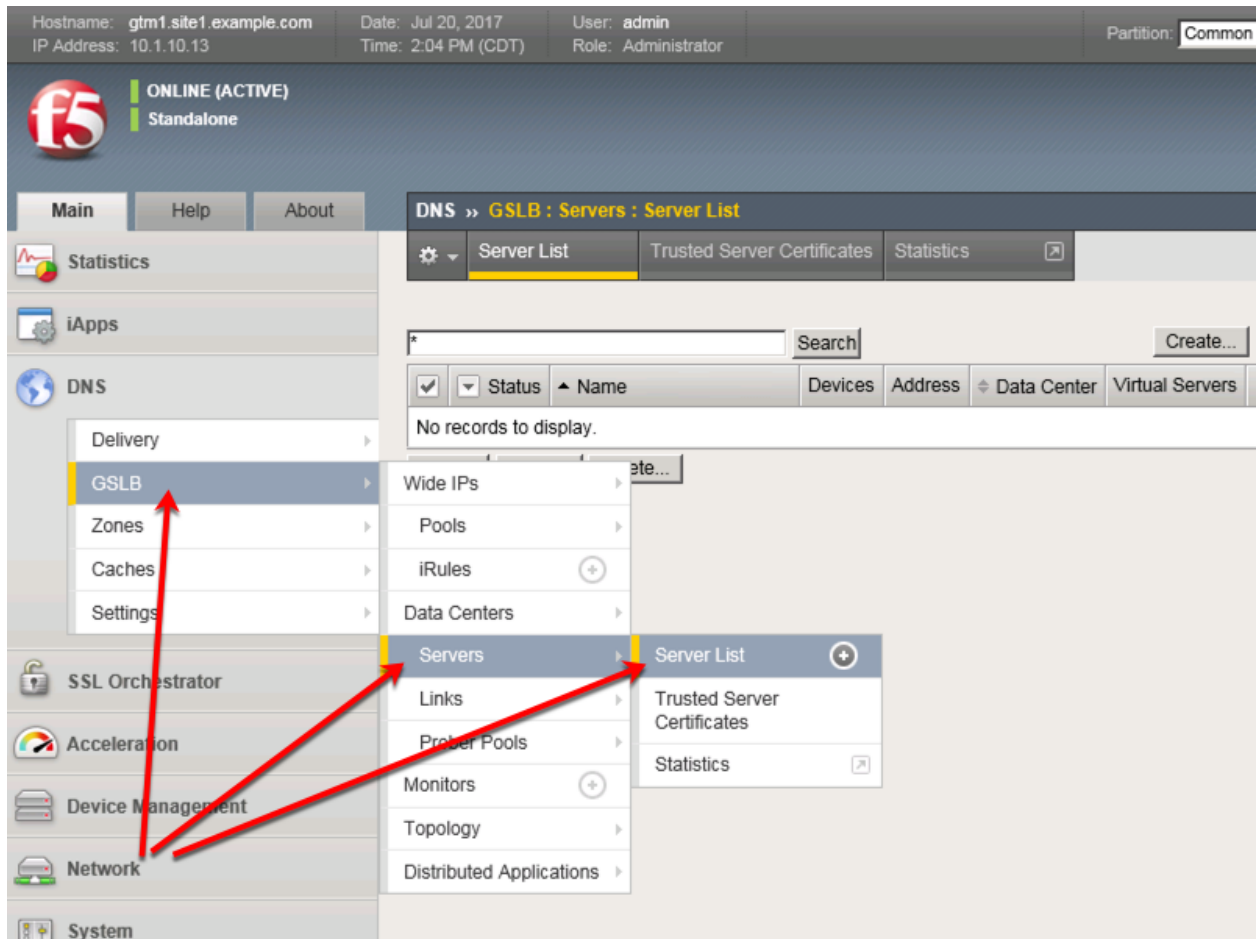
### TMSH

```
tmsh create gtm datacenter site2_datacenter
```

## 2.3.1 Servers

Server objects need to be defined and grouped into a Datacenter

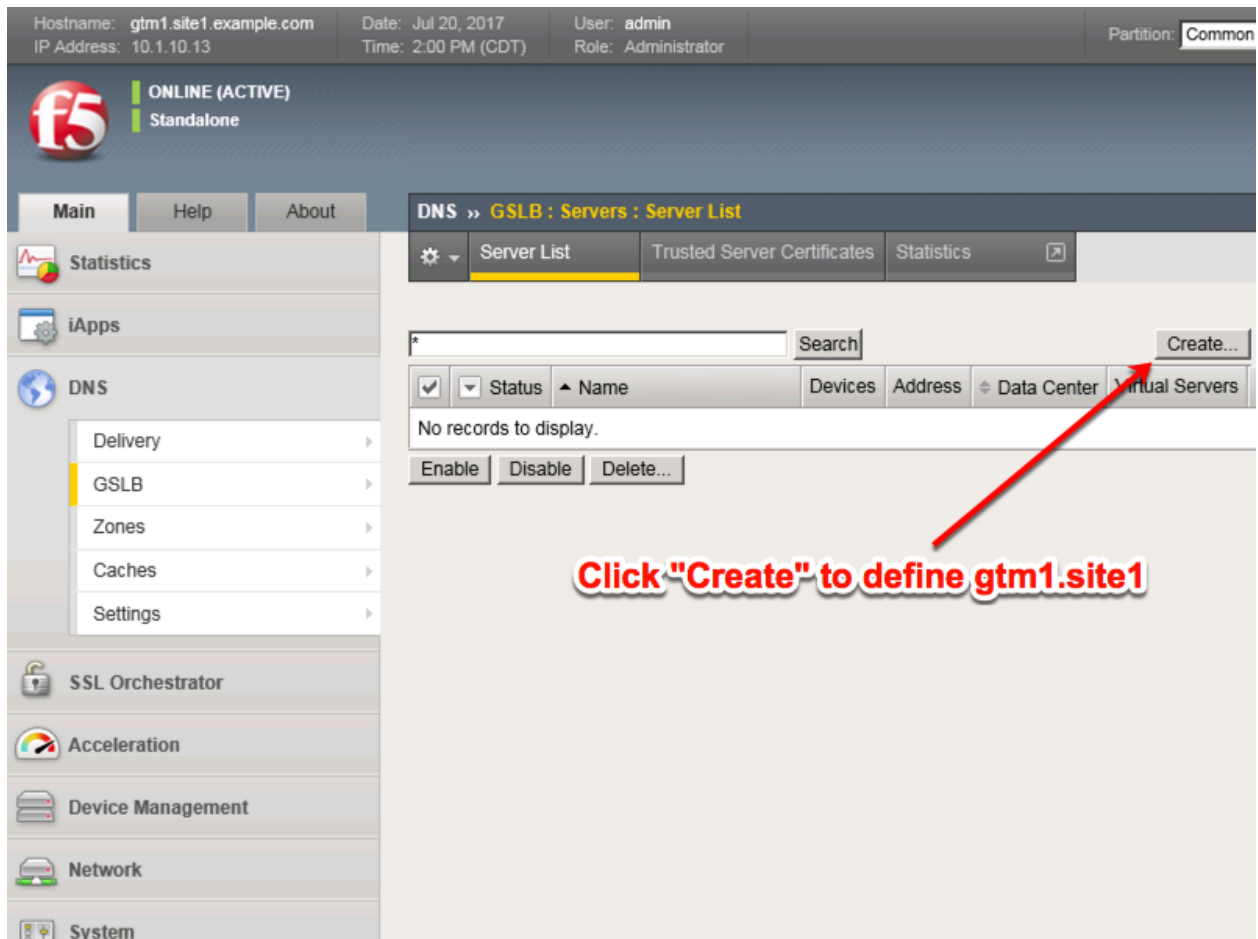
Navigate to: **DNS » GSLB : Servers : Server List**



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

**gtm1.site1**

All GTM devices need to be defined. Create a server object for gtm1.site1



Click "Create" to define gtm1.site1 as defined in the table below:

Setting	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: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 2:29 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

**DNS » GSLB : Servers : Server List » New Server...**

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name

Product

Data Center

Prober Preference

Prober Fallback

State

**Devices**

**Click "Add"**

Add

Device Name	Address
No data available in table	

Edit Delete

- Click the "Add" button to define IP addresses



Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 2:36 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

DNS » GSLB : Servers : Server List » New Server...

Add BIG-IP System Device

General Properties

Device Name: gtm1.site1.example.com 1  
Address: 203.0.113.7 2  
Translation: (Optional)  
Link: Auto-Select  
Add 3  
203.0.113.7  
Delete

Click "Add"

OK Cancel 4

Click "OK"

Big-IP System Devices

No data available in table

Edit Delete

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

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 2:43 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name	gtm1.site1_server
Product	BIG-IP System
Data Center	site1_datacenter
Prober Preference	Inherit From Data Center
Prober Fallback	Inherit From Data Center
State	Enabled

**Devices**

Device Name	Address
gtm1.site1.example.com	203.0.113.7

Add Edit Delete

**Configuration:** Advanced

Health Monitors	<div>Selected</div> <div>/Common bigip</div> <div>Available</div> <div>/Common gateway_icmp gtp http http_head_f5</div>
Availability Requirements	All Health Monitors
Limit Settings	Bits: Disabled Packets: Disabled Current Connections: Disabled
iQuery Options	Service Check <input checked="" type="checkbox"/> Path <input checked="" type="checkbox"/> SNMP <input checked="" type="checkbox"/>

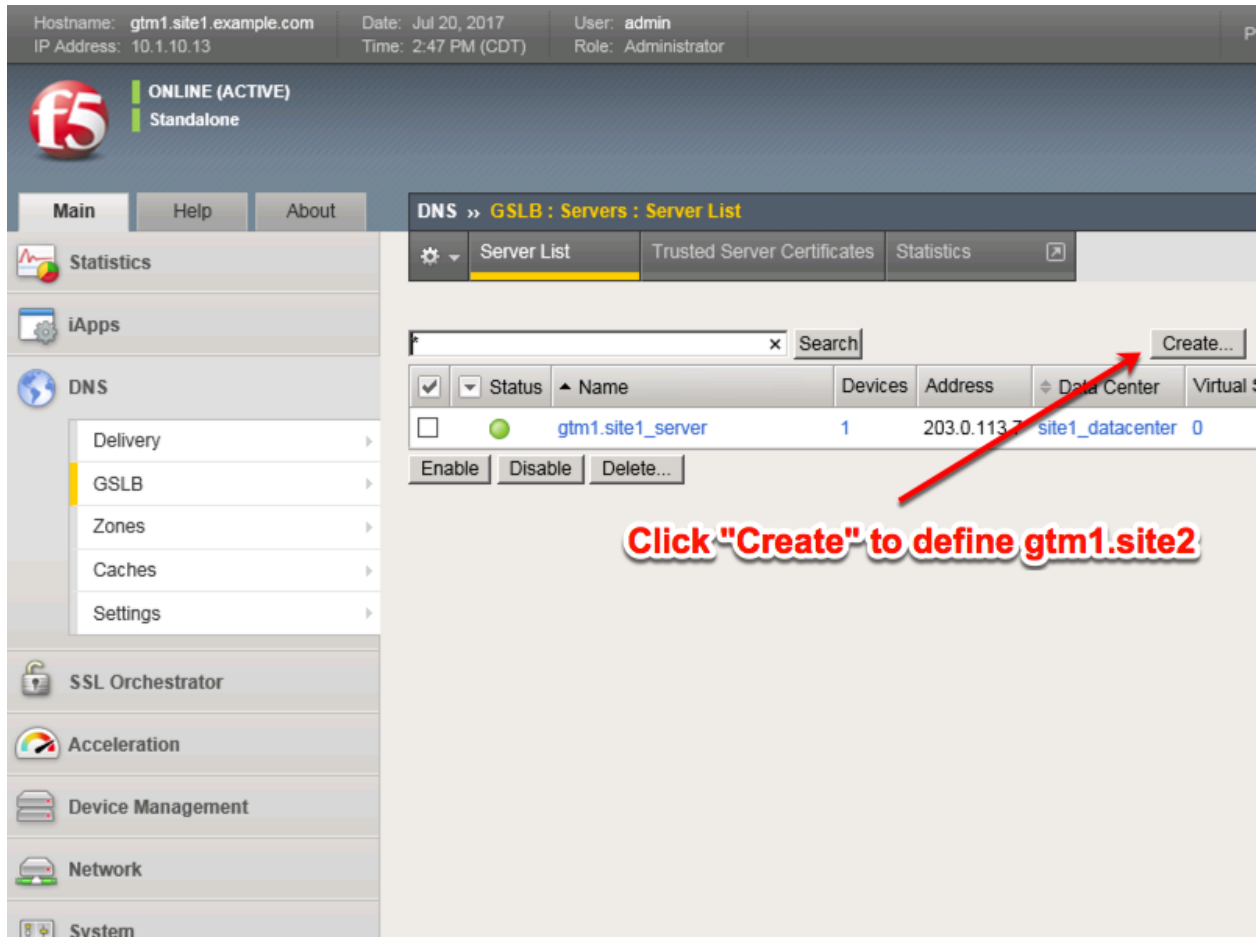
<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/server/create.jsp>

## TMSH

```
tmsl 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
```

**gtm1.site2**

All GTM devices need to be defined. Create a server object for gtm1.site2



Click "Create" to define gtm1.site2 as defined in the table below:

Setting	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: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 3:18 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

**DNS » GSLB : Servers : Server List » New Server...**

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name

Product

Data Center

Prober Preference

Prober Fallback

State

**Devices**

**Click "Add"**

Add

Device Name	Address
No data available in table	

Edit Delete

- Click the "Add" button to define IP addresses

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 3:30 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

DNS » GSLB : Servers : Server List » New Server...

Add BIG-IP System Device

General Properties

Device Name: gtm1.site2.example.com  
Address: 198.51.100.39  
Translation: (Optional)  
Link: Auto-Select

Prober Preference Add  
Prober Fallback 198.51.100.39

State

Devices

Add  
Delete

OK Cancel

Click "Add"

Click "OK"

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

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 3:37 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name	gtm1.site2_server
Product	BIG-IP System
Data Center	site2_datacenter
Prober Preference	Inherit From Data Center
Prober Fallback	Inherit From Data Center
State	Enabled

**Devices**

Device Name	Address
gtm1.site2.example.com	198.51.100.39

Add Edit Delete

**Configuration:** Advanced

Health Monitors	<div>Selected</div> <div>/Common bigip</div>	<div>Available</div> <div>/Common gateway_icmp gtp http http_head_f5</div>
Availability Requirements	All Health Monitors	
Limit Settings	Bits: Disabled Packets: Disabled Current Connections: Disabled	
iQuery Options	Service Check <input checked="" type="checkbox"/> Path <input checked="" type="checkbox"/> SNMP <input checked="" type="checkbox"/>	

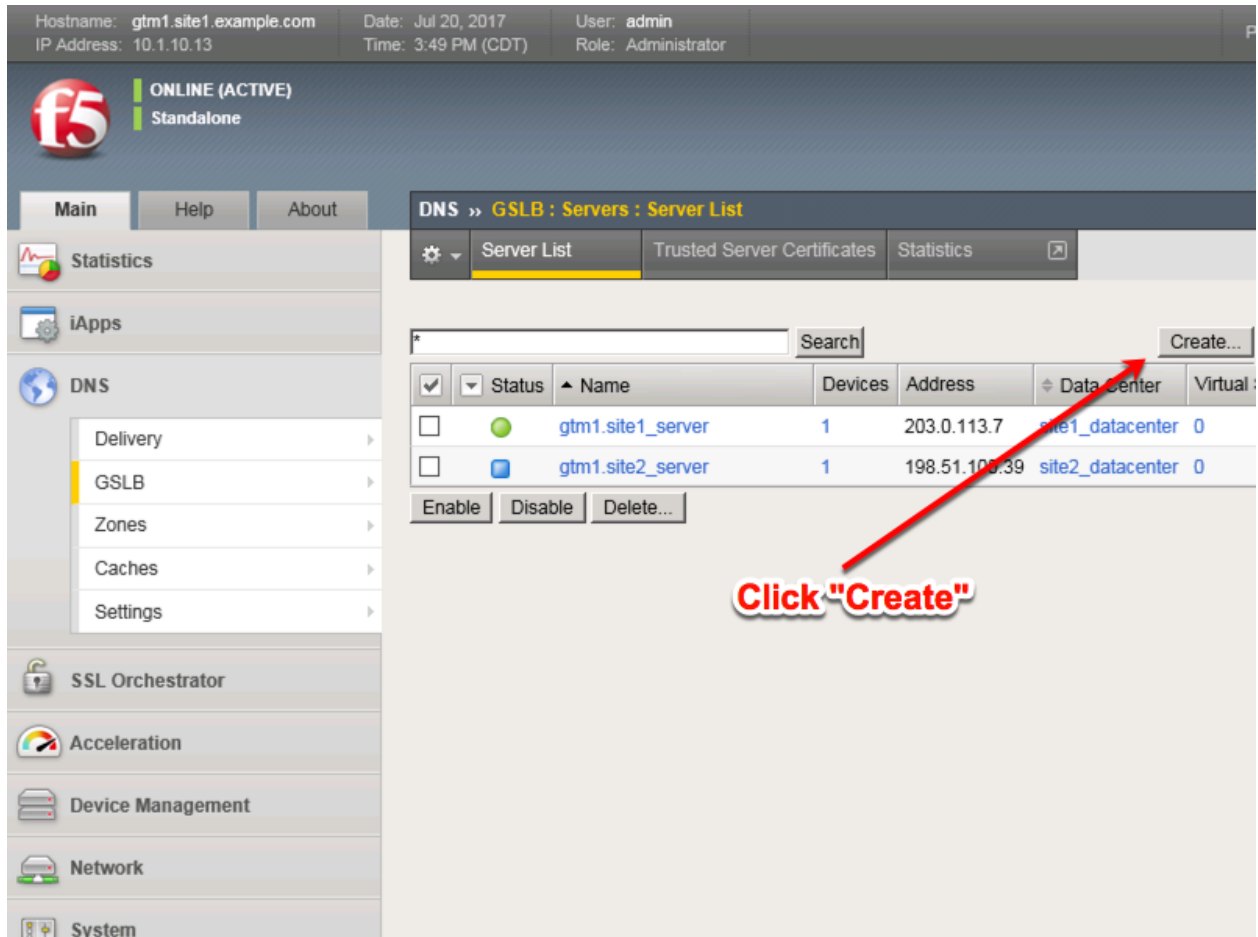
<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/server/create.jsp>

## 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
```

## site1\_ha-pair

LTM devices need to be defined. Create a server object for the bigip1.site1 and bigip2.site1 HA pair



Create a Server Object as defined in the table below:

Setting	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 Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 3:58 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

**DNS » GSLB : Servers : Server List » New Server...**

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name   
Product   
Data Center   
Prober Preference   
Prober Fallback   
State

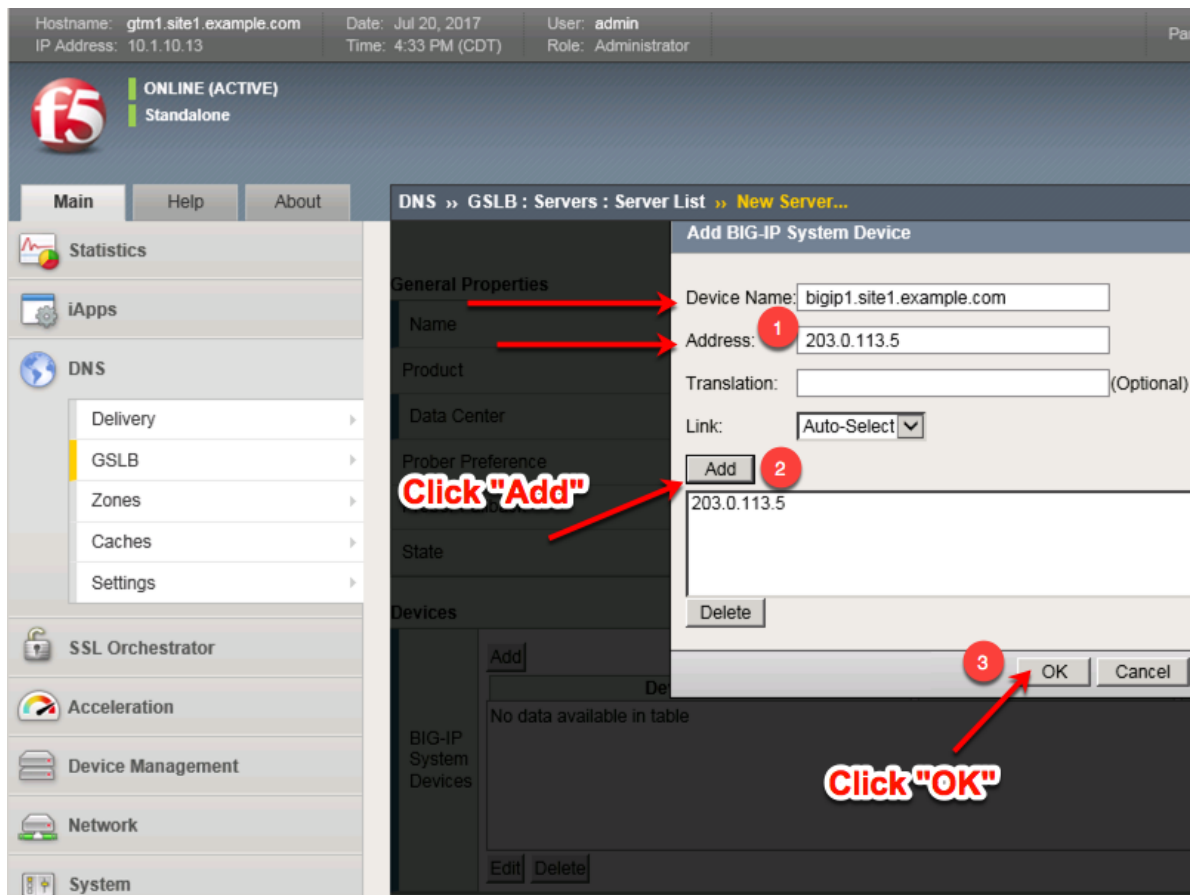
**Devices**

**Click "Add"**

Device Name	Address
No data available in table	

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





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

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 4:38 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name	site1_ha-pair
Product	BIG-IP System
Data Center	site1_datacenter
Prober Preference	Inherit From Data Center
Prober Fallback	Inherit From Data Center
State	Enabled

**Devices**

Add

Device Name	Address
bigip1.site1.example.com	203.0.113.5

Edit Delete

**Click "Add" .....again**

- Click the "Add" button to define IP addresses

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 4:53 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

DNS » GSLB : Servers : Server List » New Server...

Add BIG-IP System Device

General Properties

Name Device Name: bigip2.site1.example.com  
Address: 203.0.113.6  
Product  
Translation: (Optional)  
Link: Auto-Select  
Add  
Delete

Click "Add"

Devices

Add  
bigip1.site1.example.com 203.0.113.5  
Delete

Click "OK"

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

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 5:00 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name	site1_ha-pair
Product	BIG-IP System
Data Center	site1_datacenter
Prober Preference	Inherit From Data Center
Prober Fallback	Inherit From Data Center
State	Enabled

**Devices**

Device Name	Address
bigip1.site1.example.com	203.0.113.5
bigip2.site1.example.com	203.0.113.6

**Add the "bigip" Health Monitor**

Configuration: Advanced

Health Monitors

Selected	Available
/Common bigip	/Common gateway_icmp gtp http http_head_f5

Availability Requirements: All Health Monitors

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

**Resources**

Virtual Server Discovery	Enabled
Link Discovery	Enabled

Cancel Repeat Finished

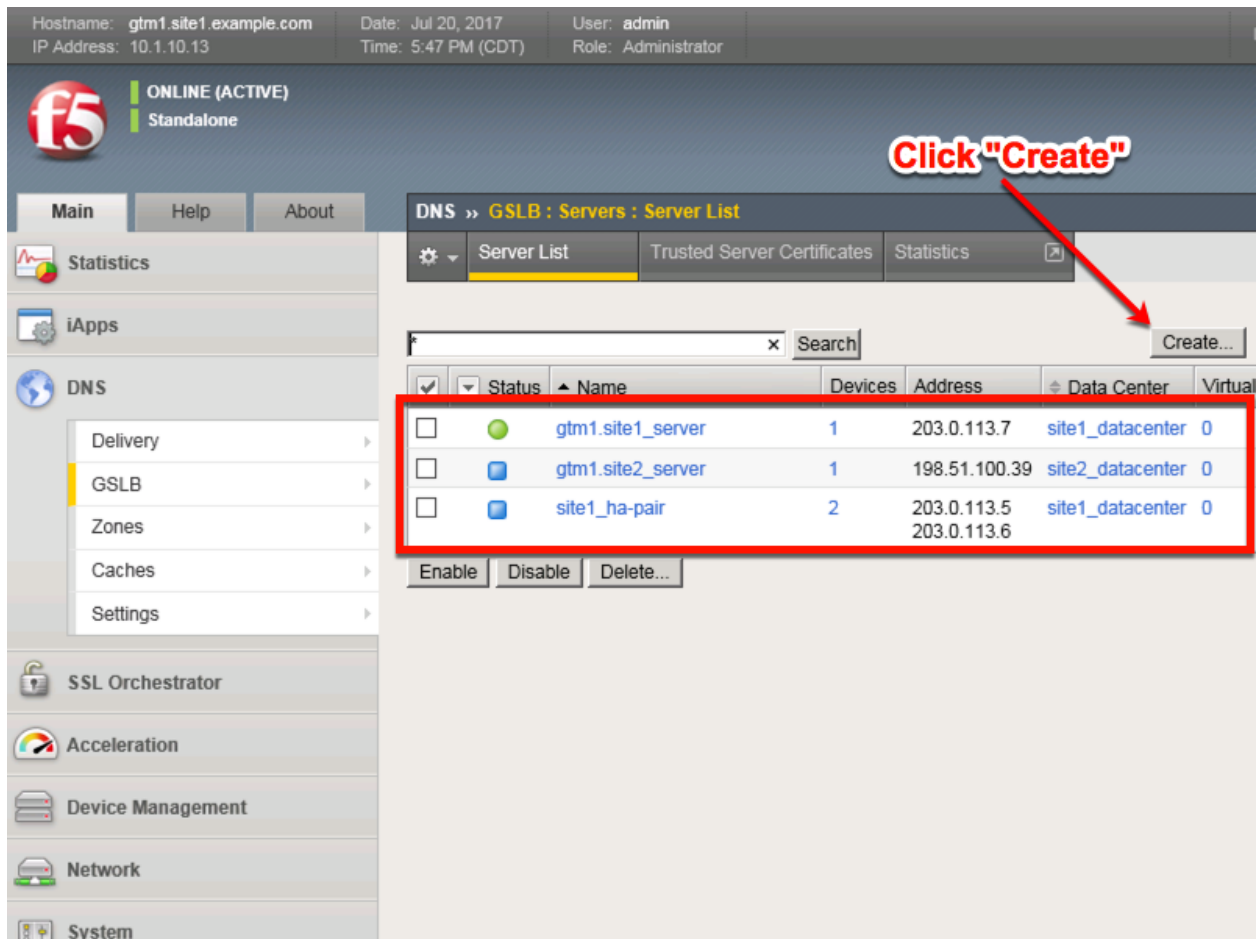
<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/server/create.jsp>

## TMSH

```
tmsh create gtm server site1_ha-pair datacenter site1_datacenter devices add { bigip1.site1.example.com
{ addresses add { 203.0.113.5 { } } } bigip2.site1.example.com { addresses add { 203.0.113.6 { } } } } link-
discovery enabled monitor bigip product bigip virtual-server-discovery enabled
```

## site2\_ha-pair

LTM devices need to be defined. Create a server object for the bigip1.site2 and bigip2.site2 HA pair



Create a Server Object as defined in the table below:

Setting	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: Jul 20, 2017    User: admin  
IP Address: 10.1.10.13    Time: 5:52 PM (CDT)    Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main    Help    About    DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
  Delivery  
  GSLB  
  Zones  
  Caches  
  Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name	site2_ha_pair
Product	BIG-IP System
Data Center	site2_datacenter
Prober Preference	Inherit From Data Center
Prober Fallback	Inherit From Data Center
State	Enabled

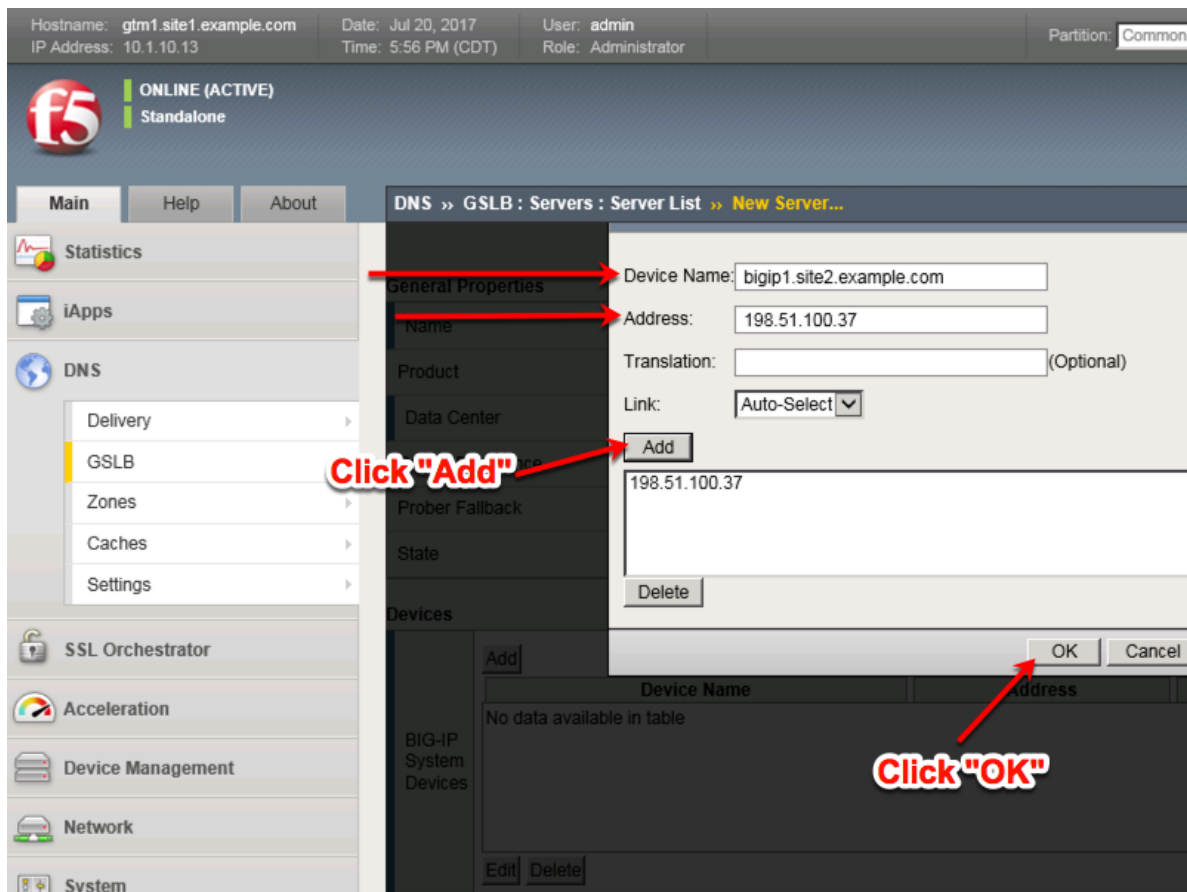
**Devices**

Big-IP System Devices

Add    Device Name    No data available in table    Edit    Delete

**Click "Add"**

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



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

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 6:13 PM (CDT) Role: Administrator Partition: Common

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name   
Product   
Data Center   
Prober Preference   
Prober Fallback   
State

**Devices**

**Click "Add"**

Device Name	Address
bigip1.site2.example.com	198.51.100.37

Edit Delete

- Click the "Add" button to define IP addresses



Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 6:22 PM (CDT) Role: Administrator Partition: Common

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

DNS » GSLB : Servers : Server List » New Server...

**General Properties**

Device Name: bigip2.site2.example.com  
Address: 198.51.100.38  
Translation: (Optional)  
Link: Auto-Select  
Add  
Delete

**Click "Add"**

**Devices**

Device Name	Address
bigip1.site2.example.com	198.51.100.37

**Click "OK"**

OK Cancel

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

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 7:55 PM (CDT) Role: Administrator Partition: Common

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name	site2_ha_pair
Product	BIG-IP System
Data Center	site2_datacenter
Prober Preference	Inherit From Data Center
Prober Fallback	Inherit From Data Center
State	Enabled

**Devices**

Device Name	Address
bigip1.site2.example.com	198.51.100.37
bigip2.site2.example.com	198.51.100.38

Add Edit Delete

**Configuration:** Advanced

Health Monitors

Availability Requirements: All Health Monitors

Selected: /Common bigip

Available: /Common gateway\_icmp gtp http http\_head\_f5

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

**Resources**

Virtual Server Discovery	Enabled
Link Discovery	Enabled

Cancel Repeat Finished

<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/server/create.jsp>

## 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
```

### 2.3.2 Device Trust

A mesh of F5 DNS servers need to exchange keys to establish a trusted mechanism for HA communications.

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 8:05 PM (CDT) Role: Administrator Partition: Common

ONLINE (ACTIVE)  
Standalone

Main Help About

DNS » **GSLB : Servers : Server List**

Server List Trusted Server Certificates Statistics

Search

<input type="checkbox"/>	Status	Name	Devices	Address	Data Center	Virtual Servers	Pr
<input type="checkbox"/>		gtm1.site1_server	1	203.0.113.7	site1_datacenter	0	Blk
<input type="checkbox"/>		gtm1.site2_server	1	198.51.100.39	site2_datacenter	0	Blk
<input type="checkbox"/>		site1_ha-pair	2	203.0.113.5 203.0.113.6	site1_datacenter	0	Blk
<input type="checkbox"/>		site2_ha-pair	2	198.51.100.37 198.51.100.38	site2_datacenter	0	Blk

Enable Disable Delete...

**Three other servers need to "establish trust"**

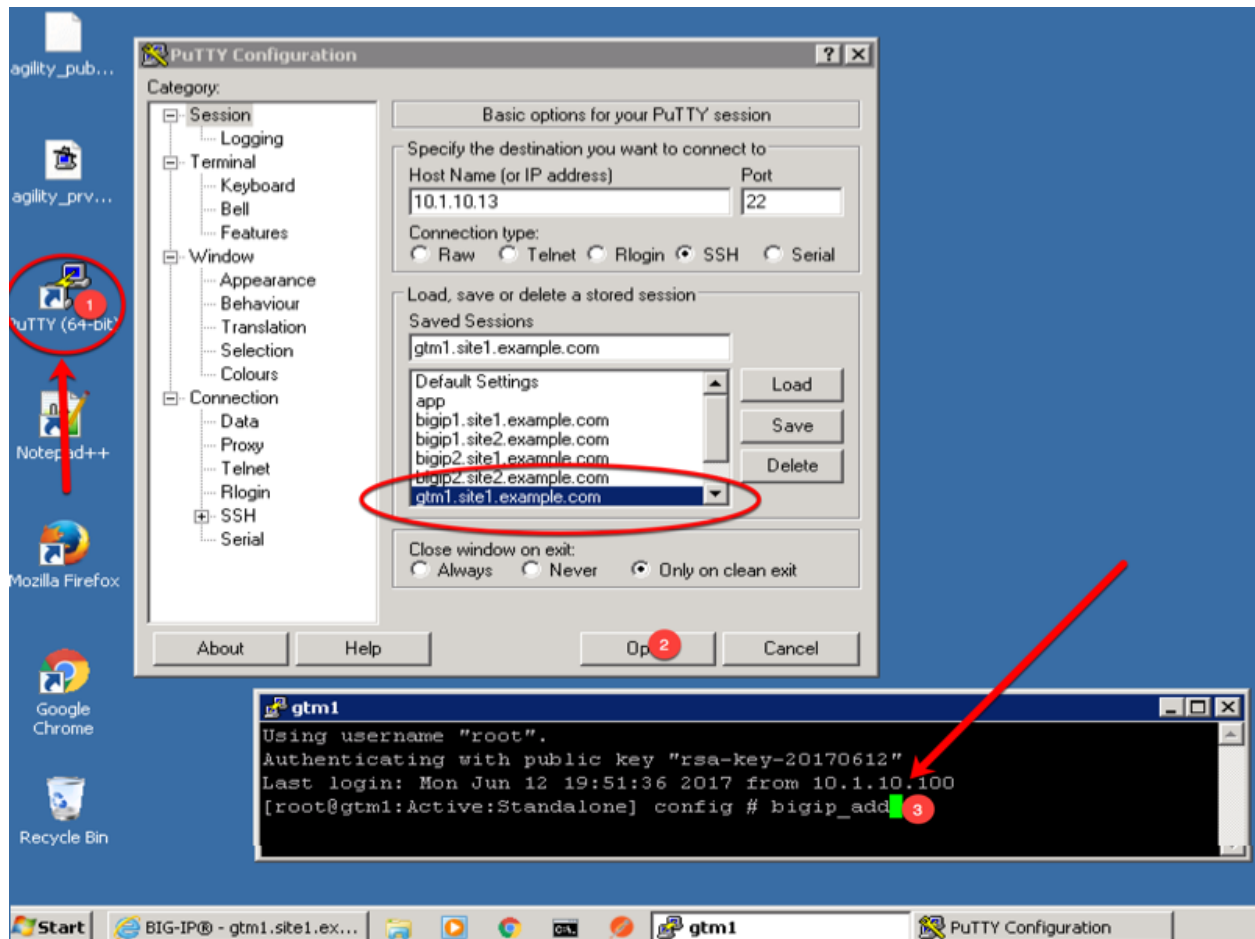
Launch Putty and login to gtm1.site1.example.com

Run the following command:

When prompted for a password use "default".

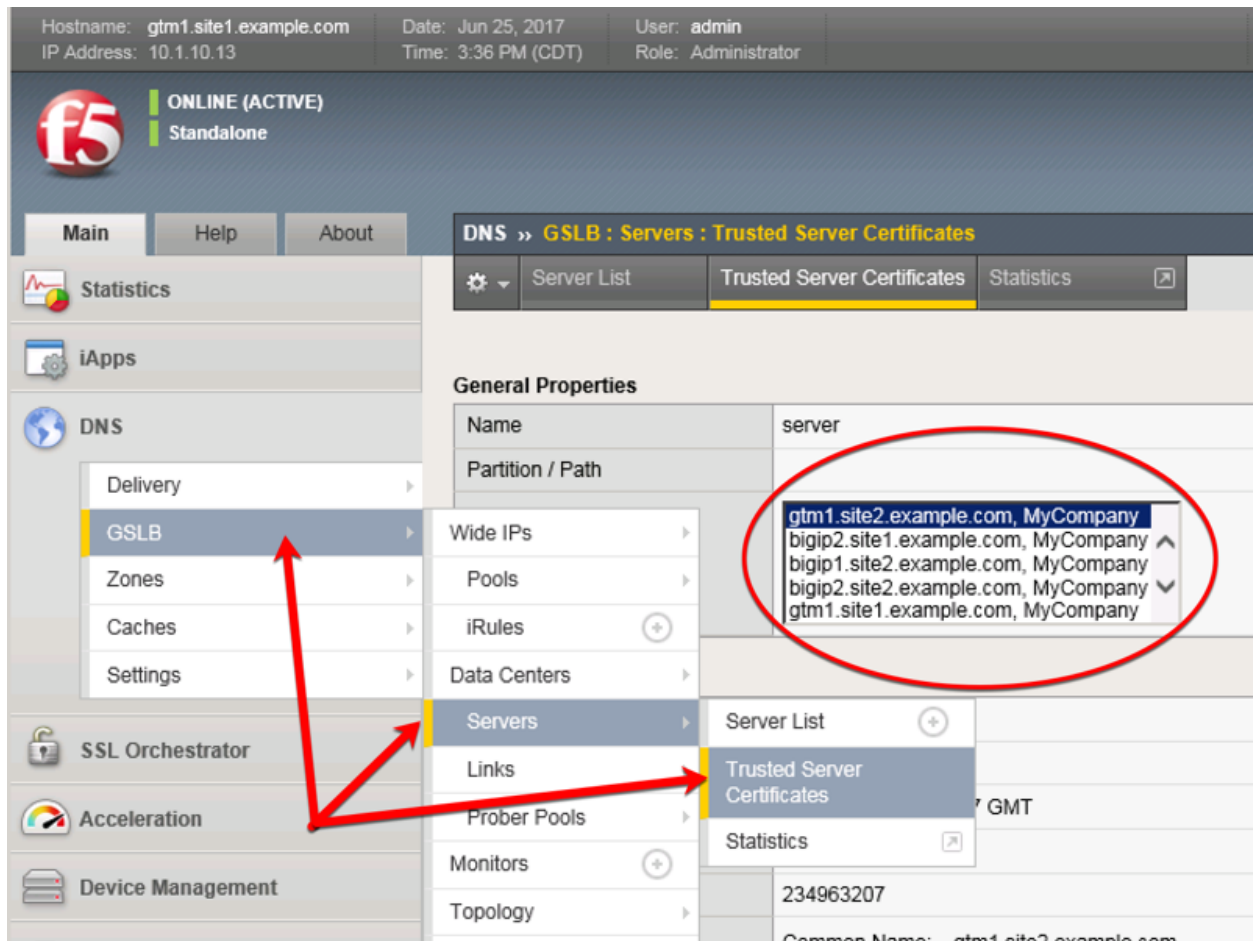
#### TMSH

bigip\_add



Navigate to: **DNS » GSLB : Servers : Trusted Server Certificates**

[https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/localb/ssl\\_certificate/properties.jsp?certificate\\_name=server&store=iquery](https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/localb/ssl_certificate/properties.jsp?certificate_name=server&store=iquery)



### 2.3.3 Sync Group

After the BIG-IP DNS server in datacenter 2 is joined to the sync group, administrators may make changes to either F5 DNS server.

Changes will be automatically replicated across all F5 DNS servers.

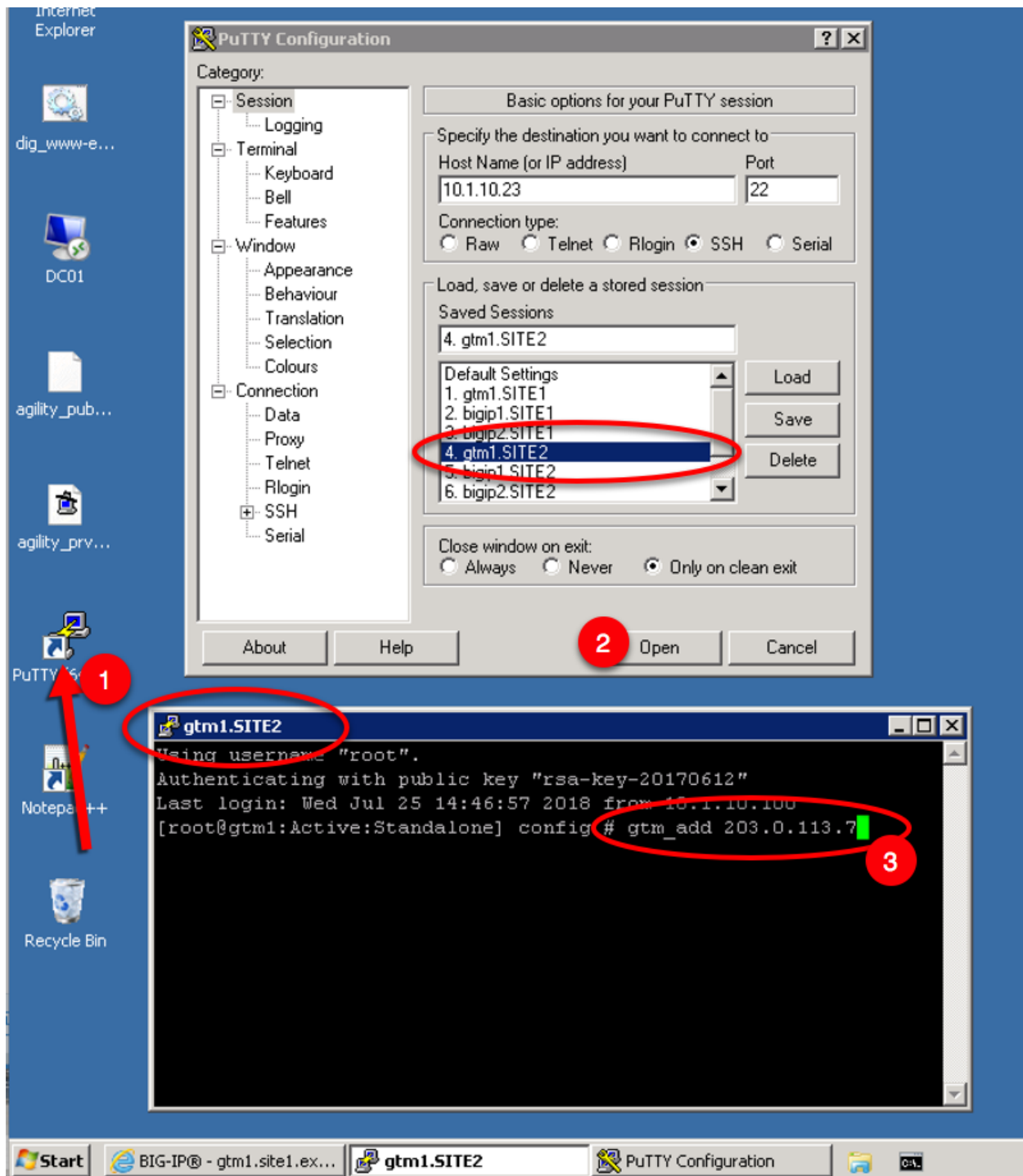
Launch Putty and log in to gtm1.site2

Run the following command: Enter the password “default” when prompted.

Select “y” to allow the bigip-ip to join the mesh.

#### TMSH

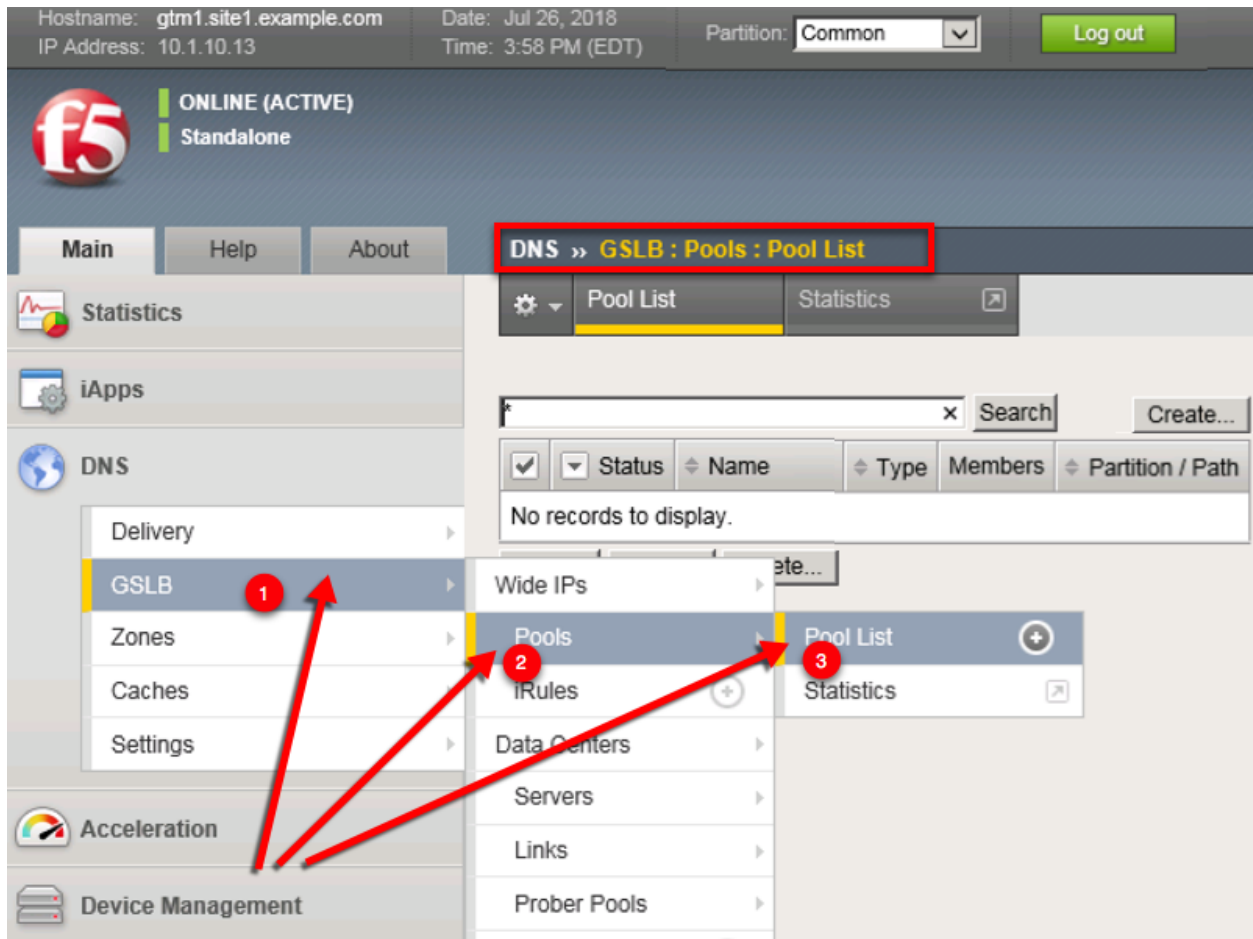
```
gtm_add 203.0.113.7
```



## 2.4 Pools

LTM virtual server objects are grouped together into GTM pools.

Navigate to: **DNS » GSLB : Pools : Pool List**



Create a Pool of LTM Virtuals according to the following table:

Setting	Value
Name	www.example.com_pool
Type	A
member	isp1_site1_www.example.com_tcp_https_virtual
member	isp2_site2_www.example.com_tcp_https_virtual

<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/pool/create.jsp>

Hostname: gtm1.site1.example.com Date: Jul 26, 2018 User: admin  
IP Address: 10.1.10.13 Time: 4:11 PM (EDT) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)  
Standalone

Main Help About **DNS » GSLB : Pools : Pool List » New Pool...**

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name:  x  
Type:   
State:

**Configuration**

Health Monitors: Selected:  Available:   
Availability Requirements:   
Limit Settings: Bits:  Packets:  Current Connections:   
Manual Resume: ☐  
TTL:   
Dynamic Ratio: ☐  
Maximum Answers Returned:   
Verify Member Availability: ☒

**Members**

Load Balancing Method: Preferred:  Alternate:  Fallback:   
Fallback IP:   
Virtual Server:   
Ratio:   
  
Member List:

**Select two LTM VIP's and click "Add"**

TMSH command to run on only gtm1.site1:

## TMSH

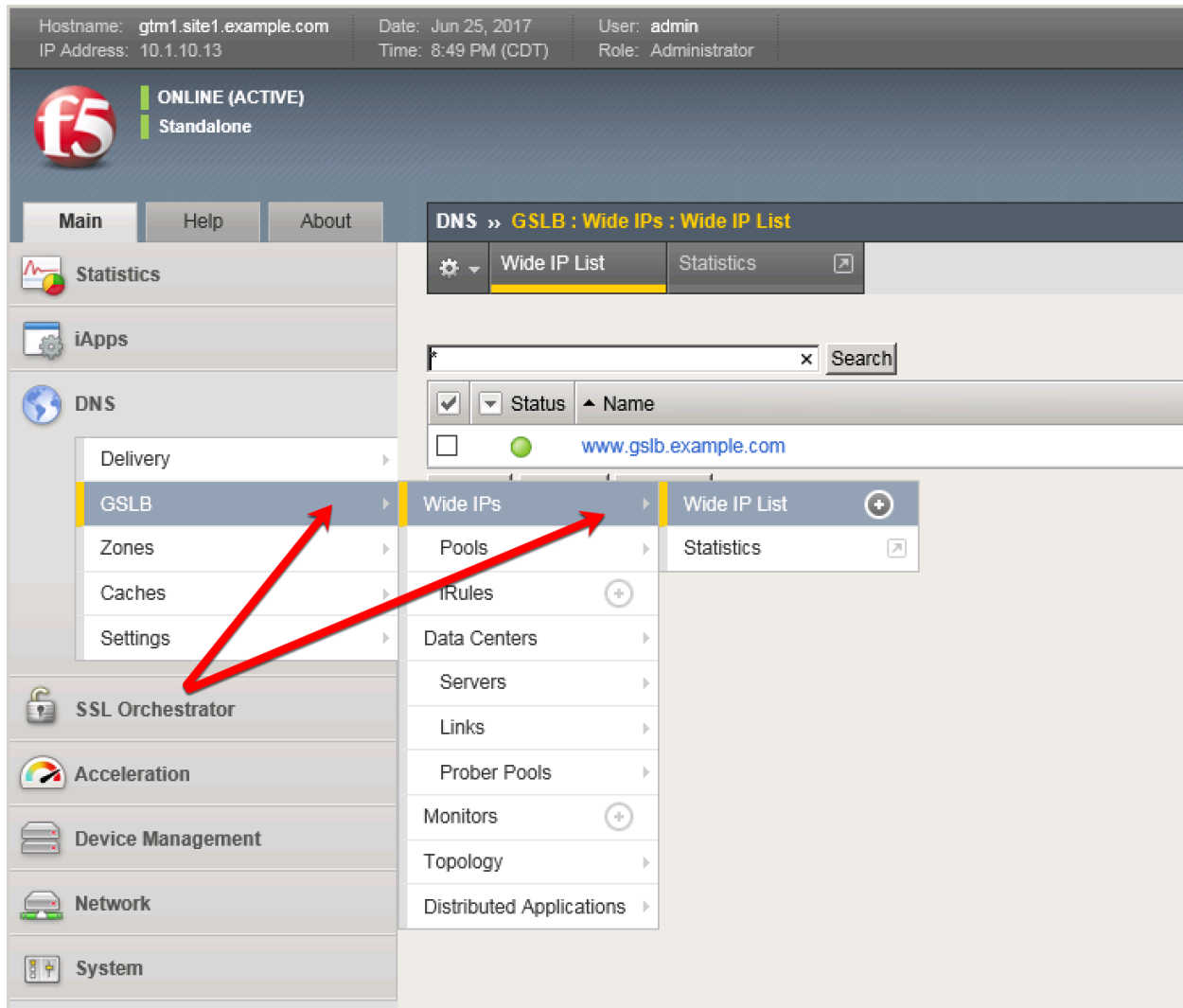
```
tmsh create gtm pool a www.example.com_pool { members add { site1_ha-  
pair:/Common/isp1_site1_www.example.com_tcp_https_virtual { member-order 0 } site2_ha-  
pair:/Common/isp2_site2_www.example.com_tcp_https_virtual { member-order 1 } }
```

## 2.5 FQDN

F5 refers to an FQDN as a “wide-ip”, or “wip”.



Navigate to: **DNS » GSLB : Wide IPs : Wide IP List**



Create an F5 “wide IP”

Setting	Value
Name	www.gslb.example.com
Type	A
Pool	www.example.com_pool

Hostname: gtm1.site1.example.com Date: Jul 29, 2018 User: admin  
IP Address: 10.1.10.13 Time: 4:13 PM (EDT) Role: Administrator Partition: Common Log out

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

DNS » GSLB : Wide IPs : Wide IP List » New...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
Acceleration  
Device Management  
Network  
System

General Properties: Advanced

Name: **www.example.com**  
Type: A  
Description:  
Alias: **www.gslb.example.com**  
Add  
Alias List: **www.gslb.example.com**  
Delete  
State: Enabled  
Minimal Response: Enabled  
Return Code On Failure: Disabled  
Load-Balancing Decision Log: ☒ Pool Selection  
☒ Pool Traversal  
☒ Pool Member Selection  
☒ Pool Member Traversal

iRules  
iRule List  
Selected Available  
Up Down  
iRule List  
Selected Available  
Up Down

Pools  
Load Balancing Method: Round Robin  
Persistence: Disabled  
Pool: Select...  
Ratio: 1  
Add

**For troubleshooting purposes enable verbose logging**

**Chapter 2 - Class 1 - Intro to GSLB**

<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globalb/wideip/list.jsp>

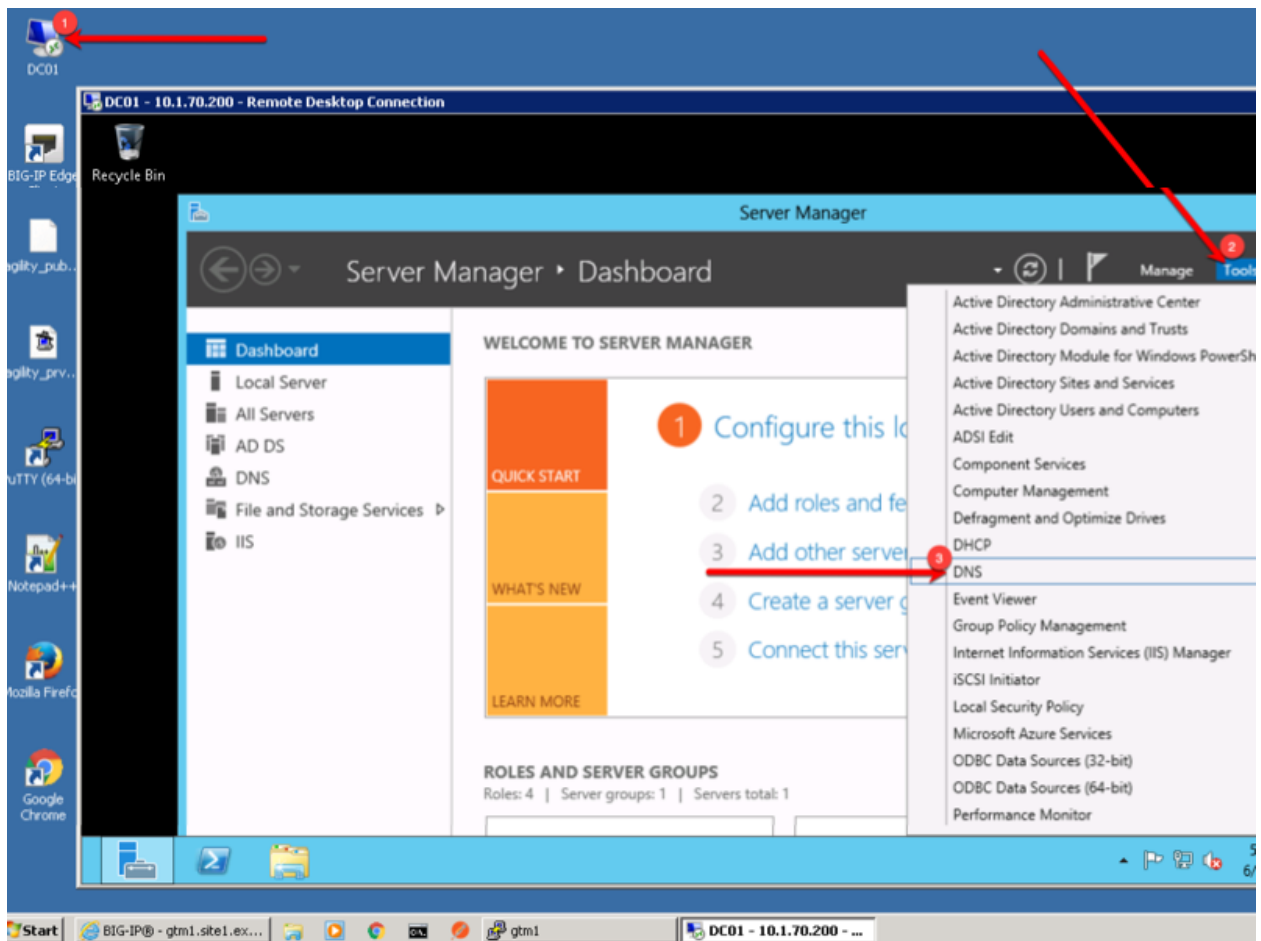
TMSH command to run on only gtm1.site1:

## TMSH

```
tmsl create gtm wideip a www.gslb.example.com { pools add { www.example.com_pool { order 0 } } }
```

## 2.6 Delegation

Log in to the DNS server from the jumpbox (username: user password: Agility1) , and open the DNS management UI:

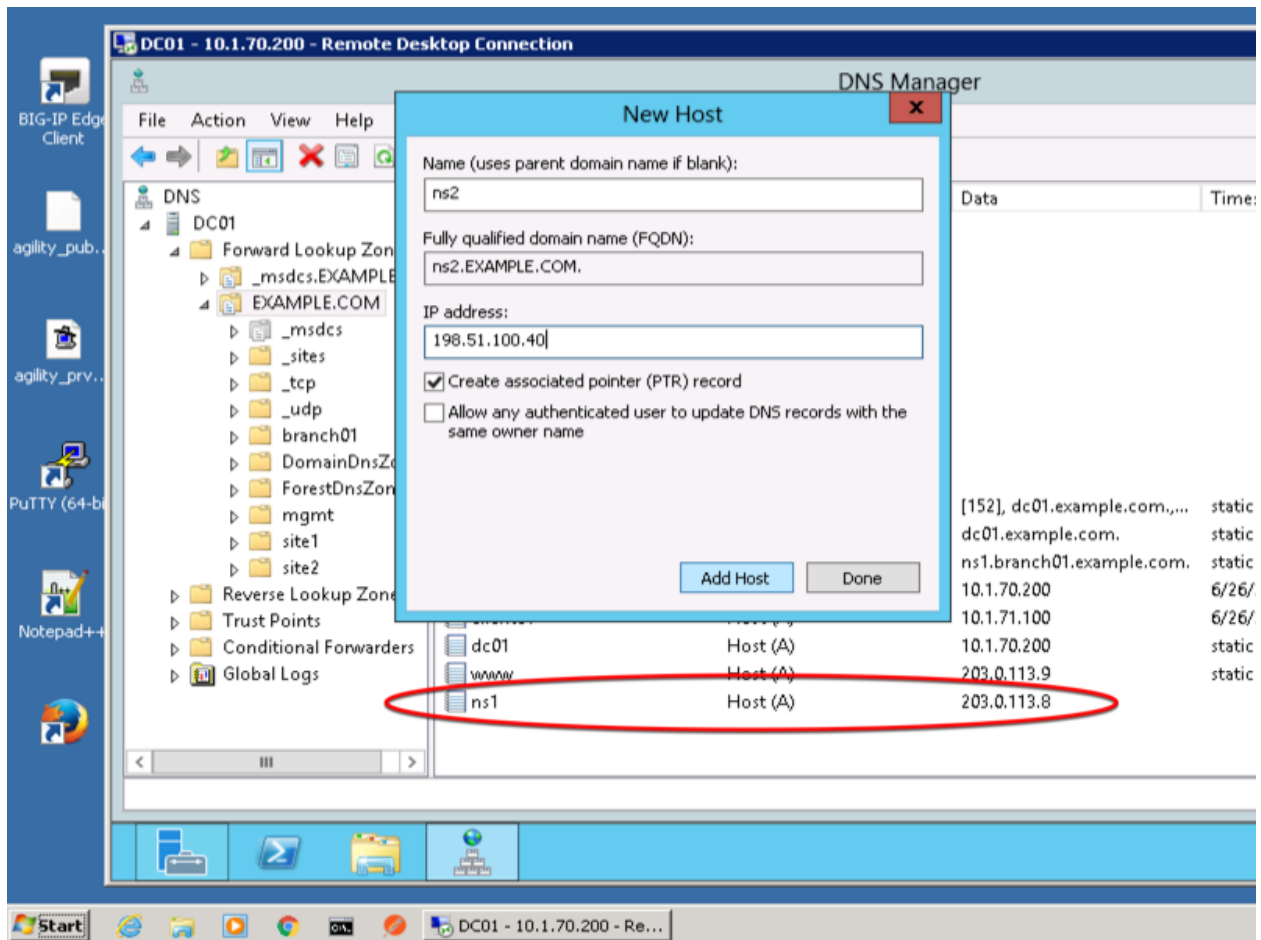


### 2.6.1 A Records

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

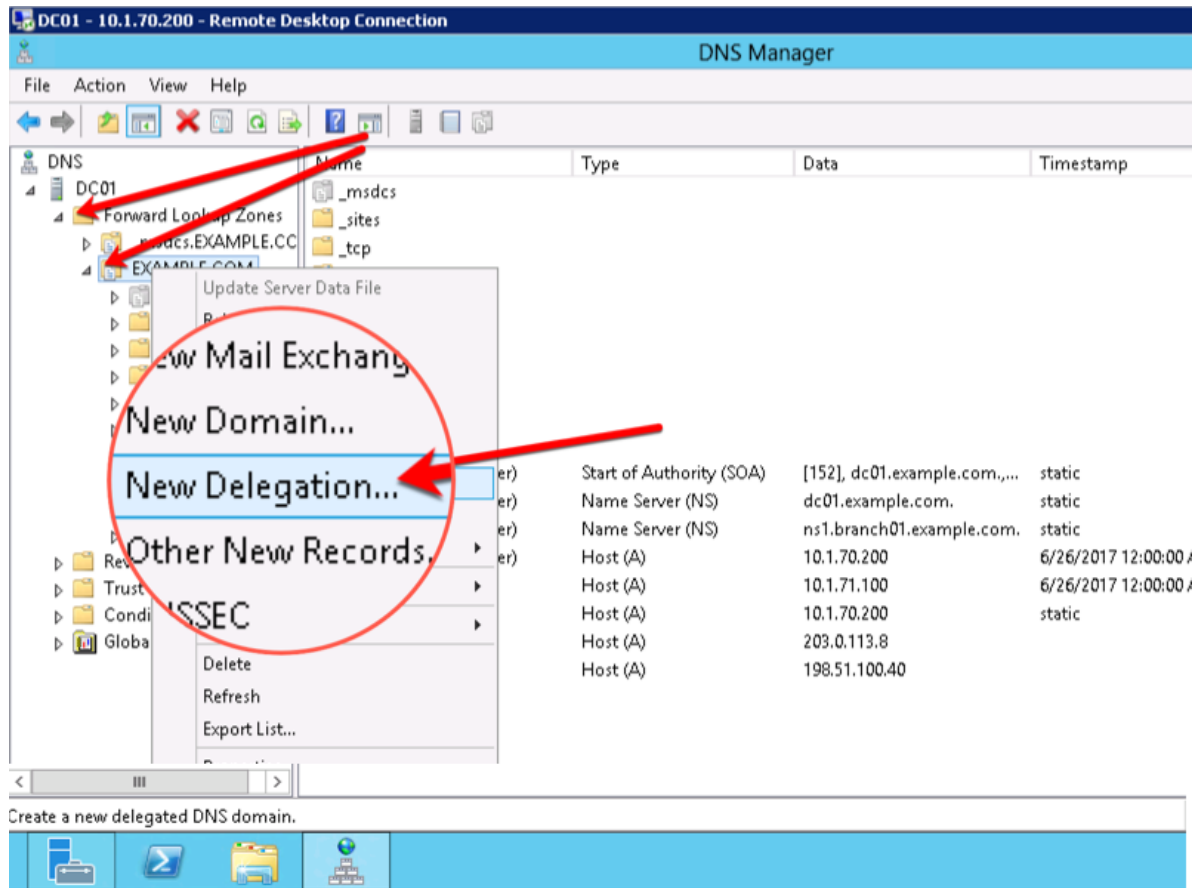
Setting	Value
ns1	203.0.113.8
ns2	198.51.100.40

Expand “Forward Lookup Zones”, right click on EXAMPLE.COM and select “New Host”

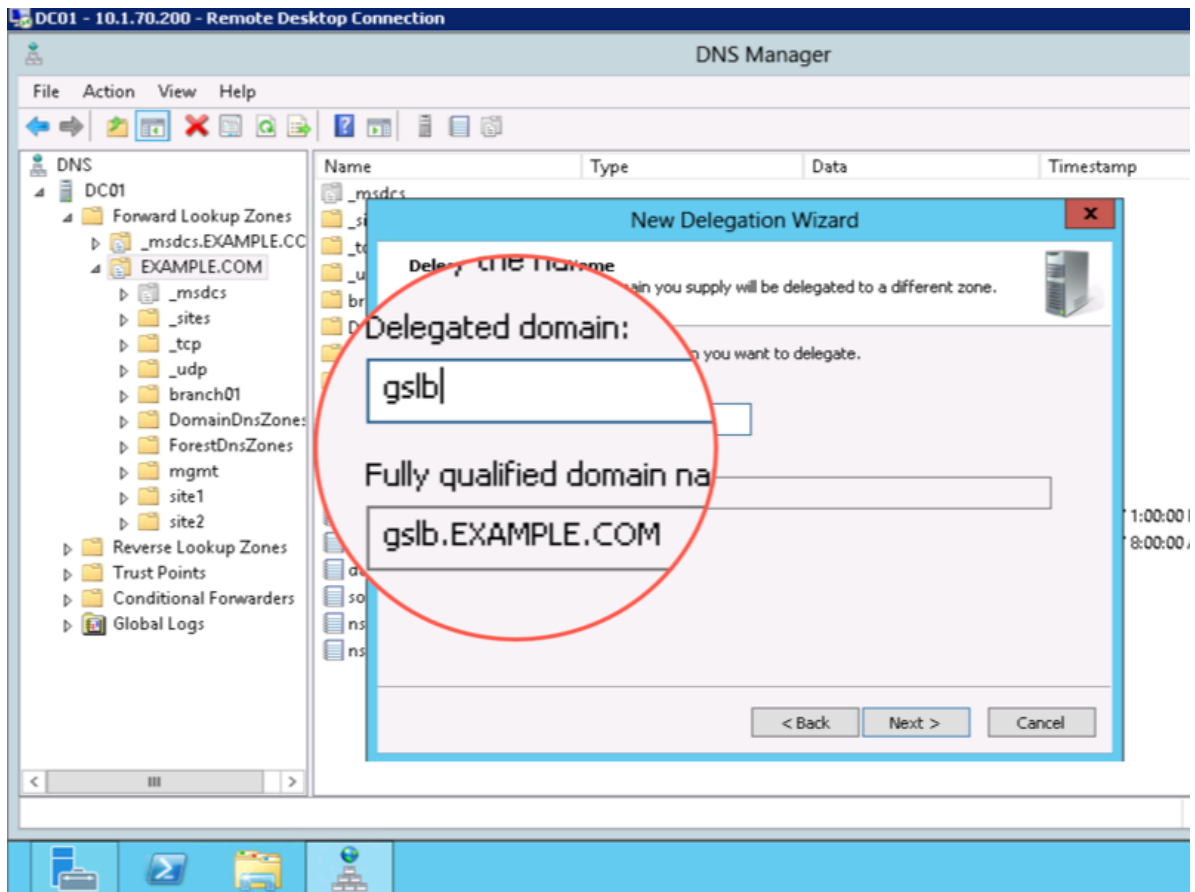


## 2.6.2 Sub Domain

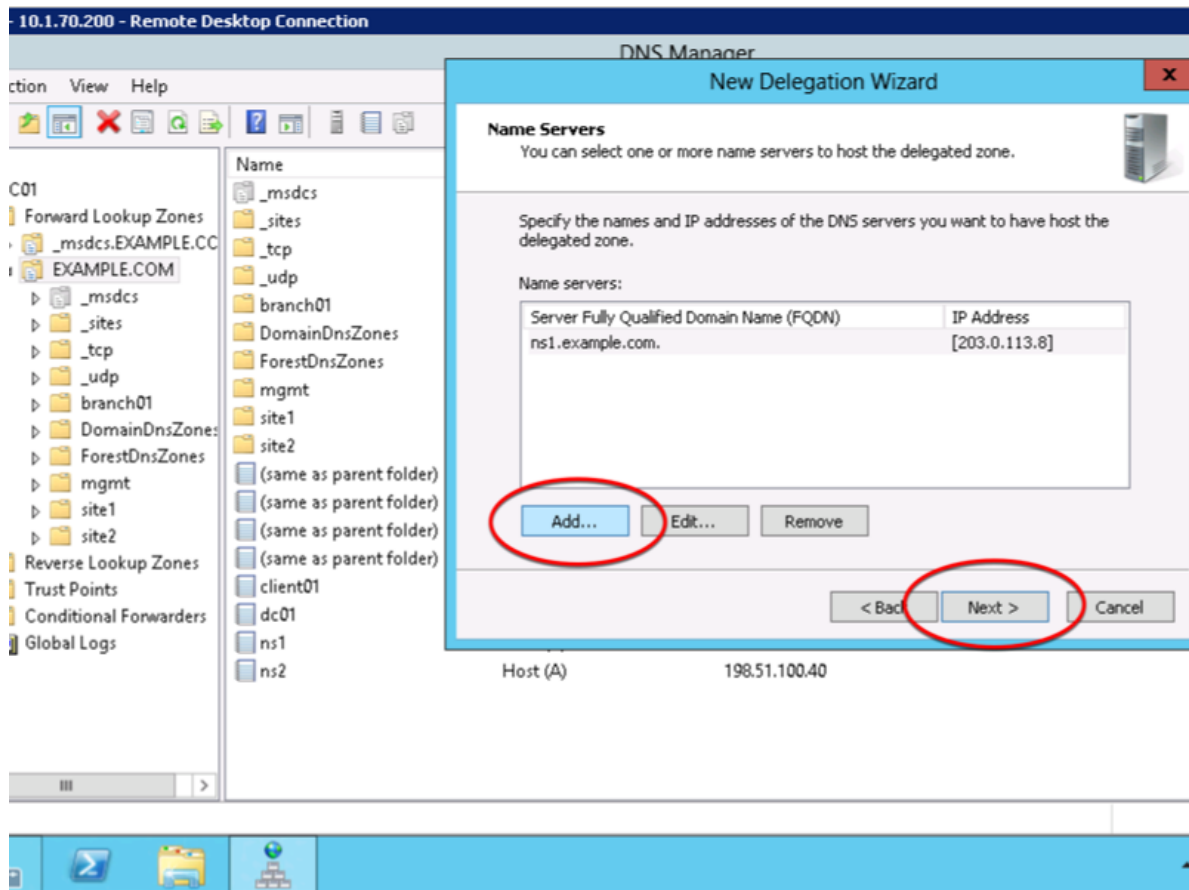
1. Expand “Forward Lookup Zones”, and right click on “EXAMPLE.com



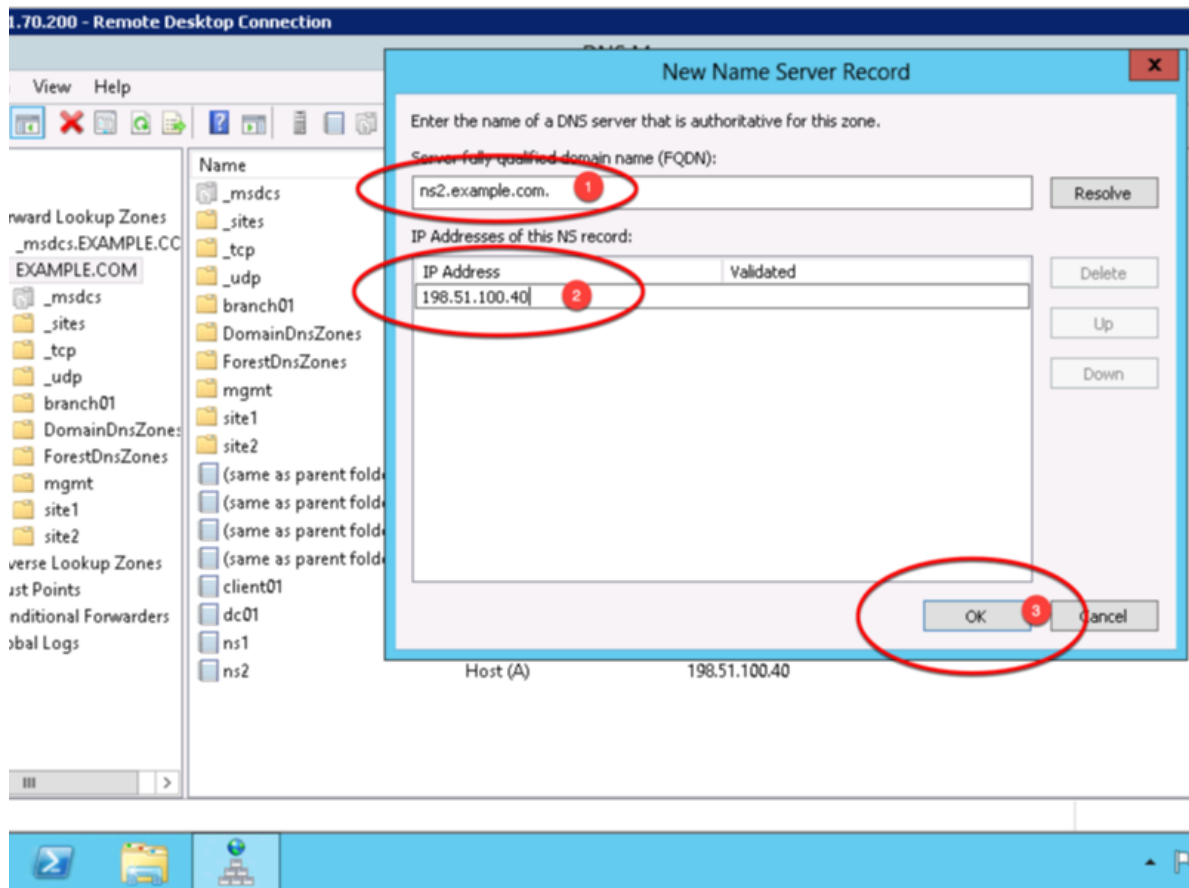
2. Create the "gslb" subdomain.



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

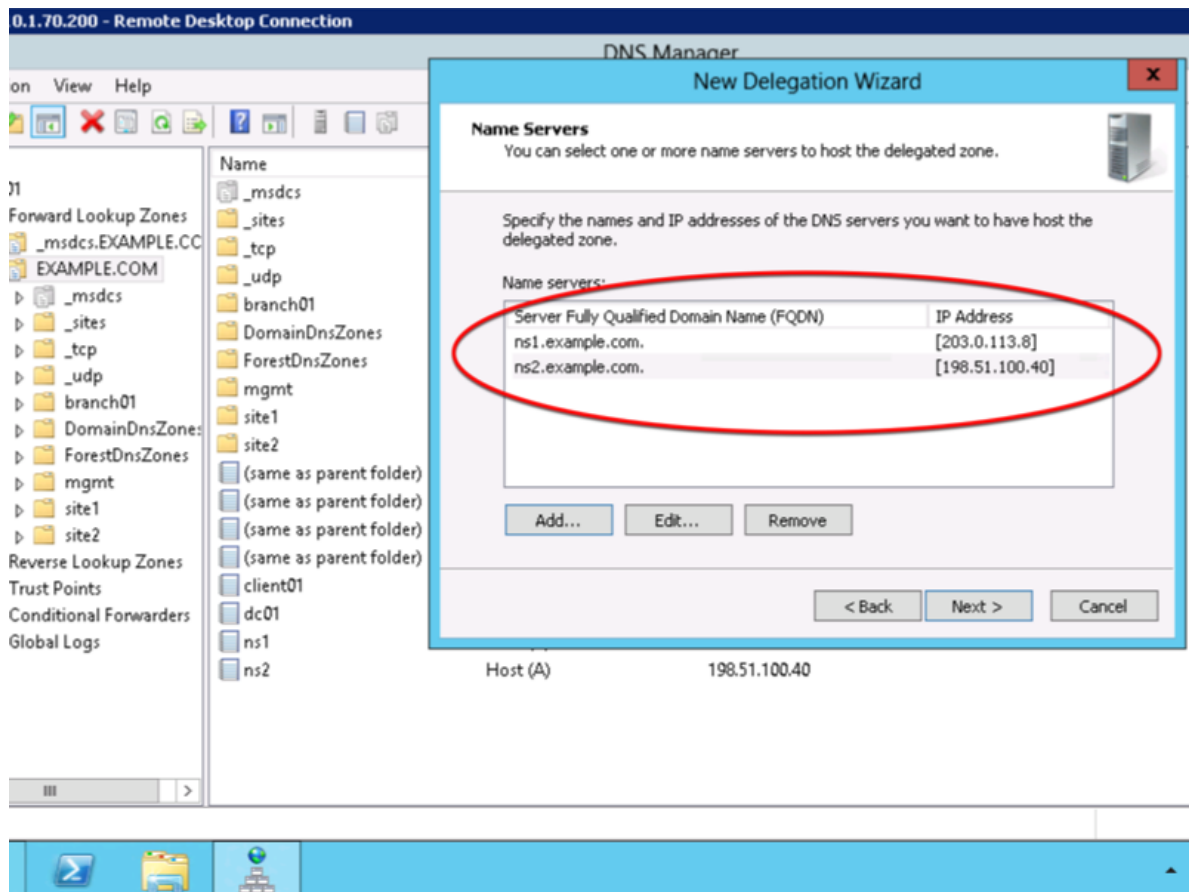


4. Also add "ns2.example.com - 198.51.100.40"

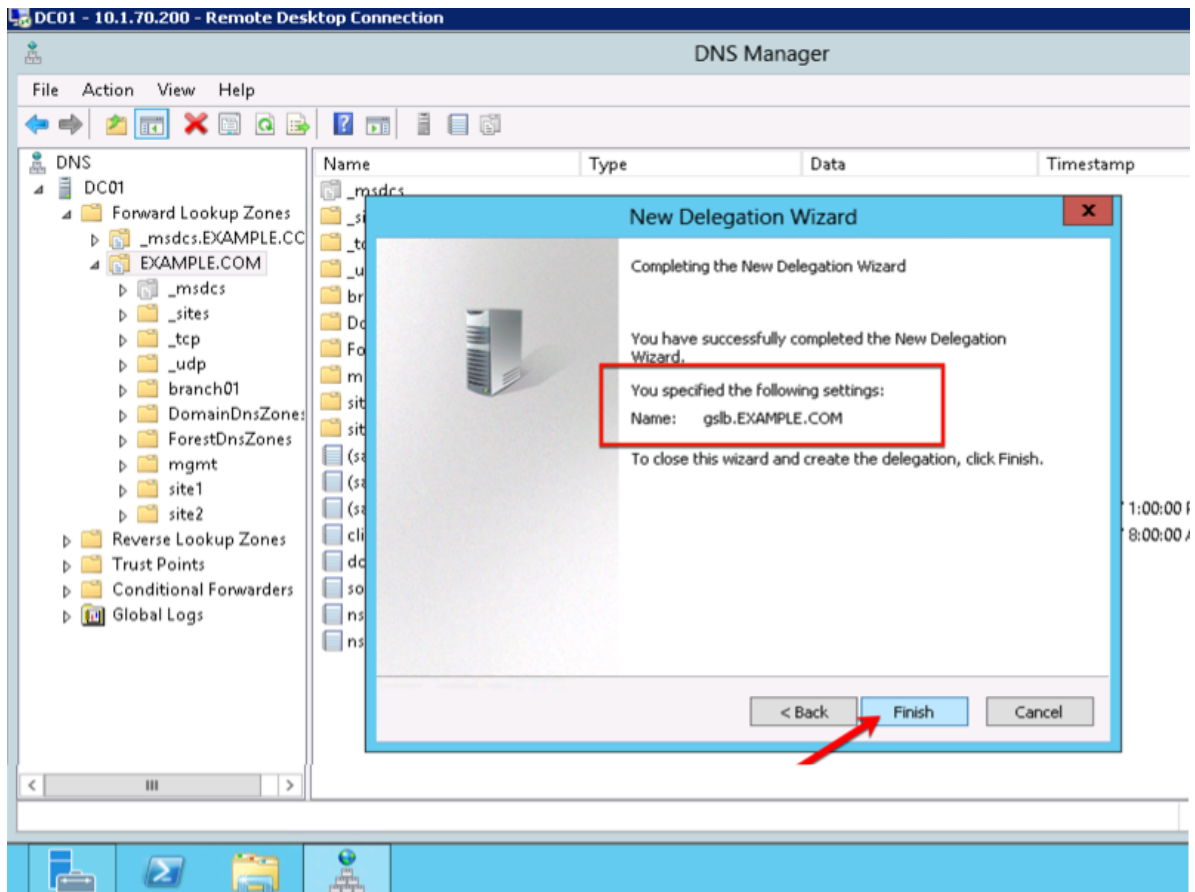


5. Make sure both ns1.example.com and ns2.example.com are added



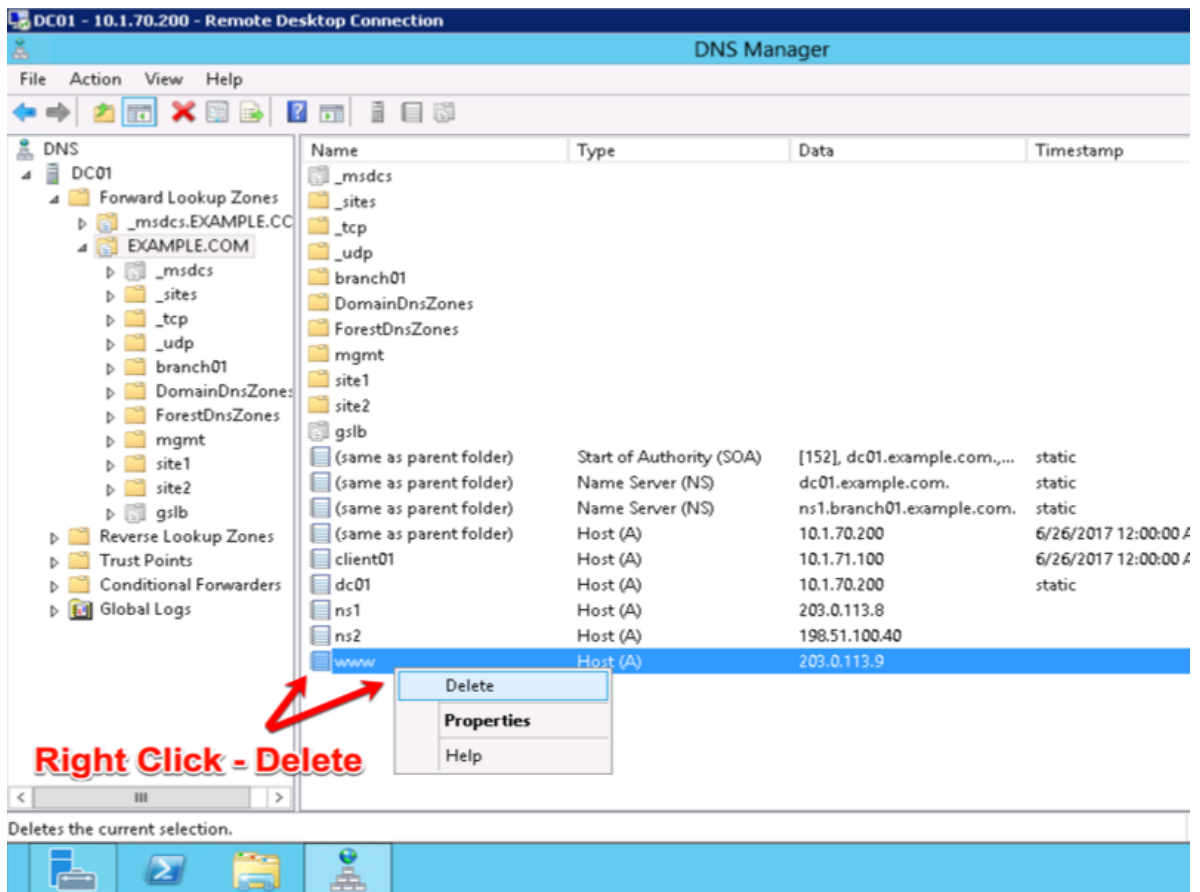


6. Click "Finish"

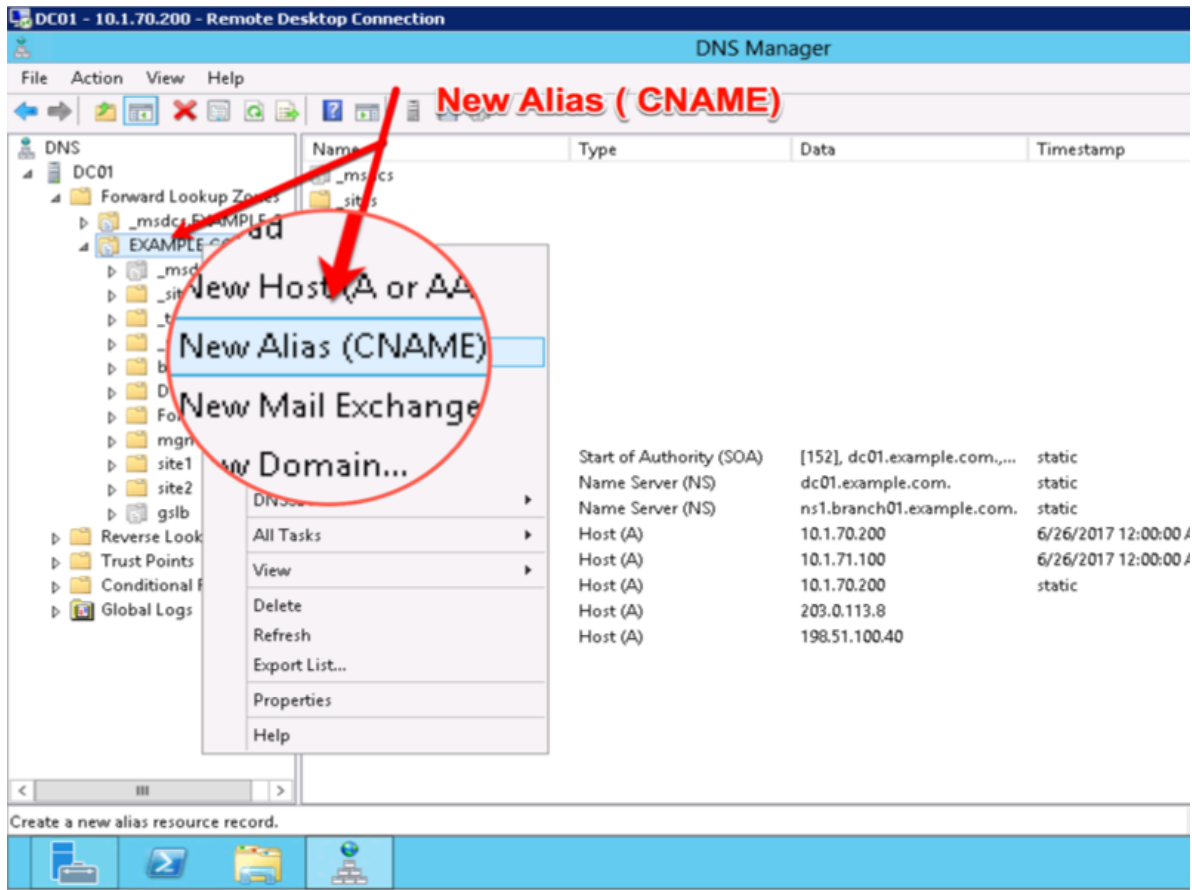


## 2.6.3 CNAME

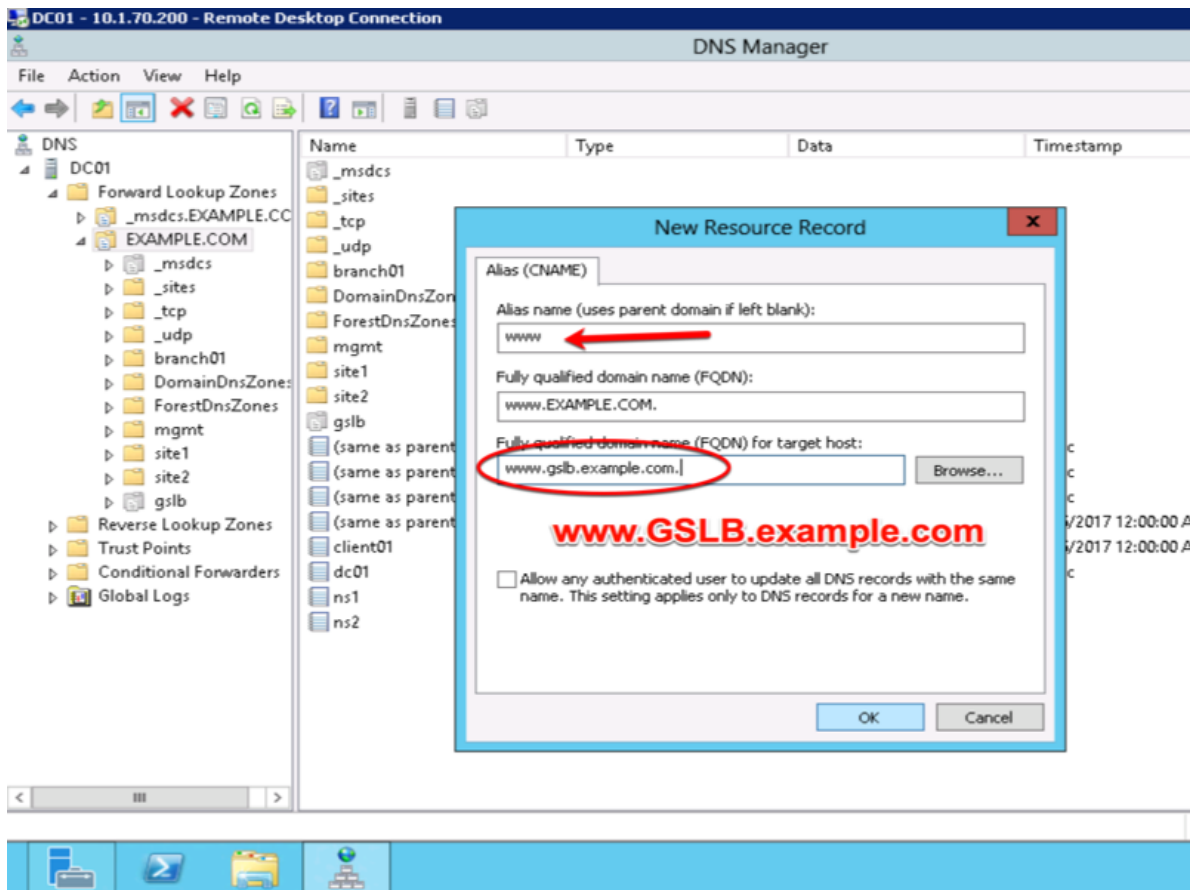
1. Make sure "Forward Lookup Zones" and "EXAMPLE.COM" is expanded. Right click on "www", and select delete.



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

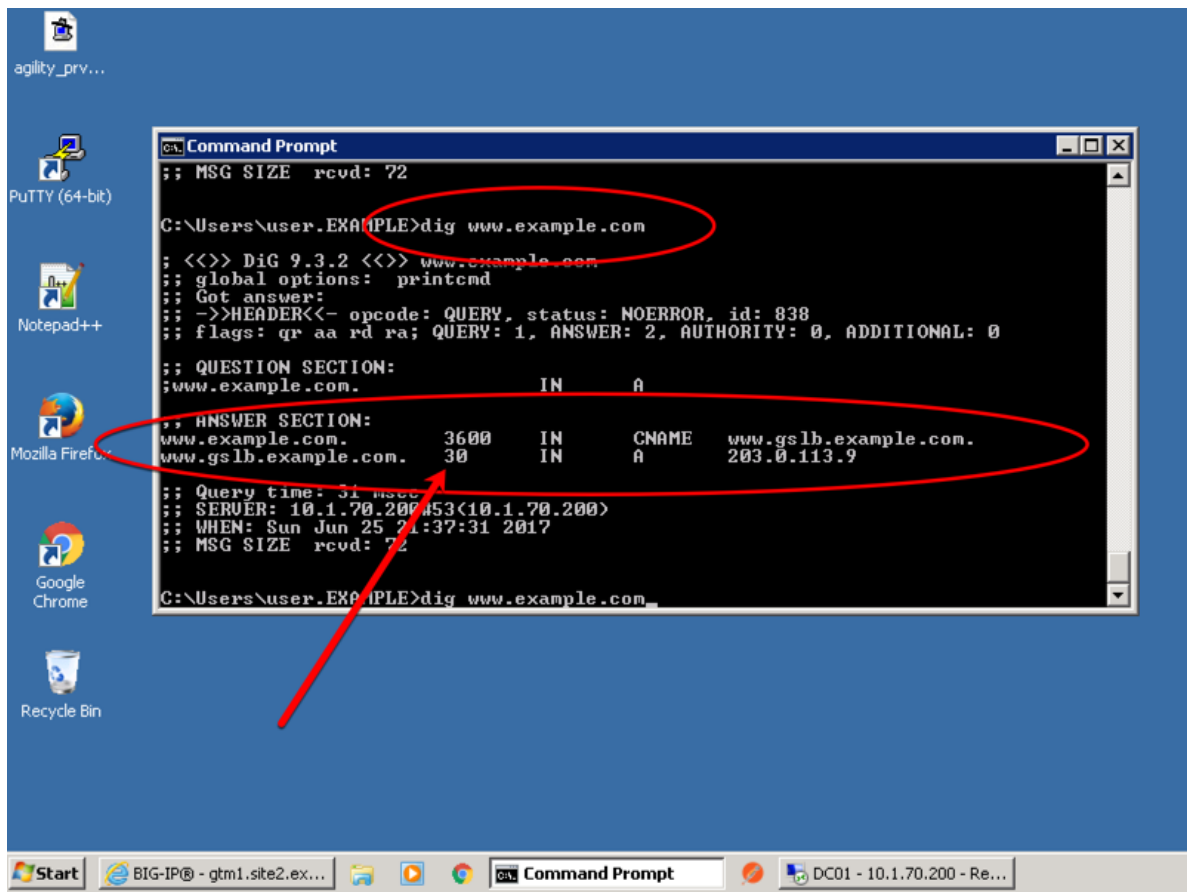


3. Add "www - www.gslb.example.com"



## 2.7 Results

1. From the Workstation command prompt type "dig www.example.com"



2. Observe WIDEIP statistics on gtm1.site1: **Statistics » Module Statistics : DNS : GSLB » Wide IPs : www.gslb.example.com : A**

[https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globalb/stats/wideip/stats\\_detail.jsp?name=%2FCommon%2Fwww.gslb.example.com&type=1&identity=www.gslb.example.com+%3A+A](https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globalb/stats/wideip/stats_detail.jsp?name=%2FCommon%2Fwww.gslb.example.com&type=1&identity=www.gslb.example.com+%3A+A)

Hostname: gtm1.site1.example.com Date: Jul 17, 2017 User: admin  
IP Address: 10.1.10.13 Time: 11:41 AM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

DNS » GSLB : Wide IPs : Wide IP List » Properties : www.gslb.example.com : A

Statistics iRules Pools **Statistics**

General Properties: **Advanced**

Name: www.gslb.example.com  
Partition / Path: Common

**Click Statistics**

DNS

- Delivery
- GSLB**
  - Wide IPs**
    - Wide IP List
    - Statistics**
  - Pools
  - iRules
  - Data Centers
  - Servers
  - Links
  - Prober Pools
  - Monitors
  - Topology
  - Distributed Applications
- Zones
- Caches
- Settings

SSL Orchestrator

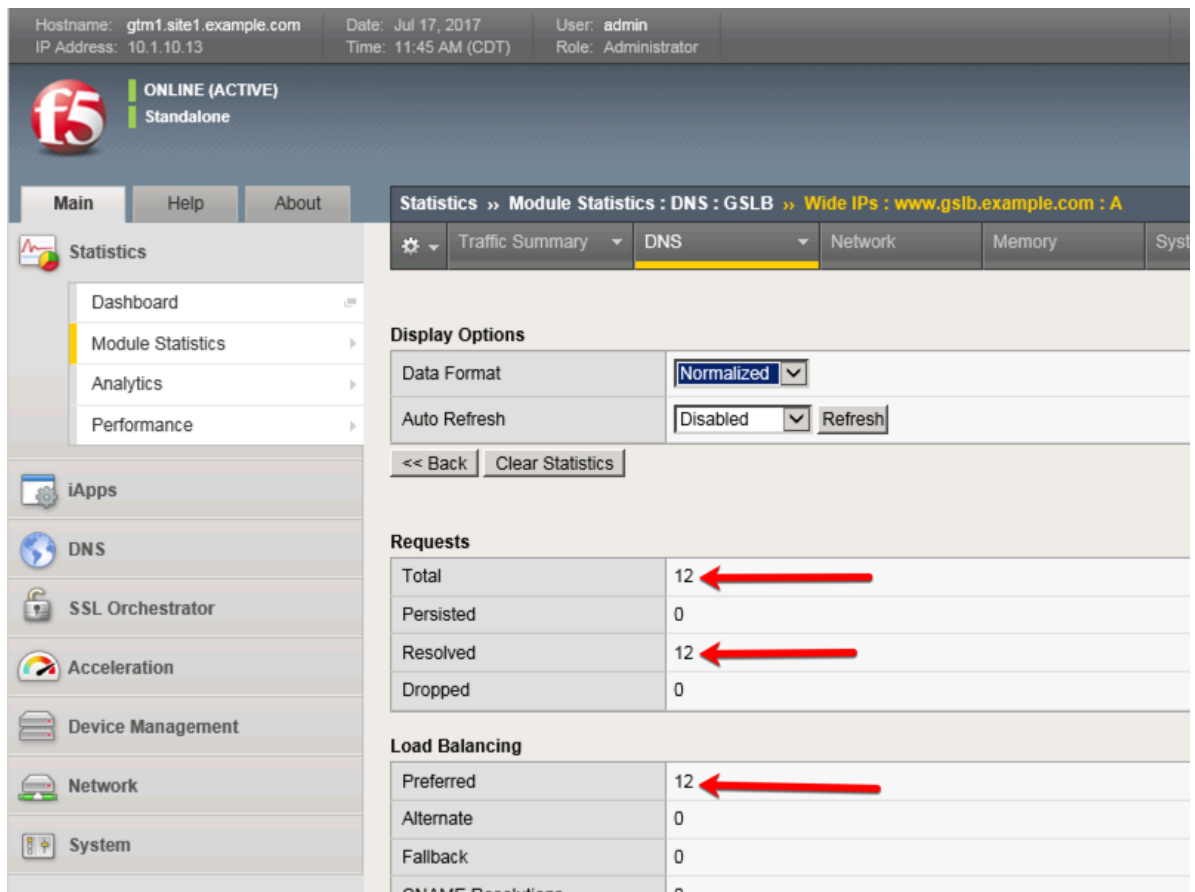
Acceleration

Device Management

Network

System

Alias:   
Add  
Delete  
Available (Enabled) - Available  
Enabled  
Enabled  
Return Code On Failure: Disabled



## TMSH

tmsh show gtm wideip a www.gslb.example.com

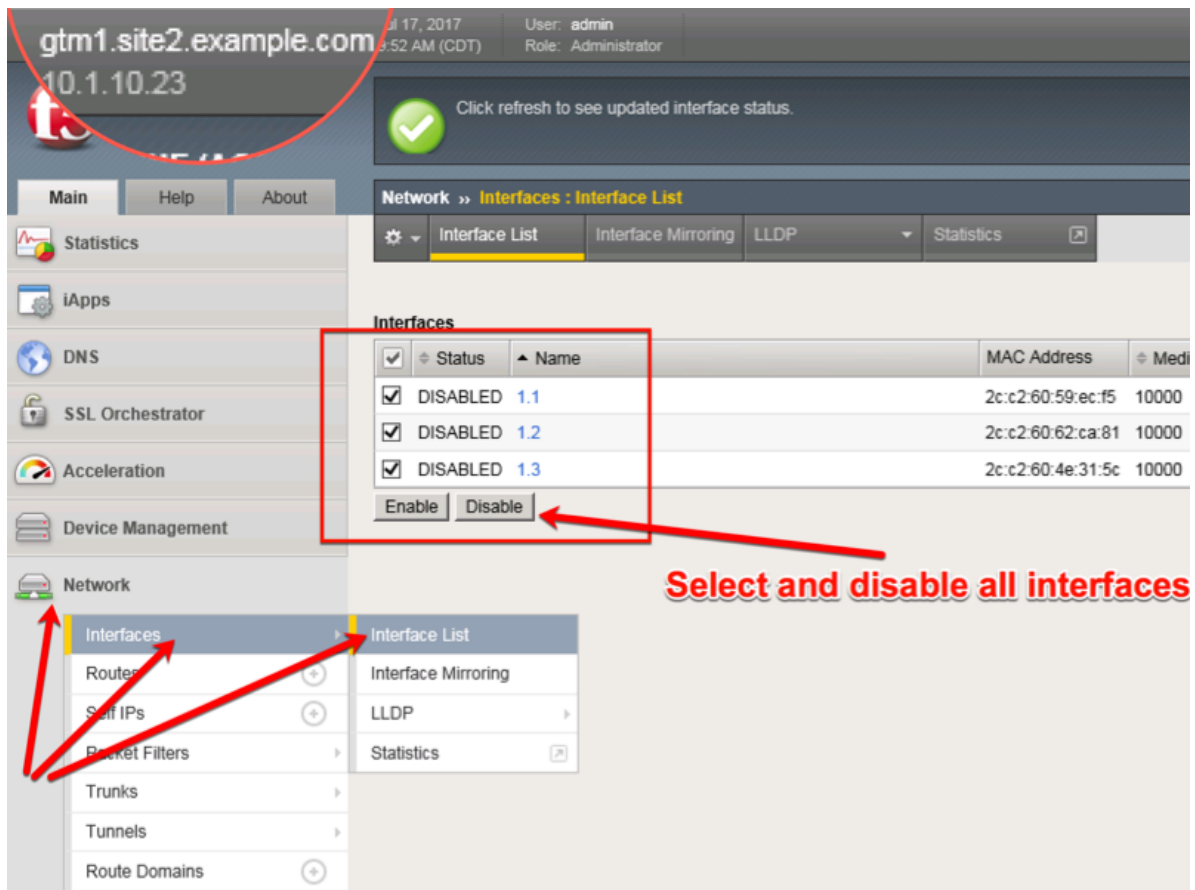
- Observe WIDEIP statistics on gtm1.site2: **Statistics » Module Statistics : DNS : GSLB » Wide IPs : www.gslb.example.com : A**

[https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/globalb/stats/wideip/stats\\_detail.jsp?name=%2FCommon%2Fwww.gslb.example.com&type=1&identity=www.gslb.example.com+%3A+A](https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/globalb/stats/wideip/stats_detail.jsp?name=%2FCommon%2Fwww.gslb.example.com&type=1&identity=www.gslb.example.com+%3A+A)

- Disable physical interfaces on gtm1.site2:

[https://gtm1.site2.example.com/tmui/Control/form?\\_\\_handler=/tmui/locallb/network/interface/list&\\_\\_source=disable&\\_\\_linked=false&\\_\\_fromError=false](https://gtm1.site2.example.com/tmui/Control/form?__handler=/tmui/locallb/network/interface/list&__source=disable&__linked=false&__fromError=false)





TMSH command to run on only gtm1.site2:

#### TMSH

tmsh modify net interface all disabled

5. Refresh statistics on gtm1.site1 and make sure DNS requests are still resolving.

[https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globalb/stats/wideip/stats\\_detail.jsp?name=%2FCommon%2Fwww.gslb.example.com&type=1&identity=www.gslb.example.com+%3A+A](https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globalb/stats/wideip/stats_detail.jsp?name=%2FCommon%2Fwww.gslb.example.com&type=1&identity=www.gslb.example.com+%3A+A)

6. Re-enable interfaces on gtm1.site2, disable interfaces on gtm1.site1. Observe statistics on gtm1.site2 and make sure DNS requests are still resolving.

TMSH command to run on only gtm1.site2:

#### TMSH

tmsh modify net interface all enabled

7. Observe pool statistics on gtm1.site1: **Statistics >> Module Statistics : DNS : GSLB >> Pools : www.example.com\_pool : A**

[https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globalb/stats/pool/stats\\_detail.jsp?name=%2FCommon%2Fwww.example.com\\_pool&pool\\_type=1&identity=www.example.com\\_pool+%3A+A](https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globalb/stats/pool/stats_detail.jsp?name=%2FCommon%2Fwww.example.com_pool&pool_type=1&identity=www.example.com_pool+%3A+A)

Hostname: gtm1.site1.example.com Date: Jul 17, 2017 User: admin  
IP Address: 10.1.10.13 Time: 12:32 PM (CDT) Role: Administrator Partition: Common

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

Statistics » Module Statistics : DNS : GSLB » Pools : www.example.com\_pool : A

Statistics

- Dashboard
- Module Statistics
- Analytics
- Performance

iApps

DNS

SSL Orchestrator

Acceleration

Device Management

Network

System

Display Options

Data Format: Normalized

Auto Refresh: Disabled Refresh

<< Back

Pool Details: "www.example.com\_pool : A"

Status	Pool Member	Server	Virtual Server	Preferred	Weight
●	198.51.100.41:443	site2_ha-pair	/Common/isp2_site2_www.example.com_tcp_https_virtual	43	0
●	203.0.113.9:443	site1_ha-pair	/Common/isp1_site1_www.example.com_tcp_https_virtual	44	0

**TMSH**

```
show gtm pool a www.example.com_pool
```

8. Using Putty, ssh into gtm1.site1 and run the following command to watch logs:

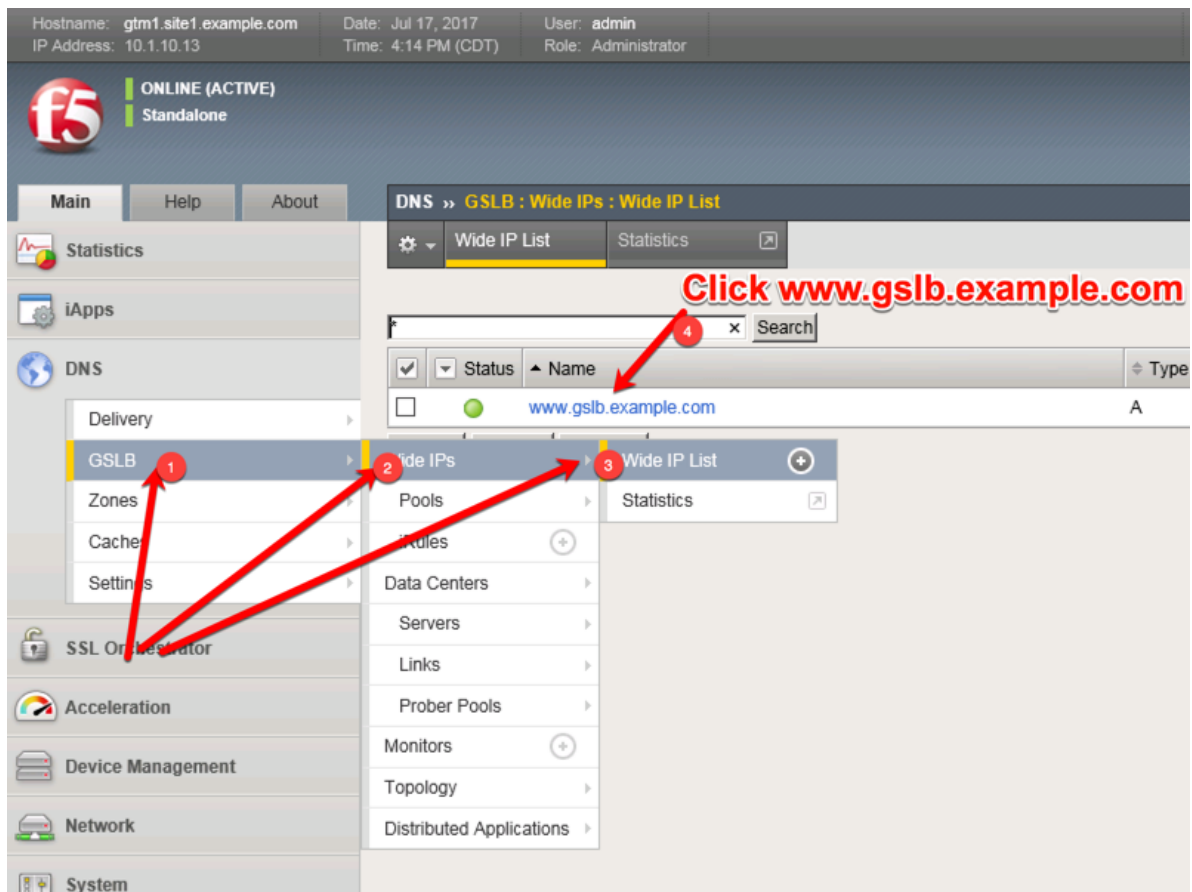
**TMSH**

```
tail -f /var/log/ltm
```

## 2.8 Persistence

Modify the GSLB configuration so that LDNS servers continually receive the same DNS answer.

1. On gtm1.site1 navigate to: **DNS » GSLB : Pools : Pool List » Members : www.example.com\_pool**



<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/wideip/list.jsp>

2. Click into the "Pools" tab:

Hostname: gtm1.site1.example.com Date: Jul 17, 2017 User: admin  
IP Address: 10.1.10.13 Time: 4:18 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

DNS » GSLB : Wide IPs : Wide IP List » Properties : www.gslb.example.com : A

Statistics iApps DNS SSL Orchestrator Acceleration Device Management Network System

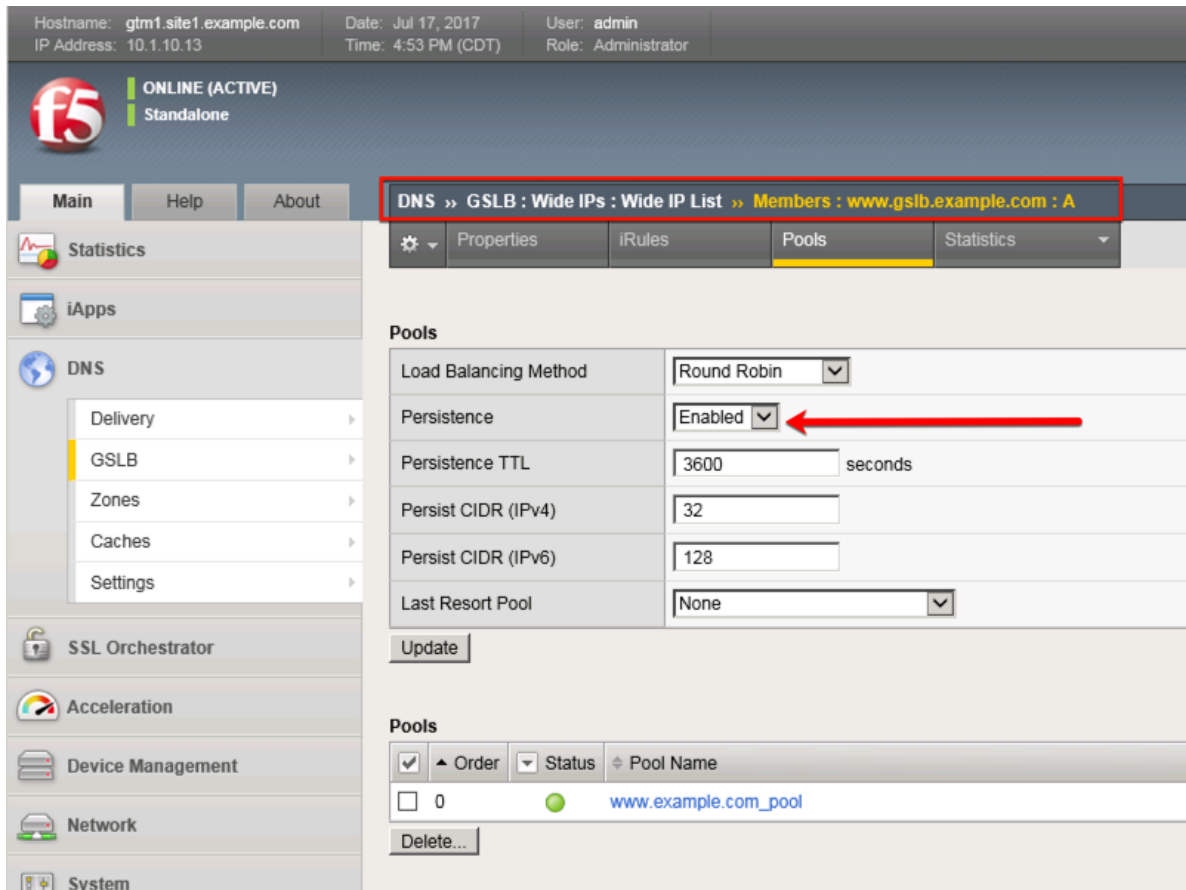
General Properties: **Advanced**

Name	www.gslb.example.com
Partition / Path	Common
Type	A
Description	
Alias List	Alias: <input type="text"/> Add <input type="text"/> Delete
Availability	Available (Enabled) - Available
State	Enabled
Minimal Response	Enabled
Return Code On Failure	Disabled

**Click "Pools"**

<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globalb/wideip/pools.jsp?name=%2FCommon%2Fwww.gslb.example.com&type=1&identity=www.gslb.example.com>

### 3. Enable Persistence



### TMSH

tmsh modify gtm wideip a www.gslb.example.com persistence enabled

#### 4. View Persistence Records

### TMSH

tmsh show gtm persist

## 2.9 LB Methods

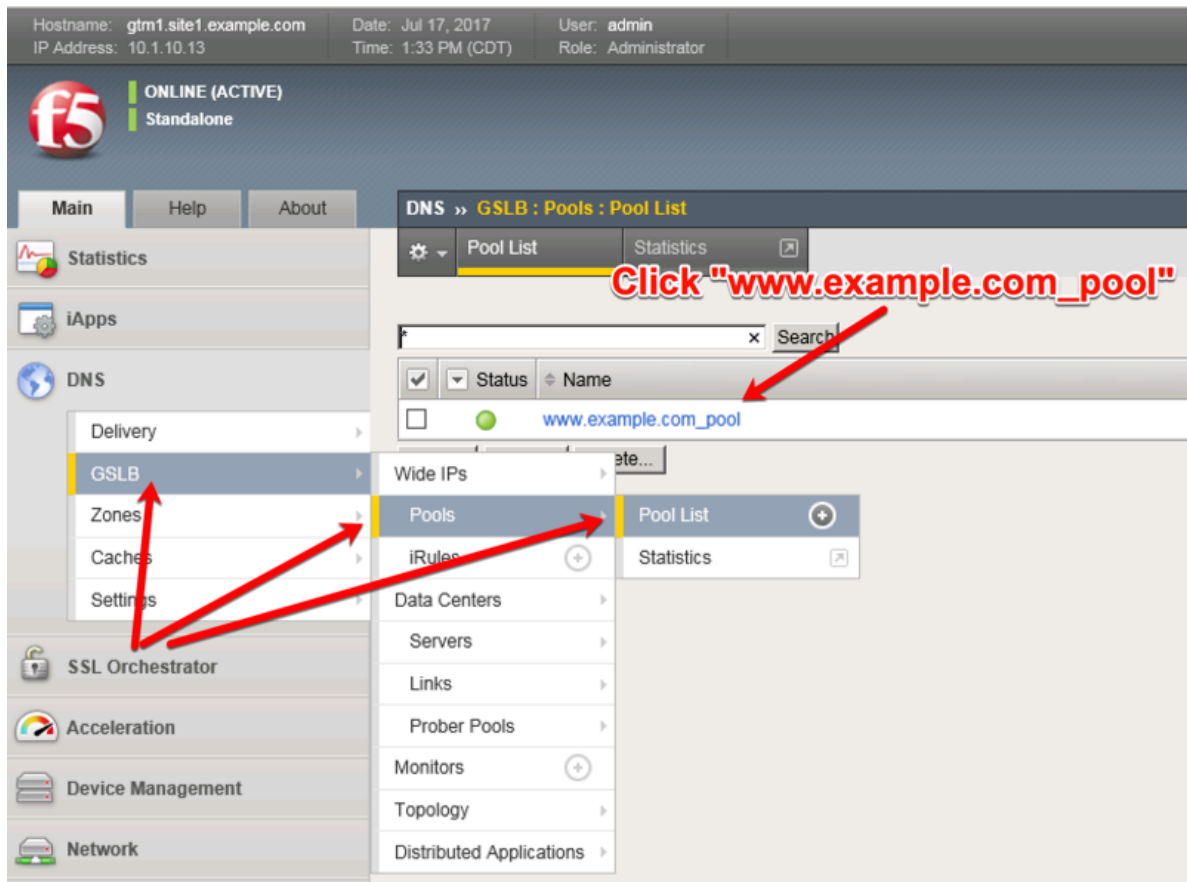
Modify the GSLB configuration so that site2 is a standby DR site.

Introduce a network problem that causes the isp1 link monitor to fail.

An ISP network outage can automatically cause DR activation.

1. On gtm1.site1 navigate to: **DNS >> GSLB : Pools : Pool List >> Members : www.example.com\_pool**

[https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globalb/pool/members.jsp?name=%2FCommon%2Fwww.example.com\\_pool&pool\\_type=1&identity=www.example.com\\_pool](https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globalb/pool/members.jsp?name=%2FCommon%2Fwww.example.com_pool&pool_type=1&identity=www.example.com_pool)



2. Modify the "Load Balancing Method" -> "Preferred" to "Global Availability"

Hostname: gtm1.site1.example.com Date: Jul 17, 2017 User: admin  
IP Address: 10.1.10.13 Time: 1:51 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

DNS » GSLB : Pools : Pool List » Members : www.example.com\_pool : A

Statistics iApps DNS

Delivery  
GSLB  
Zones  
Caches  
Settings

SSL Orchestrator Acceleration Device Management Network

Properties Members Statistics

**Click "Members"**

**Load Balancing**

Load Balancing Method Preferred: Global Availability  
Alternate: Round Robin  
Fallback: Return to DNS  
Fallback IP: 0.0.0.0

Update

**Members**

<input checked="" type="checkbox"/>	Member Order	Status	Member	Member Address	Partition	Mem
<input type="checkbox"/>	0	●	/Common/site1_ha-pair	203.0.113.9	Common	/Cor
<input type="checkbox"/>	1	●	/Common/site2_ha-pair	198.51.100.41	Common	/Cor

Enable Disable Remove

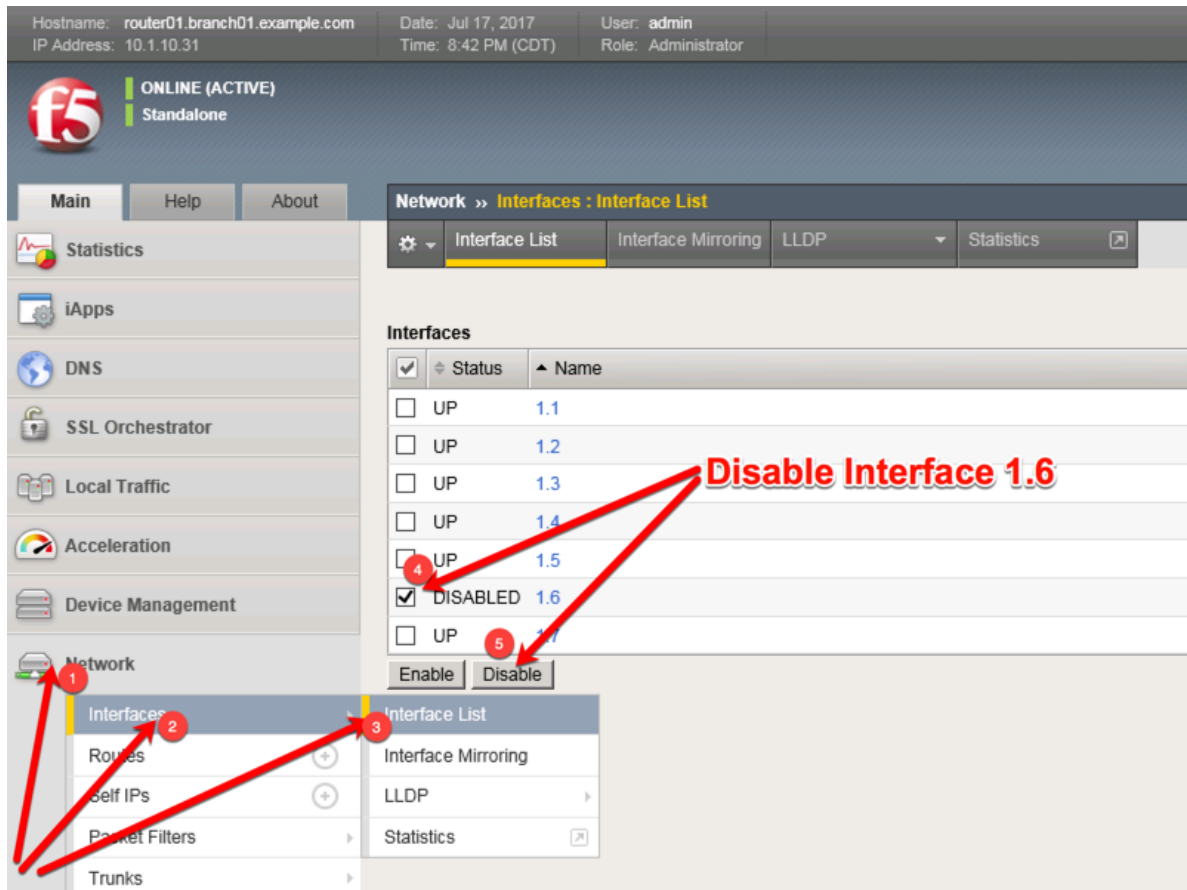
## TMSH

tmsh modify gtm pool a www.example.com\_pool load-balancing-mode global-availability

- Introduce a network problem in the ISP at site1

Log into the router and disable interface 1.6 connecting ISP1 to site1

<https://router01.branch01.example.com/tmui/Control/jspmap/tmui/localb/network/interface/list.jsp>



TMSH command to run on the router01 to simulate an ISP failure

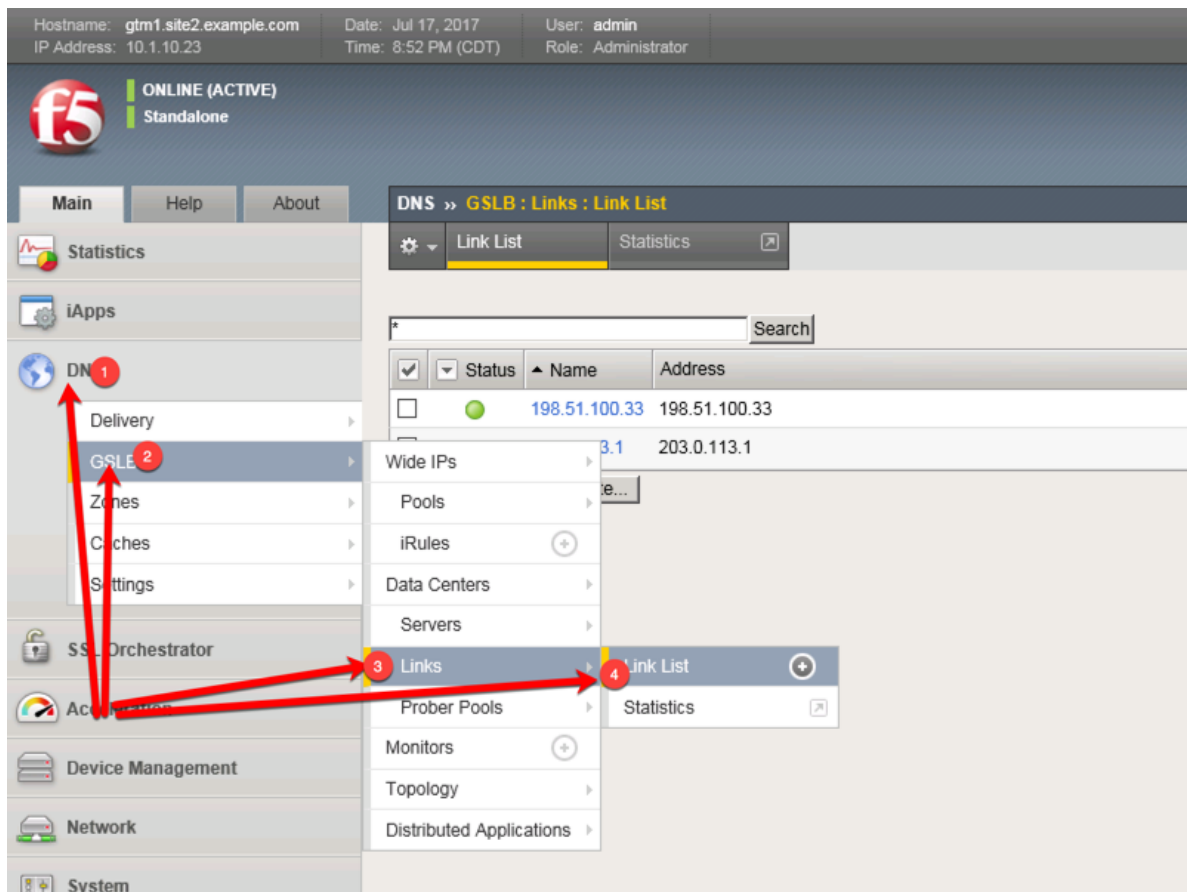
### TMSH

tmsh modify interface 1.6 disabled

#### 4. View the effect

Log into gtm1.site2 and observe the status of "Link" objects:





[https://gtm1.site2.example.com/tmui/Control/jspmap/xsl/gtm\\_link/list](https://gtm1.site2.example.com/tmui/Control/jspmap/xsl/gtm_link/list)

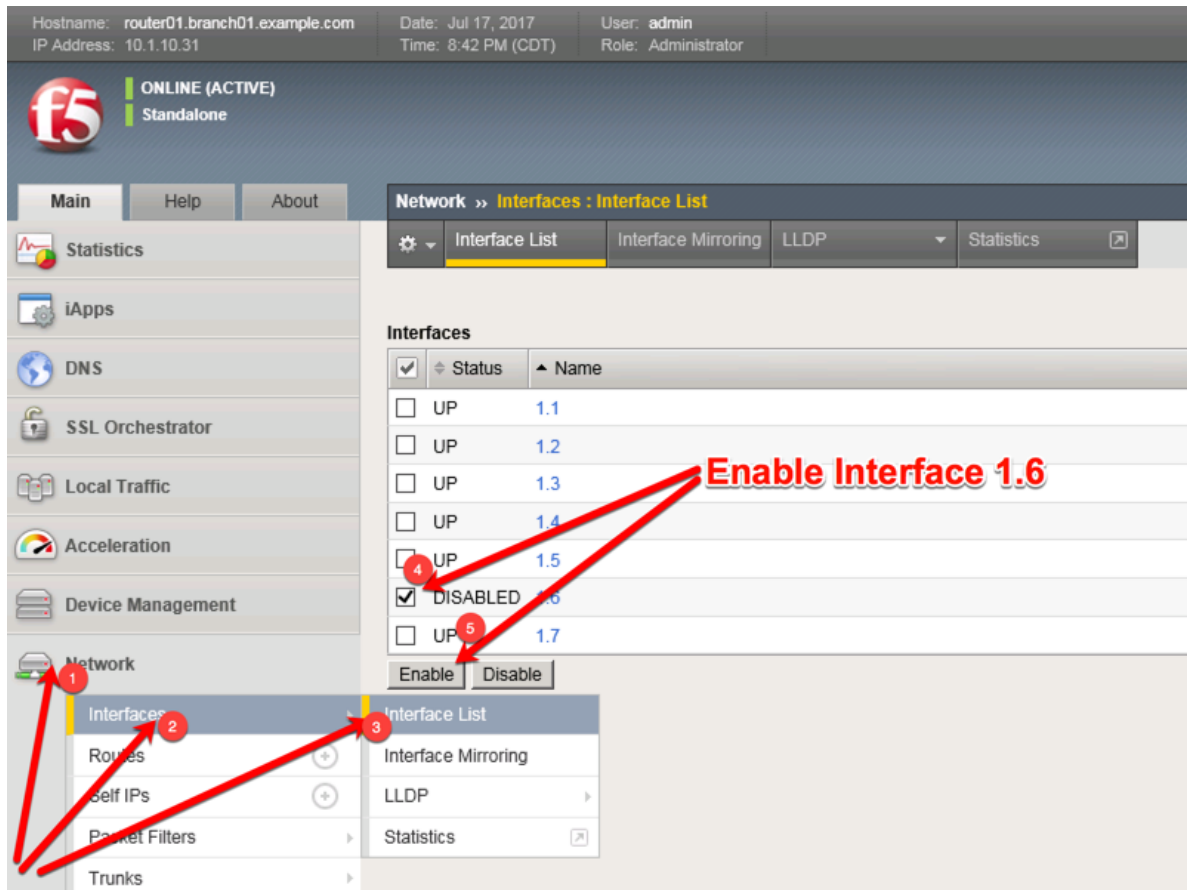
## TMSH

tmsh show gtm link

### 5. Set the site1 isp link back up

Log into the router and enable the interface 1.6 connecting ISP1 to site1

<https://router01.branch01.example.com/tmui/Control/jspmap/tmui/locallb/network/interface/list.jsp>



### TMSH

tmsh modify interface 1.6 enabled

Note: Even though you re-enabled the primary site1, a persistence record from the previous lab is still in place.

## Class 2 - Next Generation DNS Services

The lab section for this class will cover the following topics:

1. Transparent Cache
2. DNS Express with a Hidden Master
3. DNSSEC
4. Validating Resolver
5. RPZ
6. URL Categorization

The lab environment consists of BIG-IPs along with Linux hosts interacting with DNS Servers.

The F5 device is directly connected to the internet.

Below is a lab diagram and connectivity information:



### 3.1 Lab Components

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

Component	VLAN/IP Address(es)	Credentials
BIG-IP DNS	<ul style="list-style-type: none"> <li>• <b>Management:</b> 10.1.1.4</li> <li>• <b>External Self:</b> 10.1.10.6</li> <li>• <b>Internal Self:</b> 10.1.20.6</li> </ul>	admin/agility2020
Ubuntu Desktop	<ul style="list-style-type: none"> <li>• <b>Management:</b> 10.1.1.6</li> <li>• <b>External:</b> 10.1.10.4</li> </ul>	ubuntu/agility2020
Ubuntu server	<ul style="list-style-type: none"> <li>• <b>Management:</b> 10.1.1.5</li> <li>• <b>Internal:</b> 10.1.20.4</li> </ul>	ubuntu/agility2020

Follow these steps to get your lab started:

Follow the instructions in your lab email to log into the F5 Unified Demo Framework (UDF) where your lab is hosted.

The UDF provides both ssh, TMUI (Web Interface) and a Web Shell access to each component in the lab. No RDP is required for this lab.

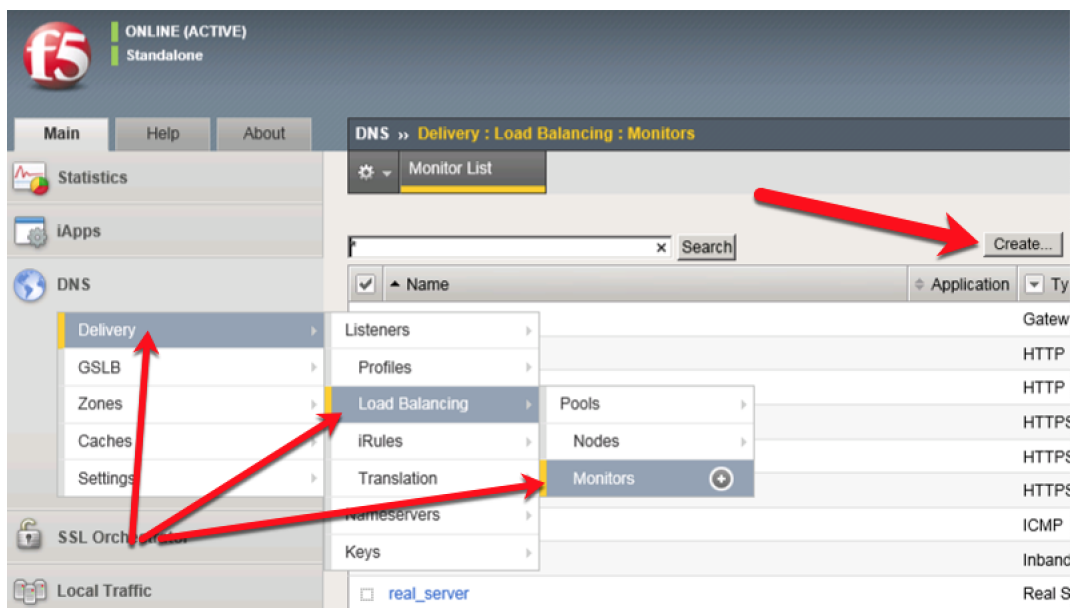
For simplicity, its suggested to use the Web Shell in a browser and not the native SSH interface as the latter requires an additional step of setting up ssh keys.

### 3.1.1 Transparent Cache

#### Monitors

A DNS application specific monitor should be used to monitor pool members.

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



Create a new monitor according to the following settings:

Setting	Value
Name	example.com_dns_monitor
Type	DNS
Query Name	www.example.com

**General Properties**

Name	example.com_dns_monitor
Description	
Type	DNS
Parent Monitor	dns

**Configuration:** Advanced

Interval	5 seconds
Up Interval	Disabled
Time Until Up	0 seconds
Timeout	16 seconds
Manual Resume	<input type="radio"/> Yes <input checked="" type="radio"/> No
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alias Address	* All Addresses
Alias Service Port	* * All Ports
Query Name	www.example.com
Query Type	a
Answer Section Contains	Query Type
Accept RCODE	No Error
Receive String	
Adaptive	<input type="checkbox"/> Enabled

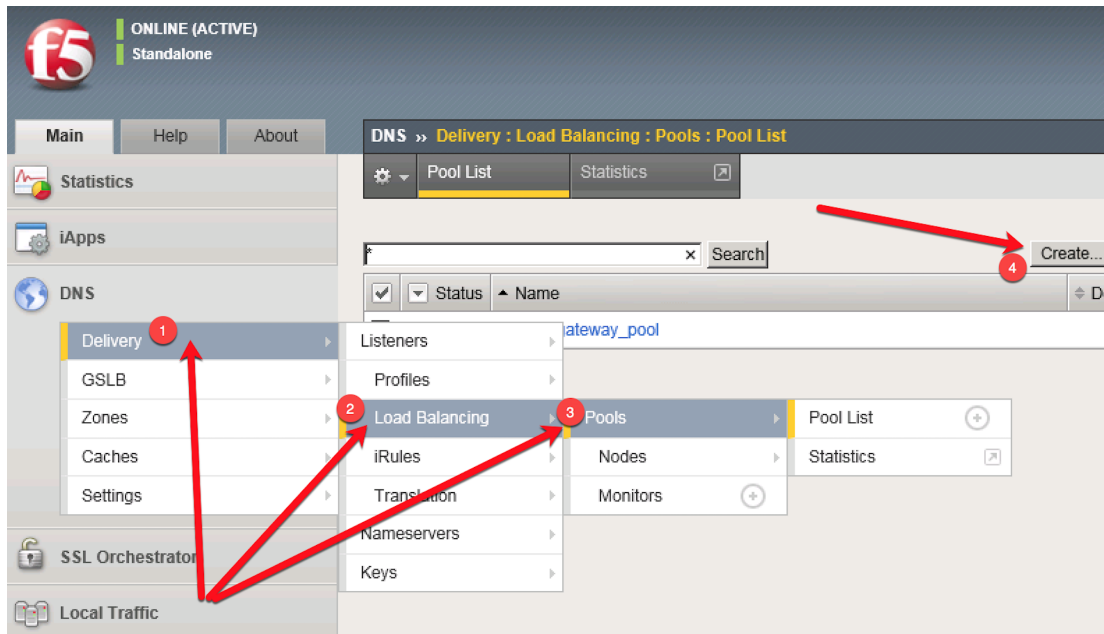
**TMSH**

```
tmsh create ltm monitor dns example.com_dns_monitor defaults-from dns qname www.example.com
```

**Load Balancing**

Create a new pool for back end load balancing of DNS queries. The Ubuntu server will be the single pool member.

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



Create a pool according to the following table:

Setting	Value
Name	dns_pool
Health Monitors	example.com_dns_monitor
Node Name	dns01_node
Address	10.1.20.4
Service Port	53

DNS » Delivery : Load Balancing : Pools : Pool List » **New Pool...**

**Configuration:** Basic ▾

<b>Name</b>	dns_pool
<b>Description</b>	
<b>Health Monitors</b>	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p style="text-align: center;">Active</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">/Common example.com_dns_monitor</div> <div style="border: 1px solid #ccc; height: 30px; margin-bottom: 5px;"></div> </div> <div style="width: 10%; text-align: center;"> &lt;&lt;  &gt;&gt; </div> <div style="width: 45%;"> <p style="text-align: center;">Available</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">/Common gateway_icmp http http_head_f5 https</div> </div> </div>

**Resources**

<b>Load Balancing Method</b>	Round Robin ▾										
<b>Priority Group Activation</b>	Disabled ▾										
<b>New Members</b>	<div style="text-align: center;"> <input checked="" type="radio"/> New Node   <input type="radio"/> New FQDN Node </div> <div style="margin-top: 5px;"> Node Name: dns01_node (Optional)  Address: 10.1.20.4  Service Port: 53   <span>Select... ▾</span> </div> <div style="text-align: center; margin-top: 5px;"> <span>Add</span> </div> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th>Node Name</th> <th>Address/FQDN</th> <th>Service Port</th> <th>Auto Populate</th> <th>Priority</th> </tr> </thead> <tbody> <tr> <td>dns01_node</td> <td>10.1.20.4</td> <td>53</td> <td></td> <td>0</td> </tr> </tbody> </table> <div style="text-align: center; margin-top: 5px;"> <span>Edit</span>   <span>Delete</span> </div>	Node Name	Address/FQDN	Service Port	Auto Populate	Priority	dns01_node	10.1.20.4	53		0
Node Name	Address/FQDN	Service Port	Auto Populate	Priority							
dns01_node	10.1.20.4	53		0							

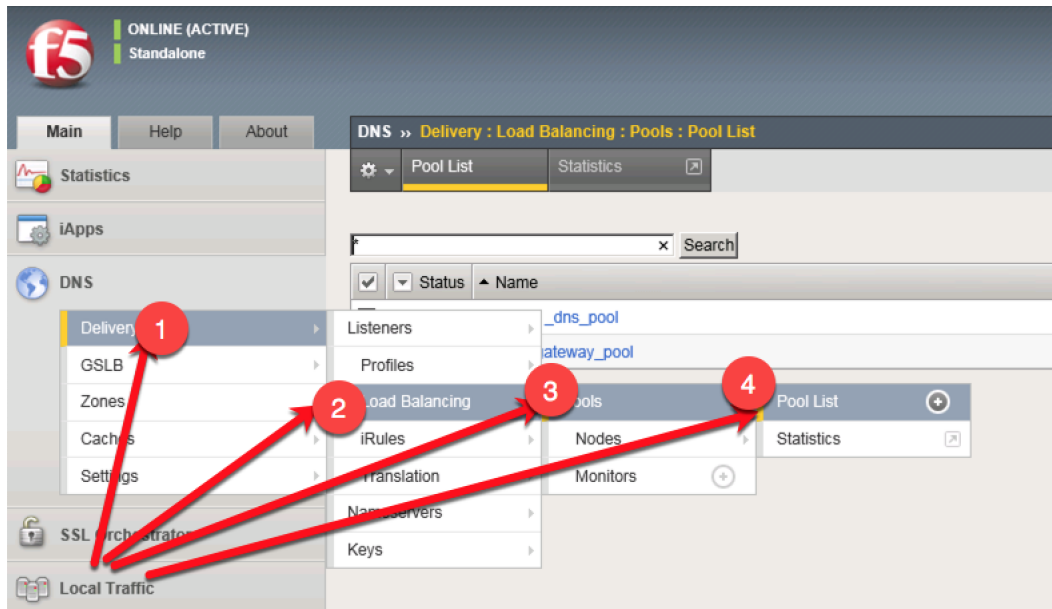
Cancel
Repeat
Finished

**TMSH**

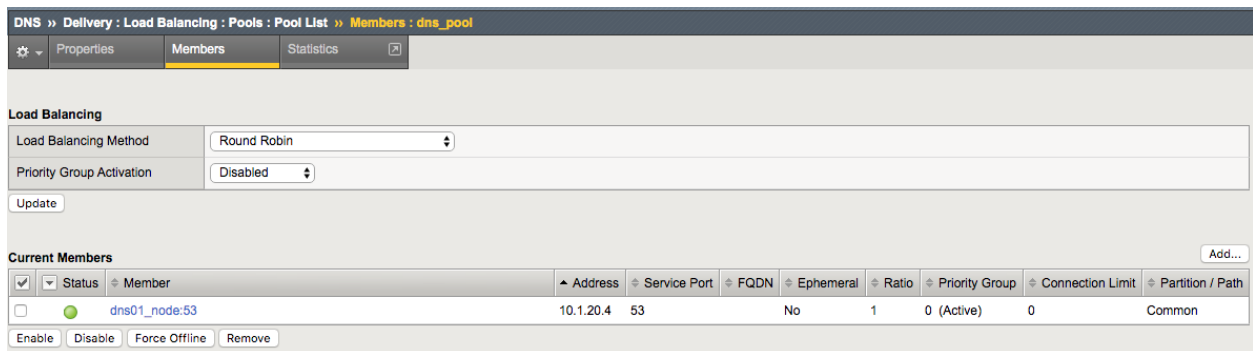
```
tmsh create ltm pool dns_pool members add { dns01_node:53 { address 10.1.20.4 } } monitor example.com_dns_monitor
```

**Results**

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



1. Click to select *dns\_pool*, and then select *Members*
2. Observe the health status of the pool (green is good)



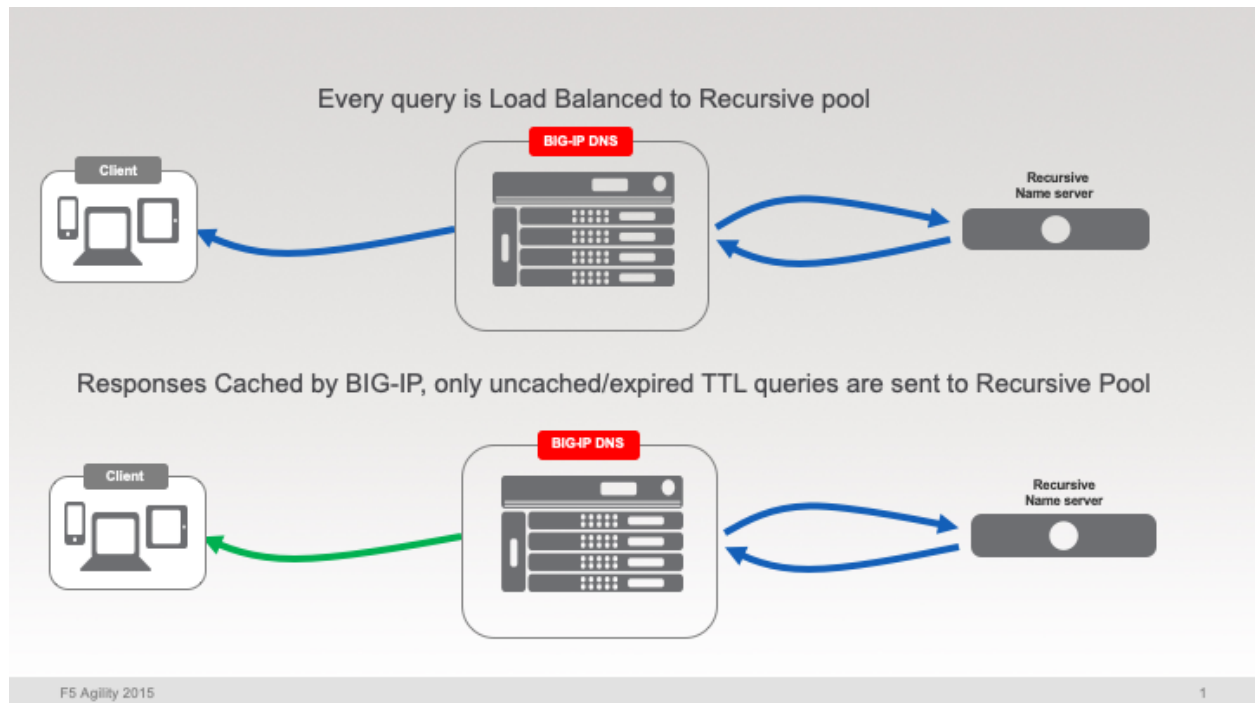
## TMSH

tmsh show ltm pool dns\_pool detail

In this module we will implement all the configuration objects required for a transparent DNS cache on the BIG-IP.

Enabling a transparent cache offloads the back end DNS servers from responding to every query which frees resources on the servers.



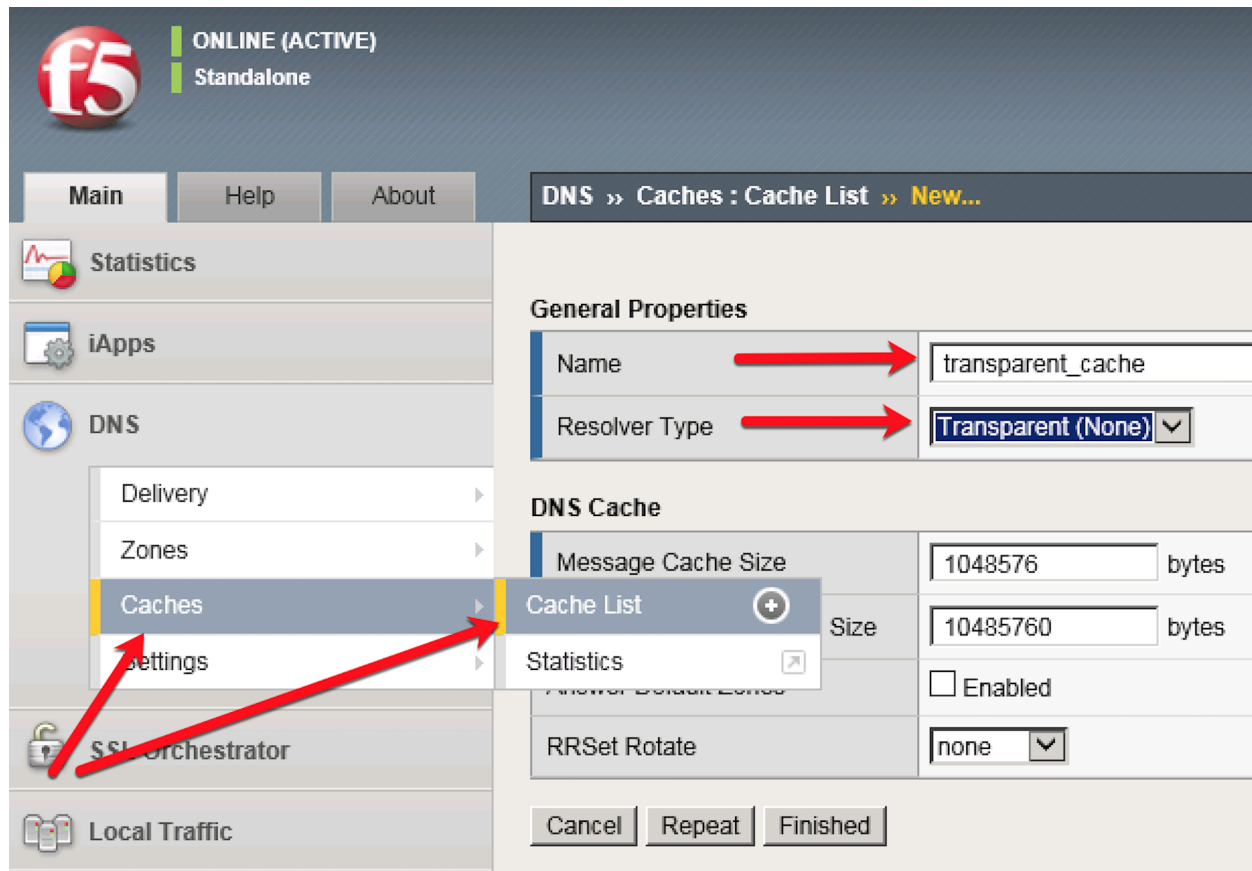


Log into *BIG-IP DNS* using either the TMUI or webshell interface with credentials `u:admin p:agility2020`

Navigate to **DNS » Caches » Cache List**

then click the *Create* button to create a transparent cache with the following settings:

Setting	Value
Name	transparent_cache
Resolver Type	Transparent



## TMSH

```
tmsh create ltm dns cache transparent transparent_cache
```

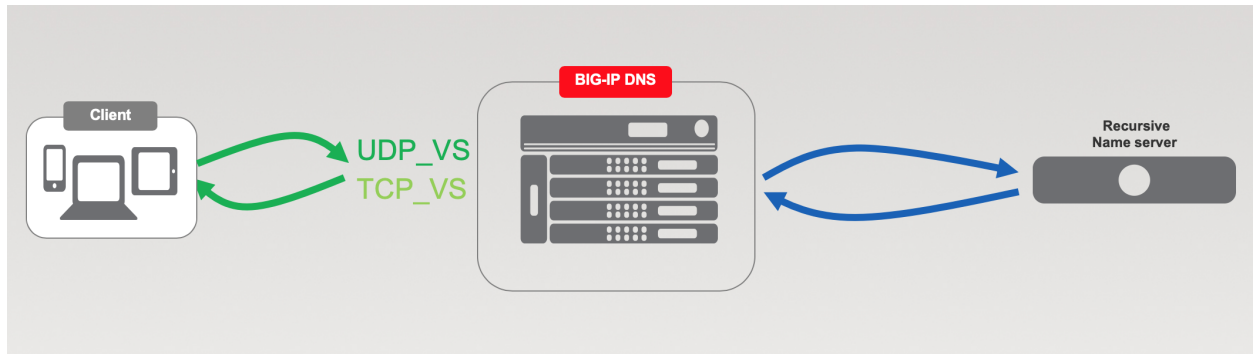
### 3.1.2 Listeners

A Listener object is synonymous with a virtual server. In the DNS Delivery interface on a BIG-IP, Listeners are configured to process DNS traffic.

We will be creating both TCP and UDP based listeners as remember DNS can use both TCP and UDP!

BIG-IP can be configured for multiple functions from the Listener, starting with simple load balancing, transparent or full caching, along with optional security functions.

After this module, we will have enabled the BIG-IP to process and cache DNS requests.



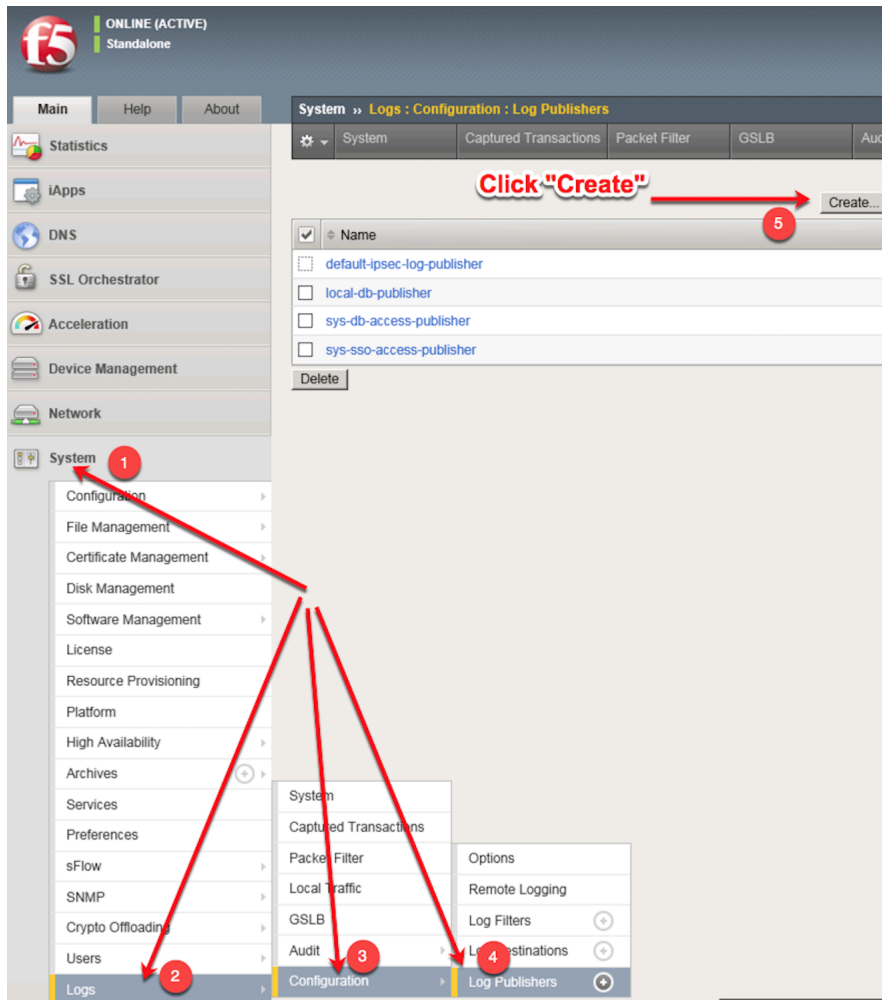
## Log Profile

In order to Log DNS queries, responses, or both, a logging profile must be created. The log profile specifies both the formatting and destination of the log messages which is typically off the BIG-IP using High Speed Logging (HSL).

Normally due to log volume, DNS logs would be sent off the BIG-IP, but for the purpose of the lab we will use a local syslog destination to easily see log messages.

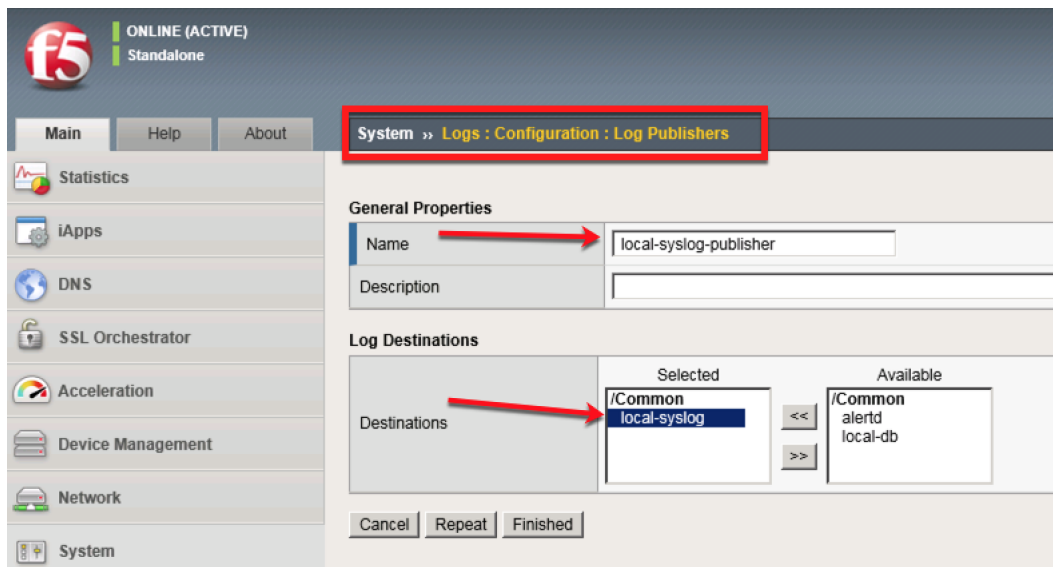
1. Create a “Log Publisher” for local syslog.

Navigate to: **System » Logs : Configuration : Log Publishers**



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

Setting	Value
Name	local-syslog-publisher
Destinations	local-syslog

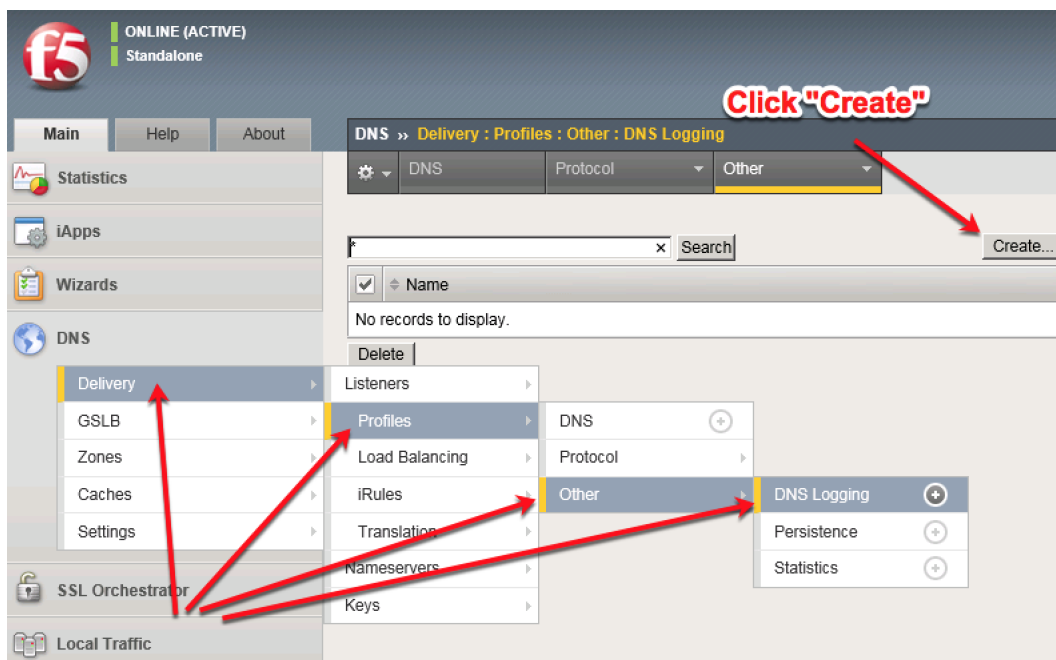


## TMSH

```
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**



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

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

ONLINE (ACTIVE)  
Standalone

Main Help About

**DNS >> Delivery : Profiles : Other : DNS Logging >> New...**

Statistics  
iApps  
Wizards  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Local Traffic  
Traffic Intelligence  
Acceleration

**General Properties**

Name: example\_dns\_logging\_profile  
Description:

**Configuration**

Log Publisher: local-syslog-publisher  
Log Queries: ☒ Enabled  
Log Responses: ☒ Enabled

**Log Fields**

Include Complete Answer: ☒ Enabled  
Include Query ID: ☒ Enabled  
Include Source: ☒ Enabled  
Include Timestamp: ☒ Enabled  
Include View: ☒ Enabled

Cancel Repeat Finished

### TMSH

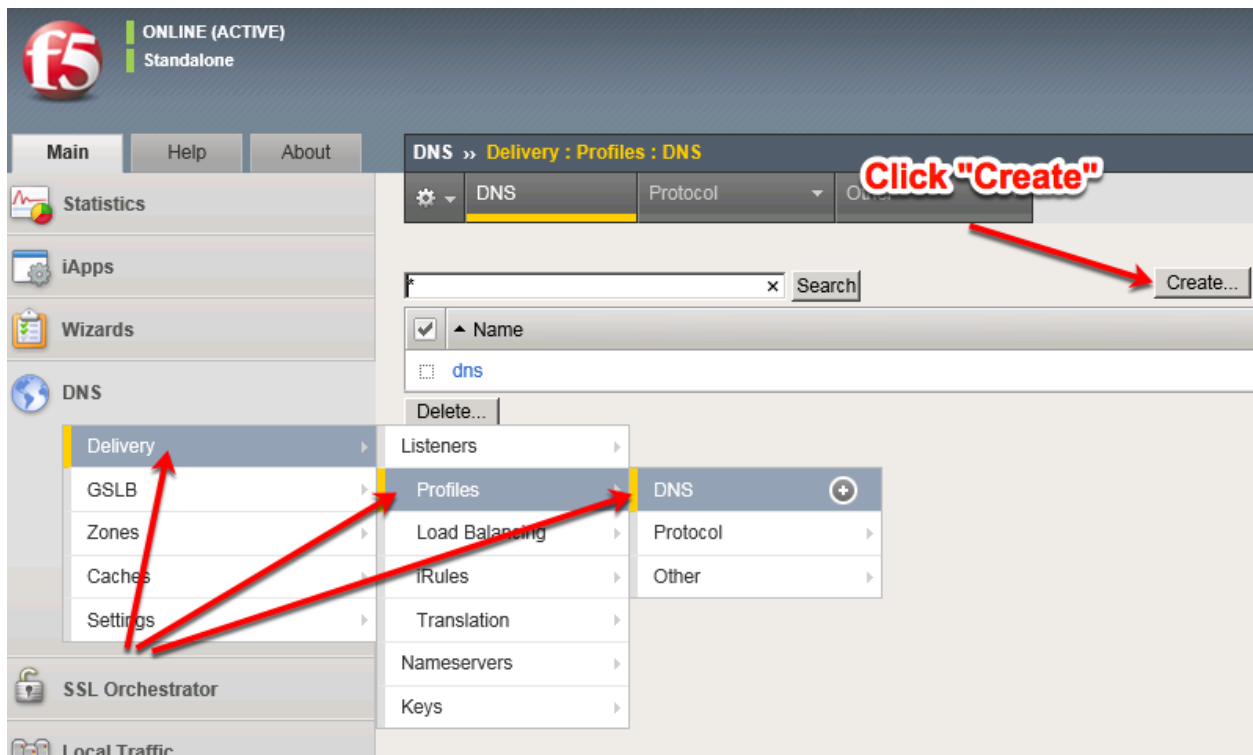
```
tmsh create ltm profile dns-logging example_dns_logging_profile enable-response-logging yes
include-query-id yes log-publisher local-syslog-publisher
```

### DNS Profile

The DNS profile unlocks all BIG-IP features by making the BIG-IP fully aware of DNS as a protocol.

Without a DNS profile applied to a listener, the TMOS does not parse DNS requests and load balance UDP/TCP packets.

Navigate to: **DNS >> Delivery : Profiles : DNS**



Create a DNS profile as shown in the table below. Check boxes on the right to enable editing and overriding default properties.

*Note: AVR sampling in production should be a ratio of queries so as not to overload local database.*

Setting	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 Date: Jul 25, 2017 User: admin Partition: Common Log out  
IP Address: 10.1.10.31 Time: 11:40 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About **DNS » Delivery : Profiles : DNS » New DNS Profile...**

Statistics  
iApps  
Wizards  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Local Traffic  
Traffic Intelligence  
Acceleration  
Access  
Device Management  
Network  
System

**General Properties**

Name example.com\_dns  
Parent Profile dns

**Denial of Service Protection** Custom ☐

Rapid Response Mode Disabled  
Rapid Response Last Action Drop

**Hardware Acceleration**

Protocol Validation Disabled  
Response Cache Disabled

**DNS Features**

DNSSEC Enabled  
GSLB Enabled  
DNS Express Enabled  
DNS Cache Enabled  
DNS Cache Name transparent\_cache  
DNS IPv6 to IPv4 Disabled  
Unhandled Query Actions Allow  
Use BIND Server on BIG-IP Disabled

**DNS Traffic**

Zone Transfer Disabled  
DNS Security Disabled  
DNS Security Profile Name Select...  
Process Recursion Desired Enabled

**Logging and Reporting**

Logging Enabled  
Logging Profile example\_dns\_logging\_profile  
AVR Statistics Sample Rate ☒ Enabled 1/ 1 queries sampled

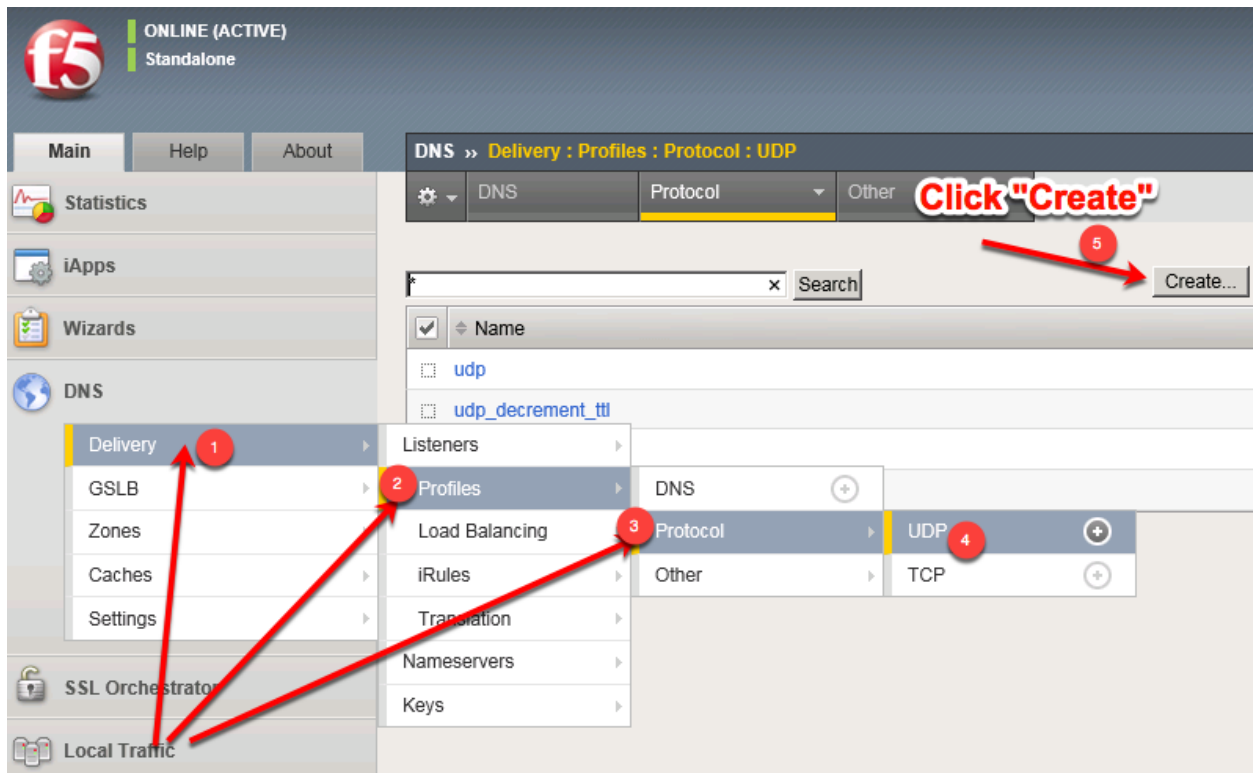


```
tmsh create ltm profile dns example.com_dns_profile { avr-dnsstat-sample-rate 1 cache transparent_cache
defaults-from dns enable-cache yes enable-logging yes log-profile example_dns_logging_profile use-local-
bind no }
```

## UDP Profile

A UDP profile is a protocol profile that controls the way BIG-IP processes UDP traffic. With DNS, custom UDP profiles are often used to set low idle times so as not to fill the connection table as DNS tends to be a lot of short lived connections.

Navigate to: **DNS » Delivery : Profiles : Protocol : UDP**



Create a UDP profile as shown in the following table. By inheriting from *udp\_gtm\_dns* profile, notice the idle timeout setting.

Setting	Value
Name	example.com_udp-dns_profile
Parent Profile	udp_gtm_dns

ONLINE (ACTIVE)  
Standalone

Main Help About

DNS >> Delivery : Profiles : Protocol : UDP >> New UDP Profile...

Statistics  
iApps  
Wizards  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Local Traffic  
Traffic Intelligence

**General Properties**

Name example.com\_udp-  
Parent Profile udp\_gtm\_dns

**Settings**

Proxy Maximum Segment ☐  
Idle Timeout Specify... 5 seconds  
IP ToS Specify... 0  
Link QoS Specify... 0  
Datagram LB ☒ Enabled  
Allow No Payload ☐  
TTL Mode Proxy  
Don't Fragment Mode PMTU

Cancel Repeat Finished

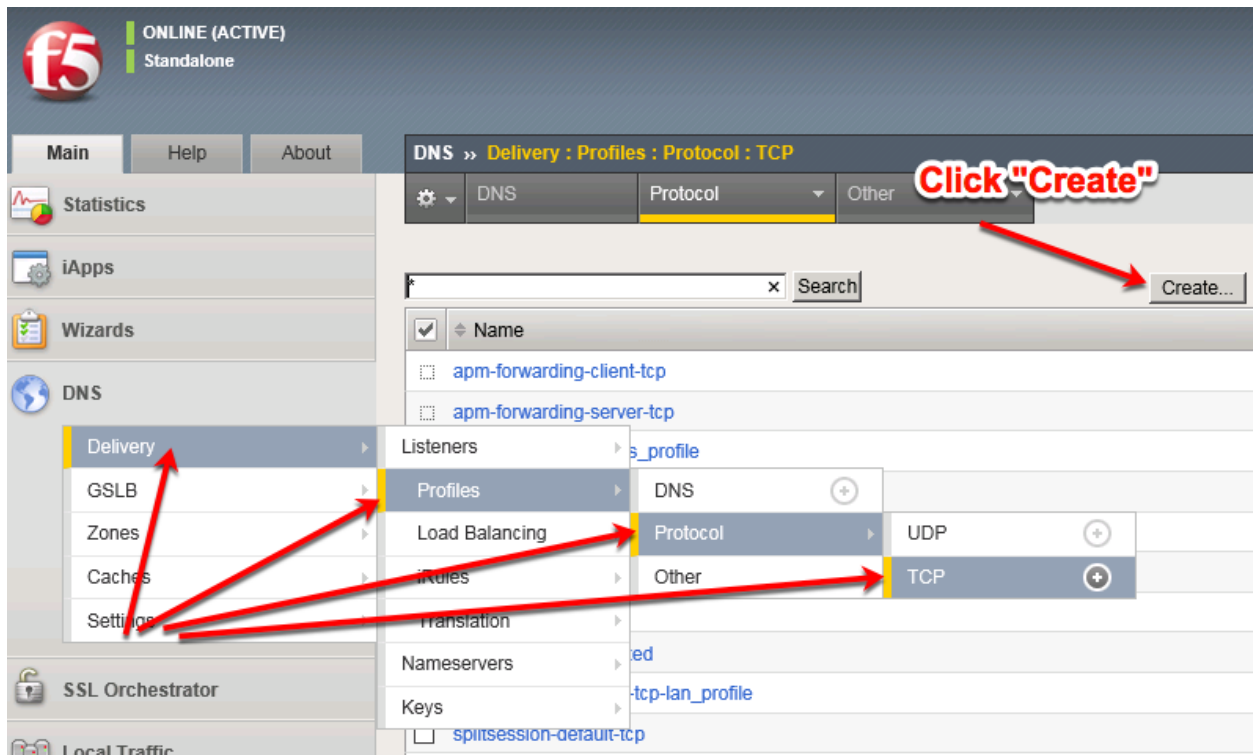
## TMSH

```
tmsh create ltm profile udp example.com_udp-dns_profile defaults-from udp_gtm_dns
```

## TCP Profile

Like the UDP profile, a TCP profile controls properties of TCP connections on the BIG-IP.

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



Create a TCP profile as shown in the following table.

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

ONLINE (ACTIVE)  
Standalone

Main Help About

Local Traffic » Profiles : Protocol : TCP » New TCP Profile...

Statistics  
iApps  
DNS  
SSL Orchestrator  
Local Traffic  
Network Map  
Virtual Servers  
Policies  
Profiles  
Ciphers  
iRules  
Pools  
Nodes  
Monitors  
Traffic Class

**General Properties**

Name	example.com_tcp-
Parent Profile	f5-tcp-lan

**Timer Management**

Close Wait	Specify...	5	seconds
Fin Wait 1	Specify...	5	seconds
Fin Wait 2	Specify...	300	seconds
Idle Timeout	Specify...	300	seconds
Keep Alive Interval	Specify...	1800	seconds
Minimum RTO	200	milliseconds	
Reset On Timeout	<input checked="" type="checkbox"/> Enabled		
Time Wait	Specify...	2000	milliseconds
Time Wait Recycle	<input checked="" type="checkbox"/> Enabled		
Zero Window Timeout	Specify...	20000	milliseconds

## TMSH

```
tmsh create ltm profile tcp example.com_tcp-dns_profile defaults-from f5-tcp-lan
```

## UDP Listener

Now that all of our profiles are created, we can create our listeners starting with the UDP listener.

Navigate to: **DNS » Delivery : Listeners : Listener List**



Main Help About DNS » Delivery : Listeners : Listener List » New...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
Local Traffic  
Acceleration  
Device Management  
Shared Objects  
Network  
System

**General**

Name: udp\_53\_virtual  
Description:  
State: Enabled

**Listener:** Advanced

Destination: Type: Host Network  
Address: 10.1.10.53

Service Port: DNS 53

VLAN Traffic: Enabled on...

VLANs and Tunnels: Selected: /Common external Available: /Common http-tunnel internal socks-tunnel

Source Address Translation: None

Address Translation: ☐ Enabled

Port Translation: ☐ Enabled

Route Advertisement: ☐ Enabled

Auto Last Hop: Default

Last Hop Pool: None

**Service:** Advanced

Protocol: UDP

Protocol Profile (Client): example.com\_udp-dns\_profile

Protocol Profile (Server): (Use Client Profile)

DNS Profile: example.com\_dns\_profile

**Load Balancing**

Default Pool: dns\_pool

Default Persistence Profile: None

Fallback Persistence Profile: None

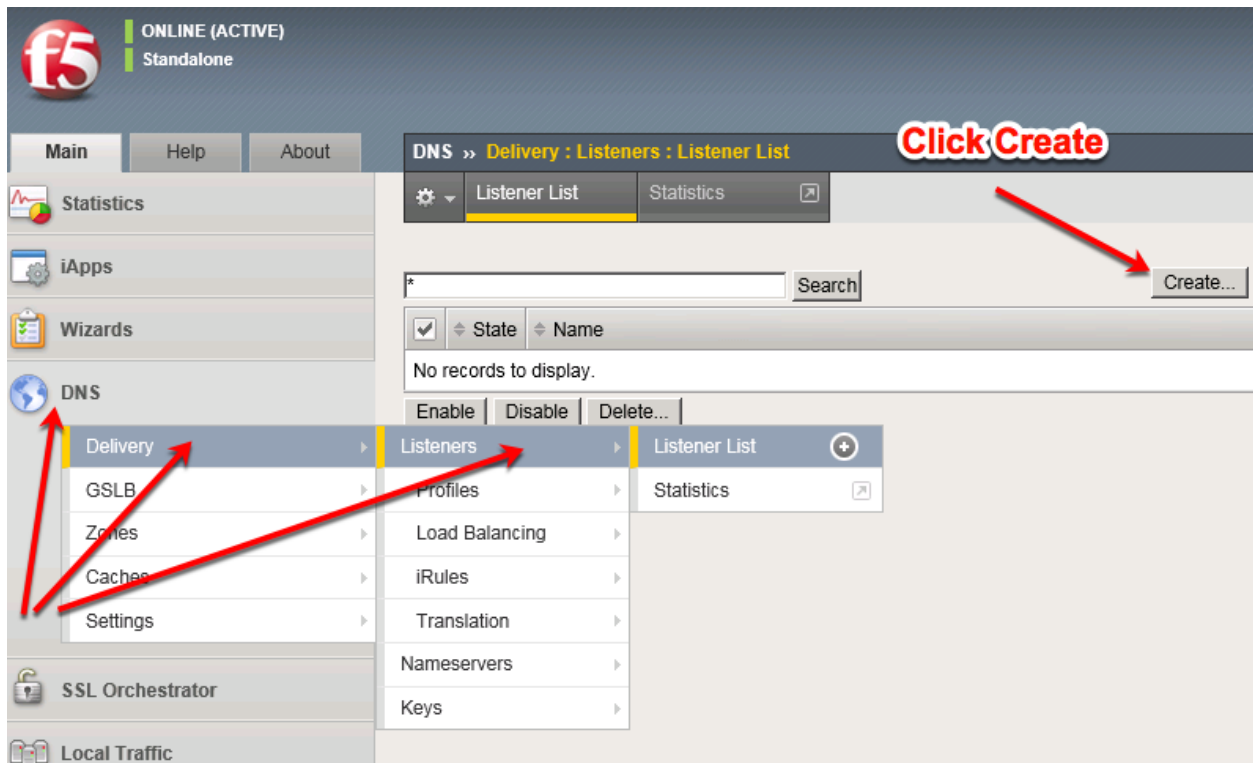
## TMSH

```
tmsl create gtm listener udp_53_virtual address 10.1.10.53 port 53 translate-address enabled ip-protocol
udp pool dns_pool profiles add { example.com_dns_profile example.com_udp-dns_profile } vlans add {
external } vlans-enabled
```

## TCP Listeners

Next, create the TCP listener

Navigate to: **DNS » Delivery : Listeners : Listener List**



Create two TCP listeners according to the table below:

**Pro-tip:** You can use the 'Repeat' button to easily create the second virtual server

Setting	Value
Name	tcp_53_virtual
Destination Address	10.1.10.53
Service Port (Advanced Settings)	DNS 53
VLAN and Tunnel Traffic -> Enabled on..	external
Address Translation	Enabled
Protocol	TCP
Protocol Profile (Client)	example.com_tcp-dns_profile
DNS Profile	example.com_dns_profile
Pool	dns_pool

Main	Help	About	DNS » Delivery : Listeners : Listener List » New...
<div> <div>Statistics</div> <div>IAApps</div> <div>DNS           <div>Delivery</div> <div>GSLB</div> <div>Zones</div> <div>Caches</div> <div>Settings</div> </div> <div>Local Traffic</div> <div>Traffic Intelligence</div> <div>Acceleration</div> <div>Subscriber Management</div> <div>Device Management</div> <div>Shared Objects</div> <div>Security</div> <div>Network</div> <div>System</div> </div>			
<div> <div>General</div> <div> <div>Name</div> <div>tcp_53_virtual</div> </div> <div> <div>Description</div> <div></div> </div> <div> <div>State</div> <div>Enabled</div> </div> </div>			
<div> <div>Listener: Advanced</div> <div> <div> <div>Destination</div> <div> <div>Type: Host Network</div> <div>Address: 10.1.10.53</div> </div> </div> <div> <div>Service Port</div> <div> <div>DNS</div> <div>53</div> </div> </div> <div> <div>VLAN Traffic</div> <div>Enabled on...</div> </div> <div> <div>VLANs and Tunnels</div> <div> <div> <div>Selected</div> <div>/Common</div> <div>external</div> </div> <div> <div>Available</div> <div>/Common</div> <div>http-tunnel</div> <div>internal</div> <div>socks-tunnel</div> </div> </div> <div> <div>Source Address Translation</div> <div>None</div> </div> <div> <div>Address Translation</div> <div>Enabled</div> </div> <div> <div>Port Translation</div> <div>Enabled</div> </div> <div> <div>Route Advertisement</div> <div>Enabled</div> </div> <div> <div>Auto Last Hop</div> <div>Default</div> </div> <div> <div>Last Hop Pool</div> <div>None</div> </div> </div> </div> </div>			
<div> <div>Service: Advanced</div> <div> <div>Protocol</div> <div>TCP</div> </div> <div> <div>Protocol Profile (Client)</div> <div>example.com_tcp-dns_profile</div> </div> <div> <div>Protocol Profile (Server)</div> <div>(Use Client Profile)</div> </div> <div> <div>DNS Profile</div> <div>example.com_dns_profile</div> </div> </div>			
<div> <div>Load Balancing</div> <div> <div>Default Pool</div> <div>dns_pool</div> </div> <div> <div>Default Persistence Profile</div> <div>None</div> </div> <div> <div>Fallback Persistence Profile</div> <div>None</div> </div> </div>			

## TMSH

```
tmsh create gtm listener tcp_53_virtual address 10.1.10.53 port 53 translate-address enabled ip-protocol tcp pool dns_pool profiles add { example.com_dns_profile example.com_tcp-dns_profile } vlans add { external } vlans-enabled
```

## Results

1. From the Ubuntu client, open a Web Shell or SSH session. Using the *dig* utility, we can query the listeners.



Repeat some of the same queries multiple times

```
dig @10.1.10.53 www.f5.com
dig @10.1.10.53 +tcp www.wikipedia.org
```

## 2. Viewing Cache Statistics

Navigate to: **Statistics » Module Statistics : DNS : Caches » Caches** and then choose **Caches** from the 'Statistics Type' drop-down.

The screenshot shows the F5 BIG-IP web interface. The breadcrumb navigation is **Statistics » Module Statistics : DNS : Caches » Caches**. The 'Statistics Type' is set to 'Caches'. The 'Data Format' is 'Normalized' and 'Auto Refresh' is 'Disabled'. A table lists DNS caches, with 'transparent\_cache' selected. A red arrow points to the 'View' link in the 'transparent\_cache' row.

DNS Queries		Failures			
Queries	Responses	Sync	Async	Resolve	Connect
7	4	4	0	0	0

Examine the Query, Failure, and Cache details below.

The screenshot shows the F5 BIG-IP web interface for the 'transparent\_cache' statistics. The 'Summary' tab is selected. The 'Data Format' is 'Normalized' and 'Auto Refresh' is 'Disabled'. The 'Query Details' section shows 7 Queries and 4 Responses. The 'Failure Details' section shows 0 Resolve, 0 Connection, 0 Server, and 0 Send. The 'Cache Details' section shows 4 Hits and 3 Misses for the DNS Message Cache.

Query Details	
Queries	Responses
7	4

Failure Details	
Resolve	Connection
0	0

Cache Details	
Hits	Misses
4	3

Login to the BIG-IP using a Web Shell or SSH session. You can view the contents of the cache with

the following TMSH command:

### TMSH

tmsh show ltm dns cache records rrset cache transparent\_cache

```
root@(ip-10-1-1-4)(cfg-sync Standalone)(Active)(/Common)(tmsh)# show ltm dns cache records rrset cache transparent_cache
-----
Ltm::DNS-Cache/Resolver RR Records
-----
Owner                               TTL    Type    Class  rdata
-----
dyna.wikimedia.org.                 225    A       IN     198.35.26.96
www.wikipedia.org.                  86025  CNAME   IN     dyna.wikimedia.org.
wikimedia.org.                      86025  NS       IN     ns1.wikimedia.org.
wikimedia.org.                      86025  NS       IN     ns0.wikimedia.org.
wikimedia.org.                      86025  NS       IN     ns2.wikimedia.org.
dwbfwz8xncmgm.cloudfront.net.       24     A       IN     13.224.29.57
dwbfwz8xncmgm.cloudfront.net.       24     A       IN     13.224.29.121
dwbfwz8xncmgm.cloudfront.net.       24     A       IN     13.224.29.79
dwbfwz8xncmgm.cloudfront.net.       24     A       IN     13.224.29.75
dwbfwz8xncmgm.cloudfront.net.       1273   NS       IN     ns-1645.awsdns-13.co.uk.
dwbfwz8xncmgm.cloudfront.net.       1273   NS       IN     ns-111.awsdns-13.com.
dwbfwz8xncmgm.cloudfront.net.       1273   NS       IN     ns-1438.awsdns-51.org.
dwbfwz8xncmgm.cloudfront.net.       1273   NS       IN     ns-683.awsdns-21.net.
Total records returned (tmm2): 13
```

To view the cache statistics similar to what you saw in the GUI you can use:

### TMSH

tmsh show ltm 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. Note, this will clear the actual DNS cache on the BIG-IP. If you want to clear the cache statistics, select the cache and hit the **Reset** button.

#### 4. Back End Visibility

Log onto the Ubuntu Server using a Web SHell. You can then run tcpdump to view DNS queries and see what hits the back end and what does not.

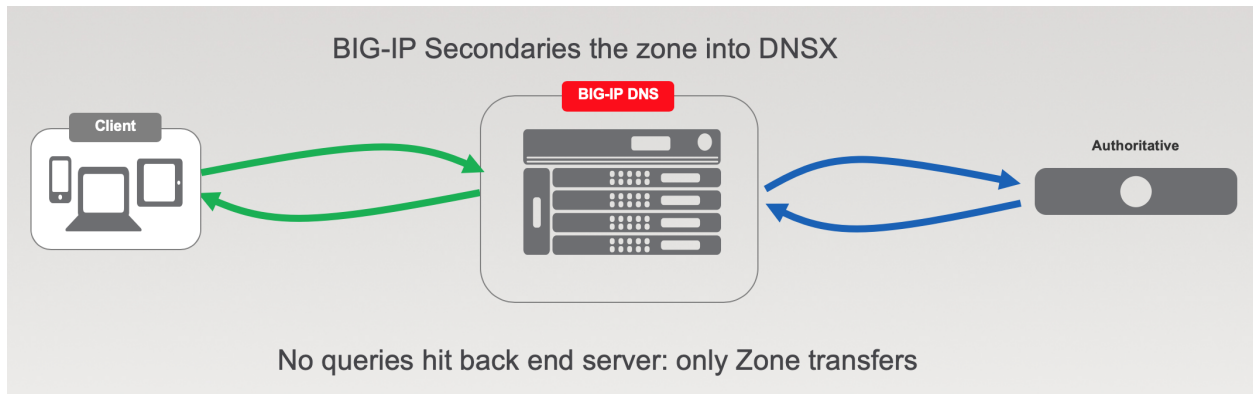
Use the Ubuntu Client to issue DNS queries for various domains.

```
tcpdump -nni eth1 port 53

Hit *Control-C* to exit the *tcpdump*
```

### 3.1.3 DNS Express with a Hidden Master

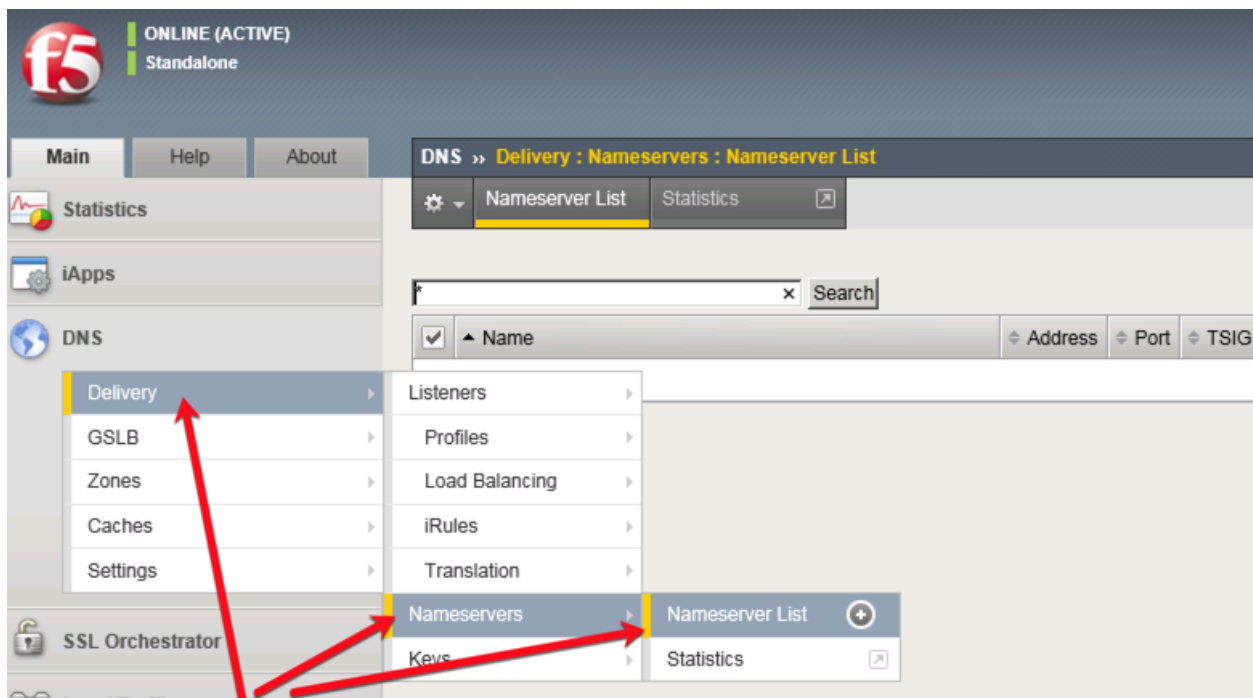
The Ubuntu Server is authoritative for the *example.com* zone. Using DNS Express (DNSX), the BIG-IP can be a high speed secondary for the zone.



## Name Server

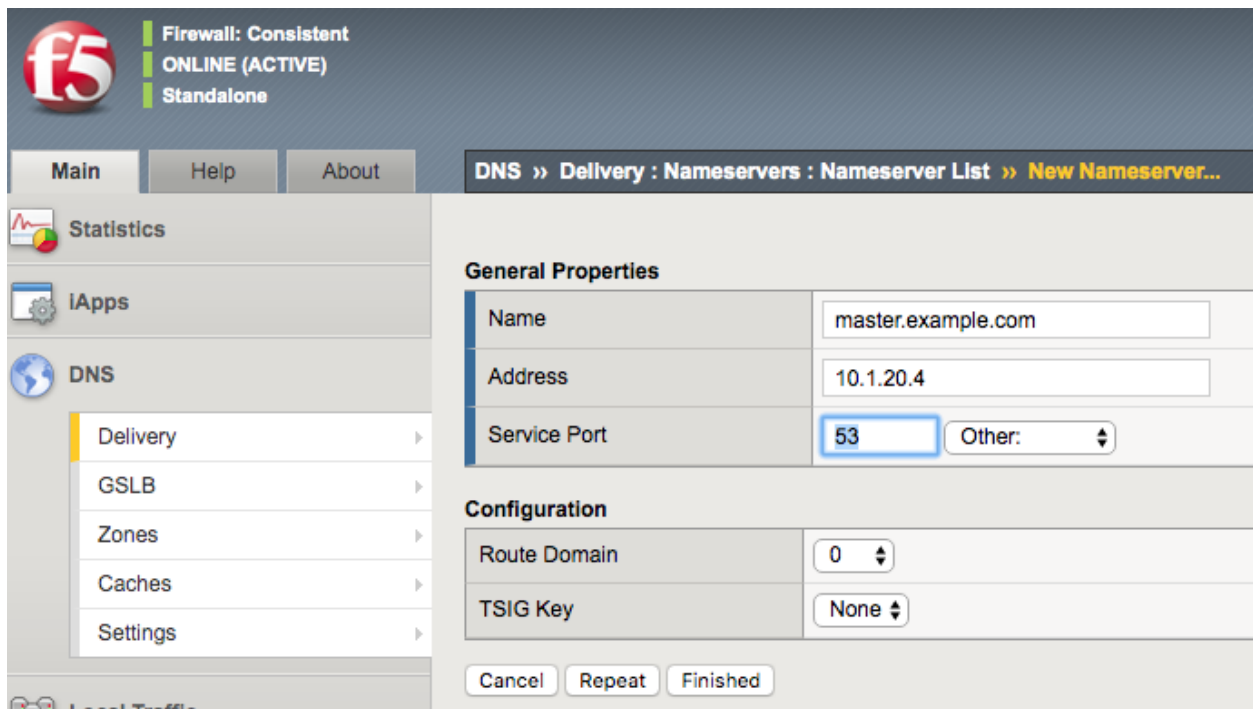
First, we define the Ubuntu server as a *nameserver* and initiate a zone transfer.

Navigate to **DNS » Delivery : Nameservers : Nameserver List**



Create a nameserver according to the following table:

Setting	Value
Name	master.example.com
Address	10.1.20.4



The screenshot shows the F5 DNS configuration interface. At the top, the status bar indicates 'Firewall: Consistent', 'ONLINE (ACTIVE)', and 'Standalone'. The navigation bar includes 'Main', 'Help', and 'About' tabs. The breadcrumb trail is 'DNS » Delivery : Nameservers : Nameserver List » New Nameserver...'. The left sidebar contains 'Statistics', 'IApps', 'DNS', and 'Local Traffic'. Under 'DNS', the 'Delivery' menu is expanded, showing 'GSLB', 'Zones', 'Caches', and 'Settings'. The main configuration area is titled 'General Properties' and contains the following fields:

General Properties	
Name	master.example.com
Address	10.1.20.4
Service Port	53 Other: ▾

Below the 'General Properties' section is the 'Configuration' section with the following fields:

Configuration	
Route Domain	0 ▾
TSIG Key	None ▾

At the bottom of the configuration area are three buttons: 'Cancel', 'Repeat', and 'Finished'.

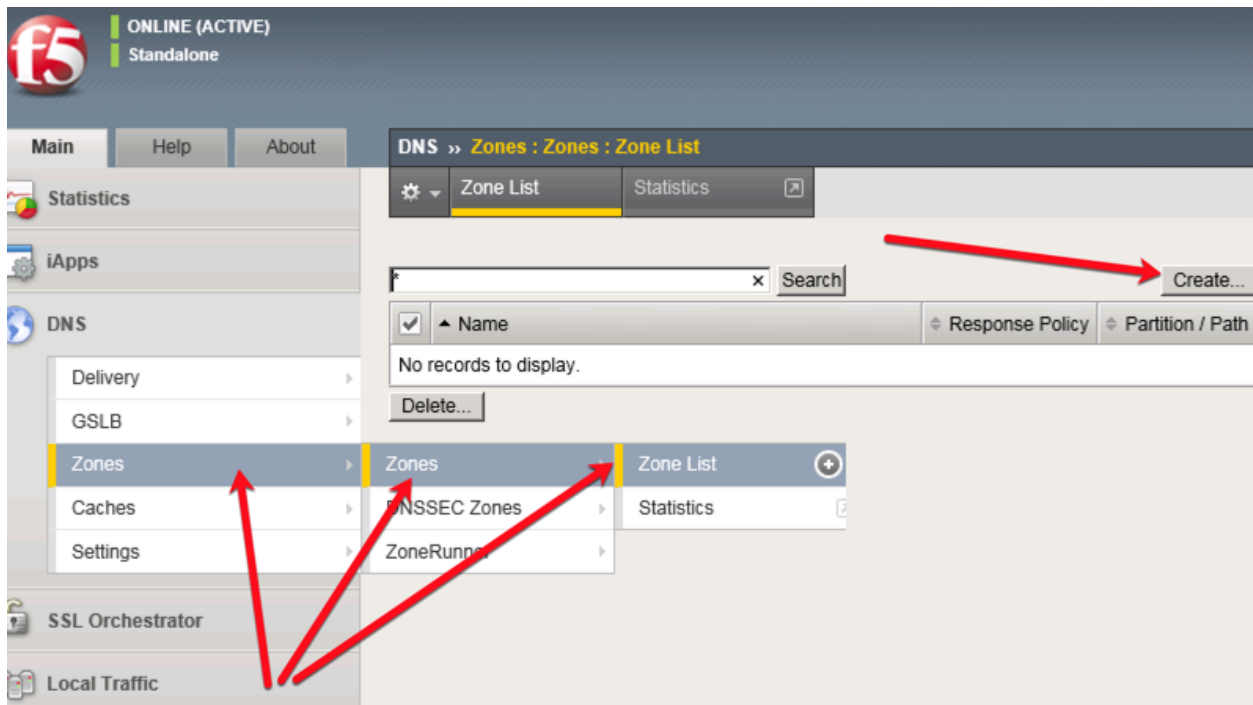
## TMSH

```
tmsh create ltm dns nameserver master.example.com { address 10.1.20.4 }
```

## DNS Express

Now that we have a nameserver defined, we must configure the DNSX zone. When completed, the BIG-IP will begin requesting zone transfers for *example.com* from that name server.

Navigate to **DNS » Zones : Zones : Zone List**



Create a DNS Express zone according to the following table:

Setting	Value
Name	example.com
Server	master.example.com
Allow NOTIFY From	10.1.20.4
Verify Notify TSIG	disable (uncheck box)

The screenshot shows a web-based DNS configuration interface. On the left is a sidebar with navigation links: Main, Help, About, Statistics, IApps, DNS (selected), Local Traffic, Traffic Intelligence, Acceleration, and Subscriber Management. Under the 'DNS' link, there is a sub-menu with Delivery, GSLB, Zones (highlighted), Caches, and Settings. The main content area is titled 'DNS » Zones : Zones : Zone List » New Zone...'. It contains two sections: 'General Properties' and 'DNS Express'. In 'General Properties', the 'Name' field is set to 'example.com'. In 'DNS Express', the 'Server' is 'master.example.com', 'Availability' is 'Unknown', 'State' is 'Enabled', and 'Notify Action' is 'Consume'. The 'Allow NOTIFY From' section shows an 'Address' of '10.1.20.4' with an 'Add' button and a 'Delete' button. The 'Verify Notify TSIG' checkbox is checked, and the 'Response Policy' checkbox is unchecked.

General Properties	
Name	example.com

DNS Express	
Server	master.example.com
Availability	<input type="checkbox"/> Unknown
State	Enabled
Notify Action	Consume
Allow NOTIFY From	<div>Address: 10.1.20.4 <input type="button" value="Add"/></div> <div>10.1.20.4</div> <div><input type="button" value="Delete"/></div>
Verify Notify TSIG	<input checked="" type="checkbox"/>
Response Policy	<input type="checkbox"/>

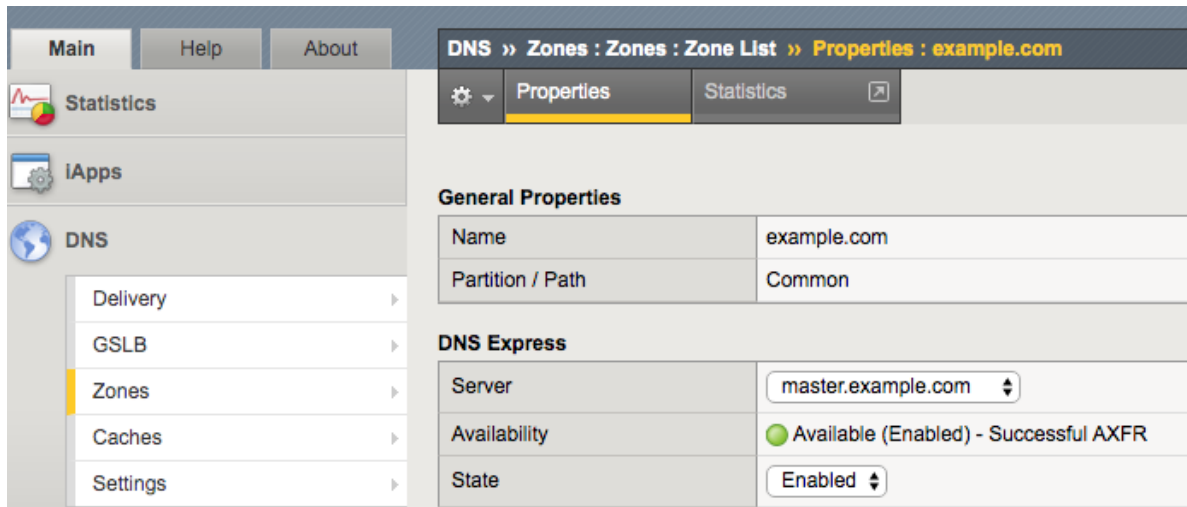
## TMSH

```
tmsh create ltm dns zone example.com { dns-express-allow-notify add { 10.1.20.4 } dns-express-notify-tsig-verify no dns-express-server master.example.com }
```

## Results

Now that the BIG-IP has transferred the zone, we can look at status and if needed dump the zone. To check the status:

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



You can use the **dnsxdump** utility to view the DNS Express database information, which includes zone information and statistics.

- The **DB Dump** section of the **dnsxdump** utility output displays the zone information for all configured DNS Express zones.
- The **DB Stats** section of the **dnsxdump** utility output displays a cumulative count of records for all configured DNS Express zones.

1. From the Web Shell of SSH session to the BIG-IP:

Run the following command to see the contents of the DNS Express database from the Advanced Shell (not tmsh):

```
#dnsxdump | less
```

Examine the results

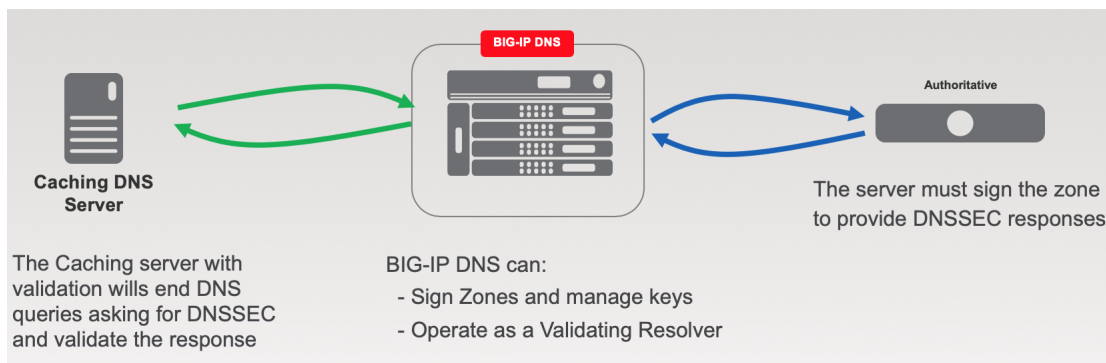
To see or troubleshoot zone transfers, we can refer to the `/var/log/ltn` log file. A quick examination of the log should show a successful zone transfer in the lab:

```
#tail -100 /var/log/ltn | grep zxfrd
```

[illegible]

### 3.1.4 DNSSec

Security Extension for DNS (DNSSEC) has several components. It starts with signing zone information to provide DNSSEC signed responses. Additionally, the resolver being used needs to be a *validating resolver* which forwards queries asking for a DNSSEC signed response.

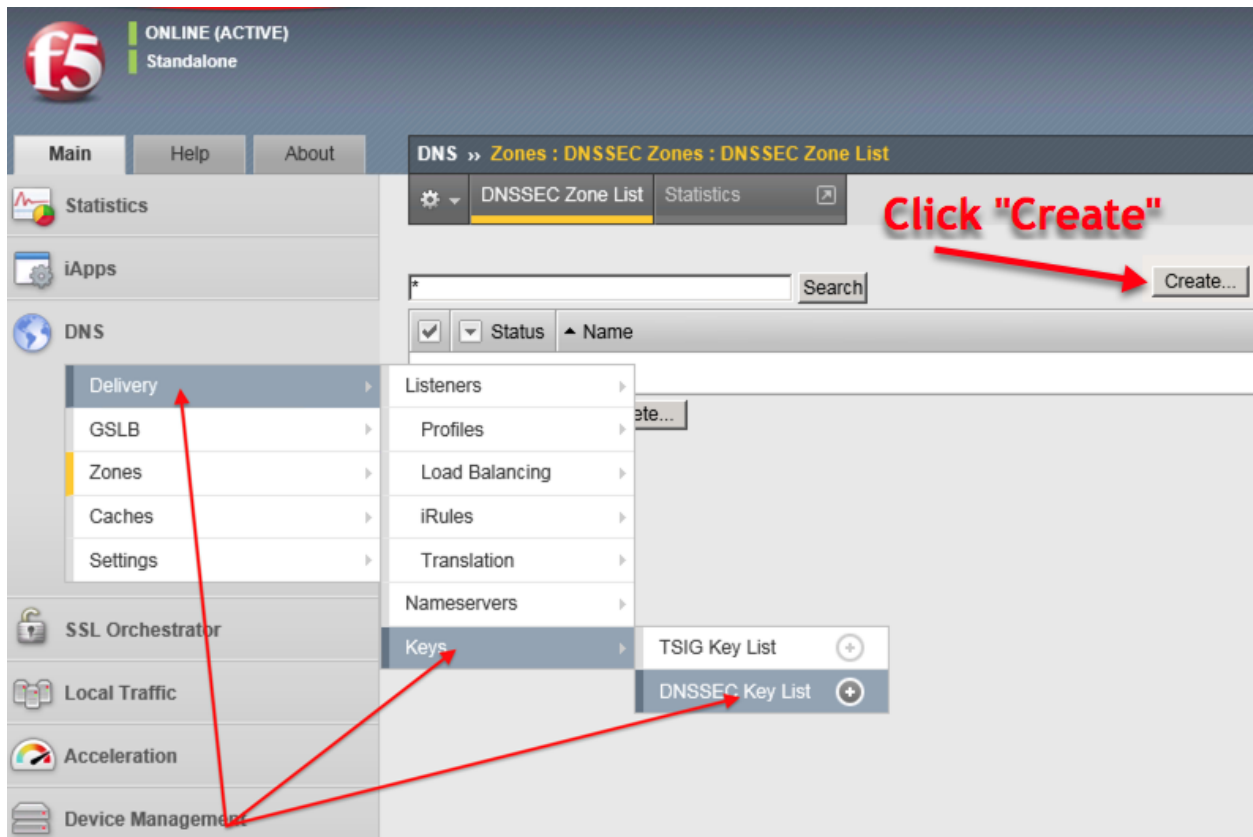


## Zone Signing Key

Managing keys is an administrative task that the BIG-IP can do automatically. In order to sign zones, we must first create keys!

Navigate to: **DNS » Delivery : Keys : DNSSEC Key List**





Create zone signing key according the following table:

Setting	Value
Name	example.com_zsk
Type	Zone Signing Key
Key Management	Manual
Certificate	default.crt
Private Key	default.key

ONLINE (ACTIVE)  
Standalone

Main Help About

DNS » Delivery : Keys : DNSSEC Key List » New DNSSEC Key...

Statistics  
IApps  
Wizards  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator

**General Properties**

Name	example.com_zsk
Type	Zone Signing Key ▼
State	Enabled ▼
Hardware Security Module	None ▼
Algorithm	RSA/SHA1 ▼
Key Management	Manual ▼

**Key Settings**

Certificate	default.crt ▼
Private Key	default.key ▼

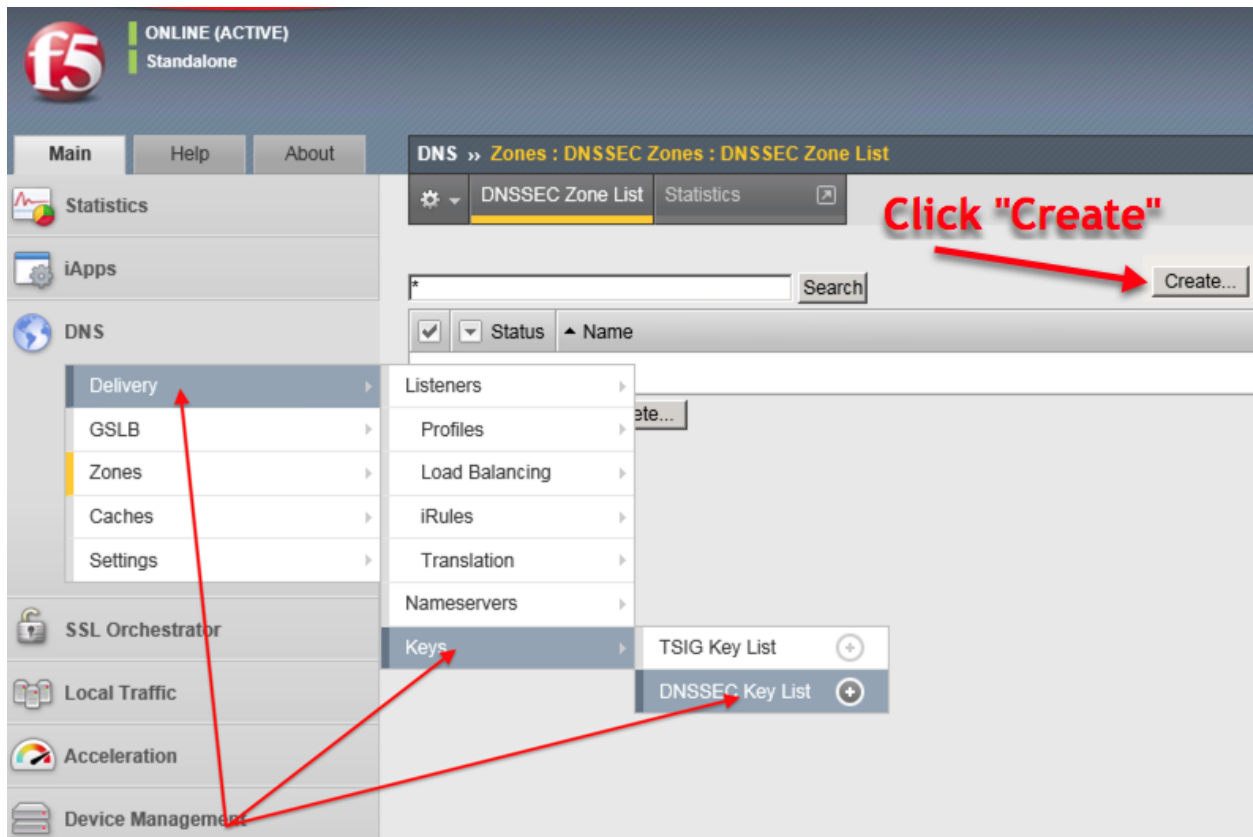
Cancel Repeat Finished

### TMSH

```
tmsh create ltm dns dnssec key example.com_zsk key-type zsk certificate-file default.crt key-file default.key
```

### Key Signing Key

Navigate to: **DNS » Delivery : Keys : DNSSEC Key List**



Create a key signing key according to the following table:

Setting	Value
Name	example.com_ksk
Type	Key Signing Key
Key Management	Manual
Certificate	default.crt
Private Key	default.key

ONLINE (ACTIVE)  
Standalone

Main Help About

DNS » Delivery : Keys : DNSSEC Key List » New DNSSEC Key...

Statistics  
iApps  
Wizards  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Local Traffic

**General Properties**

Name	example.com_ksk
Type	Key Signing Key
State	Enabled
Hardware Security Module	None
Algorithm	RSA/SHA1
Key Management	Manual

**Key Settings**

Certificate	default.crt
Private Key	default.key

Cancel Repeat Finished

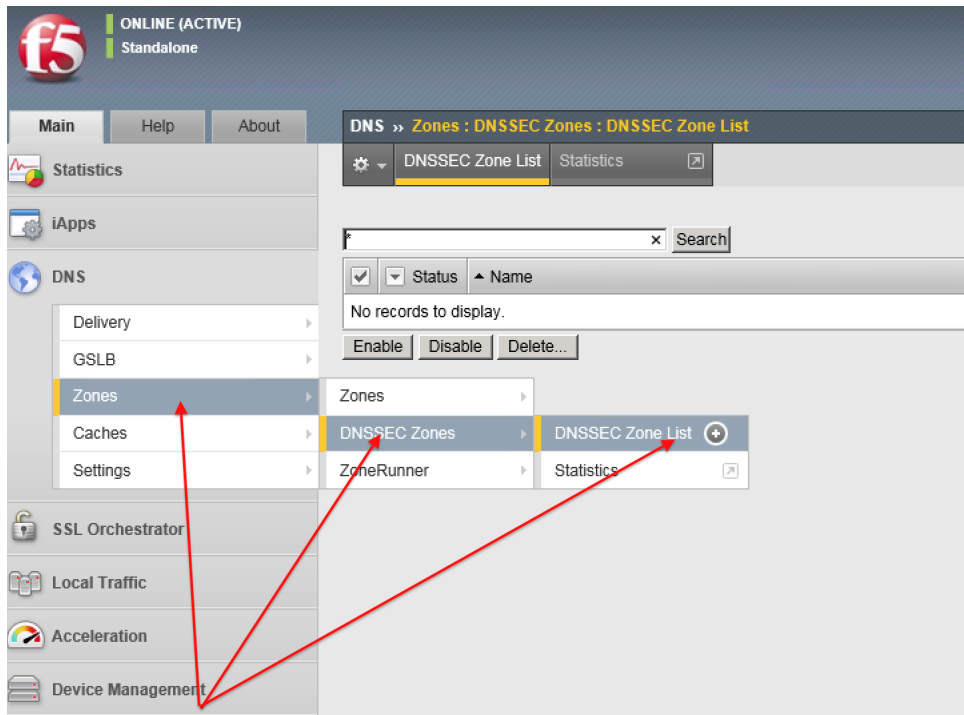
TMSH commands for Key Signing key creation:

### TMSH

```
tmsh create ltm dns dnssec key example.com_ksk key-type ksk certificate-file default.crt key-file default.key
```

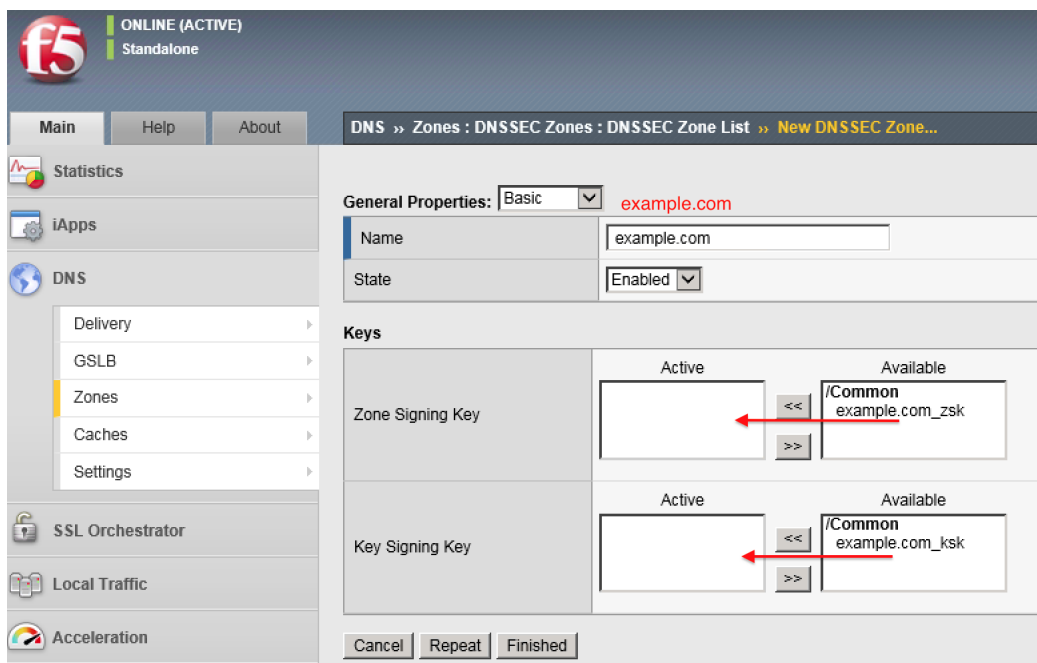
### Signed Zone

Navigate to: **DNS » Zones : DNSSEC Zones : DNSSEC Zone List**



Create DNS Express zone signed by DNSSEC

Setting	Value
Name	example.com
Zone Signing Key	example.com_zsk
Key Signing Key	example.com_ksk



TMSH commands for DNSSEC signed zone creation:

## TMSH

```
tmsm create ltm dns dnssec zone example.com keys add { example.com_ksk example.com_zsk }
```

## Results

Lets look at the results from both the client along with the logged messages on the BIG-IP.

From the CLI on the BIG-IP run `tail -f /var/log/ltm | grep -i tmm`

From the Ubuntu Client , terminal prompt run these two queries: `dig @10.1.10.53 example.com; dig @10.1.10.53 example.com +dnssec`

The BIG-IP log will show the queries, and the Ubuntu Client the unsigned and signed responses. Do you see the different in logged messages on the BIG-IP?

```
<<>> DiG 9.10.3-P4-Ubuntu <<>> @10.1.10.53 example.com
; (1 server found)
; global options: +cmd
; Got answer:
; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 14446
; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.com.                IN      A

;; AUTHORITY SECTION:
example.com.                  7200    IN      SOA     master.example.com. master.example.com. 2020020200 21600 3600 604800 86400

;; Query time: 0 msec
;; SERVER: 10.1.10.53#53(10.1.10.53)
;; WHEN: Tue Feb 04 18:03:30 UTC 2020
;; MSG SIZE rcvd: 83

<<>> DiG 9.10.3-P4-Ubuntu <<>> @10.1.10.53 example.com +dnssec
; (1 server found)
; global options: +cmd
; Got answer:
; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 34830
; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;example.com.                IN      A

;; AUTHORITY SECTION:
example.com.                  7200    IN      SOA     master.example.com. master.example.com. 2020020200 21600 3600 604800 86400
example.com.                  7200    IN      RRSIG   SOA 7 2 7200 20200211180329 20200204180329 56039 example.com. a4EJUKonY8y5h4h7aXWZlwdNXRSI0Sj9rudcWnfpUpPLKLY6SPK
DNeXZ WA7Atnv20faE0Ed0CsbFO1AjoAcM0KfKDSuURjR0s6AI+9AsLosL8XaT PIZF0SHUf039RjXZP/08xSMkj4o49xXVLv0XnxZvighb+jFHJL4vnc2F W0e42jJ0GT4loe26erU0sd8HwgT7Jef/hBeycyCfC
BmZ+oog60Age0esB 1zx3tVCjUAY18za0g/PnFvuCAgacTJN9tItIGR4rMNGVPxSwRv/ZGmaH agJmJY8DGT0T/+19NSXnR86P01LRMDYPACAvPSPHB4jHoJvJTjvELvu dA1Vxg==
gga5m9gr6jqp5hautn186j92m76fe8L.example.com. 86400 IN NSEC3 1 0 1 C9015CCC84330E4F GGA5M9GR6JQNP5HAUTNI86j92m76FE8M NS SOA RRSIG DNSKEY NSEC3PARAM
gga5m9gr6jqp5hautn186j92m76fe8L.example.com. 86400 IN RRSIG NSEC3 7 3 86400 20200211180329 20200204180329 56039 example.com. VVfJLhcM3csnVbZLj73WYXERthQXWCJfc0
sJX+50Pr0SoKcFbjwB1VN p0G0IW/9MLWiu71BGHJMloowI/DcsYQKJIG9gt4lGLELQ9XhLYSf1lqG 6MnXAe5pYMDBiVfCDQYNIxpactNOLY9htKURXVYwFBVfI0435/nUizxL HYQ4CgYUr7Lh4mswJlLb5of4
lK/ydbMSDwgjmH8/3Q0wyL6orrrKTSZ HEJXS3t6z0FET5s8LuL6Lp9Pa3a1nR+txev4I6cXwdgFOHN+oAp9l48M zFWiacrMHUFx0Ld7HSFWlPLZD4HPZwL1vo9p72fNPrbNmVaZujj7AgxN Zpbr8g==

;; Query time: 3 msec
;; SERVER: 10.1.10.53#53(10.1.10.53)
;; WHEN: Tue Feb 04 18:03:30 UTC 2020
;; MSG SIZE rcvd: 769
```

### 3.1.5 Validating Resolver

#### Trust Anchors

Next, create a trust anchor to validate DNS payloads in a DNSSEC response.

Begin by connecting to the BIG-IP via a web shell and run the commands shown below:

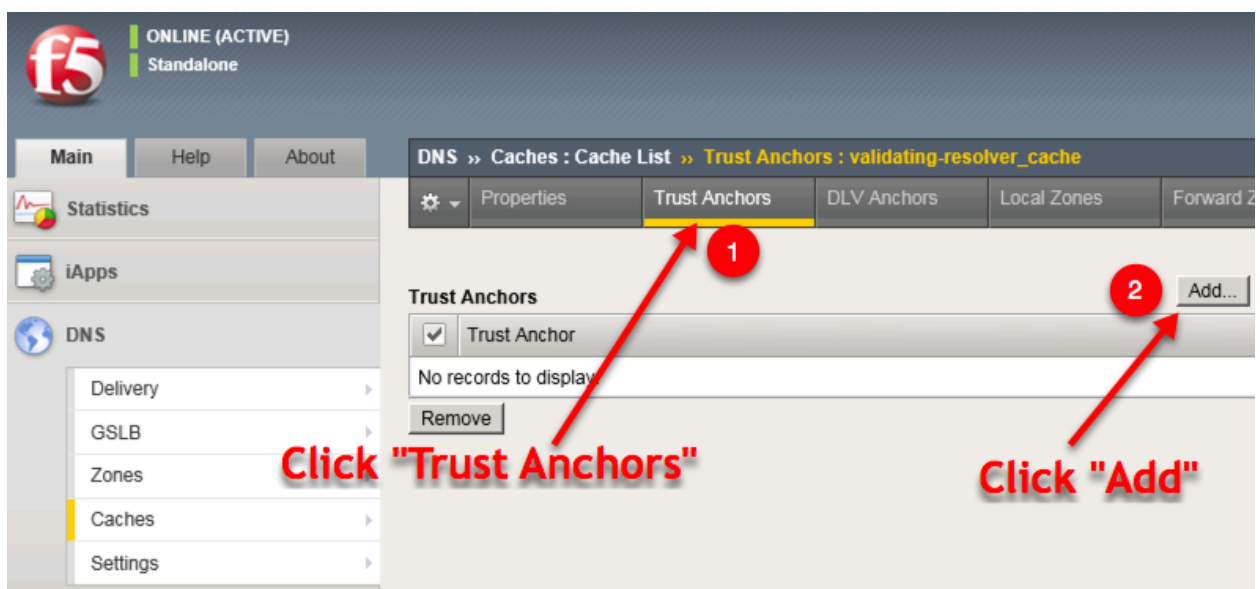
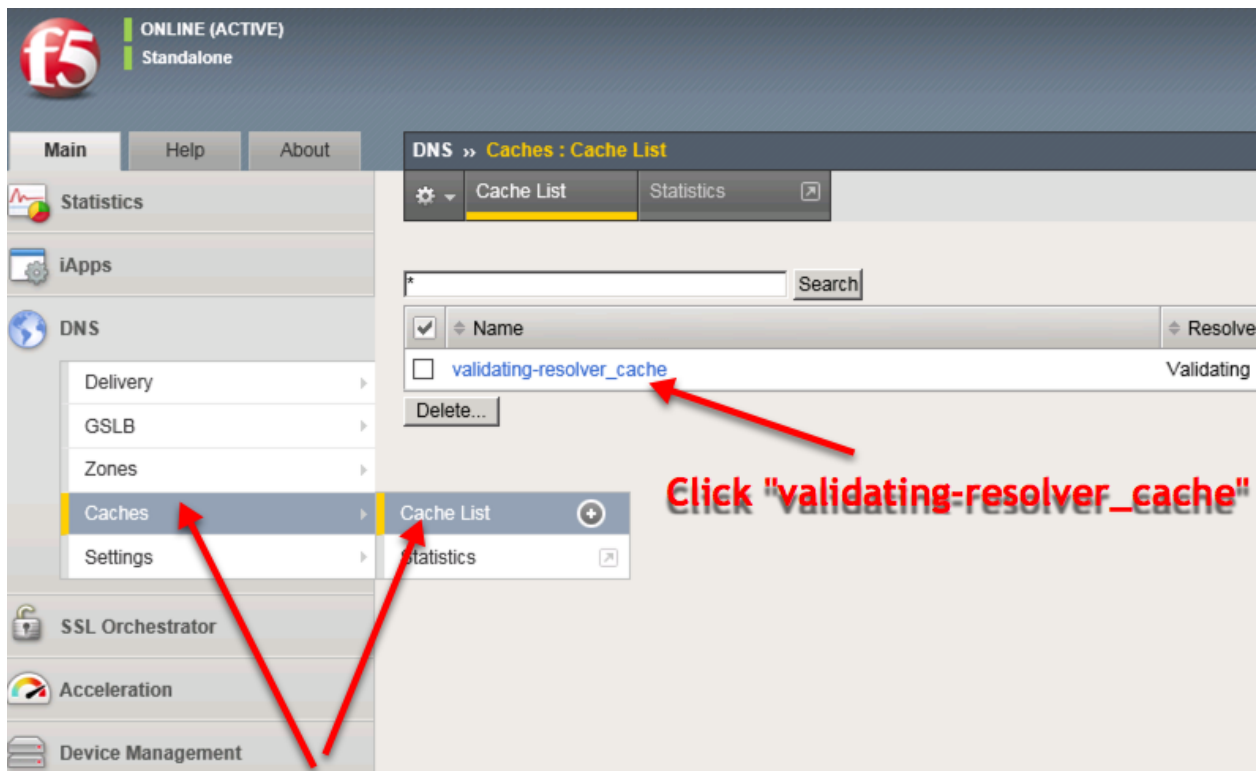
```
dig dnskey . | grep 257 > /root/dnskey.txt

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

```
[root@ip-10-1-1-4:Active:Standalone] config # dig dnskey . | grep 257 > /root/dnskey.txt
[root@ip-10-1-1-4:Active:Standalone] config # dnssec-dsfromkey -f /root/dnskey.txt .
. IN DS 20326 8 1 AE1EA5B974D4C858B740BD03E3CED7EBFCBD1724
. IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
[root@ip-10-1-1-4:Active:Standalone] config #
```

Navigate to: **DNS » Caches : Cache List » validating-resolver\_cache : Trust Anchors**

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



For each *DS* record, enter them as trust anchors:

The screenshot shows the DNS configuration interface. At the top, the breadcrumb is "DNS » Caches : Cache List". Below this is the "Add Trust Anchor" dialog. The "Trust Anchor" field contains the text ". IN DS 20326 8 1 AE1EA5B974D4C858B740BD03E3CED7EBFCBD1724". Below the field are three buttons: "Cancel", "Repeat", and "Finished".

Below the dialog, the breadcrumb is "DNS » Caches : Cache List » Trust Anchors : validating-resolver\_cache". There is a tabbed interface with tabs: "Properties", "Trust Anchors" (selected), "DLV Anchors", "Local Zones", "Forward Zones", "Response Policy Zones", and "Statistics".

Under the "Trust Anchors" tab, there is a section titled "Trust Anchors". It contains a list of trust anchors. The first entry is selected with a radio button and has a checkbox checked: ". IN DS 20326 8 1 AE1EA5B974D4C858B740BD03E3CED7EBFCBD1724". The second entry is not selected: ". IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D". Below the list is a "Remove" button.

When using TMSH, enter the DS records, each surrounded by quotes (" "), and use the entire keys above for *<key 1>* and *<key 2>*

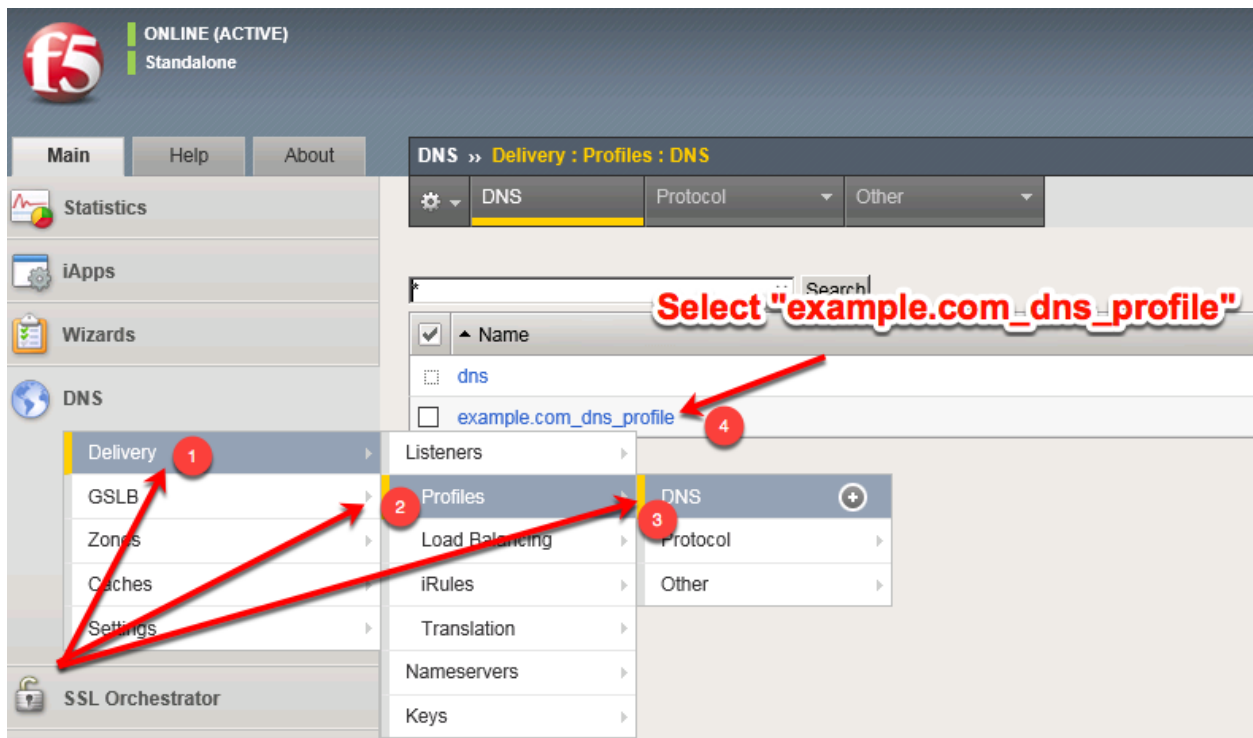
```
tmsl modify ltm dns cache validating-resolver validating-resolver_cache trust-anchors_
↔replace-all-with { "<key 1>" "<key 2>" }
```

## Modify DNS Profile

Now that we have a Validating Resolver configured with trust anchors, we can enable it by altering our existing 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.

The screenshot shows the F5 BIG-IP configuration interface. The top bar indicates the device is 'ONLINE (ACTIVE)' and 'Standalone'. The breadcrumb navigation is 'DNS » Delivery : Profiles : DNS » Properties : example.com\_dns\_profile'. The left sidebar shows the 'DNS' menu expanded, with 'Delivery' selected. The main content area shows the 'Properties' tab for the 'example.com\_dns\_profile'. The 'General Properties' section shows 'Name' as 'example.com\_dns\_profile', 'Partition / Path' as 'Common', and 'Parent Profile' as 'dns'. The 'Denial of Service Protection' section shows 'Rapid Response Mode' as 'Disabled' and 'Rapid Response Last Action' as 'Drop'. The 'Hardware Acceleration' section shows 'Protocol Validation' as 'Disabled' and 'Response Cache' as 'Disabled'. The 'DNS Features' section shows 'DNSSEC', 'GSLB', 'DNS Express', and 'DNS Cache' all set to 'Enabled'. The 'DNS Cache Name' is set to 'validating-resolver\_cache', which is highlighted with a red box and a red arrow pointing to it from the text 'Select the "validating-resolver\_cache"'. The 'DNS IPv6 to IPv4' is set to 'Disabled'.

## TMSH

```
tmsh modify ltm profile dns example.com_dns_profile cache validating-resolver_cache
```

## Results

Now let's look at results. Tail the *ltm* log on the BIG-IP

```
tail -f /var/log/ltm | grep tmm
```

From a Web shell on the Ubuntu Client, start with some DNS queries.

First, issue a DNS query that returns no response:

```
dig @10.1.10.53 nope.f5.com
```

```
[root@ip-10-1-1-4:Active:Standalone] config # tail -f /var/log/ltn | grep tmm

Feb 8 09:49:54 ip-10-1-1-4 info tmm[16605]: 2020-02-08 09:49:54 ip-10-1-1-4.us-west-2.compute.internal qid 54150 from 10.1.10.4#44569: view none: query: nope.f5.com IN A +E (10.1.10.53%)
Feb 8 09:49:54 ip-10-1-1-4 info tmm[16605]: 2020-02-08 09:49:54 ip-10-1-1-4.us-west-2.compute.internal qid 54150 to 10.1.10.4#44569: [NXDOMAIN qr,rd,ra] response: empty

root@ip-10-1-1-6:/# dig @10.1.10.53 nope.f5.com

; <<> DiG 9.10.3-P4-Ubuntu <<> @10.1.10.53 nope.f5.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NXDOMAIN, id: 54150
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;nope.f5.com.                IN      A

;; AUTHORITY SECTION:
f5.com.                      3415    IN      SOA     pdns130.f5.com. dnsadmin.f5.com. 9964 3600 900 1209600 3600

;; Query time: 1 msec
;; SERVER: 10.1.10.53#53(10.1.10.53)
;; WHEN: Sat Feb 08 17:49:54 UTC 2020
;; MSG SIZE rcvd: 93
```

Next, set the DNSSEC OK bit in the query (DO):

```
dig @10.1.10.53 dnssec-deployment.org +dnssec
```

```
Feb 8 09:51:45 ip-10-1-1-4 info tmm[16605]: 2020-02-08 09:51:44 ip-10-1-1-4.us-west-2.compute.internal qid 61180 from 10.1.10.4#49953: view none: query: dnssec-deployment.org IN A +ED (10.1.10.53%)
Feb 8 09:51:45 ip-10-1-1-4 info tmm[16605]: 2020-02-08 09:51:44 ip-10-1-1-4.us-west-2.compute.internal qid 61180 to 10.1.10.4#49953: [NOERROR qr,rd,ra,ad,dl] response: dnssec-deployment.org. 278 IN RRSIG A 5 2 300 20200222084002 20200208084002 55518 dnssec-deployment.org. ckJpHV3mR3QlPV//3LZBx6BrR+OKDKNAgmlnz9ZR9AjyqoF9fIlrPiau09cxUb+yVjr1pcTaA3T/pnacjmmmpN8iPDavtbKIq8E1rdCt9taTuleYA lQUJrS8Dcx9laUrlWB7kjd0wsB2WvQoAhtngo03wB+tawSQYDpMH/RMFj/0=;

root@ip-10-1-1-6:/# dig @10.1.10.53 dnssec-deployment.org +dnssec

; <<> DiG 9.10.3-P4-Ubuntu <<> @10.1.10.53 dnssec-deployment.org +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 61180
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;dnssec-deployment.org.      IN      A

;; ANSWER SECTION:
dnssec-deployment.org. 278    IN      A      46.43.37.10
dnssec-deployment.org. 278    IN      RRSIG  A 5 2 300 20200222084002 20200208084002 55518 dnssec-deployment.org. ckJpHV3mR3QlPV//3LZBx6BrR+OKDKNAgmlnz9ZR9AjyqoF9fIlrPiau09cxUb+yVjr1pcTaA3T/pnacjmmmpN8iPDavtbKIq8E1rdCt9taTuleYA lQUJrS8Dcx9laUrlWB7kjd0wsB2WvQoAhtngo03wB+tawSQYDpMH/RMFj/0=

;; AUTHORITY SECTION:
dnssec-deployment.org. 278    IN      NS      ns1.mia1.afilias-nst.info.
dnssec-deployment.org. 278    IN      NS      ns1.ams1.afilias-nst.info.
dnssec-deployment.org. 278    IN      NS      ns1.yyz1.afilias-nst.info.
dnssec-deployment.org. 278    IN      NS      ns1.sea1.afilias-nst.info.
dnssec-deployment.org. 278    IN      NS      ns1.hkg1.afilias-nst.info.
dnssec-deployment.org. 278    IN      RRSIG  NS 5 2 300 20200222084002 20200208084002 55518 dnssec-deployment.org. EMFblC8ccQm2i6uC0iybBNPce26K+3PpkBeIo+iLHzl0rfQ7W9WJJM Ak/3MnhFcyI+hpJe2TBXlAqPTLVLvLePSRq2V397i20eZa+s+vB72D8jcc XiXhGNhtPwf0i0356b9cwaexGafsdJnjksuEuCS9uqglGwfE6c3hqs ZU8=

;; Query time: 1 msec
;; SERVER: 10.1.10.53#53(10.1.10.53)
;; WHEN: Sat Feb 08 17:51:44 UTC 2020
;; MSG SIZE rcvd: 559
```

Finally, set the DNSSEC but observe how the response is different:

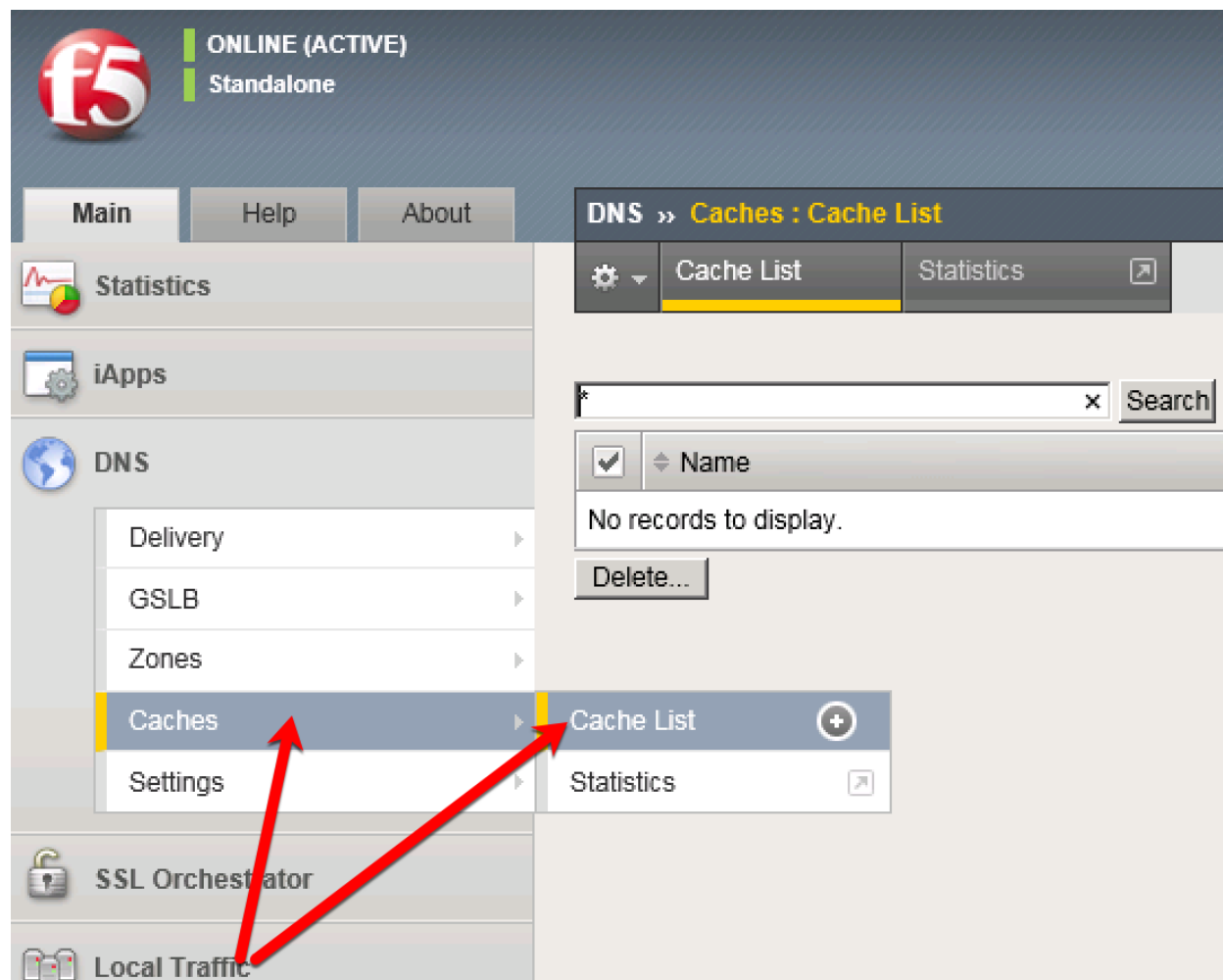
```
dig @10.1.10.53 www.google.com +dnssec
```

In this lab we will use the BIG-IP as a Validating resolver and not send any queries to the back end server.

The *validating* function of the resolver means that recursive queries are sent requesting DNSSEC, and responses are validated to authenticate validity of the response!

First lets create a new DNS cache on the BIG-IP:



Navigate to **DNS » Caches : Cache List**




Create a validating resolver cache according to the table below:

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

**General Properties**

Name	<input type="text" value="validating-resolver_cache"/> 
Resolver Type	<input type="text" value="Validating Resolver"/> 
Route Domain Name	<input type="text" value="0"/>

**DNS Cache**

Message Cache Size	<input type="text" value="1048576"/> bytes
Resource Record Cache Size	<input type="text" value="10485760"/> bytes
Name Server Cache Count	<input type="text" value="16536"/> entries
DNSSEC Key Cache Size	<input type="text" value="1048576"/> bytes
Answer Default Zones	<input checked="" type="checkbox"/> Enabled 
RRSet Rotate	<input type="text" value="none"/>

**DNS Resolver**

Use IPv4	<input checked="" type="checkbox"/> Enabled
Use IPv6	<input checked="" type="checkbox"/> Enabled
Use UDP	<input checked="" type="checkbox"/> Enabled
Use TCP	<input checked="" type="checkbox"/> Enabled
Max. Concurrent UDP Flows	<input type="text" value="8192"/>
Max. Concurrent TCP Flows	<input type="text" value="20"/>
Max. Concurrent Queries	<input type="text" value="1024"/>
Unsolicited Reply Threshold	<input type="text" value="0"/>
Allowed Query Time	<input type="text" value="200"/>
Randomize Query Character Case	<input checked="" type="checkbox"/> Enabled
Root Hints (Optional: Leave blank for defaults)	IP Address: <input type="text"/>
	<input type="button" value="Add"/>
	<div><input type="text"/></div> <input type="button" value="Delete"/>

**DNSSEC Validator**

Prefetch Key	<input checked="" type="checkbox"/> Enabled
--------------	---

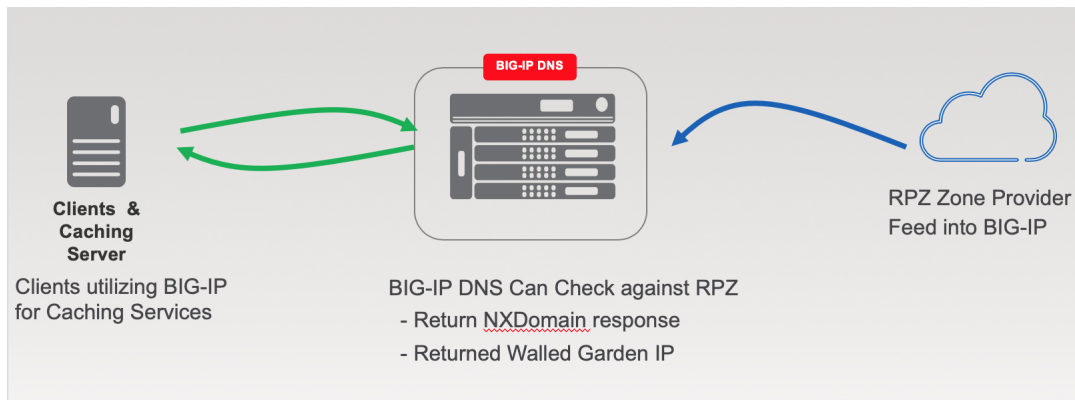
## TMSH

```
tmsh create ltm dns cache validating-resolver validating-resolver_cache answer-default-zones yes
```

### 3.1.6 RPZ

Response Policy Zone (RPZ) will be enabled to apply a policy for client queries that match black listed domains in the RPZ list.

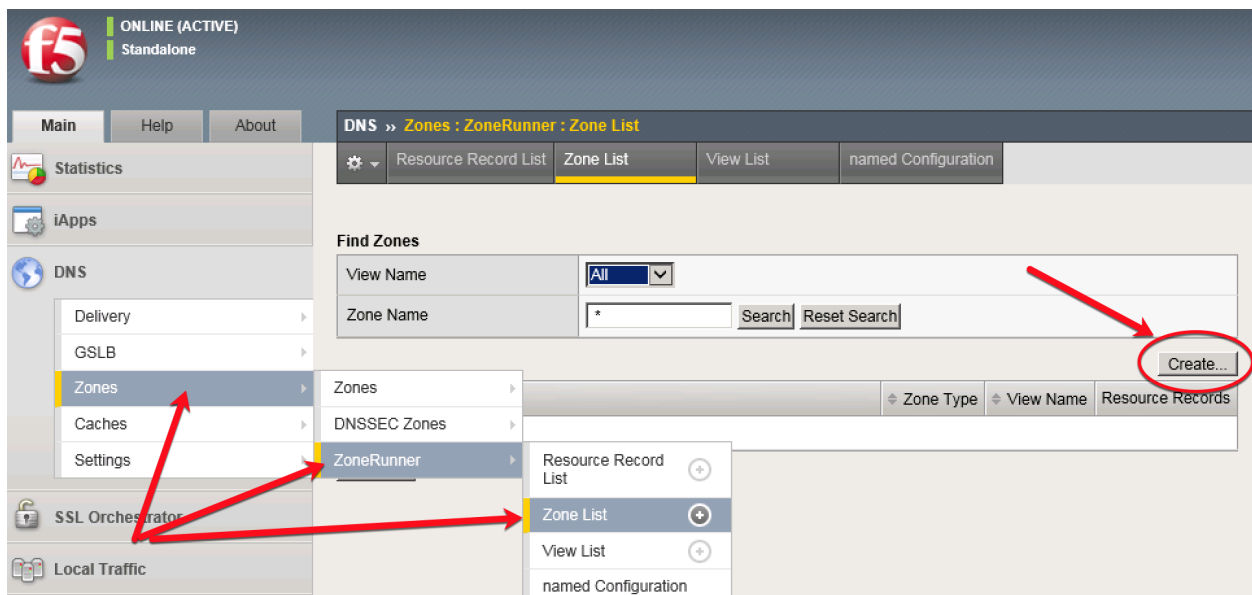
When implementing RPZ, you can control the response behavior to be an NXDomain response, or a Walled Garden IP.



## Zone Runner

For the purpose of the lab, we will utilize Zonerunner to create a RPZ zone.

Navigate to **DNS » Zones : ZoneRunner : Zone List**



Create a *new* zone according to the following table:

Setting	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	master.example.com.
Email Contact	hostmaster.master.example.com.
NS Record: TTL	300
NS Record: Nameserver	master.example.com.
Create A Record	Checked - Enabled
A Record: IP Address	10.1.10.53

DNS » Zones : ZoneRunner : Zone List » New Zone...

### General Properties

View Name	external
Zone Name	rpz.example.com
Zone Type	Master

### 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	<input type="checkbox"/> Enable

### Records Creation

SOA Record	TTL	300
	Master Server	master.example.com.
	Email Contact	hostmaster.master.example.com.
	Serial Number	2020020801
	Refresh Interval	10800 Seconds
	Retry Interval	3600 Seconds
	Expire	604800 Seconds
	Negative TTL	86400 Seconds
NS Record	TTL	300
	Nameserver	master.example.com.
Create A Record	<input checked="" type="checkbox"/> Enable	
A Record	IP Address	10.1.10.53

Cancel Repeat Finished

Next, lets create some resource records in the new zone.



Navigate to: **DNS » Zones : ZoneRunner : Resource Record List**

The screenshot shows the F5 DNS ZoneRunner interface. The top navigation bar includes 'Main', 'Help', and 'About'. The left sidebar has 'Statistics', 'iApps', and 'DNS' (with sub-items: Delivery, GSLB, Zones, Caches, Settings). The 'DNS' section is active, showing 'Zones : ZoneRunner : Resource Record List'. The main content area has tabs for 'Resource Record List', 'Zone List', 'View List', and 'named Configuration'. The 'Find Records' section contains fields for 'View Name' (All), 'Zone Name' (All Zones), 'Type' (All), 'Name' (\*), and 'RDATA'. Below these fields are buttons for 'Search', 'Reset Search', and 'Create...'. The 'Create...' button is circled in red.

Create a resource record according to the following table. Note the *Name* must not be fully qualified as its the hostname portion of the resource record!

Setting	Value
View Name	external
Zone Name	rpz.example.com
Name	*.fuzzybunnies.com
TTL	60
Type	CNAME
CNAME	.

**DNS » Zones : ZoneRunner : Resource Record List » New Resource Record...**

**Record Configuration**

View Name	external
Zone Name	rpz.example.com.
Name	*.fuzzybunnies.com
TTL	60
Type	CNAME
CNAME	.

Finally, set the type to *All* to find all records and click search to see all records:

**DNS » Zones : ZoneRunner : Resource Record List**

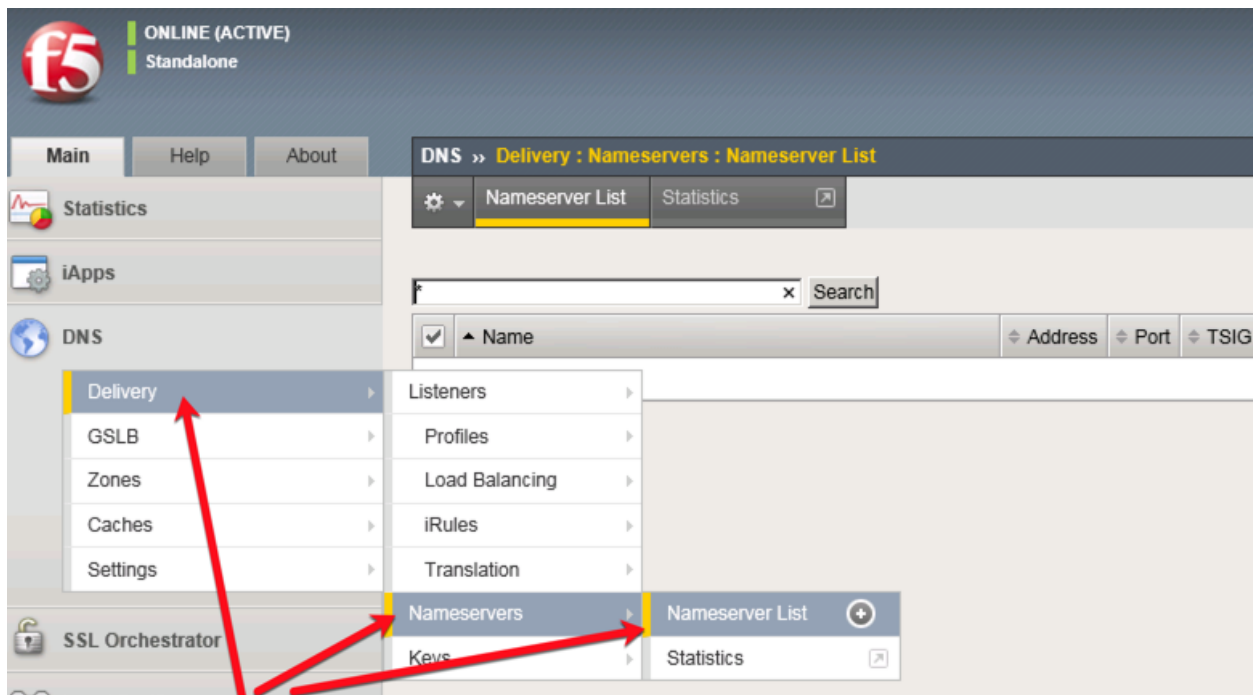
**Find Records**

View Name	All
Zone Name	All Zones (Select a View to search a specific zone)
Type	All
Name	*
RDATA	*

<input checked="" type="checkbox"/>	Name	View Name	Zone Name	TTL	Type	RDATA
<input type="checkbox"/>	*.fuzzybunnies.com.rpz.example.com.	external	rpz.example.com.	60	CNAME	.
<input type="checkbox"/>	rpz.example.com.	external	rpz.example.com.	300	NS	master.example.com.
<input type="checkbox"/>	rpz.example.com.	external	rpz.example.com.	300	SOA	master.example.com. ...

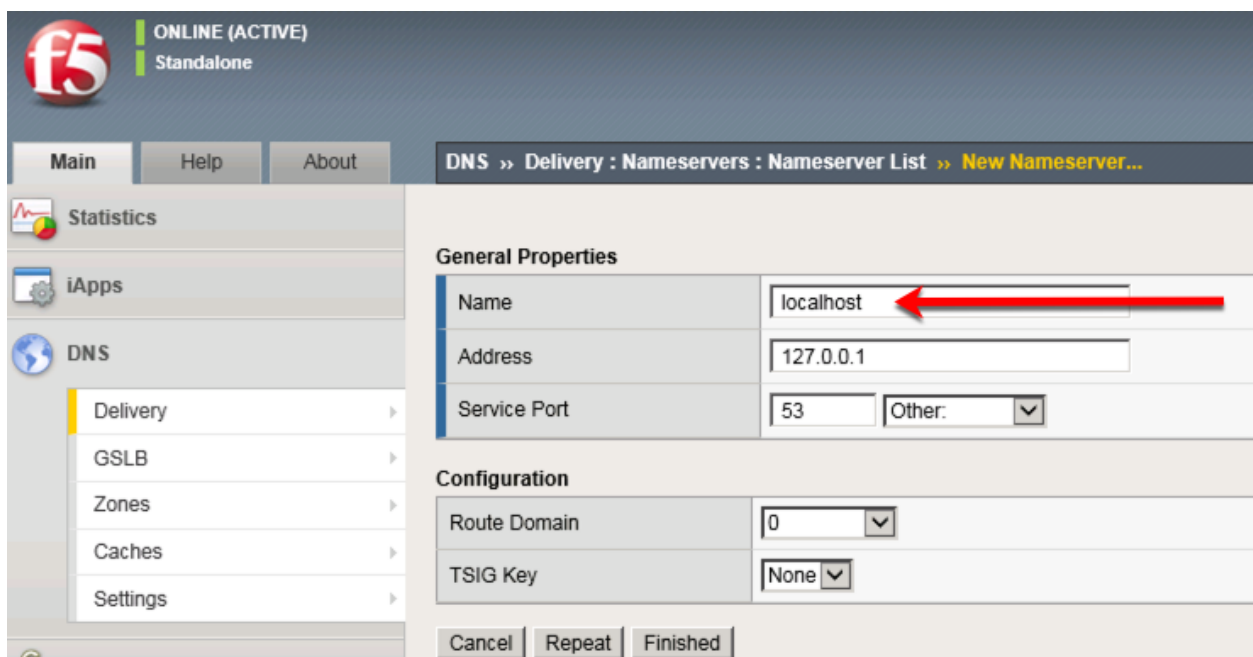
## Name Server

Navigate to **DNS » Delivery : Nameservers : Nameserver List**



Create a nameserver according to the following table:

Setting	Value
Name	localhost
Address	127.0.0.1

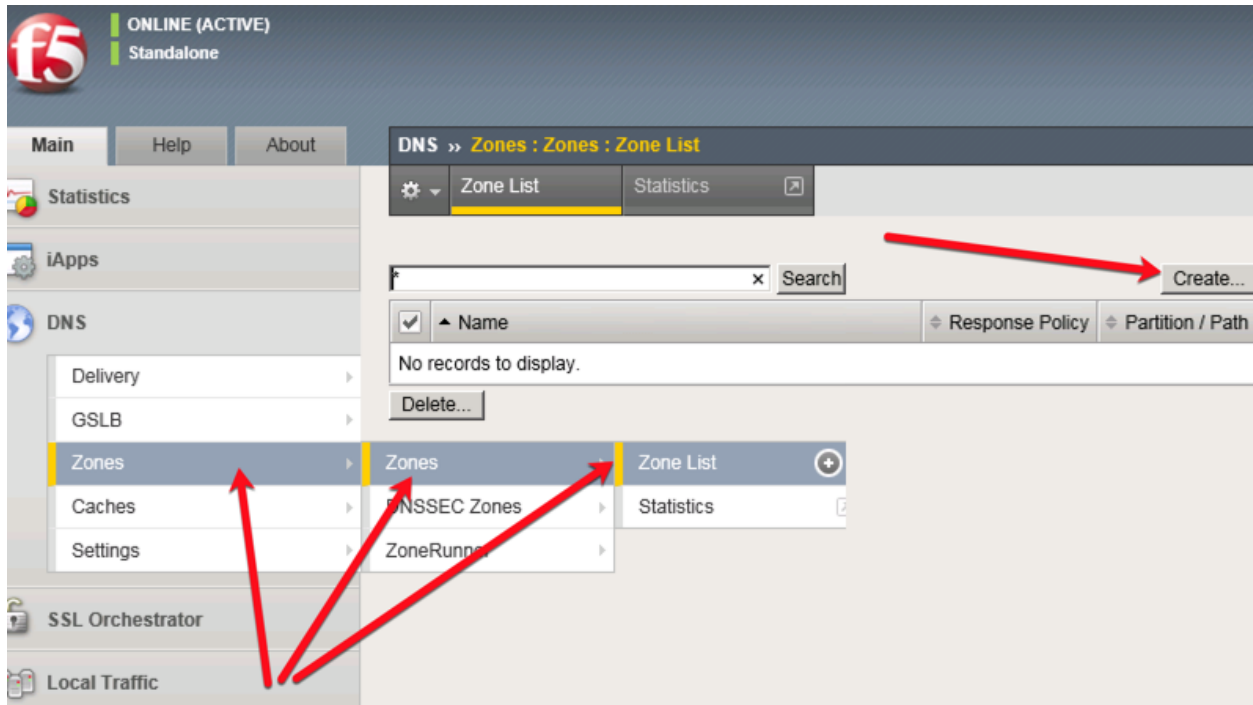


## TMSH

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

### DNS Express

Navigate to **DNS » Zones : Zones : Zone List**



Create a DNS Express zone according to the following table:

Setting	Value
Name	rpz.example.com
Server	localhost
Allow NOTIFY From	127.0.0.1
Verify Notify TSIG	un-checked
Response Policy	checked

**General Properties**

Name:

**DNS Express**

Server:

Availability: ☐ Unknown

State:

Notify Action:

Address:

127.0.0.1

Verify Notify TSIG: ☐

Response Policy: ☒

**Zone Transfer Clients**

Nameservers:

**TSIG**

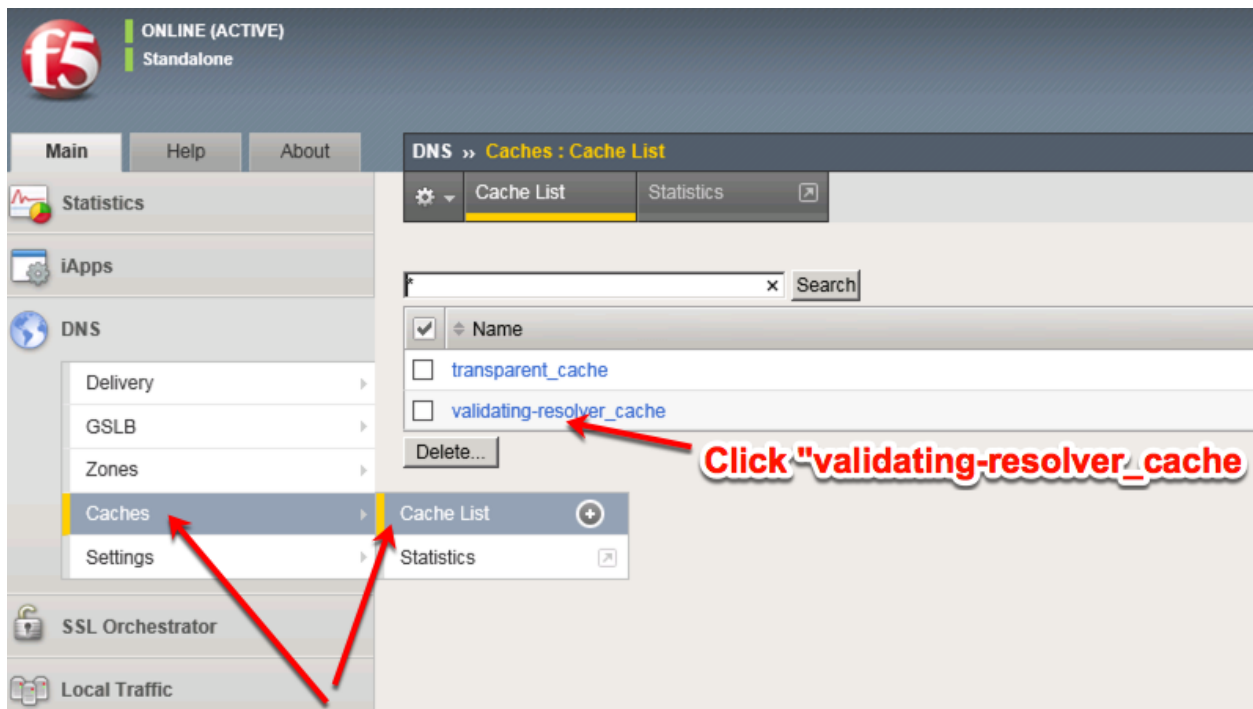
Server Key:

## TMSH

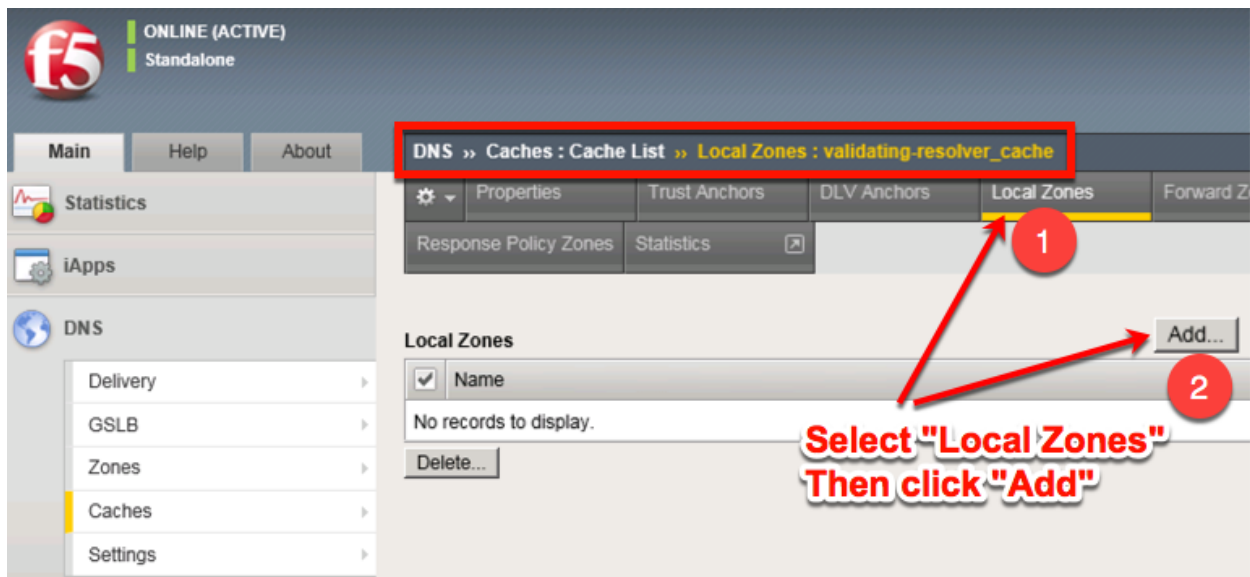
```
tmsh create ltm dns zone rpz.example.com { dns-express-server localhost response-policy yes dns-express-allow-notify add { 127.0.0.1 } dns-express-notify-tsig-verify no }
```

## Local Zone

Navigate to: **DNS » Caches : Cache List**



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



Create a local zone entry according to the following table:

Setting	Value
Name	sorry.example.com
Type	Static
Records	sorry.example.com. IN A 10.1.20.252

**Local Zone**

Name	sorry.example.com	No "dot" at the end!!
Type	Static	
Records	sorry.example.com. IN A 10.1.20.252 sorry.example.com. IN A 10.1.20.252	There is a "dot" at the end!!

Delete

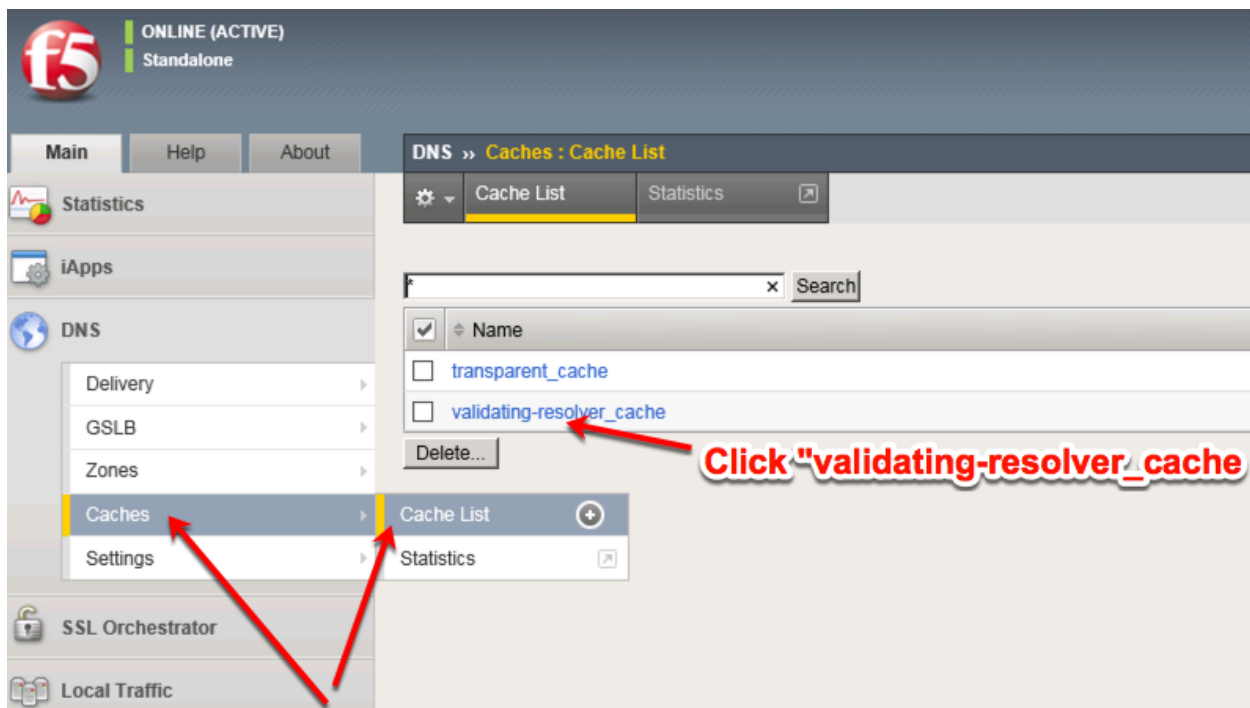
## TMSH

```
tmsl modify ltm dns cache validating-resolver validating-resolver_cache local-zones { { name
sorry.example.com records add { "sorry.example.com. IN A 10.1.20.252" } type static } }
```

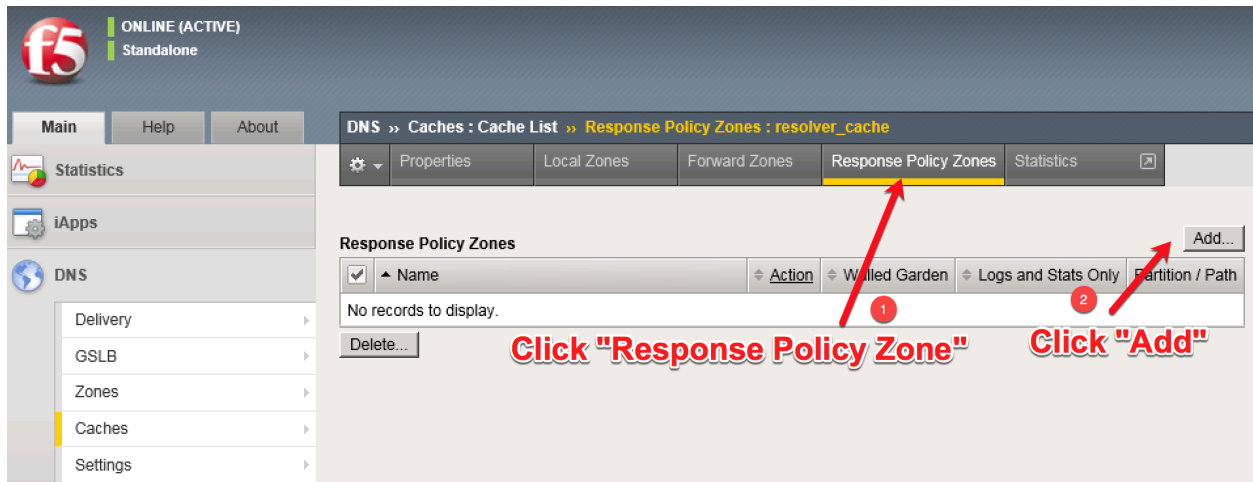
## Walled Garden

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

Click "validating-resolver\_cache"



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



Create a response policy zone entry according to the following table:

Setting	Value
Zone	rpz.example.com
Action	Walled Garden
Walled Garden	sorry.example.com

**Response Policy Zone**

Zone	<input type="text" value="rpz.example.com"/>
Action	<input type="text" value="Walled Garden"/>
Walled Garden	<input type="text" value="sorry.example.com"/>
Logs and Stats Only	<input type="checkbox"/>

## TMSH

```
tmsl modify ltm dns cache resolver validating-resolver_cache response-policy-zones add {
rpz.example.com { action walled-garden walled-garden sorry.example.com } }
```

## Results

From a shell on the Ubuntu Client:

First, a query that returns no response:

```
dig @10.1.10.53 www.fuzzybunnies.com
```



```

root@ip-10-1-1-6:/# dig @10.1.10.53 www.fuzzybunnies.com

; <<> DiG 9.10.3-P4-Ubuntu <<> @10.1.10.53 www.fuzzybunnies.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 7454
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.fuzzybunnies.com.      IN      A

;; ANSWER SECTION:
www.fuzzybunnies.com.      300     IN      CNAME   sorry.example.com.
sorry.example.com.         3600    IN      A        10.1.20.252

;; AUTHORITY SECTION:
rpz.example.com.           300     IN      SOA      master.example.com. hostmaster.master.example.com. 2020020802 10800 3600 604
800 86400

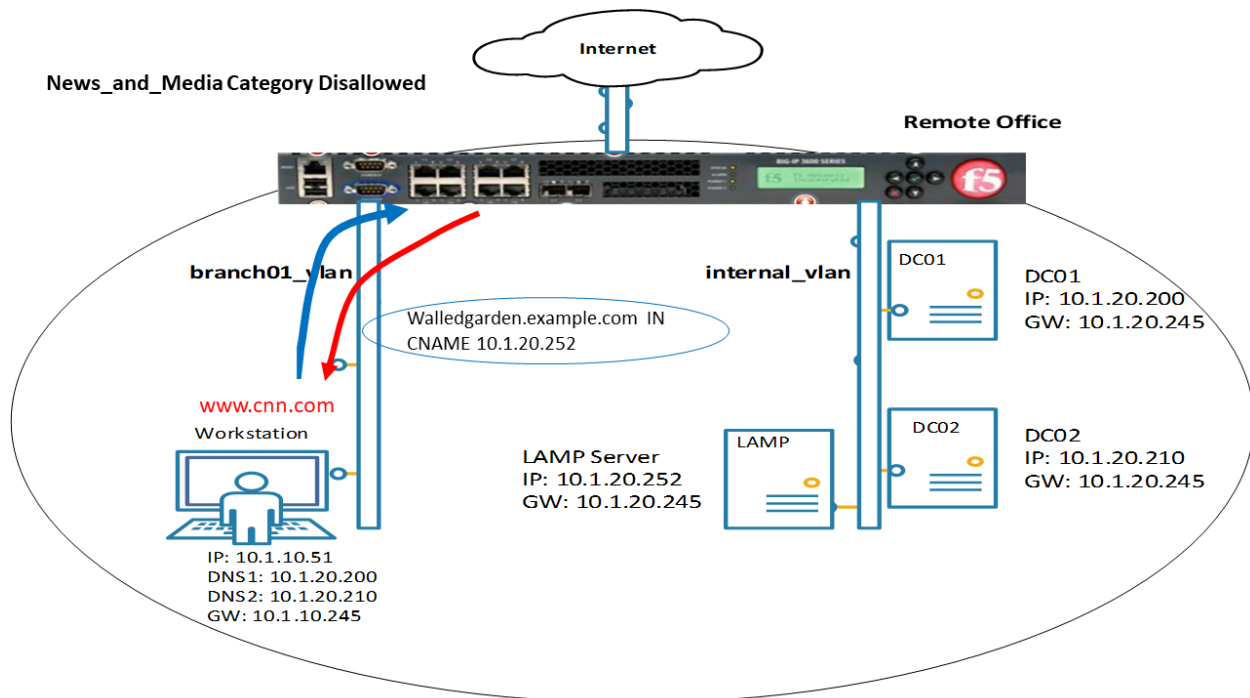
;; Query time: 0 msec
;; SERVER: 10.1.10.53#53(10.1.10.53)
;; WHEN: Sat Feb 08 19:06:27 UTC 2020
;; MSG SIZE rcvd: 165

```

Matches to RPZ will respond back with the walled garden IP from the local zone. Alternatively, the action could be changed from Walled Garden!

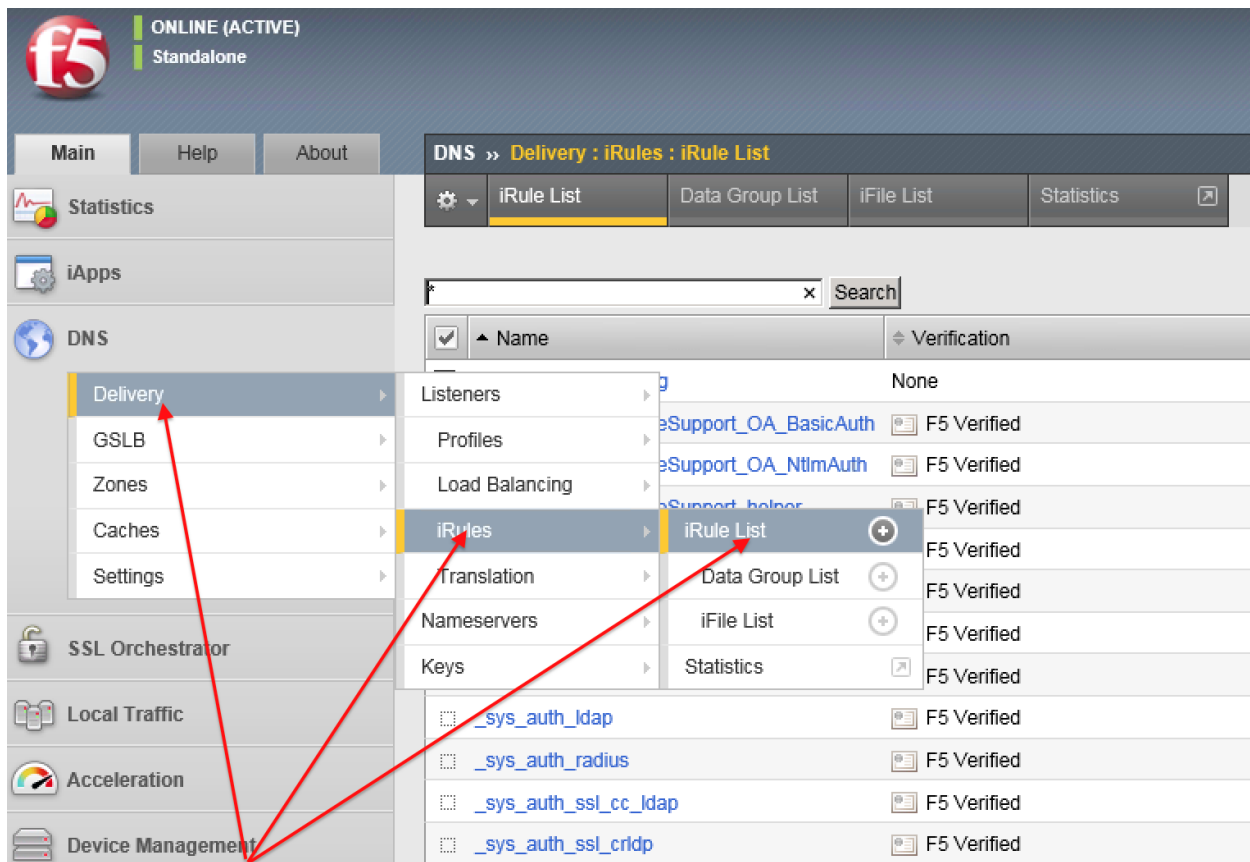
### 3.1.7 URL Categorization

For the final lab, we will configure DNS query filtering based on the category of the requested domain. This will be done with using F5 iRules and built-in categorization database.



#### Create an iRule

Navigate to: **DNS » Delivery : iRules : iRules List**



Create a new iRule by copying the content below and pasting into the iRule editor window:

Setting	Value
Name	DNS-query-filtering

```
when RULE_INIT {
  # Set categories to block for DNS hosts
  set static::blocked_categories {
    /Common/Bot_Networks
    /Common/Spyware
    /Common/Malicious_Web_Sites
    /Common/Adult_Content
    /Common/Entertainment
  }

  # CONFIGURATION
  # Check all requests by default
  set static::request_check 1
  # If the category returns as blocked, return NXDOMAIN (1)
  # Otherwise if (0), return a statically defined IP address
  set static::request_return_nxdomain 0
  set static::request_redirect_to "10.1.20.252"
  # Toggle for debug logs
  set static::request_debug 1
}
```

(continues on next page)

(continued from previous page)

```

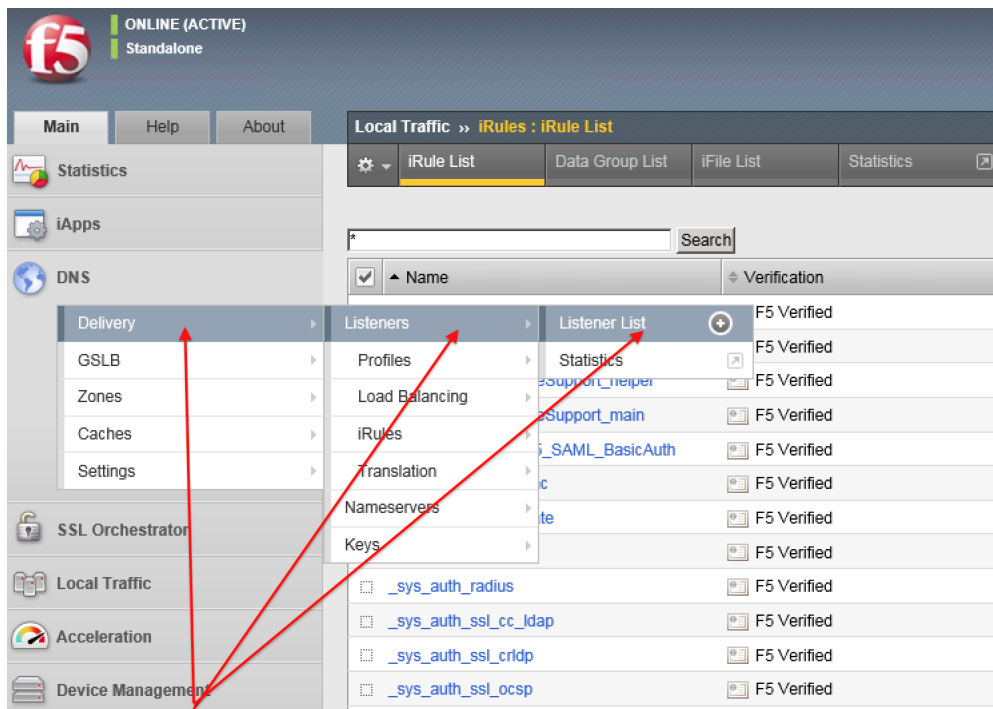
when DNS_REQUEST {
    if { $static::request_check } {
        set lookup_category [getfield [CATEGORY::lookup "http://[DNS::question name]" ] "
↪" 1]
        if { [lsearch -exact $static::blocked_categories $lookup_category] >= 1 } {
            if { $static::request_debug } {
                log local0. "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_
↪filtered"
            }
        }
    }
}
}

```

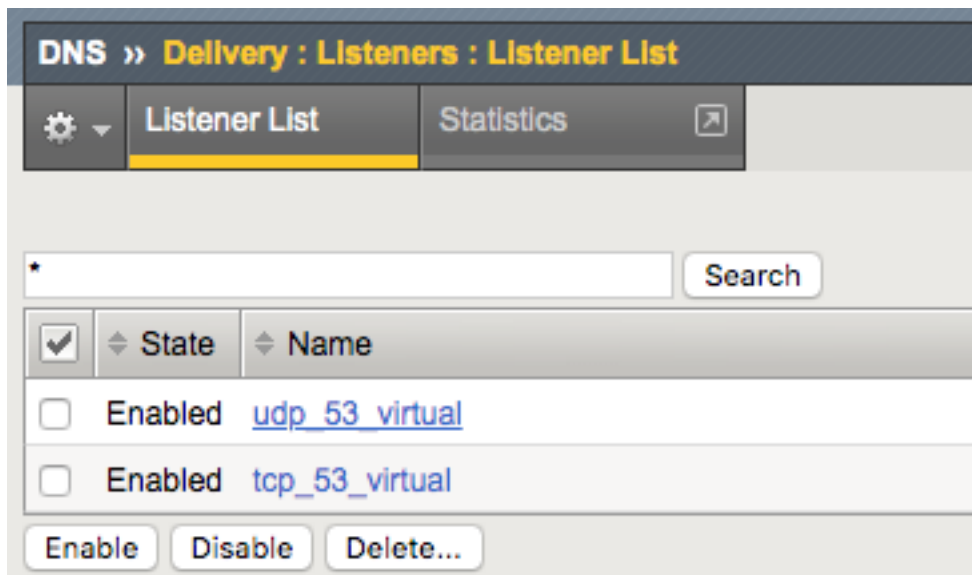
### iRule assignment

Assigned the iRule to the DNS Listeners:

Navigate to: **DNS » Delivery : Listeners : Listener List**



Navigate to the *udp\_53\_virtual* listener:



Navigate to the iRules section

**DNS » Delivery : Listeners : Listener List » Properties : udp\_53\_virtual**

**General**

Name	udp_53_virtual
Partition	Common
Description	<input type="text"/>
State	Enabled <input type="button" value="↑"/> <input type="button" value="↓"/>

Click Manage button and assign the iRule

**DNS » Delivery : Listeners : Listener List » Properties : udp\_53\_virtual**

**iRule Management**

	Selected		Available
iRules	/Common	<input type="button" value="&lt;&lt;"/> <input type="button" value="&gt;&gt;"/>	/Common
	DNS-query-filtering		_sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtimAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main
	<input type="button" value="Up"/> <input type="button" value="Down"/>		

## TMSH

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

## Results

With the iRule applied, DNS queries will be processed and log messages sent out. Open a shell to the BIG-IP and run :

```
tail -f /var/log/ltm
```

Now run DNS queries from the Ubuntu Client:

```
dig @10.1.10.53 www.f5.com
```

And analyze the results:

```
Feb 13 14:47:14 ip-10-1-1-4 info tmm[10647]: 2020-02-13 14:47:13 ip-10-1-1-4.us-west-
↳2.compute.internal qid 29530 from 10.1.10.4#43881: view none: query: www.f5.com IN
↳A +E (10.1.10.53%)
Feb 13 14:47:14 ip-10-1-1-4 info tmm3[10647]: Rule /Common/DNS-query-filtering <DNS_
↳REQUEST>: Category /Common/Uncategorized matching www.f5.com is not filtered
Feb 13 14:47:14 ip-10-1-1-4 info tmm[10647]: 2020-02-13 14:47:14 ip-10-1-1-4.us-west-
↳2.compute.internal qid 29530 to 10.1.10.4#43881: [NOERROR qr,rd,ra] response: www.
↳f5.com. 30 IN CNAME dwbfwz8xncmgm.cloudfront.net; dwbfwz8xncmgm.cloudfront.net. 60
↳IN A 99.86.33.52; dwbfwz8xncmgm.cloudfront.net. 60 IN A 99.86.33.5; dwbfwz8xncmgm.
↳cloudfront.net. 60 IN A 99.86.33.9; dwbfwz8xncmgm.cloudfront.net. 60 IN A 99.86.33.
↳53;
```

The query *www.f5.com* did not match any categories, and was resolved. Now lets try a matching query:

```
dig @10.1.10.53 www.tzm.com
```

Notice the DNS response is quite different as well as the log entry on the BIG-IP.

```
Feb 13 15:27:37 ip-10-1-1-4 info tmm[10647]: Rule /Common/DNS-query-filtering <DNS_
↳REQUEST>: BLOCKED: Category /Common/Entertainment matching www.tzm.com is filtered.
Feb 13 15:27:37 ip-10-1-1-4 info tmm[10647]: 2020-02-13 15:27:36 ip-10-1-1-4.us-west-
↳2.compute.internal qid 32427 to 10.1.10.4#55151: [NOERROR qr,rd,ad] response: www.
↳tzm.com. 111 IN A 10.1.20.252;
```

You can experiment with various queries to see the catagory of the domain name via the log messages. If you want to add a new category, edit the iRule accordingly.

To list current categories, from the BIG-IP enter the TMSH shell with *tms*, then run the following command:

```
root@(ip-10-1-1-4) (cfg-sync Standalone) (TimeLimitedModules::Active) (/Common) (tmos) #
↳list sys url-db url-category
```

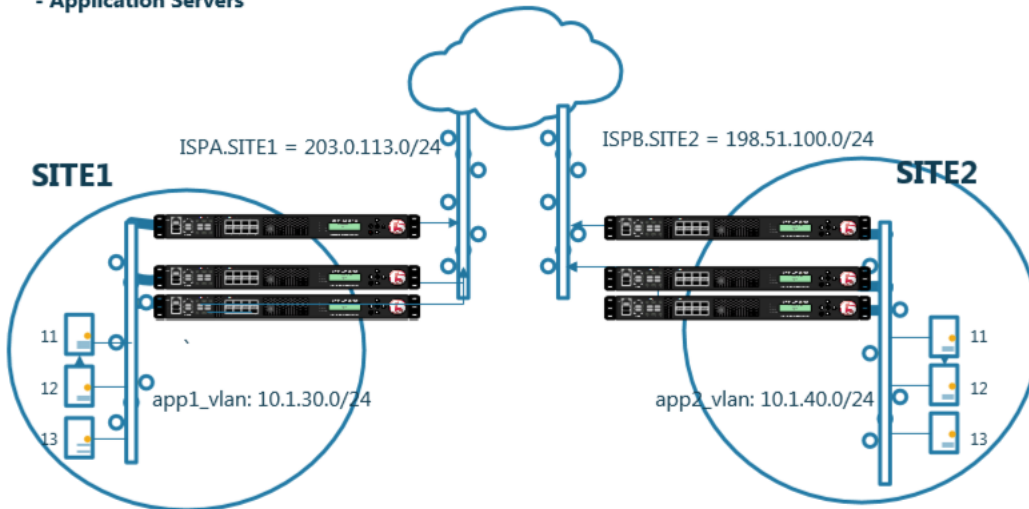
## Class 3 - Data Center Availability Services Using BIG-IP DNS

- 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.

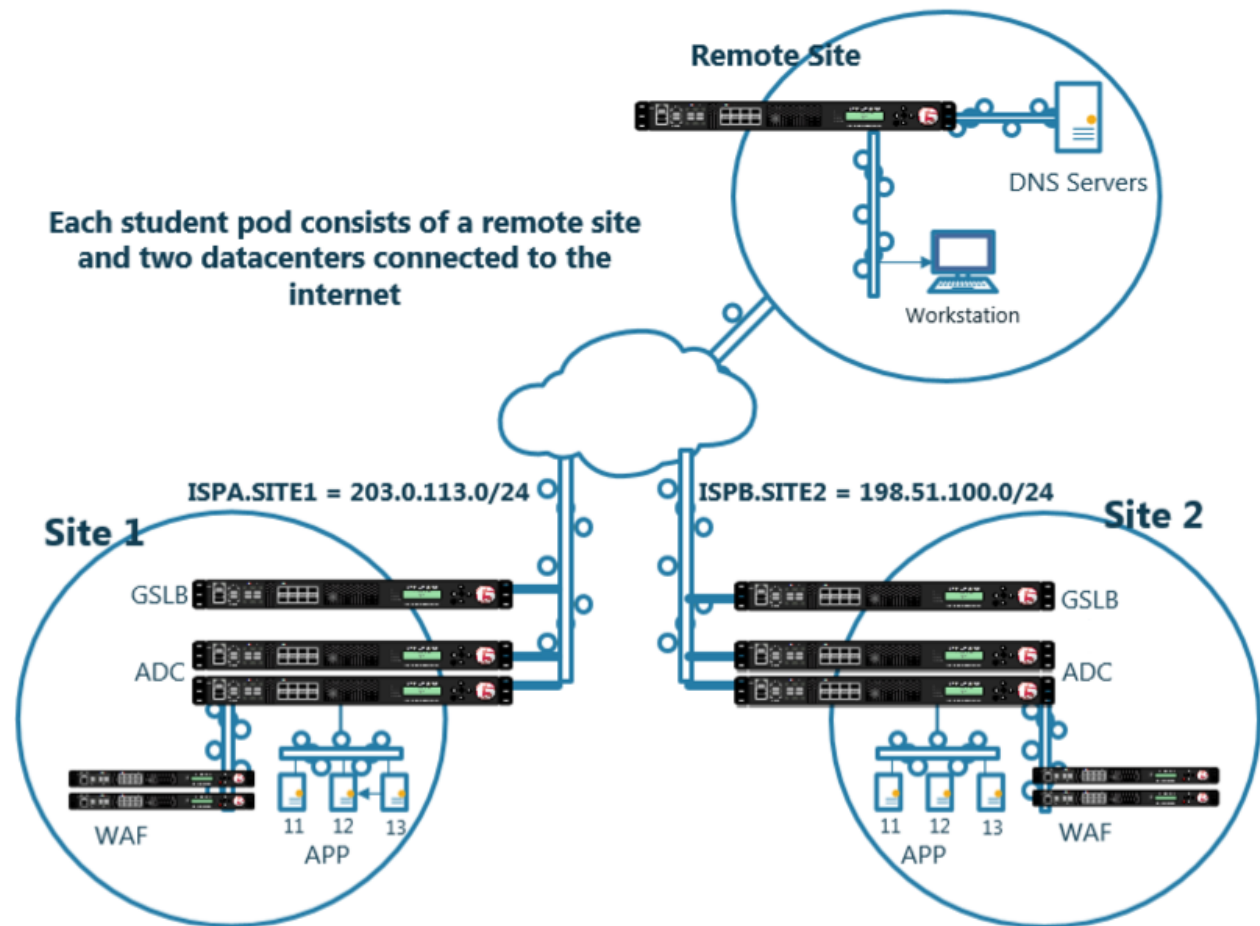
**EXAMPLE INC.** occupies two datacenters. Each datacenter is identically configured with:

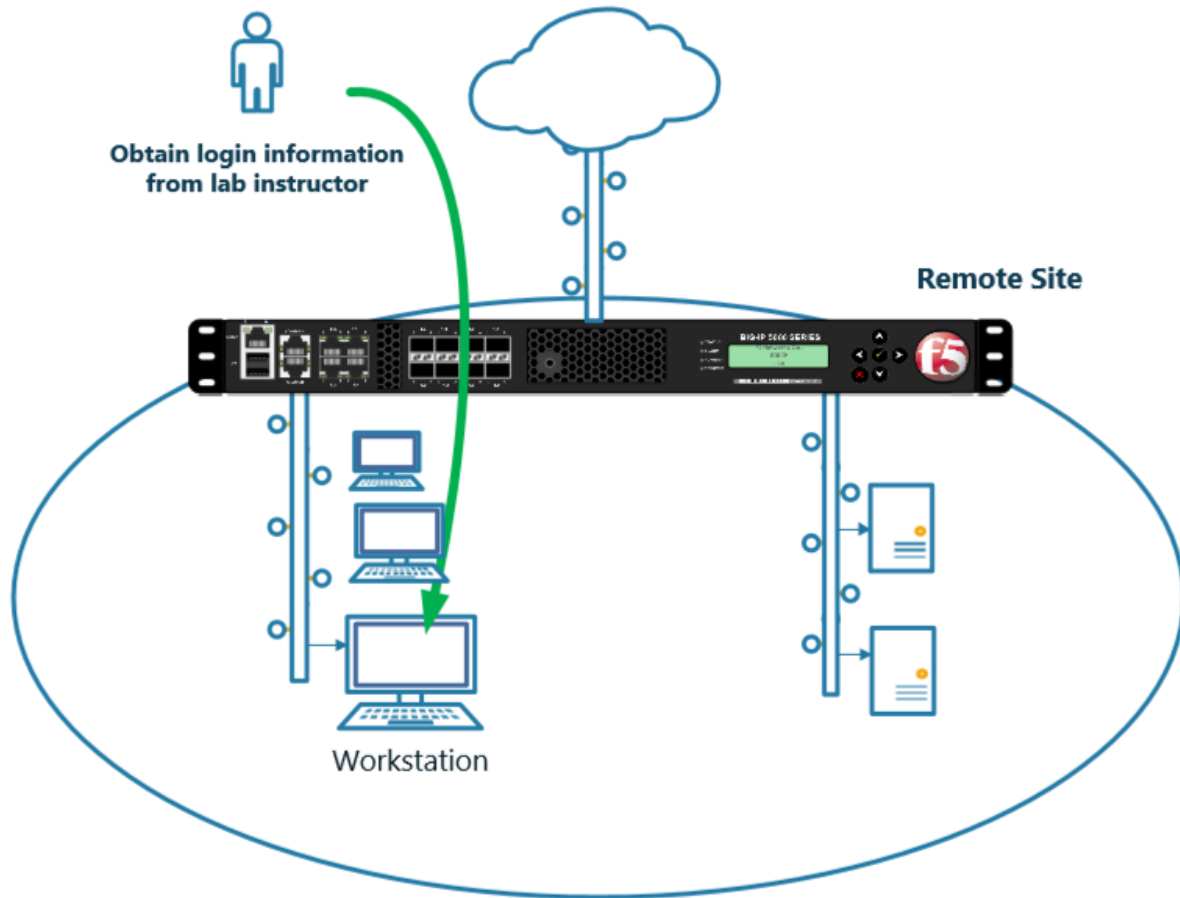
- HA pair of F5 ADC
- Standalone F5 DNS
- Application Servers

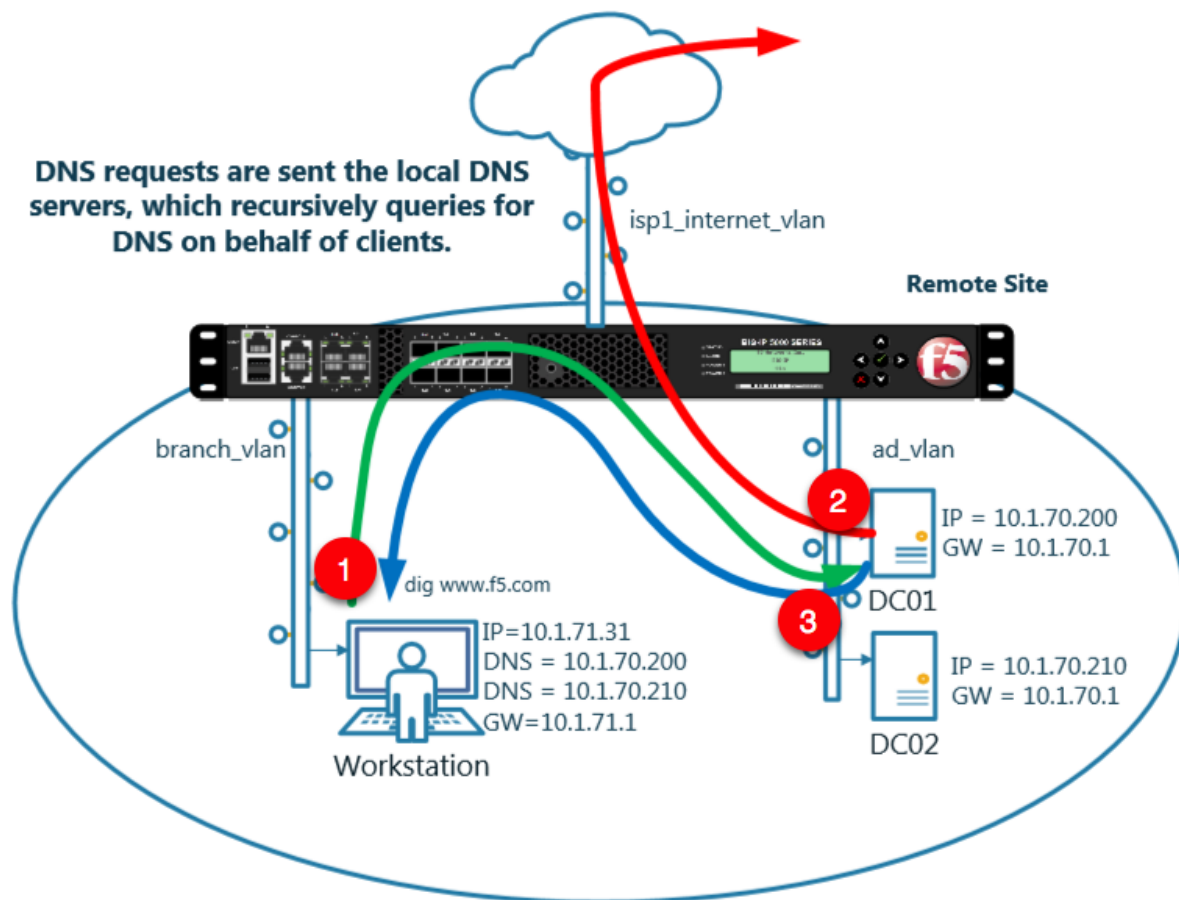


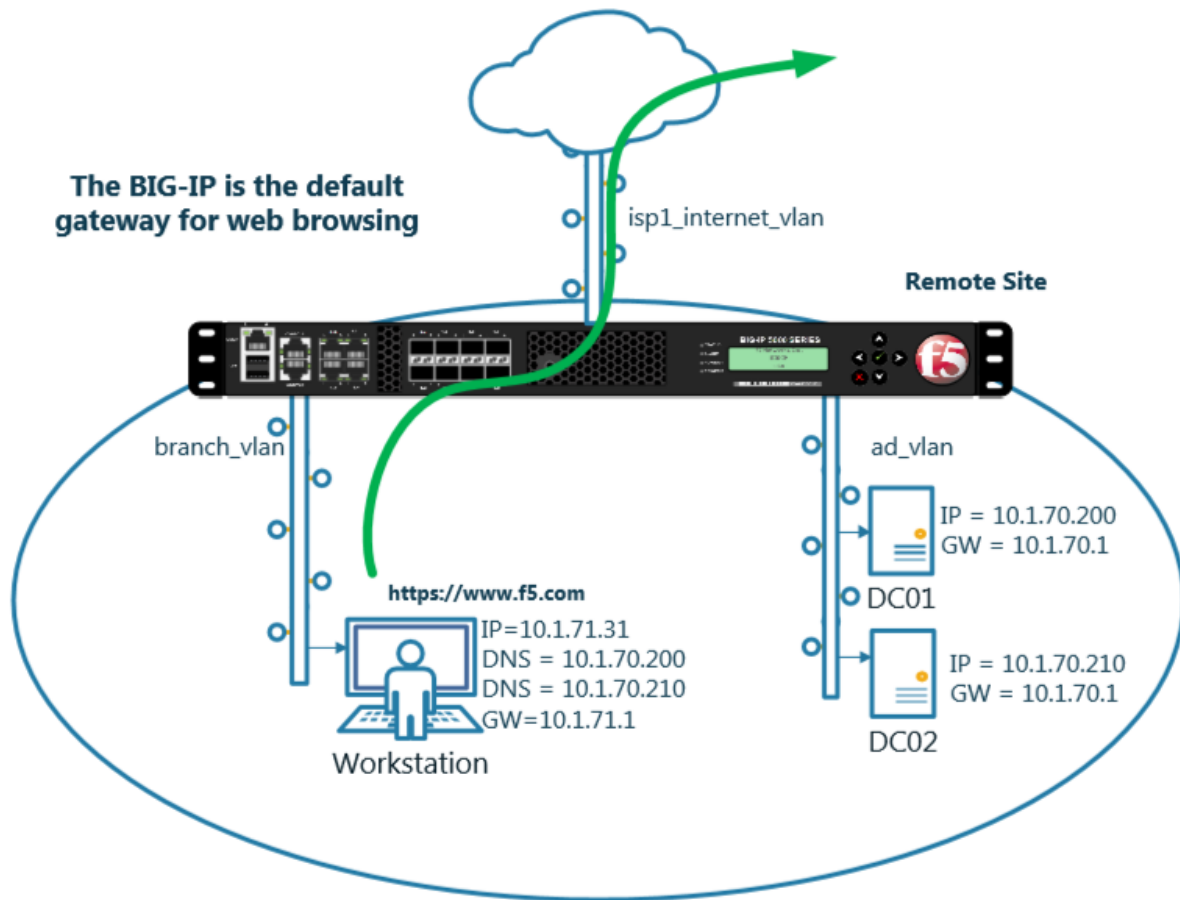


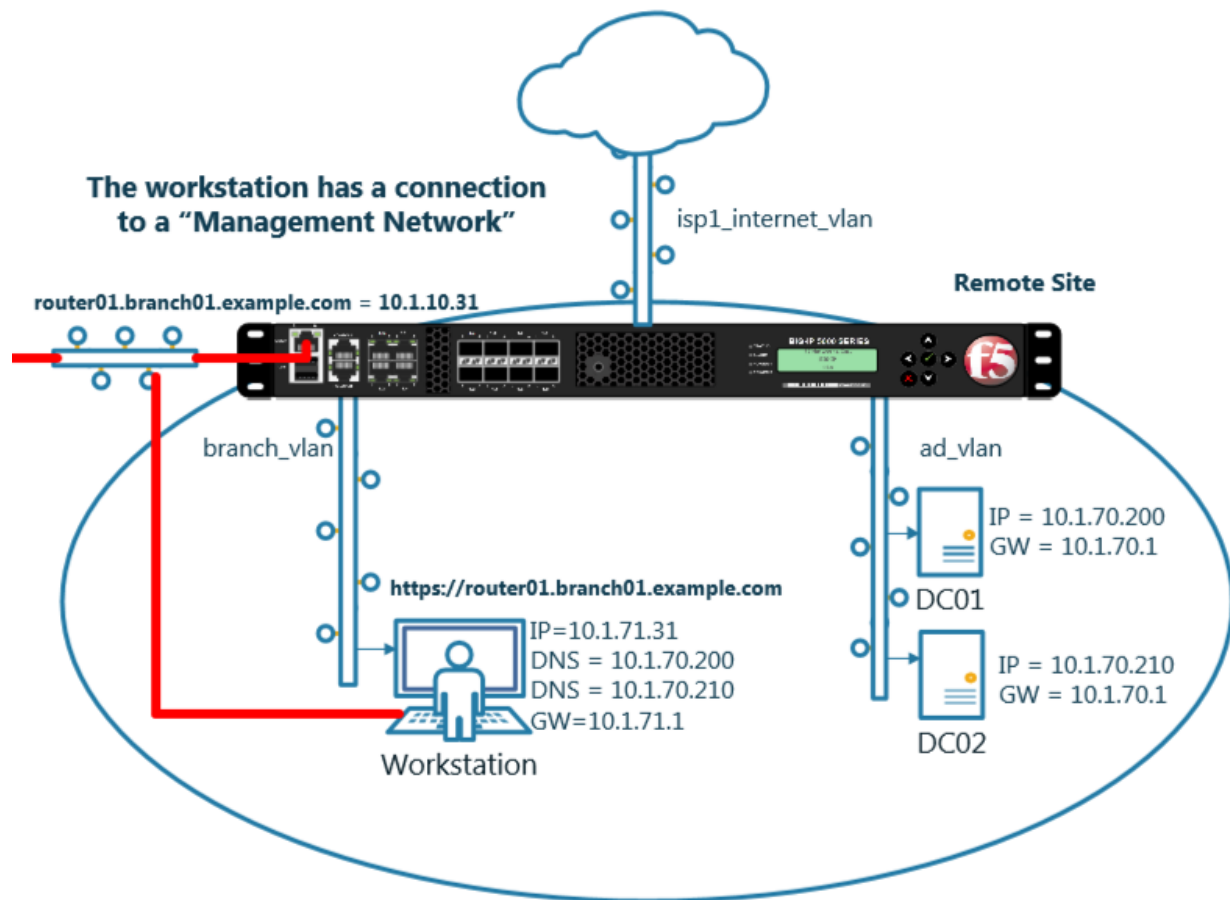
## 4.1 Network Map

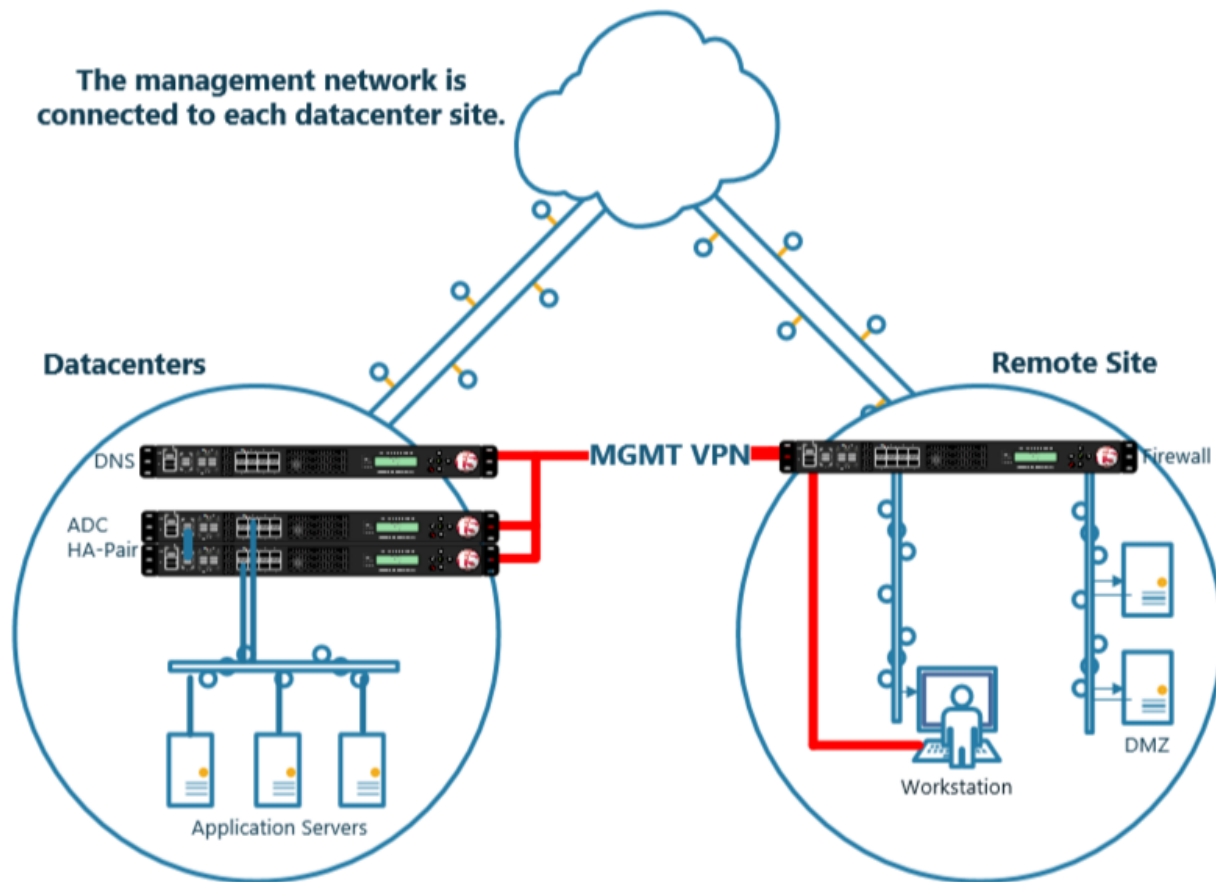












## 4.2 System

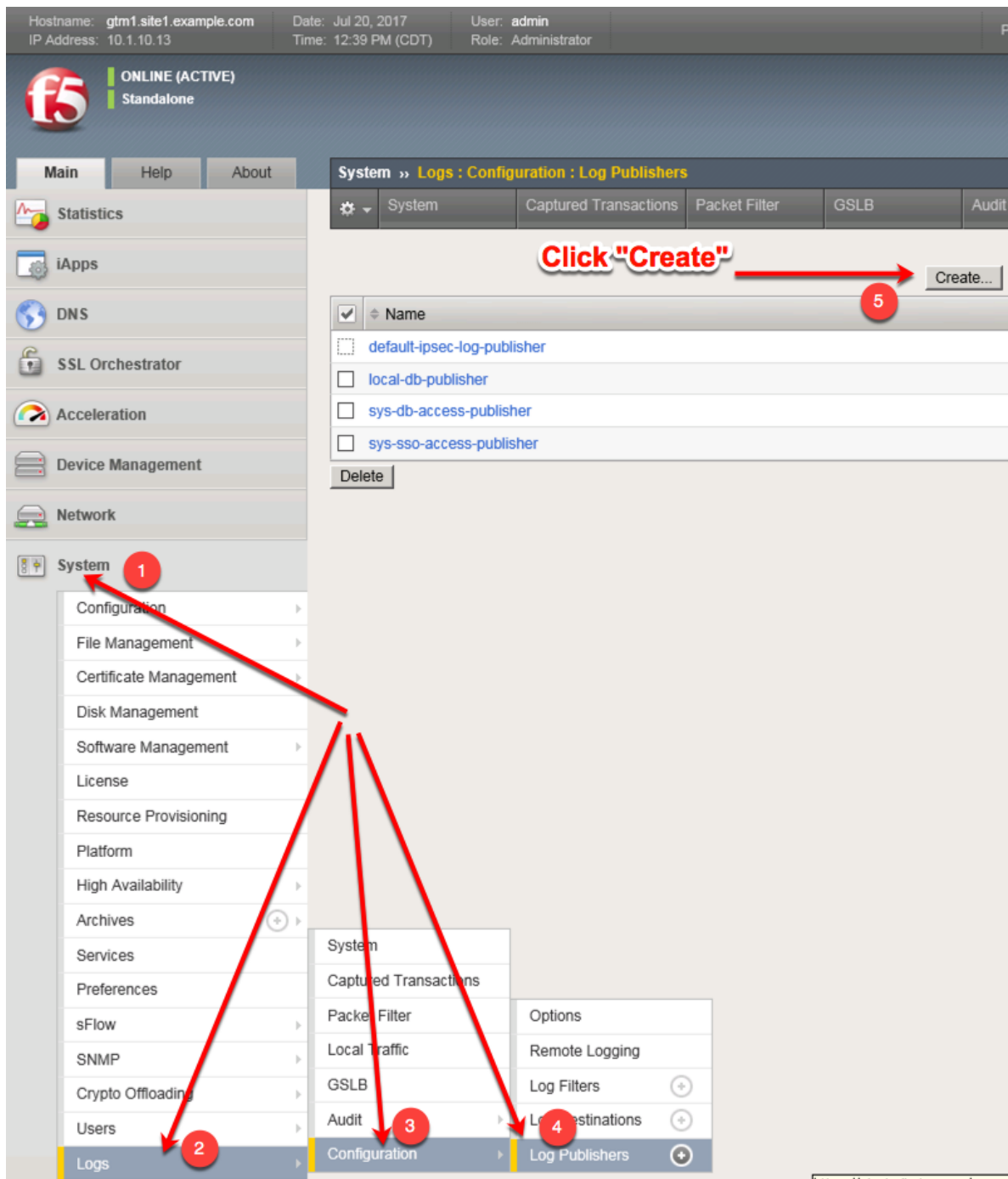
A BIG-IP System needs to be prepared before creating a GSLB configuration. Administrative tasks including SNMP/DNS/NTP settings have already been completed. The task of creating a “Logging Profile” is the beginning of this class. Create a log publisher and a DNS logging profile and then associate the 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”

---

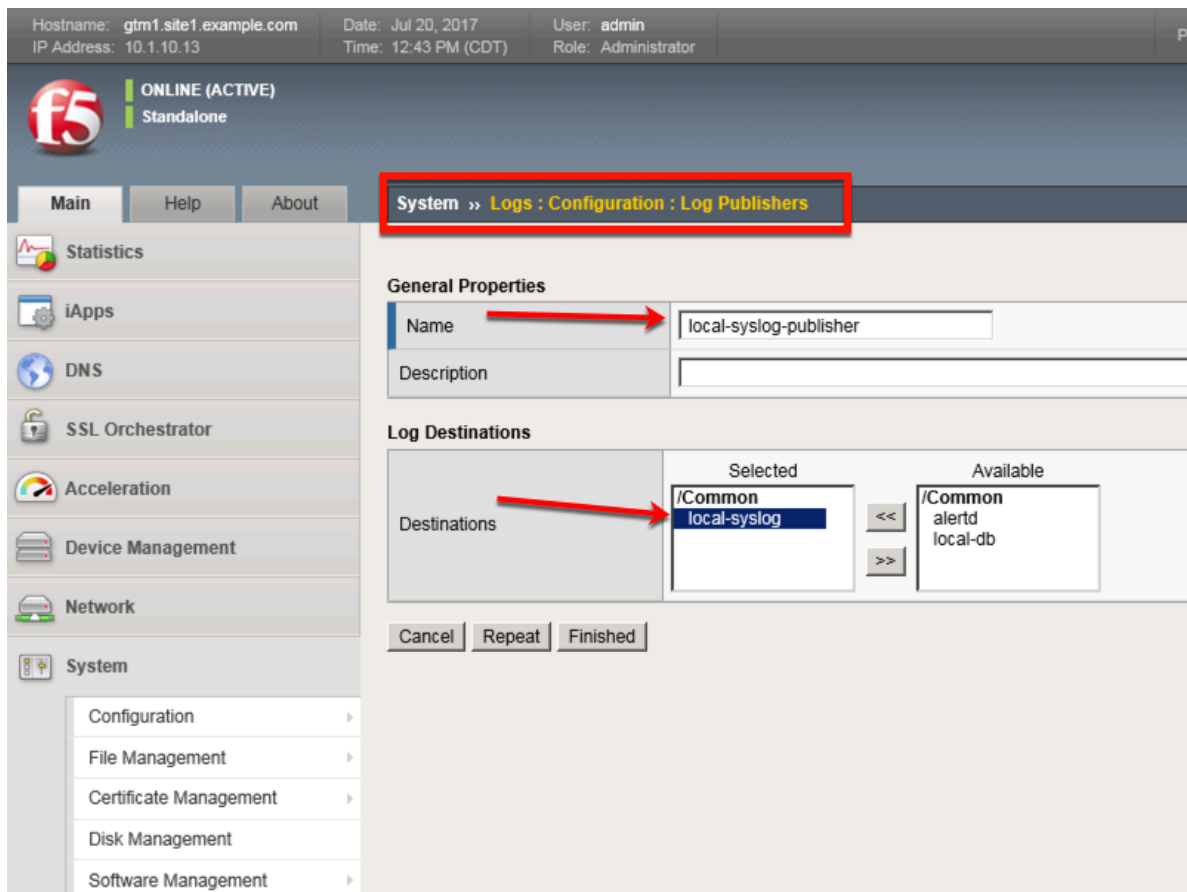
**Note:** It is required to complete the following task on both gtm1.site1 and gtm1.site2

---



Create a local syslog publisher according to the table below:

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



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

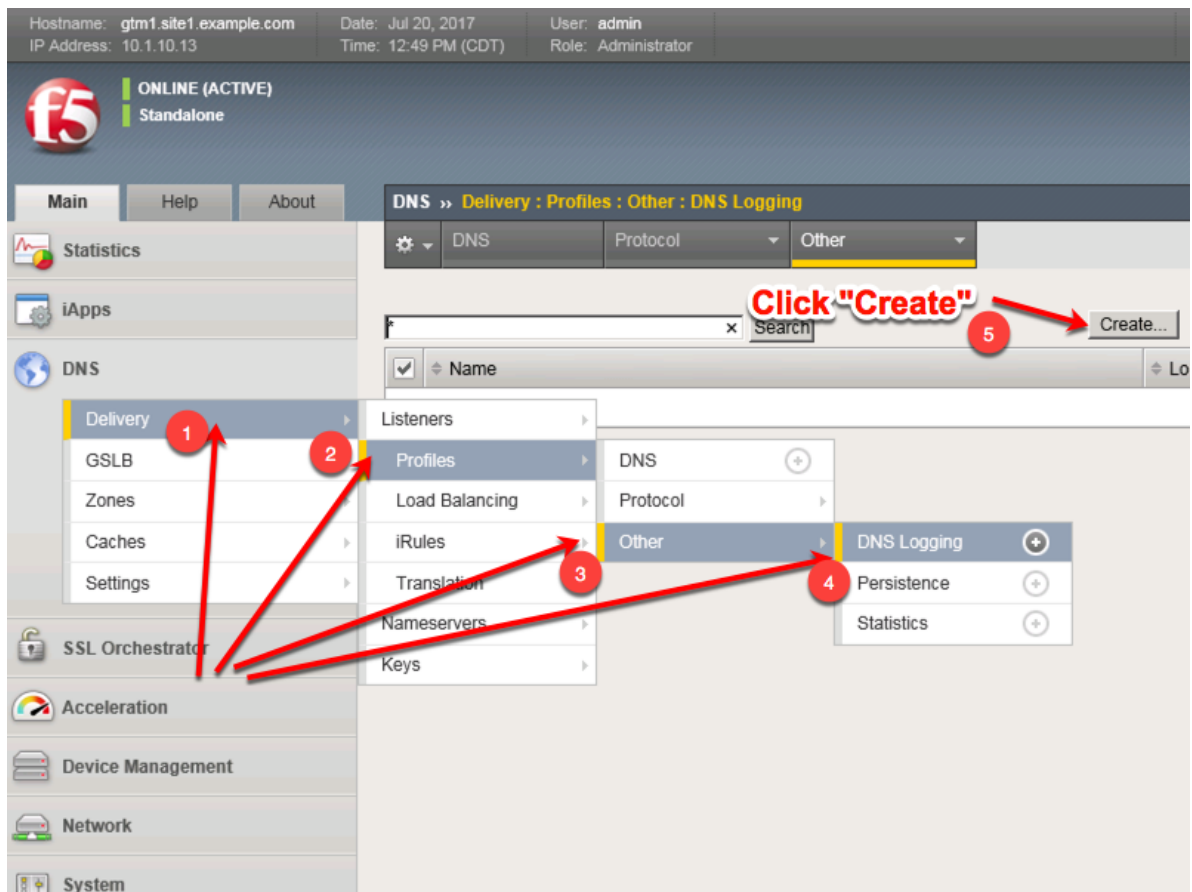
#### TMSH

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

2. Create a "Logging Profile"

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





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: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 12:52 PM (CDT) Role: Administrator

ONLINE (ACTIVE)  
Standalone

Main Help About

DNS » Delivery : Profiles : Other : DNS Logging » New...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name example\_dns\_logging\_profile  
Description

**Configuration**

Log Publisher local-syslog-publisher  
Log Queries ☒ Enabled  
Log Responses ☒ Enabled

**Log Fields**

Include Complete Answer ☒ Enabled  
Include Query ID ☒ Enabled  
Include Source ☒ Enabled  
Include Timestamp ☒ Enabled  
Include View ☒ Enabled

Cancel Repeat Finished

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

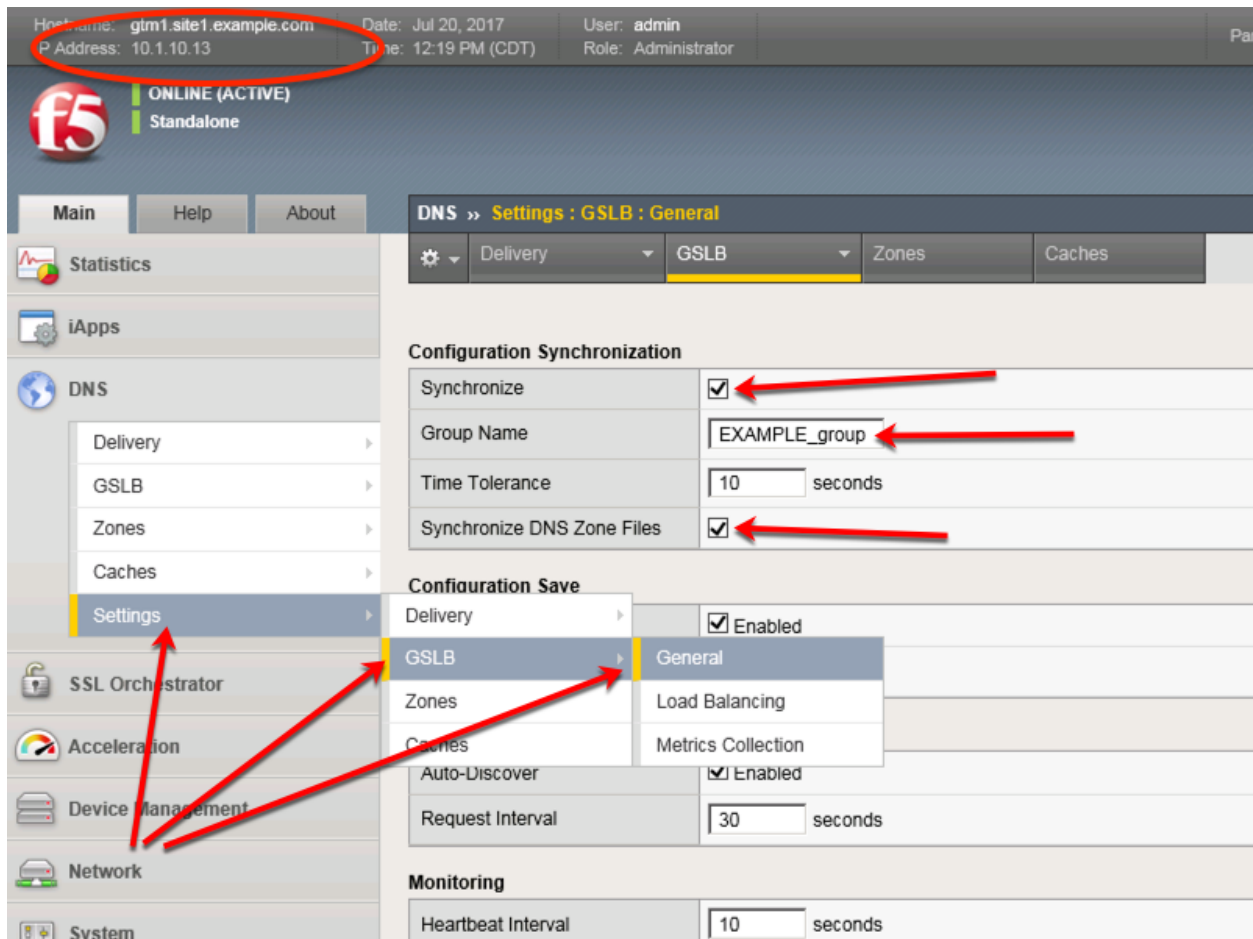
#### TMSH

```
tmsh create ltm profile dns-logging example_dns_logging_profile enable-response-logging yes
include-query-id yes log-publisher local-syslog-publisher
```

## 4.3 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.



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

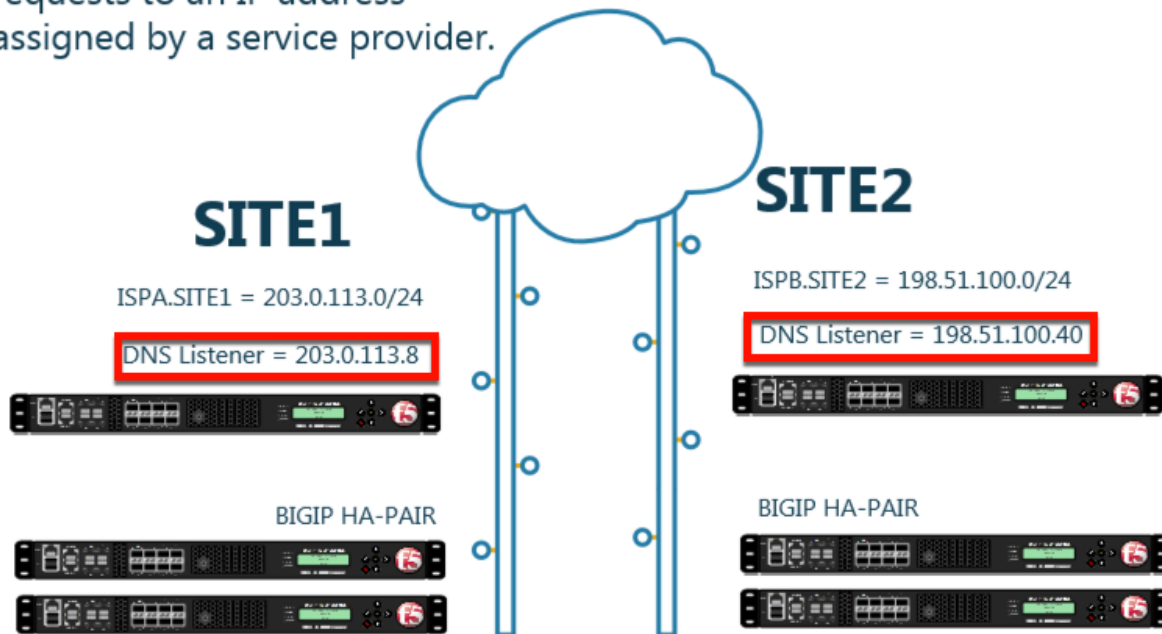
```
tmsh modify gtm global-settings general synchronization yes synchronization-group-name EXAM-
PLE_group synchronize-zone-files yes
```

## 4.4 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.

A listener will receive DNS requests to an IP address assigned by a service provider.



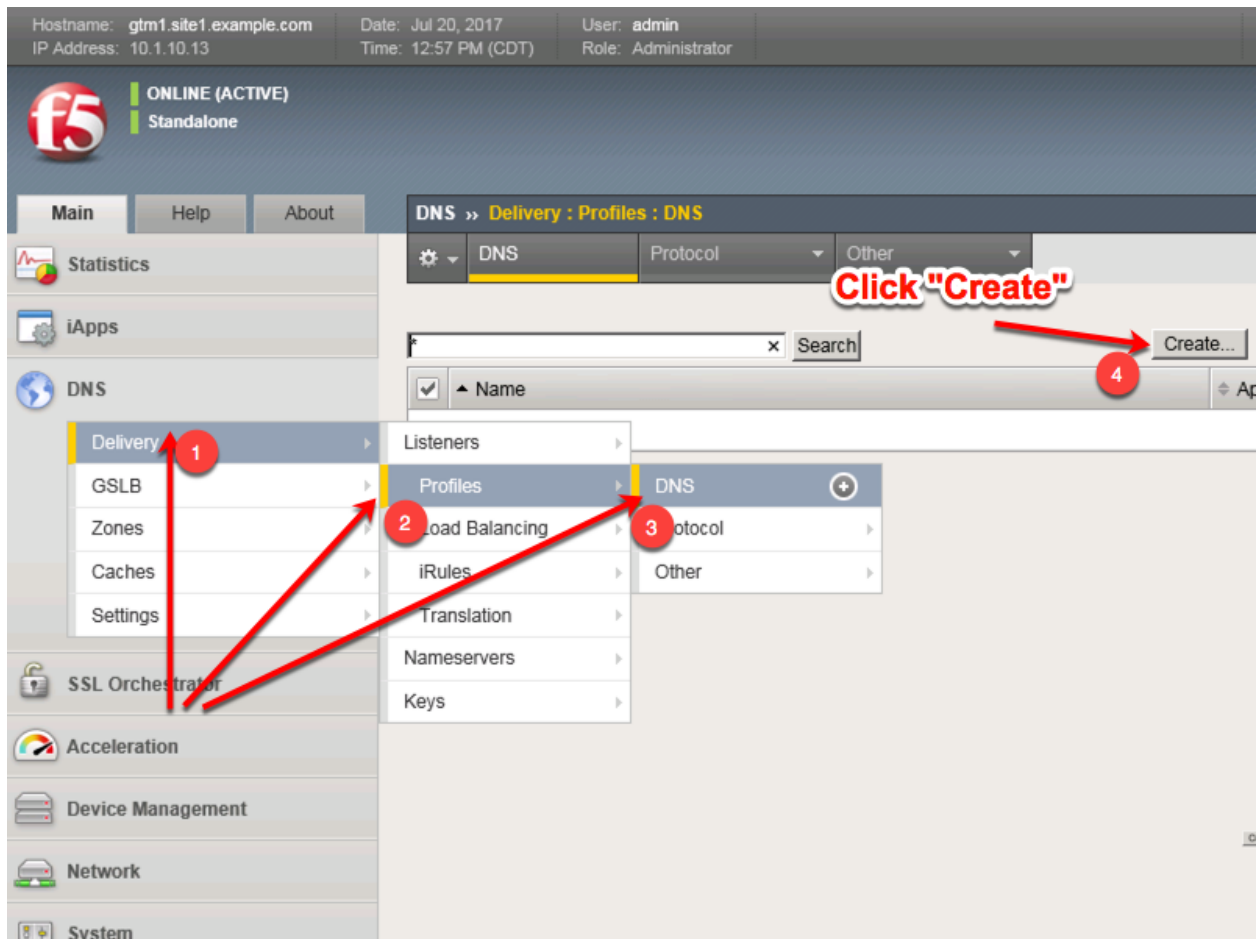
### 4.4.1 DNS Profile

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`

---



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

**General Properties**

Name	example.com_dns_profile
Partition / Path	Common
Parent Profile	dns

**Denial of Service Protection** Custom ☐

Rapid Response Mode	Disabled	<input type="checkbox"/>
Rapid Response Last Action	Drop	<input type="checkbox"/>

**Hardware Acceleration**

Protocol Validation	Disabled	<input type="checkbox"/>
Response Cache	Disabled	<input type="checkbox"/>

**DNS Features**

DNSSEC	Disabled	<input checked="" type="checkbox"/>
GSLB	Enabled	<input type="checkbox"/>
DNS Express	Disabled	<input checked="" type="checkbox"/>
DNS Cache	Disabled	<input type="checkbox"/>
DNS Cache Name	Select...	<input type="checkbox"/>
DNS IPv6 to IPv4	Disabled	<input type="checkbox"/>
Unhandled Query Actions	Drop	<input checked="" type="checkbox"/>
Use BIND Server on BIG-IP	Disabled	<input checked="" type="checkbox"/>

**DNS Traffic**

Zone Transfer	Disabled	<input type="checkbox"/>
DNS Security	Disabled	<input type="checkbox"/>
DNS Security Profile Name	Select...	<input type="checkbox"/>
Process Recursion Desired	Enabled	<input type="checkbox"/>

**Logging and Reporting**

Logging	Enabled	<input checked="" type="checkbox"/>
Logging Profile	example_dns_logging_profile	<input checked="" type="checkbox"/>
AVR Statistics Sample Rate	<input checked="" type="checkbox"/> Enabled 1/ 1 queries sampled	<input checked="" type="checkbox"/>

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

### TMSH

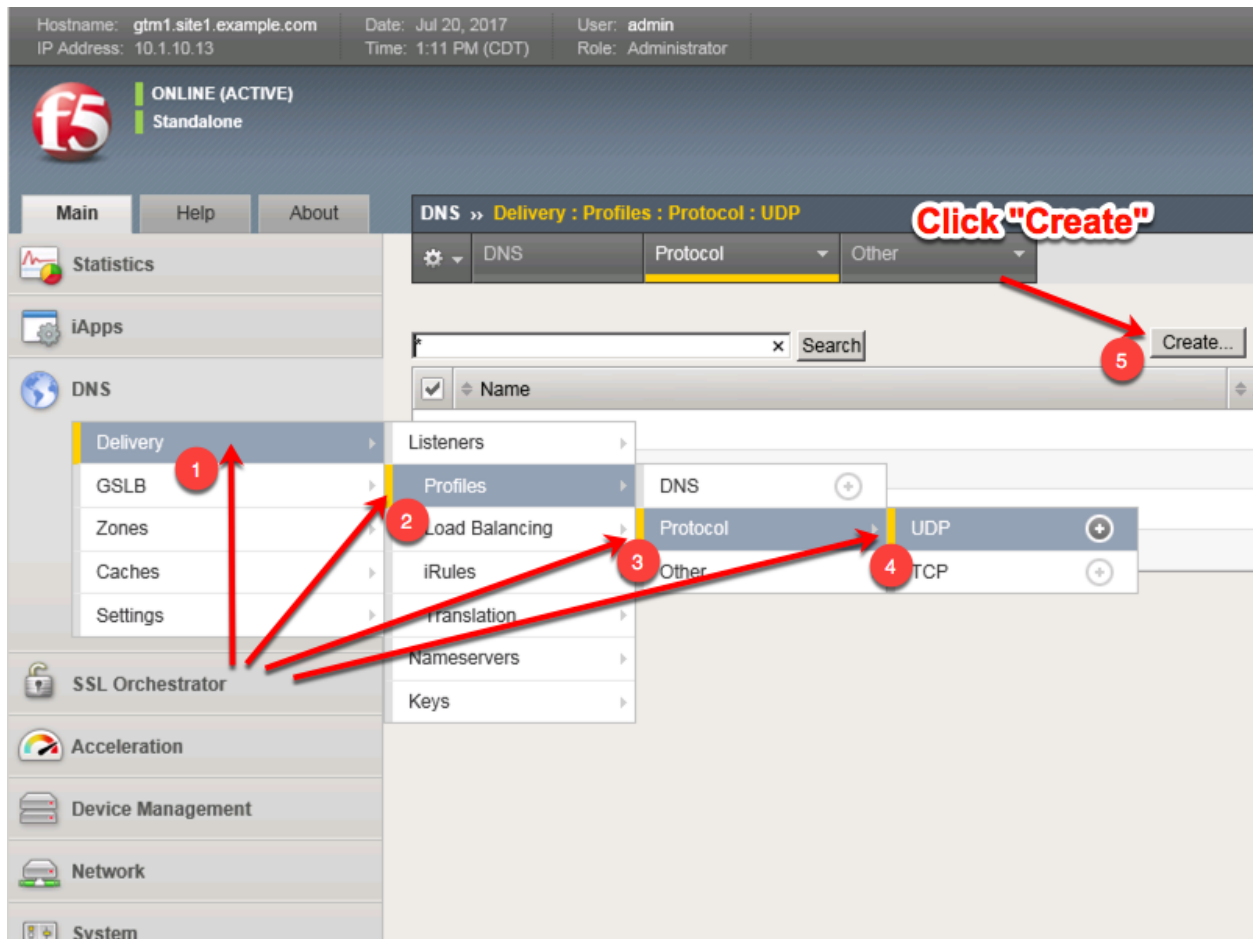
```
tms create ltm profile dns example.com_dns_profile use-local-bind no unhandled-query-action drop log-profile example_dns_logging_profile enable-logging yes avr-dnsstat-sample-rate 1 enable-dns-express no enable-dnssec no
```

## 4.4.2 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 required to complete the following task on both gtm1.site1 and gtm1.site2



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

Field	Value
Name	example.com_udp-dns_profile
Parent Profile	udp_gtm_dns

Hostname: gtm1.site1.example.com Date: Jul 26, 2018 User: admin  
IP Address: 10.1.10.13 Time: 8:17 AM (EDT) Role: Administrator Partition: Common Log out

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

**DNS » Delivery : Profiles : Protocol : UDP » New UDP Profile...**

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name   
Parent Profile

**Settings** Custom ☐

Proxy Maximum Segment	<input type="checkbox"/>	<input type="checkbox"/>
Idle Timeout	Specify... 5 seconds	<input type="checkbox"/>
IP ToS	Specify... 0	<input type="checkbox"/>
Link QoS	Specify... 0	<input type="checkbox"/>
Datagram LB	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Allow No Payload	<input type="checkbox"/>	<input type="checkbox"/>
TTL Mode	Proxy	<input type="checkbox"/>
Don't Fragment Mode	PMTU	<input type="checkbox"/>
Max Buffer Bytes	655350	<input type="checkbox"/>
Max Buffer Packets	0	<input type="checkbox"/>

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

## TMSH

```
tmsmsh create ltm profile udp example.com_udp-dns_profile defaults-from udp_gtm_dns
```

### 4.4.3 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 Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 1:23 PM (CDT) Role: Administrator Partition: Common

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About DNS » Delivery : Profiles : Protocol : TCP » New TCP Profile...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name example.com\_tcp-dns\_profile  
Parent Profile f5-tcp-wan

**Timer Management**

Close Wait	Specify...	5	seconds
Fin Wait 1	Specify...	5	seconds
Fin Wait 2	Specify...	300	seconds
Idle Timeout	Specify...	300	seconds
Keep Alive Interval	Specify...	1800	seconds
Minimum RTO		500	milliseconds
Reset On Timeout		<input checked="" type="checkbox"/> Enabled	
Time Wait	Specify...	2000	milliseconds
Time Wait Delay		<input checked="" type="checkbox"/> Enabled	
Zero Window Timeout	Specify...	20000	milliseconds

**Scroll way down to find the "Finish" button**

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

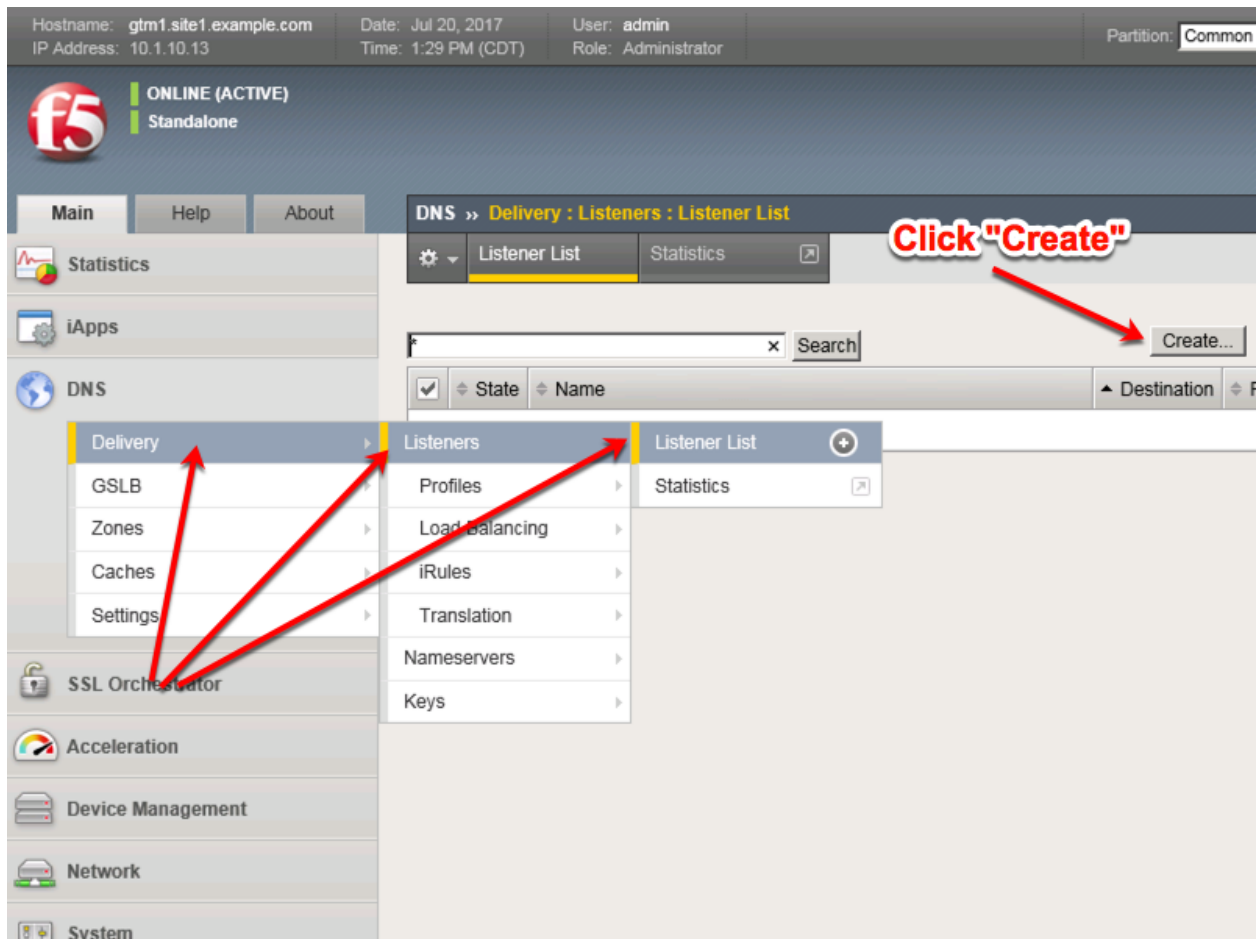
## TMSH

```
tmsh create ltm profile tcp example.com_tcp-dns_profile defaults-from f5-tcp-wan
```

### 4.4.4 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



Create a UDP listener according to the following table:

Field	gtm1.site1	gtm1.site2
Name	isp1_site1_ns1.example.com_udp_53_virtual	isp1_site2_ns2.example.com_udp_53_virtual
Destination	203.0.113.8	198.51.100.40
Protocol (Client) Profile	example.com_udp-dns_profile	example.com_udp-dns_profile
DNS Profile	example.com_dns_profile	example.com_dns_profile

Hostname: **gtm1.site1.example.com** Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 1:32 PM (CDT) Role: Administrator Partition: Common

**Be sure to create 203.0.113.8 on gtm1.SITE1**

ONLINE (ACTIVE)  
Standalone

Main Help About DNS » Delivery : Listeners : Listener List » New...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General**

Name: isp1\_site1\_ns1.example.com\_udp\_53\_virtual  
Description:  
State: Enabled

Listener: Advanced

Destination: Type: ☒ Host ☐ Network  
Address: 203.0.113.8  
Service Port: DNS 53  
VLAN Traffic: All VLANs  
Source Address Translation: None  
Address Translation: ☐ Enabled  
Port Translation: ☐ Enabled  
Route Advertisement: ☐ Enabled  
Auto Last Hop: Default  
Last Hop Pool: None

Service: Advanced

Protocol: UDP  
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: Jul 20, 2017 User: admin  
 IP Address: 10.1.10.23 Time: 1:32 PM (CDT) Role: Administrator Partition: Common

**Be sure to create 198.51.100.40 on gtm1.SITE2**

ONLINE (ACTIVE)  
Standalone

Main Help About DNS » Delivery : Listeners : Listener List » New...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General**

Name: **isp1\_site2\_ns2.example.com\_udp\_53\_virtual**  
 Description:  
 State: Enabled

Listener: Advanced

Destination: Type: ☒ Host ☐ Network  
 Address: **198.51.100.40**  
 Service Port: DNS 53  
 VLAN Traffic: All VLANs  
 Source Address Translation: None  
 Address Translation: ☐ Enabled  
 Port Translation: ☐ Enabled  
 Route Advertisement: ☐ Enabled  
 Auto Last Hop: Default  
 Last Hop Pool: None

Service: Advanced

Protocol: UDP  
 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 }
```

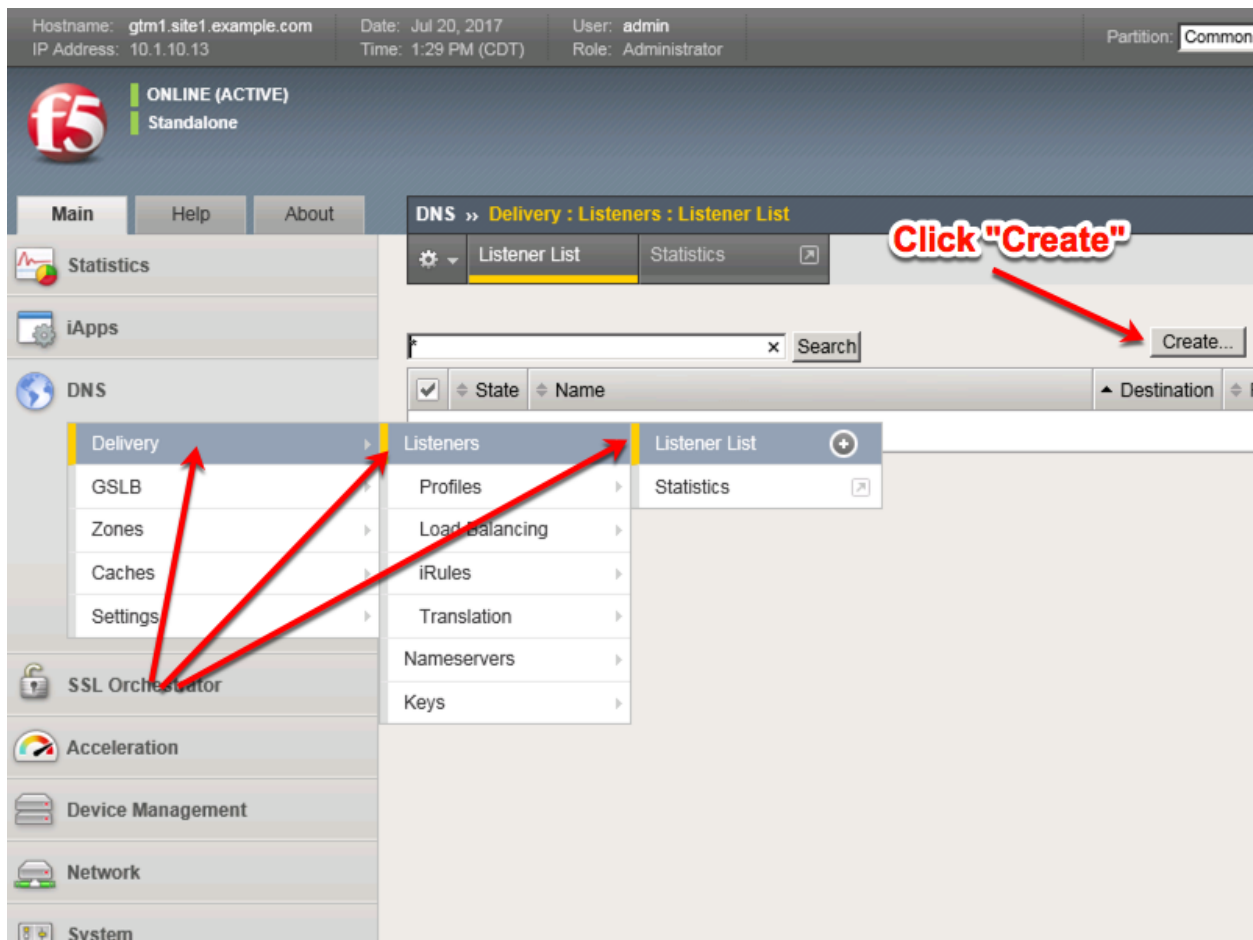
}

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

#### 4.4.5 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



Create a TCP listener.

Field	gtm1.site1	gtm1.site2
Name	isp1_site1_ns1.example.com_tcp_53_virtual	isp1_site2_ns2.example.com_tcp_53_virtual
Destination	203.0.113.8	198.51.100.40
Protocol (Client)	example.com_tcp-dns_profile	example.com_tcp-dns_profile
DNS Profile	example.com_dns_profile	example.com_dns_profile

Hostname: **gtm1.site1.example.com** Date: Jul 20, 2017 User: admin  
 IP Address: 10.1.10.13 Time: 2:18 PM (CDT) Role: Administrator Partition: Common

**Be sure to create 203.0.113.8 on gtm1.SITE1**

Main Help About DNS » Delivery : Listeners : Listener List » New...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General**

Name: **isp1\_site1\_ns1.example.com\_udp\_53**  
 Description:  
 State: Enabled

Listener: Advanced

Destination: Type: ☒ Host ☐ Network  
 Address: **203.0.113.8**  
 Service Port: DNS 53  
 VLAN Traffic: All VLANs  
 Source Address Translation: None  
 Address Translation: ☐ Enabled  
 Port Translation: ☐ Enabled  
 Route Advertisement: ☐ Enabled  
 Auto Last Hop: Default  
 Last Hop Pool: None

**Be sure to select "TCP"**

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** Date: Jul 20, 2017 User: admin  
 IP Address: 10.1.10.23 Time: 2:18 PM (CDT) Role: Administrator Partition: Common

**Be sure to create 198.51.100.40 on gtm1.SITE2**

ONLINE (ACTIVE)  
Standalone

Main Help About DNS » Delivery : Listeners : Listener List » New...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General**

Name: **isp1\_site2\_ns2.example.com\_udp\_53**  
 Description:  
 State: Enabled

Listener: Advanced

Destination: Type: ☒ Host ☐ Network  
 Address: **198.51.100.40**  
 Service Port: DNS 53  
 VLAN Traffic: All VLANs  
 Source Address Translation: None  
 Address Translation: ☐ Enabled  
 Port Translation: ☐ Enabled  
 Route Advertisement: ☐ Enabled  
 Auto Last Hop: Default  
 Last Hop Pool: None

**Be sure to select "TCP"**

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

gtm1.site1 TMSH command:

### TMSH

```
tmsl 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

```
tmsl 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 }
```

## 4.5 Data Centers

### 4.5.1 Servers

#### 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 configuration 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: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 2:29 PM (CDT) Role: Administrator

ONLINE (ACTIVE)  
Standalone

Main Help About **DNS » GSLB : Servers : Server List » New Server...**

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings

SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name

Product

Data Center

Prober Preference

Prober Fallback

State

**Devices**

**Click "Add"**

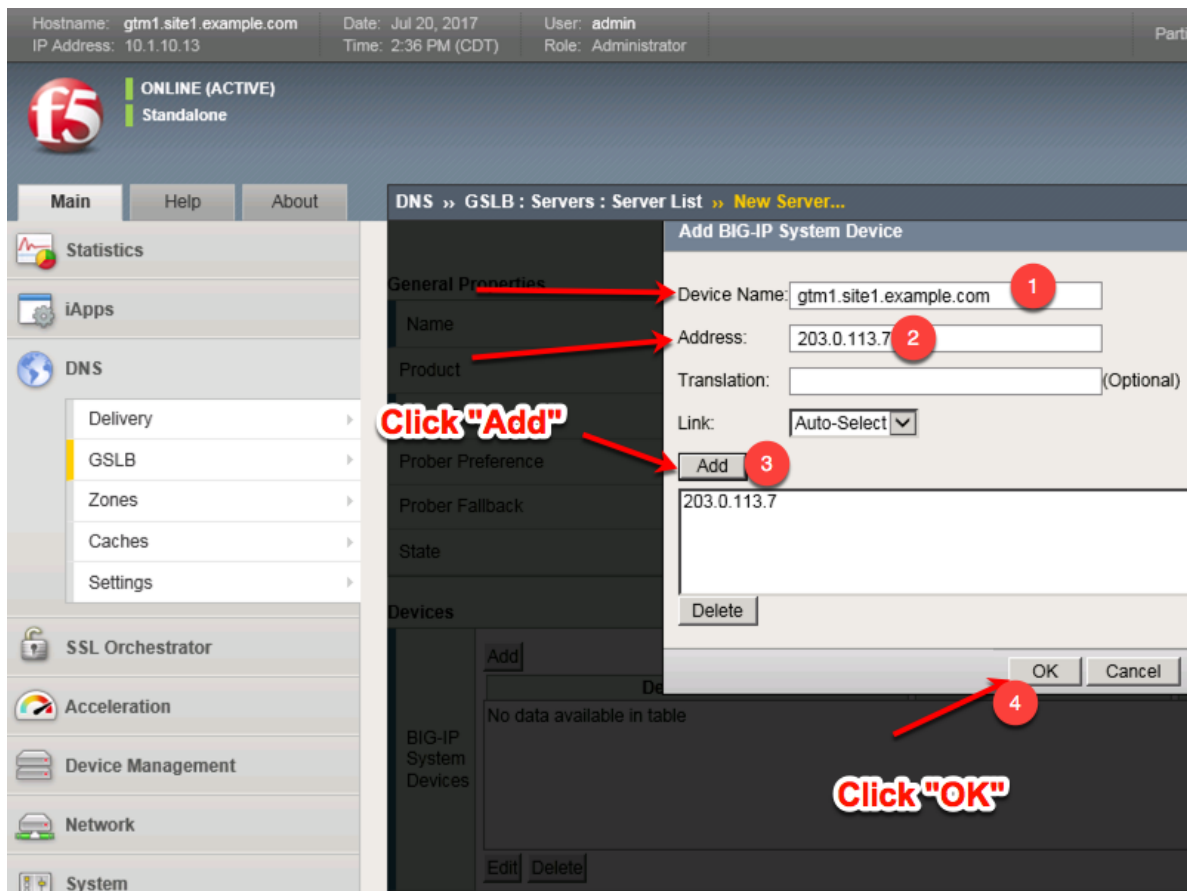
Add

Device Name Address

No data available in table

Edit Delete

- Click the “Add” button to define IP addresses



- Complete the form and associate the “bigip” “Health Monitor”

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 2:43 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name: gtm1.site1\_server  
Product: BIG-IP System  
Data Center: site1\_datacenter  
Prober Preference: Inherit From Data Center  
Prober Fallback: Inherit From Data Center  
State: Enabled

**Devices**

Add

Device Name	Address
gtm1.site1.example.com	203.0.113.7

Edit Delete

**Configuration:** Advanced

Health Monitors

Selected: /Common bigip  
Available: /Common gateway\_icmp, gtp, http, http\_head\_f5

Availability Requirements: All Health Monitors

Limit Settings

Bits: Disabled  
Packets: Disabled  
Current Connections: Disabled

iQuery Options

Service Check: ☒  
Path: ☒  
SNMP: ☒

## 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
```

## gtm1.SITE2

Continue the same configuration for gtm1.site2.

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 2:47 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

DNS » **GSLB : Servers : Server List**

Server List Trusted Server Certificates Statistics

Search Create...

<input checked="" type="checkbox"/>	Status	Name	Devices	Address	Data Center	Virtual
<input type="checkbox"/>		gtm1.site1_server	1	203.0.113.2	site1_datacenter	0

Enable Disable Delete...

**Click "Create" to define gtm1.site2**

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: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 3:18 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

DNS » GSLB : Servers : Server List » **New Server...**

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name

Product

Data Center

Prober Preference

Prober Fallback

State

**Devices**

**Click "Add"**

Device Name	Address
No data available in table	

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

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 3:30 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

DNS » GSLB : Servers : Server List » New Server...

Add BIG-IP System Device

General Properties

Device Name: gtm1.site2.example.com  
Address: 198.51.100.39  
Translation: (Optional)  
Link: Auto-Select

Prober Preference Add  
Prober Fallback 198.51.100.39  
State  
Delete

Click "Add"

Click "OK"

OK Cancel

Big-IP System Devices

No data available in table

Edit Delete

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

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 3:37 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name	gtm1.site2_server
Product	BIG-IP System
Data Center	site2_datacenter
Prober Preference	Inherit From Data Center
Prober Fallback	Inherit From Data Center
State	Enabled

**Devices**

Device Name	Address
gtm1.site2.example.com	198.51.100.39

Add Edit Delete

**Configuration:** Advanced

Health Monitors	Selected /Common bigip	Available /Common gateway_icmp gtp http http_head_f5
Availability Requirements	All Health Monitors	
Limit Settings	Bits: Disabled Packets: Disabled Current Connections: Disabled	
iQuery Options	Service Check <input checked="" type="checkbox"/> Path <input checked="" type="checkbox"/> SNMP <input checked="" type="checkbox"/>	

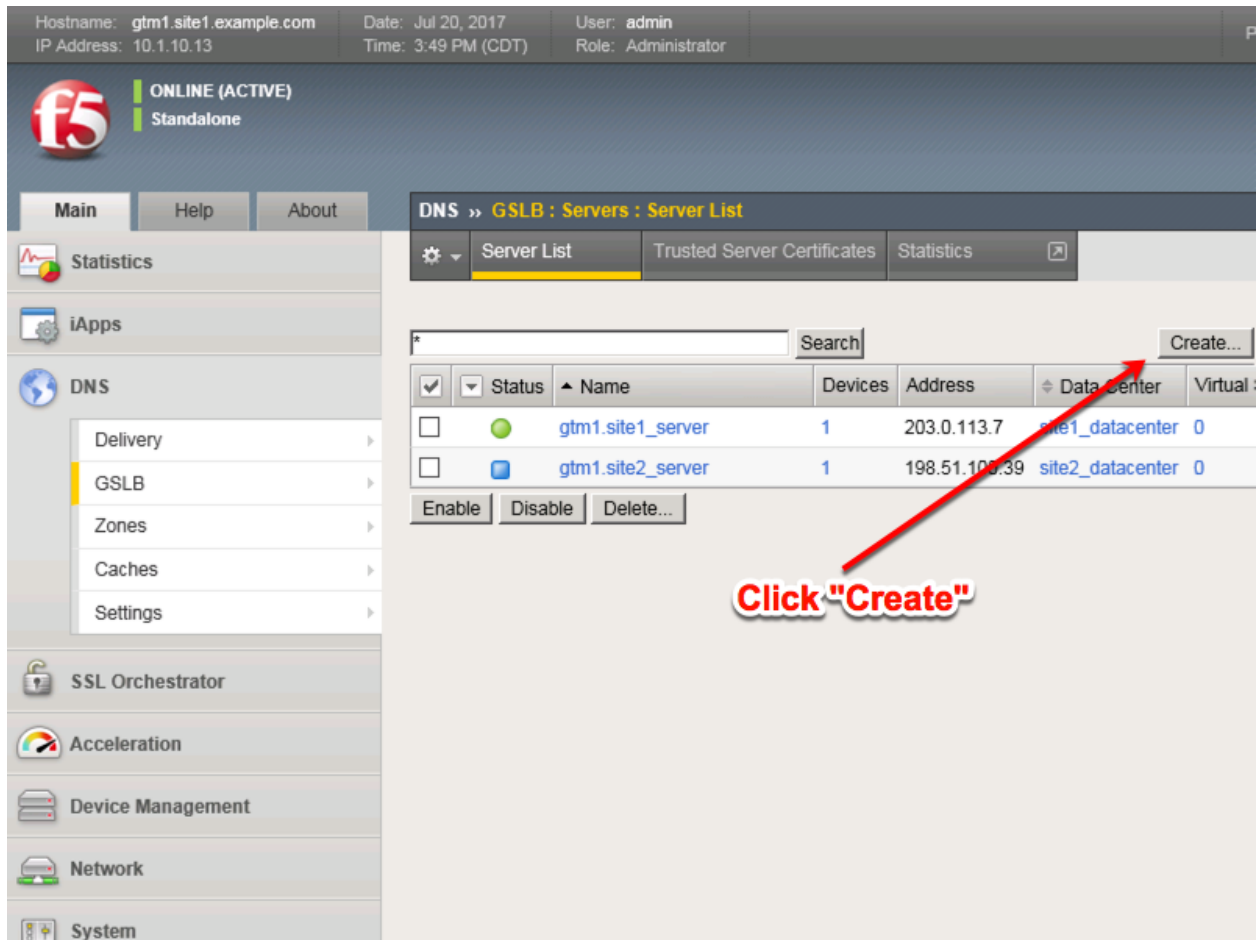
## TMSH

```
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
```

## 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.



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 Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 3:58 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

**DNS » GSLB : Servers : Server List » New Server...**

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

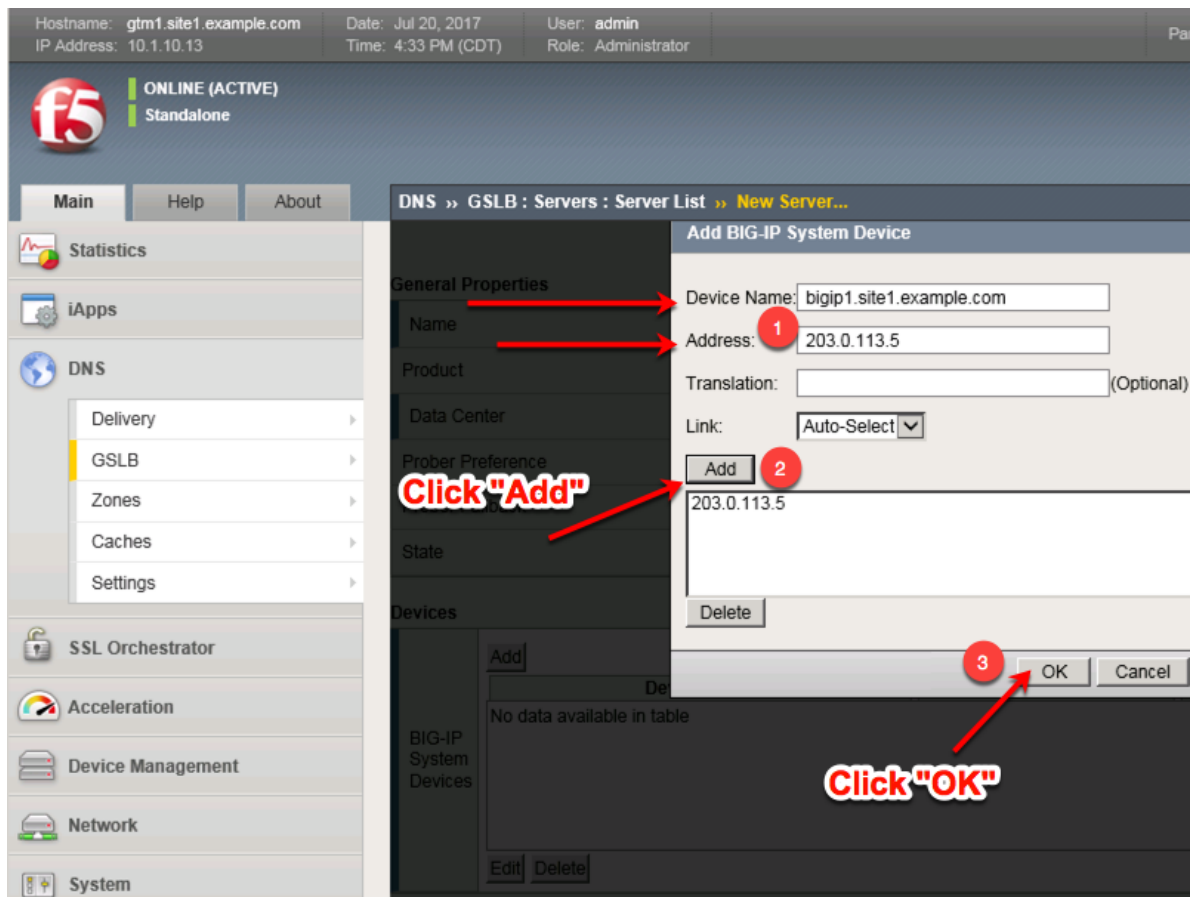
Name   
Product   
Data Center   
Prober Preference   
Prober Fallback   
State

**Devices**

**Click "Add"**

Device Name	Address
No data available in table	

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



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

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 4:38 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name	site1_ha-pair
Product	BIG-IP System
Data Center	site1_datacenter
Prober Preference	Inherit From Data Center
Prober Fallback	Inherit From Data Center
State	Enabled

**Devices**

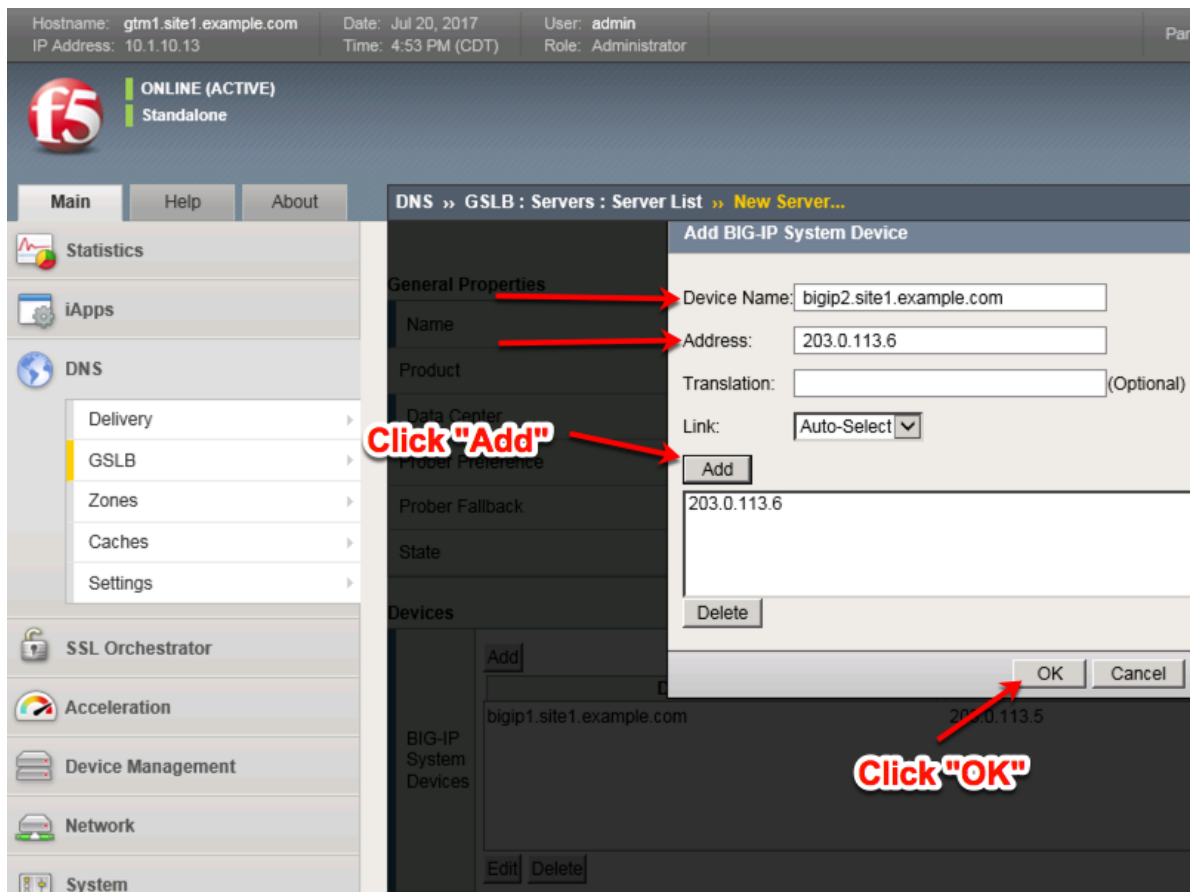
Add

Device Name	Address
bigip1.site1.example.com	203.0.113.5

Edit Delete

**Click "Add" .....again**

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



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

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 5:00 PM (CDT) Role: Administrator

ONLINE (ACTIVE)  
Standalone

Main Help About DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name	site1_ha-pair
Product	BIG-IP System
Data Center	site1_datacenter
Prober Preference	Inherit From Data Center
Prober Fallback	Inherit From Data Center
State	Enabled

**Devices**

Device Name	Address
bigip1.site1.example.com	203.0.113.5
bigip2.site1.example.com	203.0.113.6

**Add the "bigip" Health Monitor**

Configuration: Advanced

Health Monitors

Selected	Available
/Common bigip	/Common gateway_icmp gtp http http_head_f5

Availability Requirements: All Health Monitors

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

**Resources**

Virtual Server Discovery	Enabled
Link Discovery	Enabled

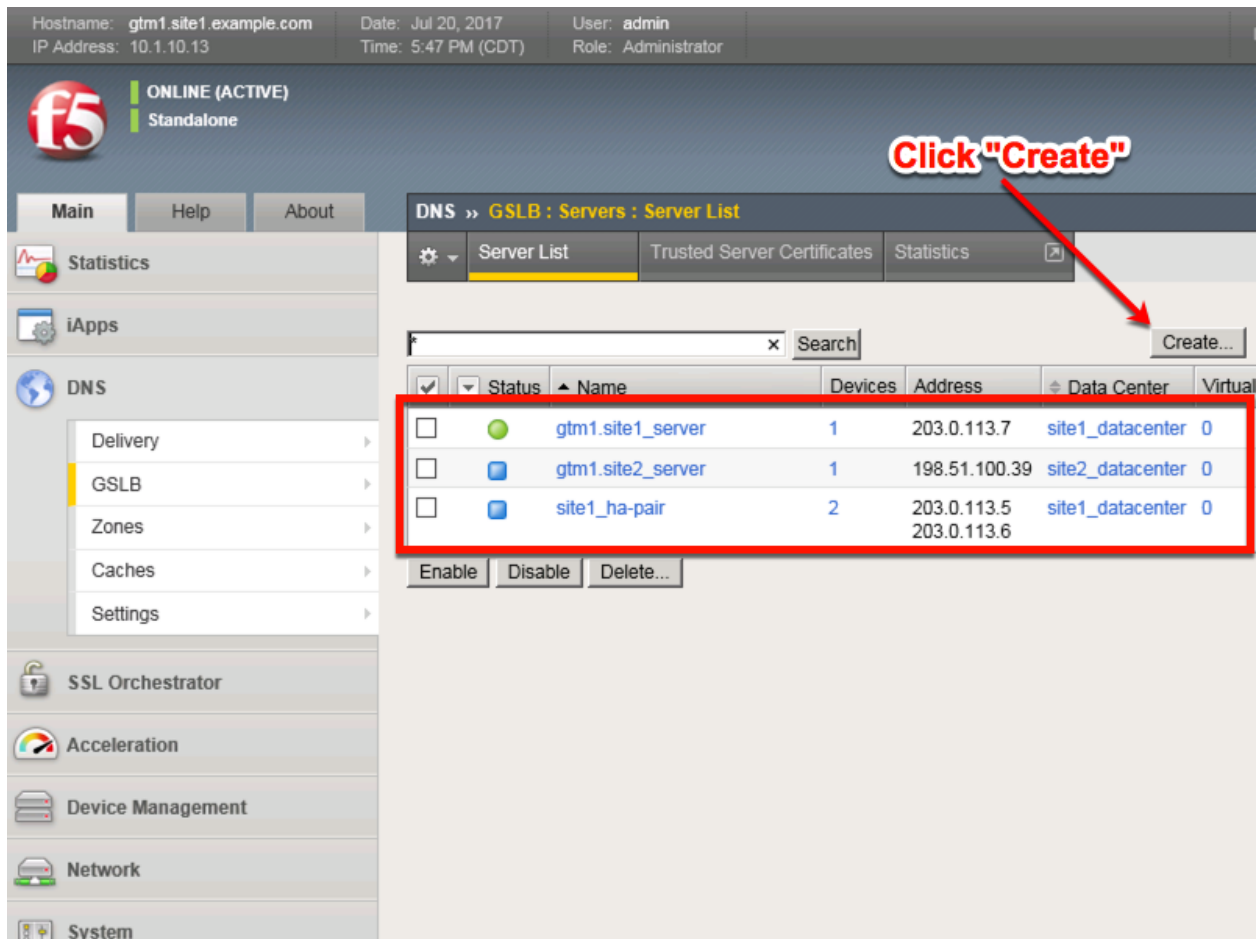
Cancel Repeat Finished

## TMSH

```
tmsh create gtm server site1_ha-pair datacenter site1_datacenter devices add { bigip1.site1.example.com
{ addresses add { 203.0.113.5 { } } } bigip2.site1.example.com { addresses add { 203.0.113.6 { } } } } link-
discovery enabled monitor bigip product bigip virtual-server-discovery enabled
```

## site2\_ha-pair

Continue 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: Jul 20, 2017    User: admin  
IP Address: 10.1.10.13    Time: 5:52 PM (CDT)    Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main    Help    About    DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
  Delivery  
  GSLB  
  Zones  
  Caches  
  Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name	site2_ha_pair
Product	BIG-IP System
Data Center	site2_datacenter
Prober Preference	Inherit From Data Center
Prober Fallback	Inherit From Data Center
State	Enabled

**Devices**

Big-IP System Devices

Add

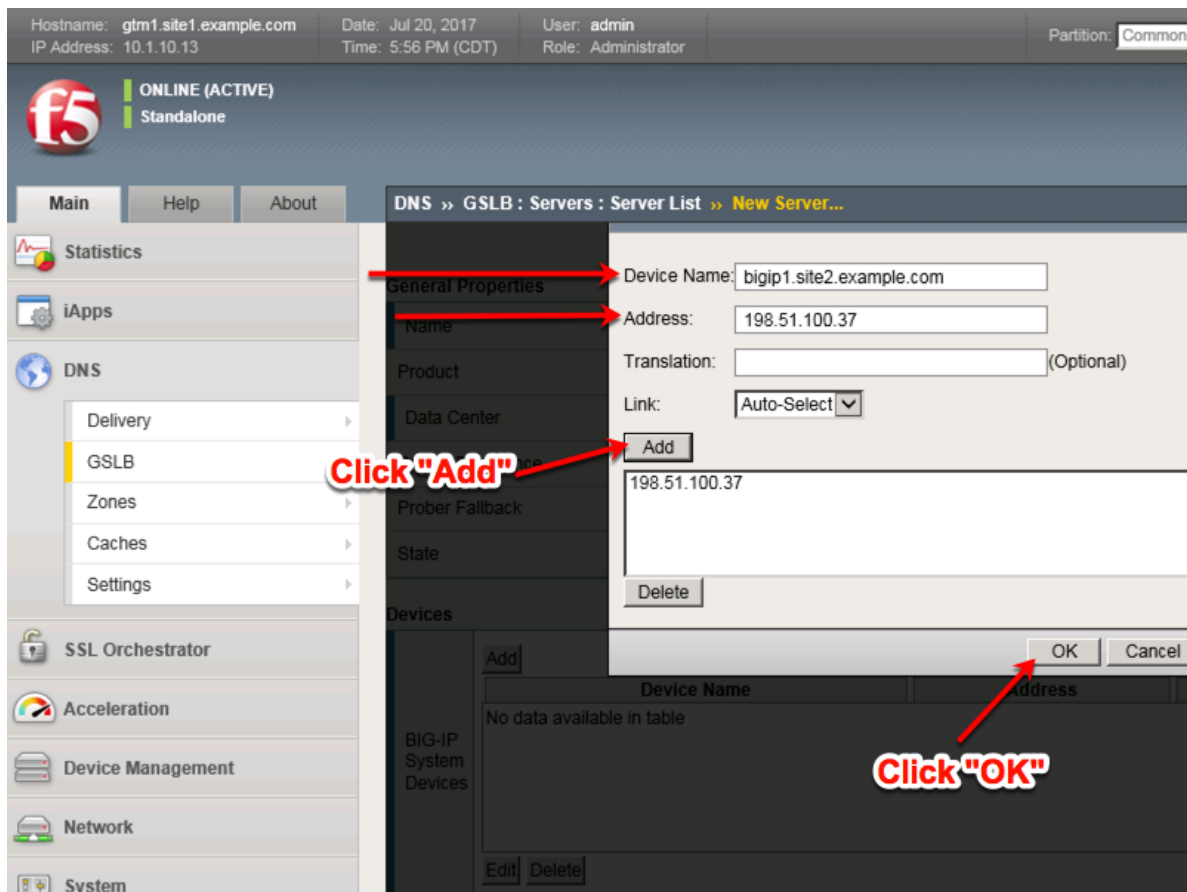
Device Name

No data available in table

Edit    Delete

**Click "Add"**

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



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



Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 6:13 PM (CDT) Role: Administrator Partition: Common

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name   
Product   
Data Center   
Prober Preference   
Prober Fallback   
State

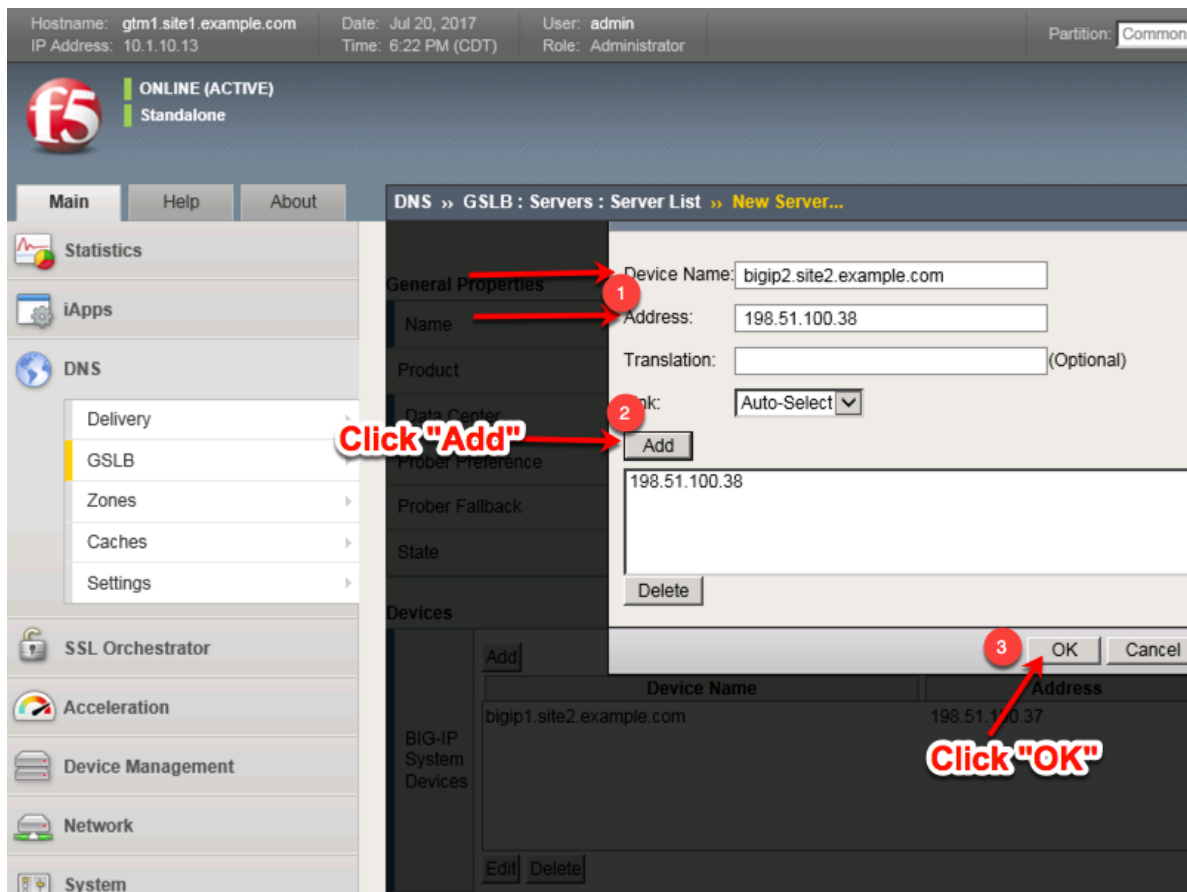
**Devices**

**Click "Add"**

Device Name	Address
bigip1.site2.example.com	198.51.100.37

Edit Delete

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



- Complete the form and associate the "bigip" "Health Monitor"

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 7:55 PM (CDT) Role: Administrator Partition: Common

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About DNS » GSLB : Servers : Server List » New Server...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name: site2\_ha\_pair  
Product: BIG-IP System  
Data Center: site2\_datacenter  
Prober Preference: Inherit From Data Center  
Prober Fallback: Inherit From Data Center  
State: Enabled

**Devices**

Add

Device Name	Address
bigip1.site2.example.com	198.51.100.37
bigip2.site2.example.com	198.51.100.38

Big-IP System Devices

Edit Delete

Configuration: Advanced

Health Monitors

Selected: /Common bigip

Available: /Common gateway\_icmp, gtp, http, http\_head\_f5

Availability Requirements: All Health Monitors

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

**Resources**

Virtual Server Discovery: Enabled

Link Discovery: Enabled

Cancel Repeat Finished

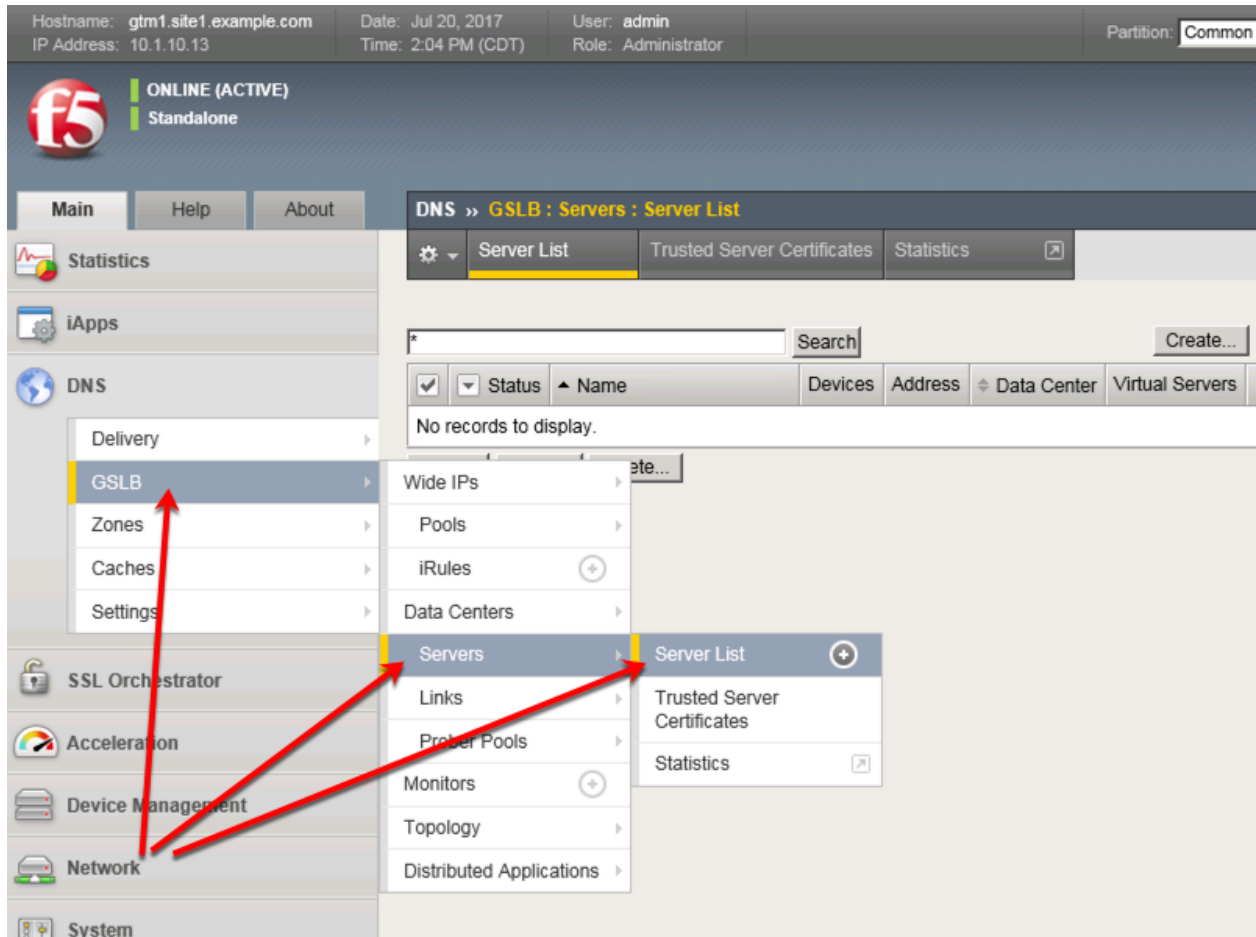
## TMSH

```
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: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 2:00 PM (CDT) Role: Administrator Partition: Common

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

DNS » **GSLB : Servers : Server List**

Server List Trusted Server Certificates Statistics

\* Search Create...

<input checked="" type="checkbox"/>	<input type="checkbox"/> Status	Name	Devices	Address	Data Center	Virtual Servers
No records to display.						

Enable Disable Delete...

**Click "Create" to define gtm1.site1**

#### 4.5.2 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.

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin  
IP Address: 10.1.10.13 Time: 8:05 PM (CDT) Role: Administrator Partition: Common

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

DNS » **GSLB : Servers : Server List**

Server List Trusted Server Certificates Statistics

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
SSL Orchestrator  
Acceleration  
Device Management  
Network  
System

Search

<input type="checkbox"/>	Status	Name	Devices	Address	Data Center	Virtual Servers	Pr
<input type="checkbox"/>		gtm1.site1_server	1	203.0.113.7	site1_datacenter	0	Blk
<input type="checkbox"/>		gtm1.site2_server	1	198.51.100.39	site2_datacenter	0	Blk
<input type="checkbox"/>		site1_ha-pair	2	203.0.113.5 203.0.113.6	site1_datacenter	0	Blk
<input type="checkbox"/>		site2_ha_pair	2	198.51.100.37 198.51.100.38	site2_datacenter	0	Blk

Enable Disable Delete...

**Three other servers need to "establish trust"**

1. Launch Putty and login to gtm1.SITE1

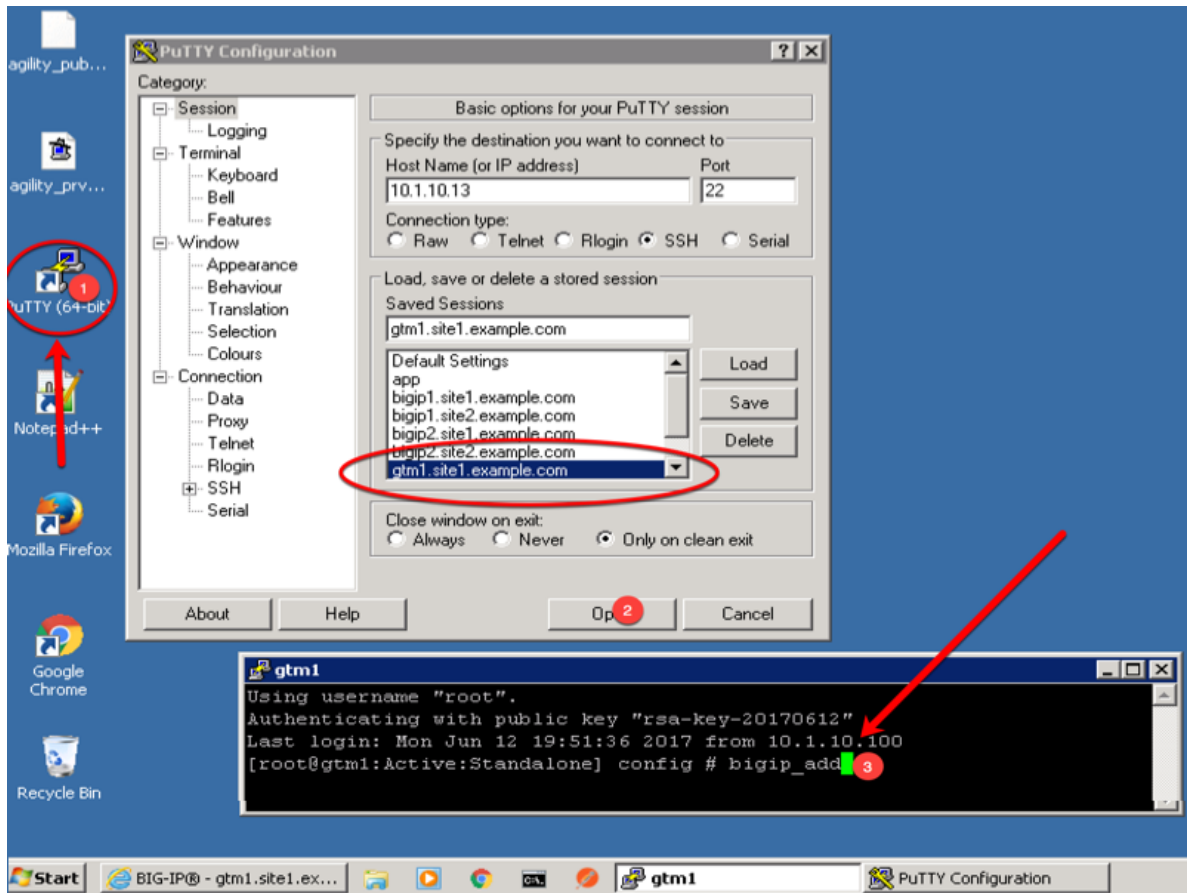
Run the following command, and when prompted for a password use "default"

---

**TMSH**

bigip\_add

---



2. Observe the exchanged certificates

Hostname: gtm1.site1.example.com Date: Jun 25, 2017 User: admin  
IP Address: 10.1.10.13 Time: 3:36 PM (CDT) Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

Statistics  
iApps  
DNS  
SSL Orchestrator  
Acceleration  
Device Management

DNS » GSLB : Servers : Trusted Server Certificates

Server List Trusted Server Certificates Statistics

General Properties

Name	server
Partition / Path	
Wide IPs	
Pools	
iRules	
Data Centers	
Servers	Server List
Links	Trusted Server Certificates
Prober Pools	
Monitors	
Topology	

gtm1.site2.example.com, MyCompany  
bigip2.site1.example.com, MyCompany  
bigip1.site2.example.com, MyCompany  
bigip2.site2.example.com, MyCompany  
gtm1.site1.example.com, MyCompany

234963207  
Common Name: gtm1.site2.example.com

3. Observe the server status



Hostname: gtm1.site1.example.com Date: Jul 26, 2018 User: admin  
IP Address: 10.1.10.13 Time: 3:44 PM (EDT) Role: Administrator Partition: Common

**f5** ONLINE (ACTIVE) Standalone

Main Help About

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
Acceleration  
Device Management  
Network  
System

DNS » GSLB : Servers : Server List

Server List Trusted Server Certificates Statistics

Search

<input checked="" type="checkbox"/>	Status	Name	Devices	Address	Data Center	Virtual Servers	Pro
<input type="checkbox"/>	●	gtm1.site1_server	1	203.0.113.7	site1_datacenter	0	BIC
<input type="checkbox"/>	●	gtm1.site2_server	1	198.51.100.39	site2_datacenter	0	BIC
<input type="checkbox"/>	●	site1_ha-pair	2	203.0.113.5 203.0.113.6	site1_datacenter	3	BIC
<input type="checkbox"/>	●	site2_ha-pair	2	198.51.100.37 198.51.100.38	site2_datacenter	2	BIC

Enable Disable Delete...

**Green Green Green !!**

**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.

### 4.5.3 Sync Group

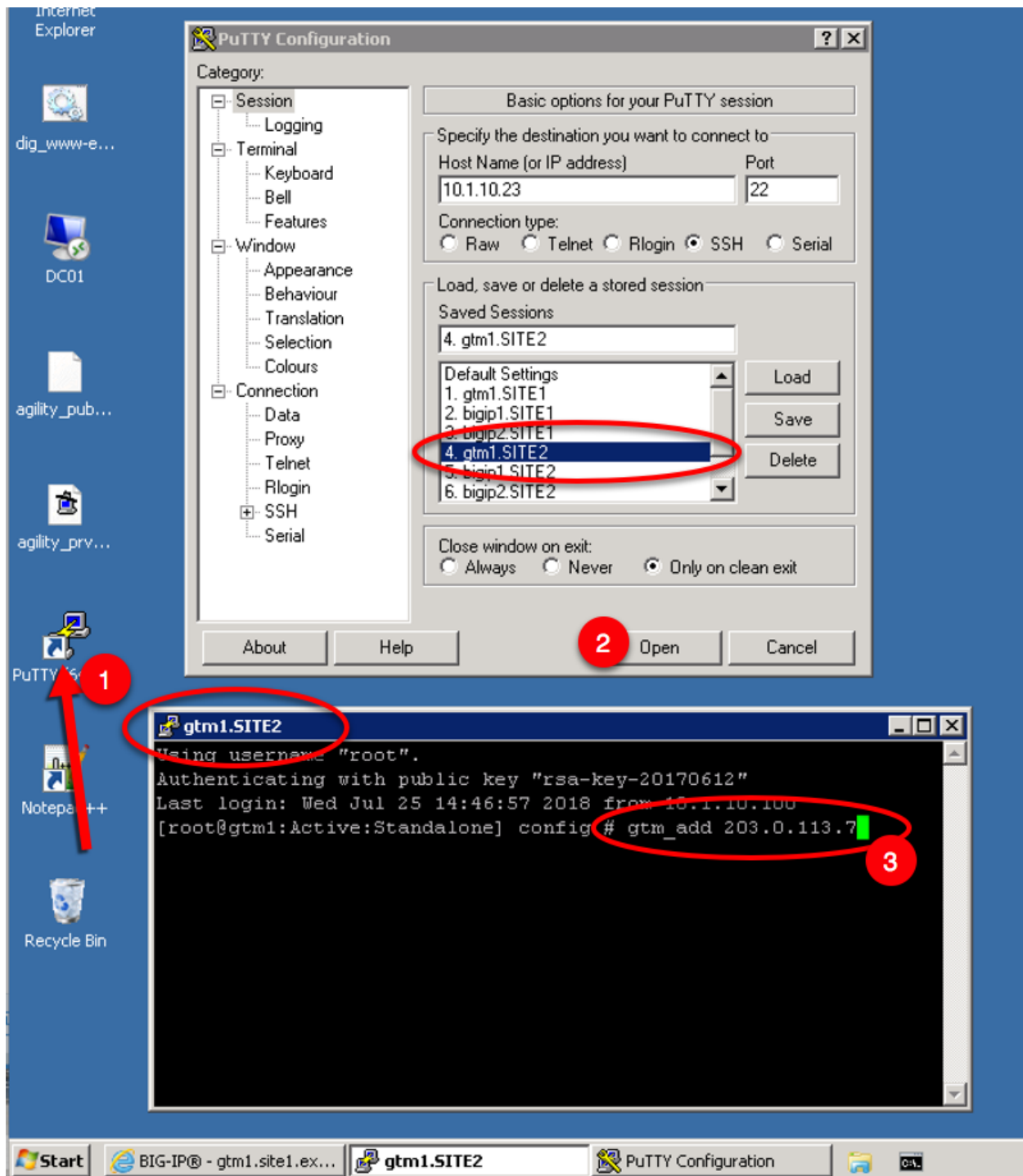
After the BIG-IP DNS server in the site 2 data center is joined to the sync group, an administrator may make changes on any of the F5 DNS servers, and changes will be automatically replicated across all F5 DNS servers.

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

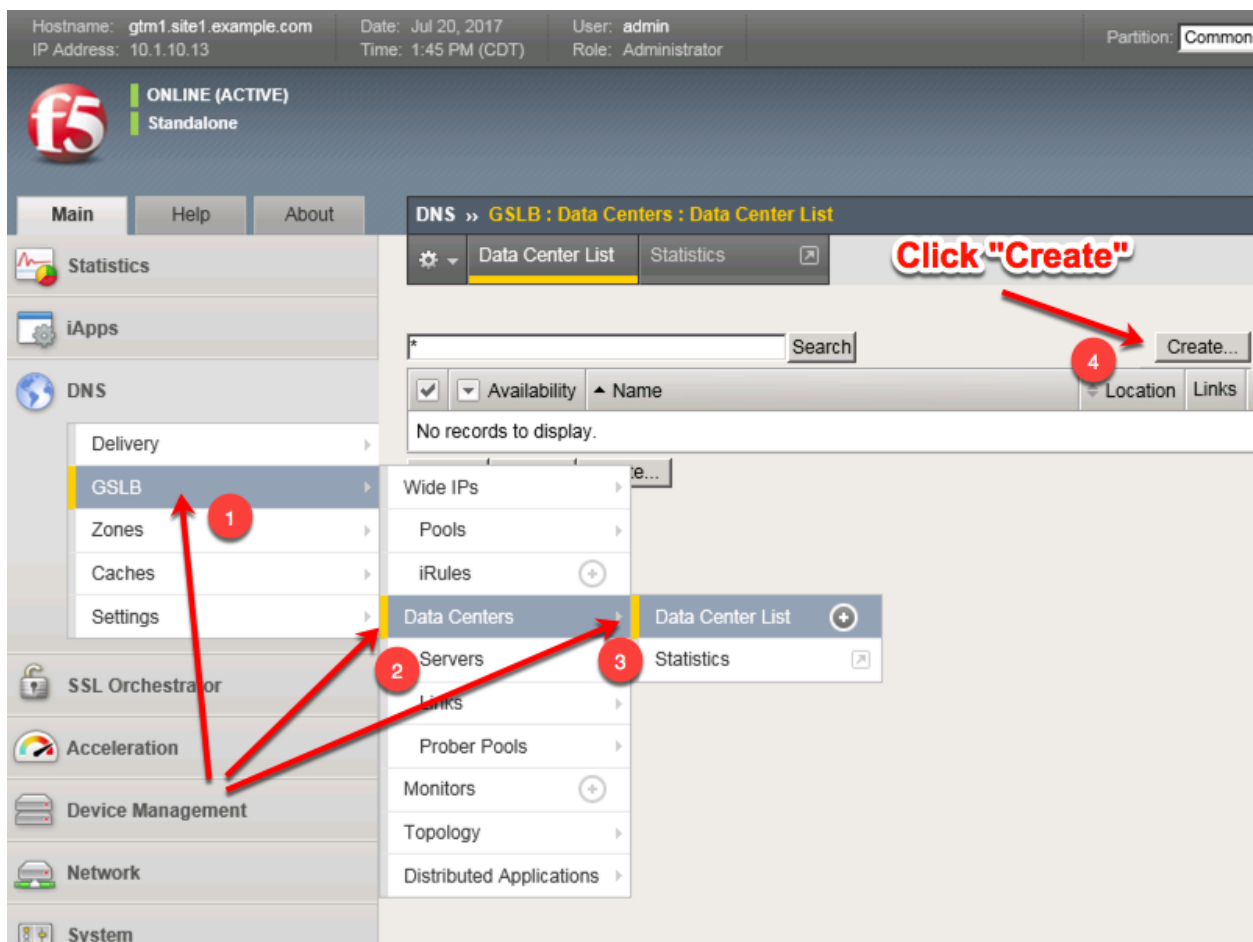
gtm\_add 203.0.113.7

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



Create two data centers according to the table below:

Field	Value
Name	site1_datacenter
Name	site2_datacenter

The screenshot shows the F5 DNS configuration interface. At the top, a status bar displays: Hostname: gtm1.site1.example.com, Date: Jul 20, 2017, User: admin, IP Address: 10.1.10.13, Time: 1:48 PM (CDT), Role: Administrator, and Partition: Common. Below this, the F5 logo and 'ONLINE (ACTIVE) Standalone' status are shown. The main navigation bar includes 'Main', 'Help', 'About', and 'DNS >> GSLB : Data Centers : Data Center List'. A left sidebar contains icons for Statistics, iApps, DNS, SSL Orchestrator, Acceleration, Device Management, Network, and System. The 'DNS' menu is expanded, showing 'Delivery', 'GSLB', 'Zones', 'Caches', and 'Settings'. The 'GSLB' menu is further expanded, showing 'Data Center List'. The 'Data Center List' configuration form is displayed, showing 'General Properties' for 'site1\_datacenter'. The 'Name' field is highlighted with a red arrow. The 'Description' field is empty. The 'Location' field is empty. The 'Contact' field is empty. The 'Prober Preference' dropdown is set to 'Inside Data Center'. The 'Prober Fallback' dropdown is set to 'Any Available'. The 'State' dropdown is set to 'Enabled'. Below the form are buttons for 'Cancel', 'Repeat', and 'Finished'. A red text overlay at the bottom of the form reads: 'Repeat this step to create "site2\_datacenter"'.

General Properties	
Name	site1_datacenter
Description	
Location	
Contact	
Prober Preference	Inside Data Center
Prober Fallback	Any Available
State	Enabled

Cancel Repeat Finished

**Repeat this step to create "site2\_datacenter"**

TMSH command for only site1.gtm1:

#### TMSH

```
tmsh create gtm datacenter site1_datacenter
```

#### TMSH

```
tmsh create gtm datacenter site2_datacenter
```

## 4.6 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.

Hostname: gtm1.site1.example.com Date: Jul 26, 2018 Partition: Common Log out  
IP Address: 10.1.10.13 Time: 3:58 PM (EDT)

**f5** ONLINE (ACTIVE) Standalone

Main Help About **DNS » GSLB : Pools : Pool List**

Statistics iApps DNS Acceleration Device Management

**DNS**

- Delivery
- GSLB**
  - Wide IPs
  - Pools**
    - Pool List**
    - Statistics
  - IRules
  - Data Centers
  - Servers
  - Links
  - Prober Pools
- Zones
- Caches
- Settings

Search Create...

☒ Status Name Type Members Partition / Path

No records to display.

1 2 3

Field	Value
Name	www.example.com_pool
Type	A
member	isp1_site1_www.example.com_tcp_https_virtual
member	isp2_site2_www.example.com_tcp_https_virtual

Hostname: gtm1.site1.example.com Date: Jul 26, 2018 User: admin  
IP Address: 10.1.10.13 Time: 4:11 PM (EDT) Role: Administrator Partition: Common Log out

**f5** ONLINE (ACTIVE) Standalone

Main Help About **DNS » GSLB : Pools : Pool List » New Pool...**

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
Acceleration  
Device Management  
Network  
System

**General Properties**

Name:  x  
Type:   
State:

**Configuration**

Health Monitors: Selected: Available: gateway\_icmp, gtp, http, http\_head\_f5  
Up Down

Availability Requirements:

Limit Settings: Bits:   
Packets:   
Current Connections:

Manual Resume: ☐

TTL:

Dynamic Ratio: ☐

Maximum Answers Returned:

Verify Member Availability: ☒

**Members**

Load Balancing Method: Preferred:   
Alternate:   
Fallback:   
Fallback IP:

Virtual Server:   
Ratio:   
**Add**

Member List:   
  
Delete Up Down

**Select two LTM VIP's and click "Add"**

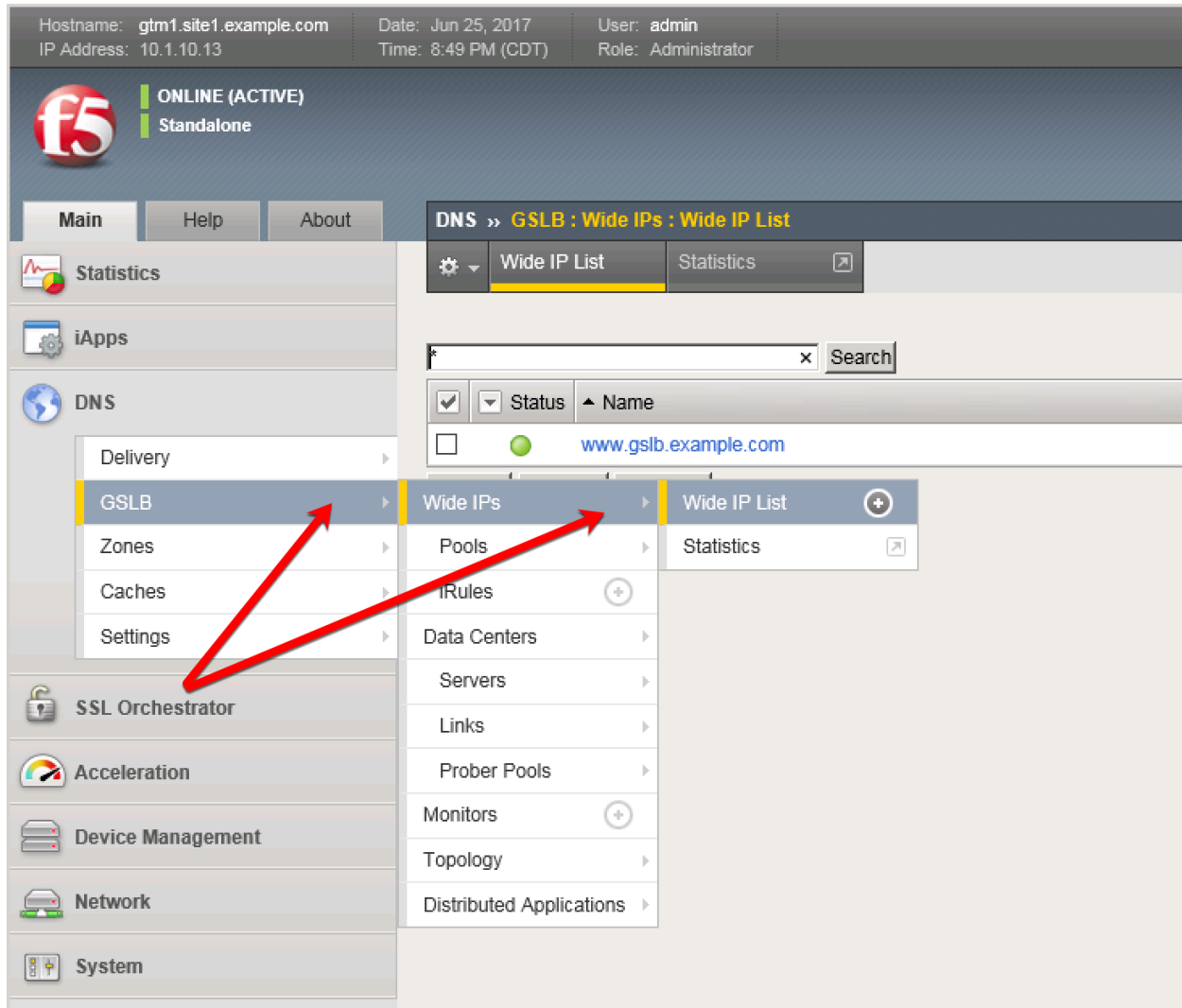
TMSH command to run on only gtm1.site1:

## TMSH

```
tmsh create gtm pool a www.example.com_pool { members add { site1_ha-  
pair:/Common/isp1_site1_www.example.com_tcp_https_virtual { member-order 0 } site2_ha-  
pair:/Common/isp2_site2_www.example.com_tcp_https_virtual { member-order 1 } }
```

## 4.7 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.



Create an F5 “wide IP” according to the following table:

Field	Value
Name	www.example.com
Type	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- lection	Checked
Load-Balancing Decision Log - Pool Member Traversal	Checked
Pool	www.example.com_pool

Hostname: gtm1.site1.example.com Date: Jul 29, 2018 User: admin  
IP Address: 10.1.10.13 Time: 4:13 PM (EDT) Role: Administrator Partition: Common Log out

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About DNS » GSLB : Wide IPs : Wide IP List » New...

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
Acceleration  
Device Management  
Network  
System

General Properties: Advanced

Name: **www.example.com**  
Type: A  
Description:  
Alias: **www.gslb.example.com**  
Add  
Alias List: **www.gslb.example.com**  
Delete  
State: Enabled  
Minimal Response: Enabled  
Return Code On Failure: Disabled  
Load-Balancing Decision Log:  
☒ Pool Selection  
☒ Pool Traversal  
☒ Pool Member Selection  
☒ Pool Member Traversal

iRules  
iRule List  
Selected Available  
Up Down  
iRule List  
Selected Available  
Up Down

Pools  
Load Balancing Method: Round Robin  
Persistence: Disabled  
Pool: Select...  
Ratio: 1  
Add

**For troubleshooting purposes enable verbose logging**

200 Chapter 4. Class 3 - Data Center Availability Services Using BIG-IP DNS



TMSH command to run on only gtm1.site1:

## TMSH

```
tmsl 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-member-traversal 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

```
C:\Users\user.EXAMPLE>dig @203.0.113.8 www.example.com
; <<>> DiG 9.3.2 <<>> @203.0.113.8 www.example.com
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 389
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.example.com.                IN      A
;; ANSWER SECTION:
www.example.com.                 30      IN      A      198.51.100.41
;; Query time: 15 msec
;; SERVER: 203.0.113.8#53(203.0.113.8)
;; WHEN: Sun Jul 29 16:42:09 2018
;; MSG SIZE rcvd: 49

C:\Users\user.EXAMPLE>dig +short @203.0.113.8 www.example.com
198.51.100.41

C:\Users\user.EXAMPLE>dig +short @203.0.113.8 www.example.com
198.51.100.41

C:\Users\user.EXAMPLE>dig +short @203.0.113.8 www.example.com
203.0.113.9

C:\Users\user.EXAMPLE>dig +short @203.0.113.8 www.gslb.example.com
203.0.113.9

C:\Users\user.EXAMPLE>dig +short @203.0.113.8 www.gslb.example.com
203.0.113.9

C:\Users\user.EXAMPLE>dig +short @203.0.113.8 www.gslb.example.com
198.51.100.41
```

Hostname: gtm1.site1.example.com Date: Jul 29, 2018 Partition: Common Log out  
IP Address: 10.1.10.13 Time: 11:11 PM (EDT)

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

DNS » **GSLB : Wide IPs : Wide IP List**

Wide IP List Statistics

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
Acceleration

Wide IP List  
Pools  
iRules  
Data Centers  
Servers  
Links

Statistics

www.example.com A www.gslb.exan

1 2 3

The screenshot shows the F5 BIG-IP DNS configuration interface. The top navigation bar includes 'Main', 'Help', and 'About'. The left sidebar contains 'Statistics', 'iApps', 'DNS', and 'Acceleration'. The 'DNS' section is expanded, showing 'Delivery', 'GSLB', 'Zones', 'Caches', and 'Settings'. The 'GSLB' section is further expanded, showing 'Wide IPs', 'Pools', 'iRules', 'Data Centers', 'Servers', and 'Links'. The 'Wide IPs' section is expanded, showing 'Wide IP List' and 'Statistics'. The 'Wide IP List' section is expanded, showing 'Statistics'. The 'Statistics' link is highlighted with a red box. Three red arrows with numbered circles (1, 2, 3) indicate the navigation path: from 'GSLB' to 'Wide IPs' to 'Wide IP List' to 'Statistics'.

Hostname: gtm1.site1.example.com Date: Jul 29, 2018 User: admin  
IP Address: 10.1.10.13 Time: 11:21 PM (EDT) Role: Administrator Partition:

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

Statistics » **Module Statistics : DNS : GSLB**

Traffic Summary DNS Subscriber Management Network

Statistics

- Dashboard
- Module Statistics
- Analytics
- Performance

iApps

DNS

Acceleration

Device Management

Network

System

**Display Options**

Statistics Type: Wide IPs

Data Format: Normalized

Auto Refresh: Disabled Refresh

\* Search

	Status	Wide IP	Type	Partition / Path	Details	Pools	Total	Resolved	Rel
<input type="checkbox"/>		www.example.com	A	Common	<a href="#">View...</a>	<a href="#">View...</a>	44	44	0

Reset

**For more details click**

## TMSH

tmsh show gtm wideip A www.example.com detail

```

gtm1.SITE1
[root@gtm1: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
  Persisted   0
  Resolved    44
  Dropped     0

Load Balancing
  Preferred    44
  Alternate    0
  Fallback     0
  CNAME Resolutions 0
  Returned from DNS 0
  Returned to DNS 0
  Failures with RCODE 0

-----
| Gtm::Pool::A www.example.com_pool
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Available
|
| Load Balancing
|   Preferred    44
|   Alternate    0
|   Fallback     0
|   Returned from DNS 0
|   Returned to DNS 0
|   Dropped     0
|
-----
| Gtm::Pool Member: www.example.com_pool:A isp1_site1_www.example.com_tcp_https_virtual:site1_ha-pair
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Available
|
| Load Balancing
|   Preferred    35
|   Alternate    0
|   Fallback     0
|
-----
| Gtm::Virtual Server: isp1_site1_www.example.com_tcp_https_virtual
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Monitor /Common/bigip from 203.0.113.5 : UP
|   Destination : 203.0.113.9:443
|   Up Time     : 10:18
|
| Link Name      203.0.113.1
|
| Global
|   Picks        35
|   Connections  0
|   Virtual Server Score 1
|
| Throughput
|   In  Out
|   Bits/sec  0  0
|   Packets/sec 0  0
|
-----
| Gtm::Pool Member: www.example.com_pool:A isp2_site1_www.example.com_tcp_https_virtual:site1_ha-pair
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Available

```

## TMSH

tail -f /var/log/ltm

```

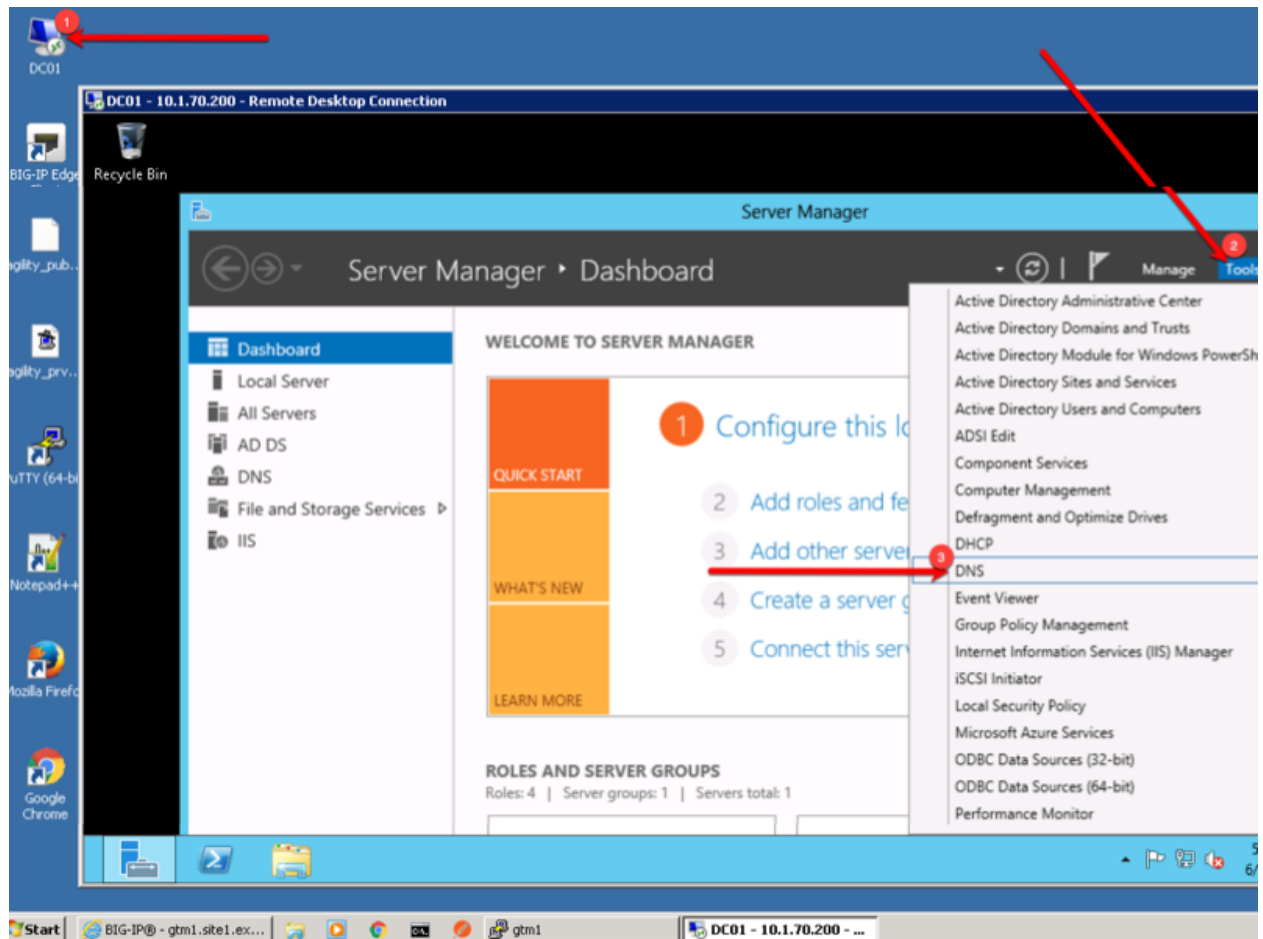
gtm1.SITE1
[root@gtm1:Active:Standalone] config # tail -f -n 12 /var/log/ltm
Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com qid 991 from 198
.51.100.68#64119: view none: query: www.gslb.example.com IN A + (203.0.113.8%0)
Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com qid 991 from 198
.51.100.68#64119 [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 00:19:49 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 A 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 A + (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 A 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 A + (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 gtm1 info tmm[11966]: 2018-07-30 00:23:43 gtm1.site1.example.com qid 261 to 203.0
.113.68#64121: [NOERROR qr,aa,rd] response: www.example.com. 30 IN A 198.51.100.41;
Jul 30 00:23:50 gtm1 info tmm[11966]: 2018-07-30 00:23:50 gtm1.site1.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 gtm1 info tmm[11966]: 2018-07-30 00:23:50 gtm1.site1.example.com qid 97 from 203.
0.113.68#64122 [www.example.com A] [round robin selected pool (www.example.com_pool)] [pool membe
r 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_https_vir
tual:203.0.113.9)]
Jul 30 00:23:50 gtm1 info tmm[11966]: 2018-07-30 00:23:50 gtm1.site1.example.com qid 97 to 203.0.

```

## 4.8 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.

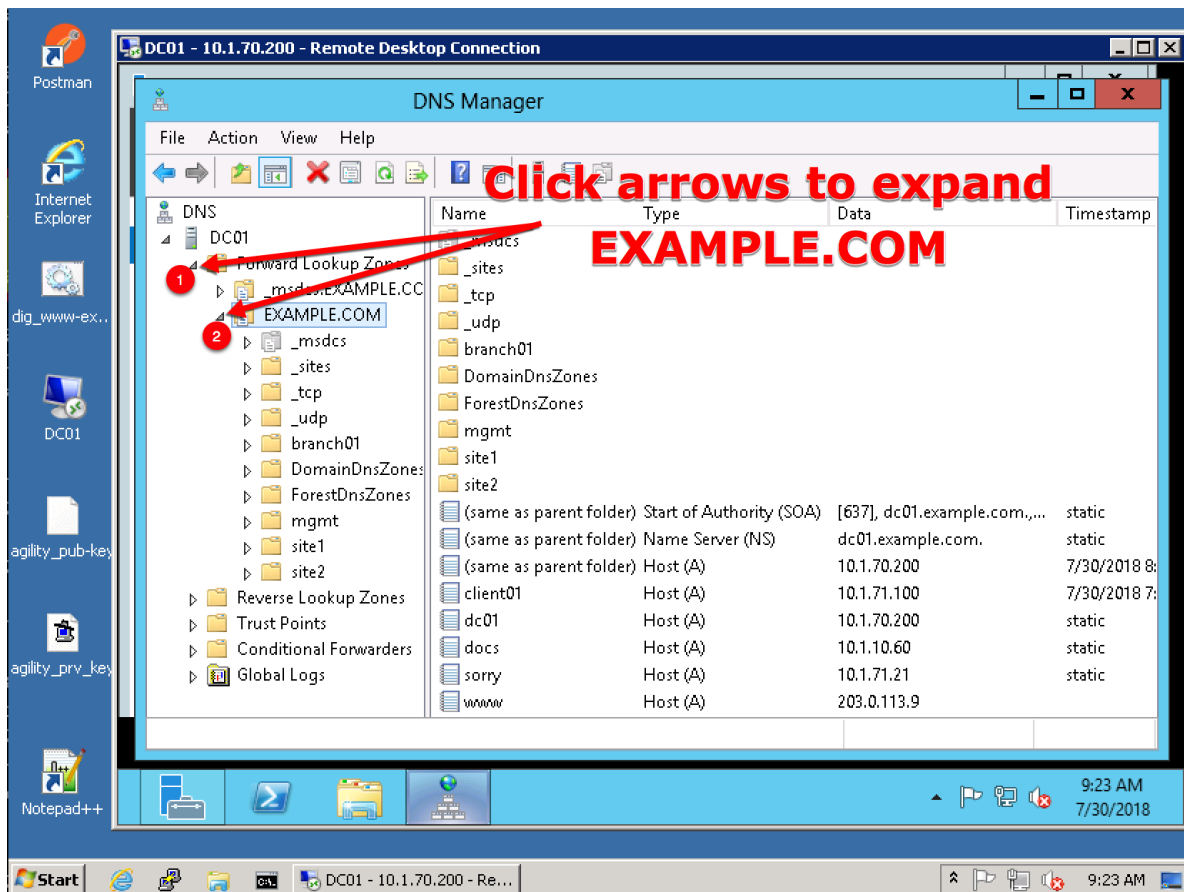
Login to the local DNS server (this should already be open) from the jumpbox, and open the DNS management UI:



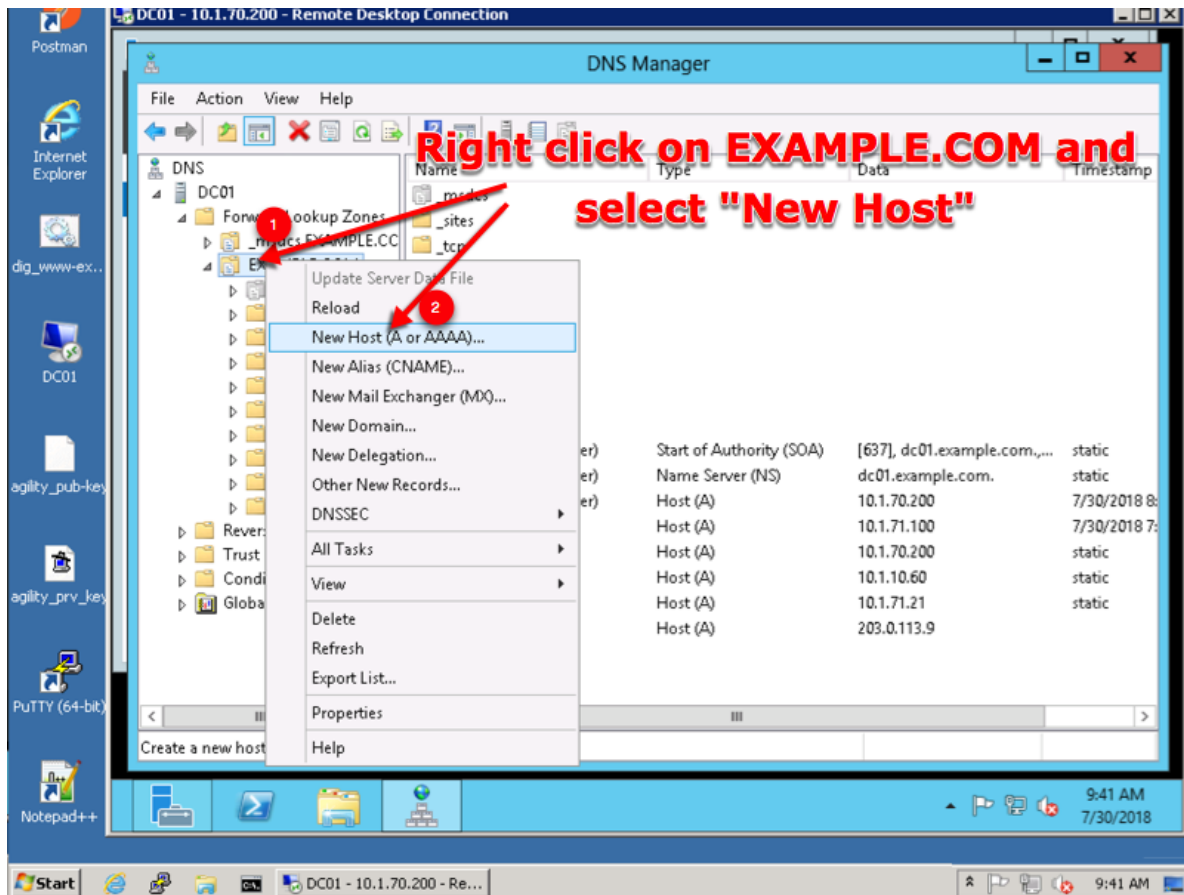
#### 4.8.1 A Records

An A record is the most common DNS query. In this type of query, 'A' refers to an IP address - the client 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"



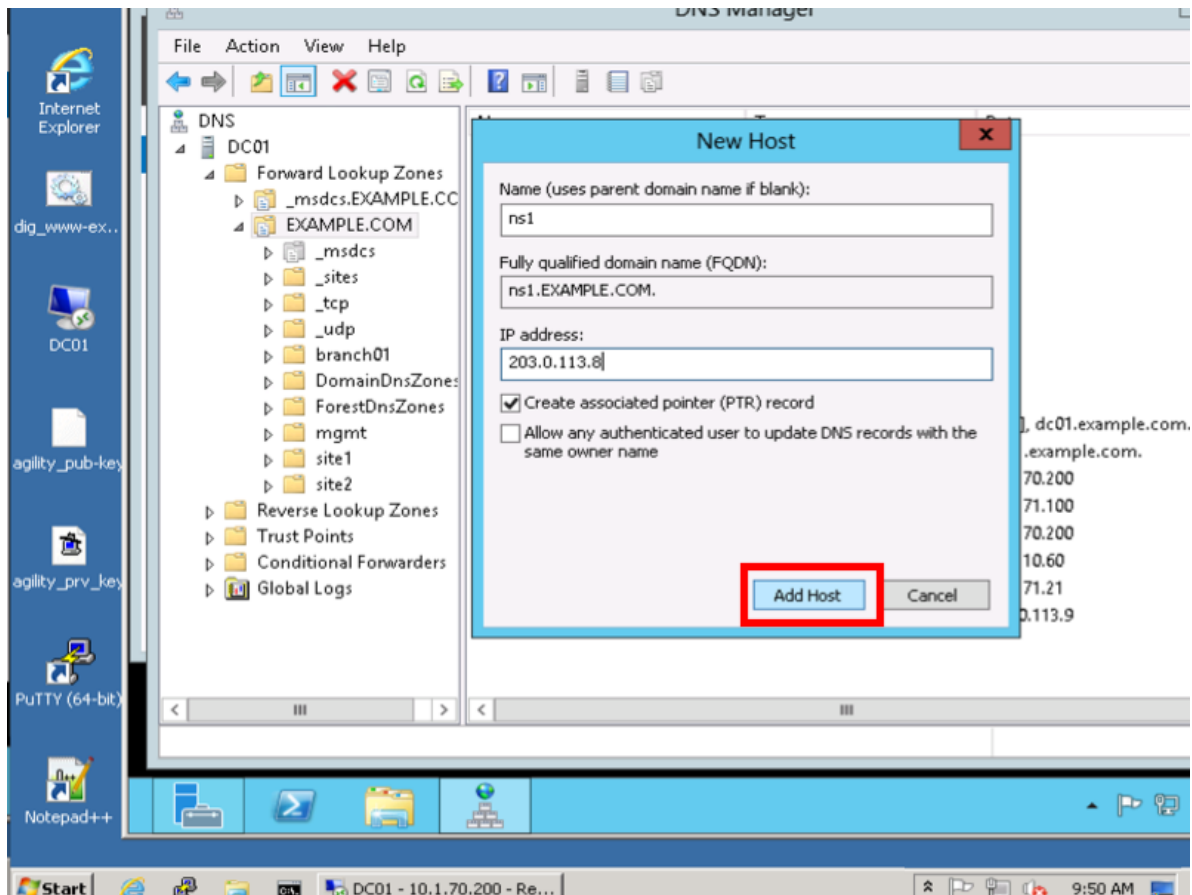
2. Right click on EXAMPLE.COM and select "New Host (A or AAAA)"



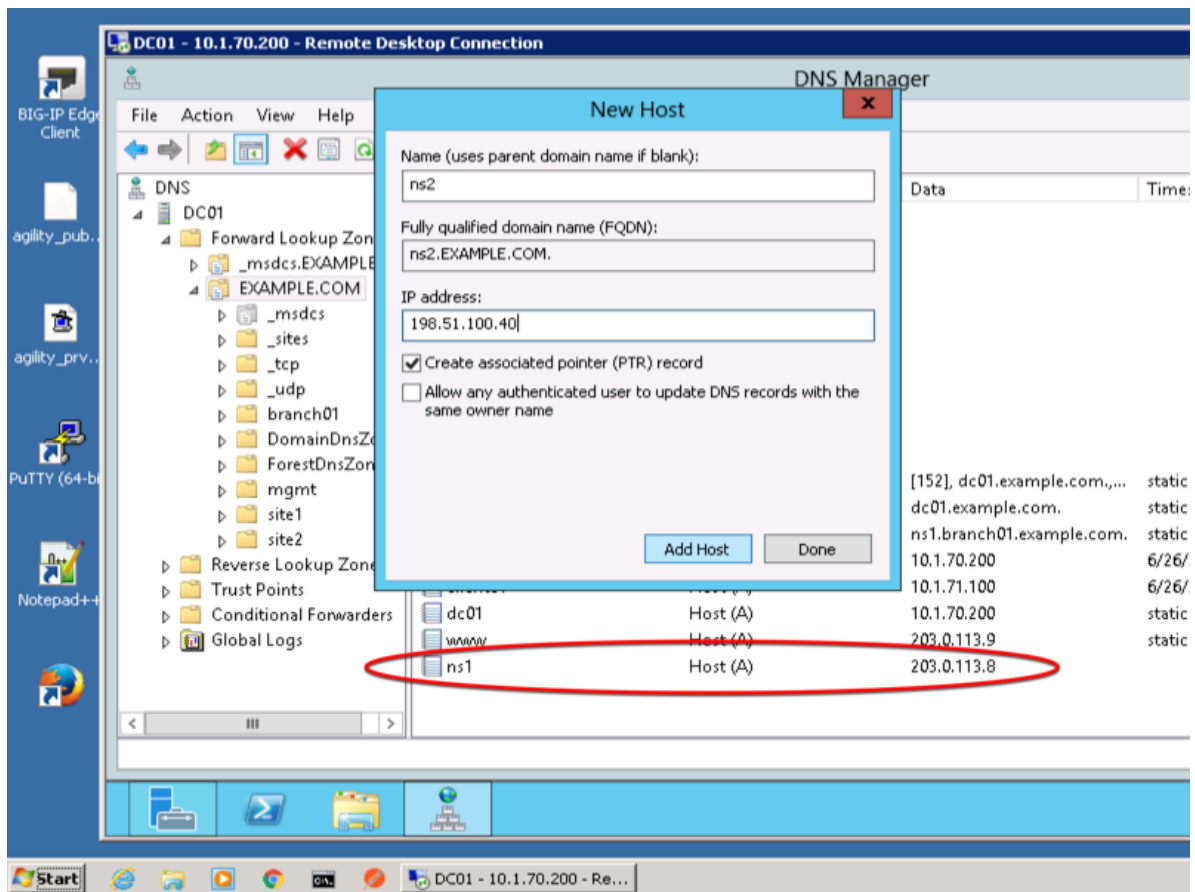
3. Create two new A records for the new BIG-IP nameservers.

Field	Value
ns1	203.0.113.8
ns2	198.51.100.40





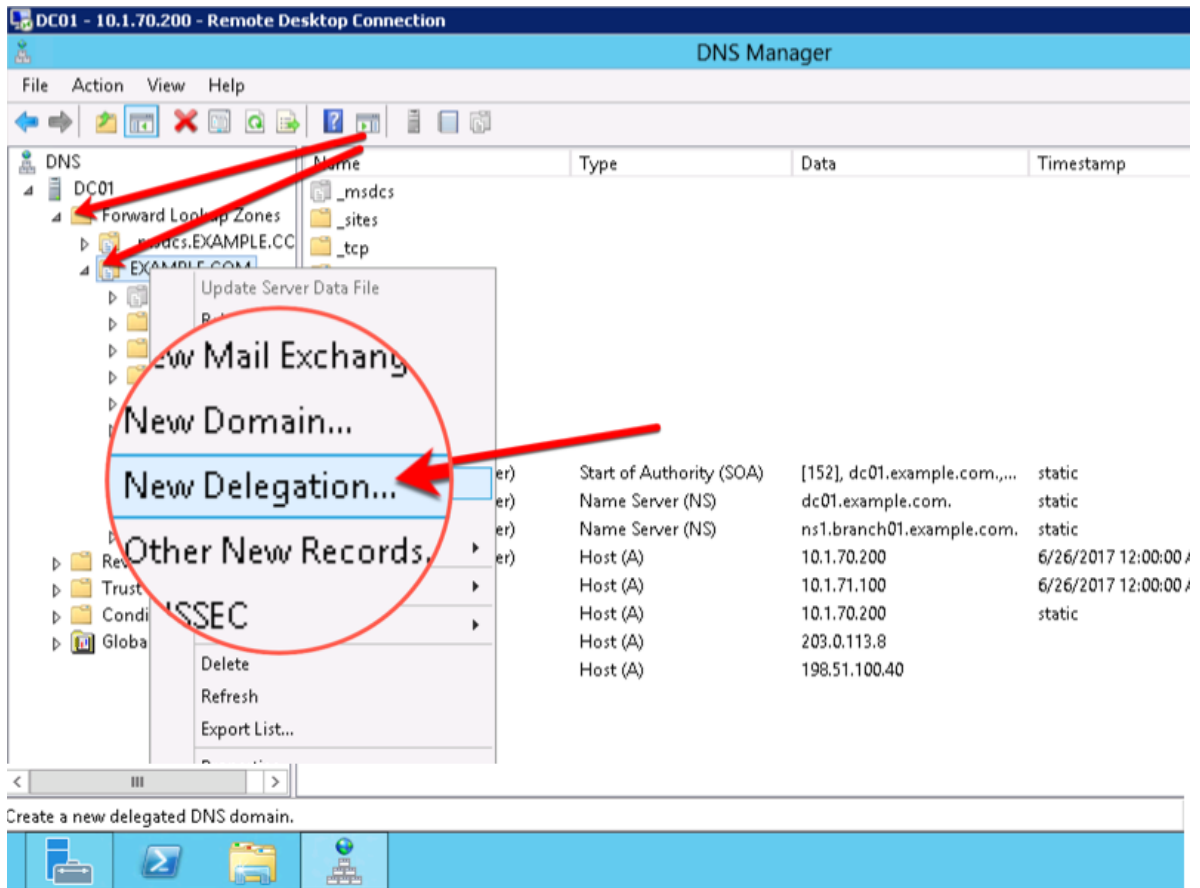
Create ns2.example.com



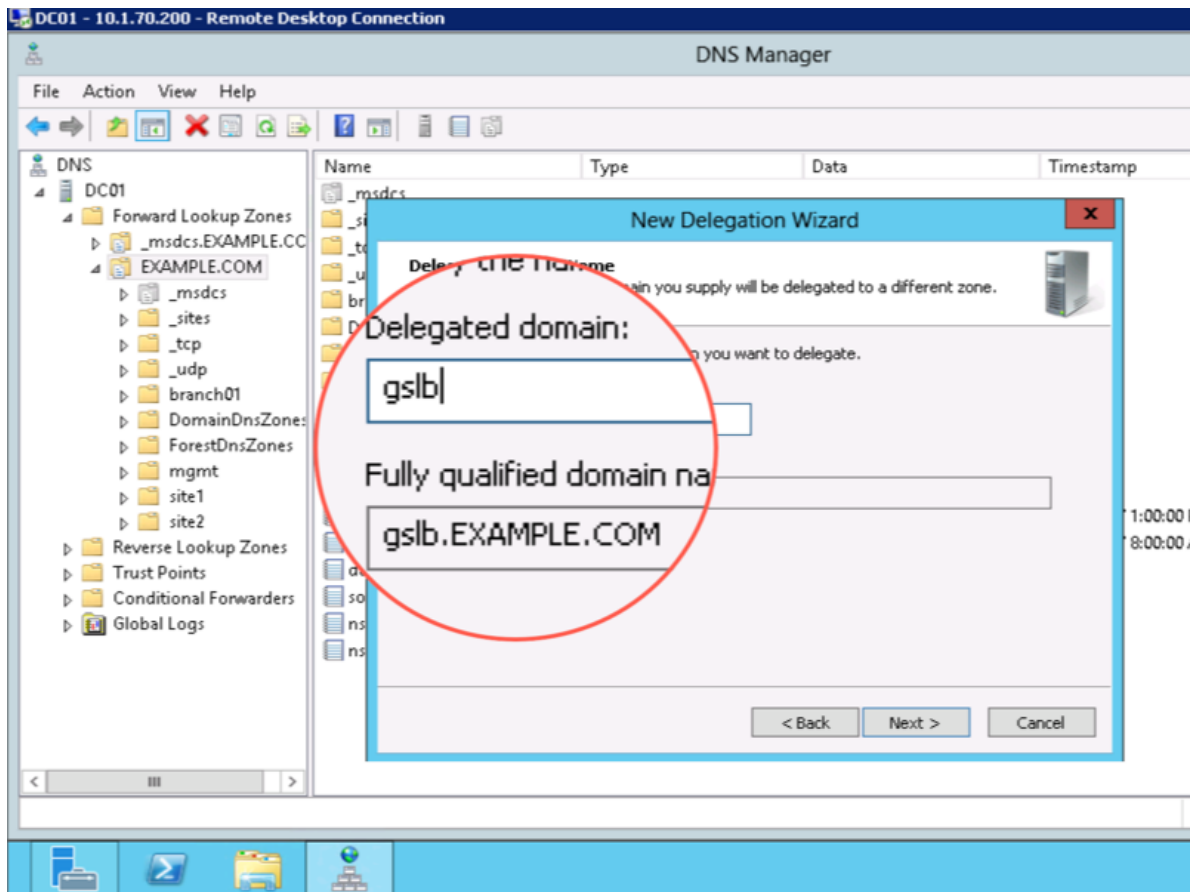
## 4.8.2 Sub Domain

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

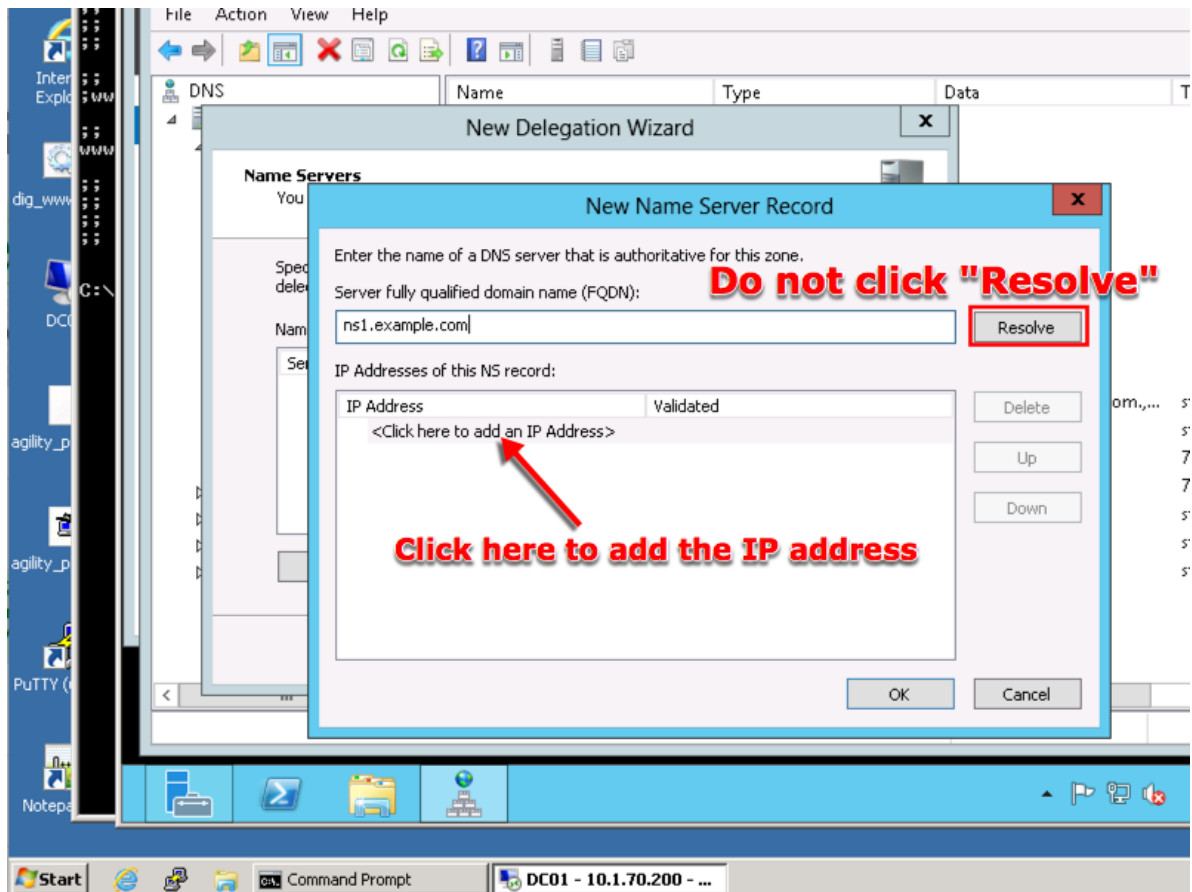
1. Expand "Forward Lookup Zones", and right click on "EXAMPLE.com"



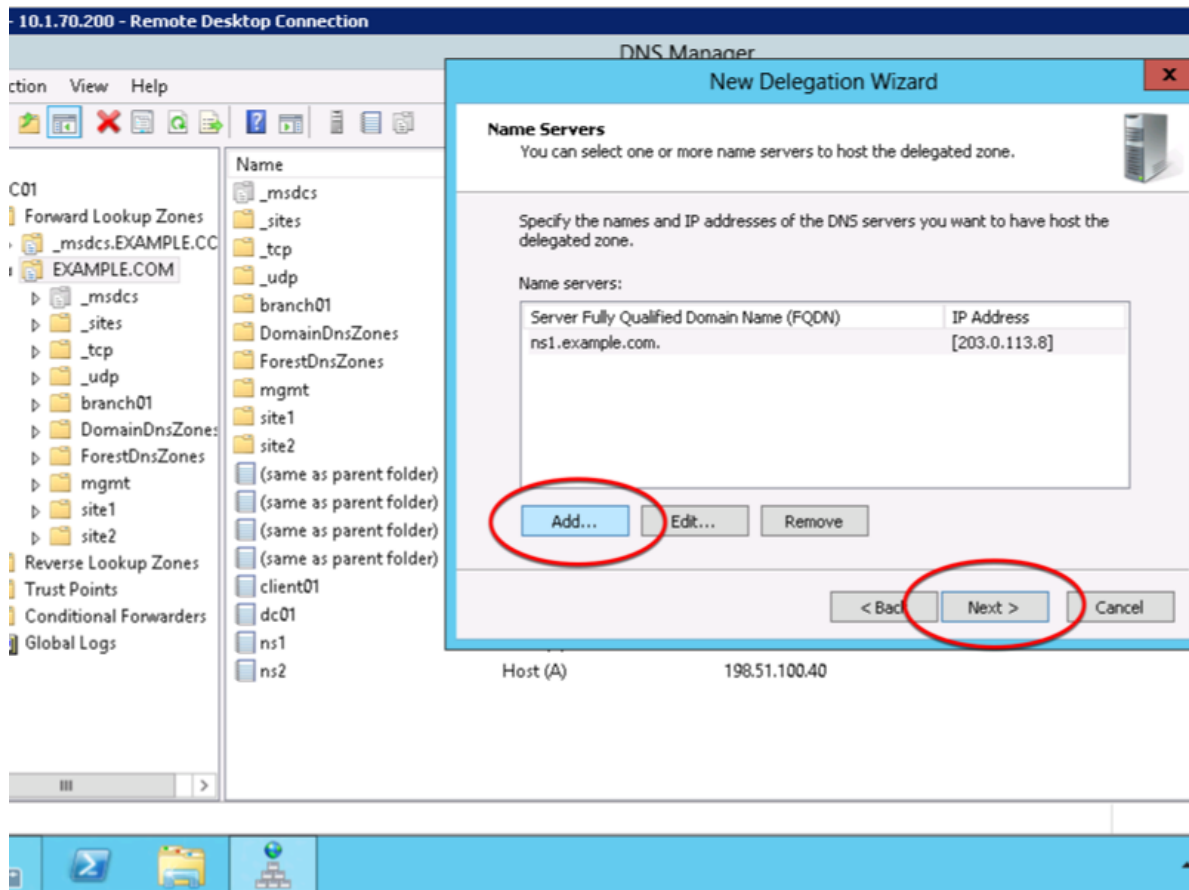
2. Create the "gslb" subdomain.



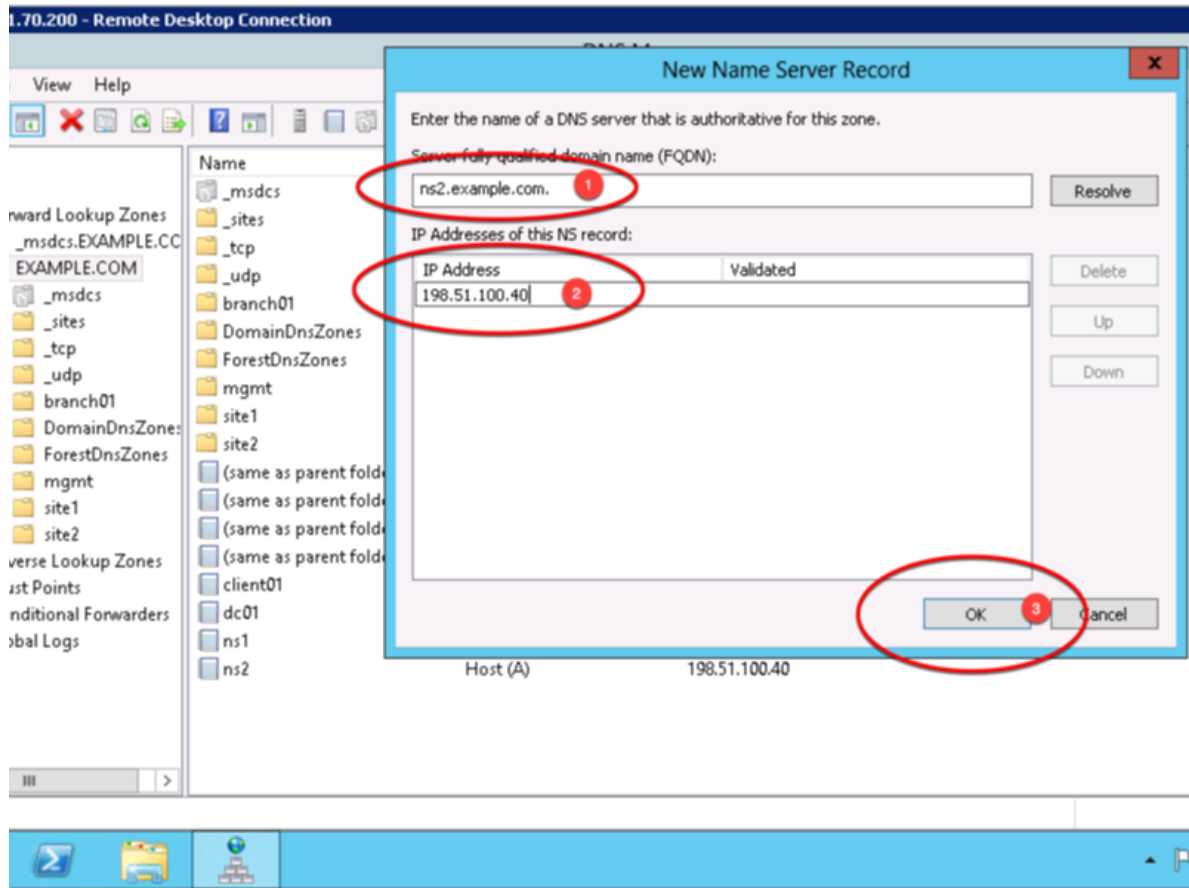
3. Step through the Delegation Wizard. Add "ns1.example.com - 203.0.113.8"



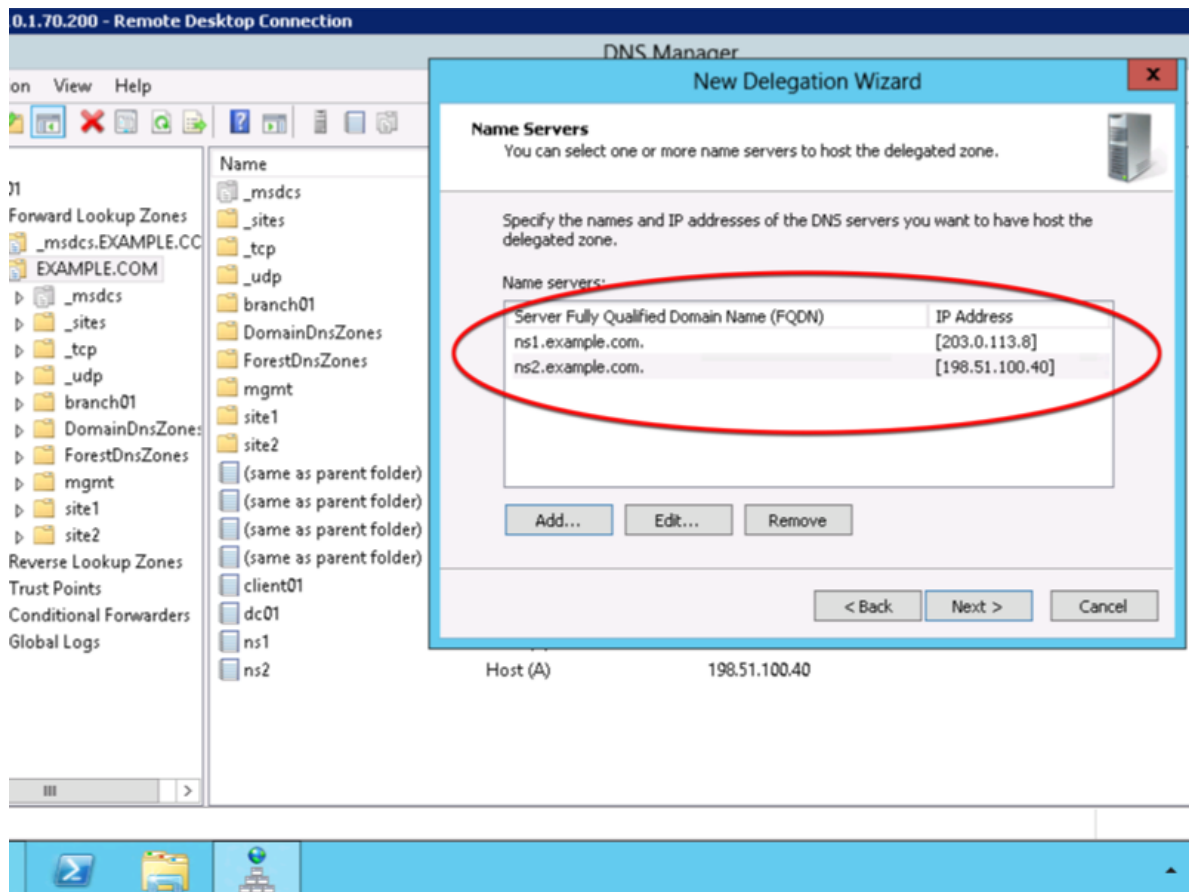
Repeat to add ns2.example.com



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

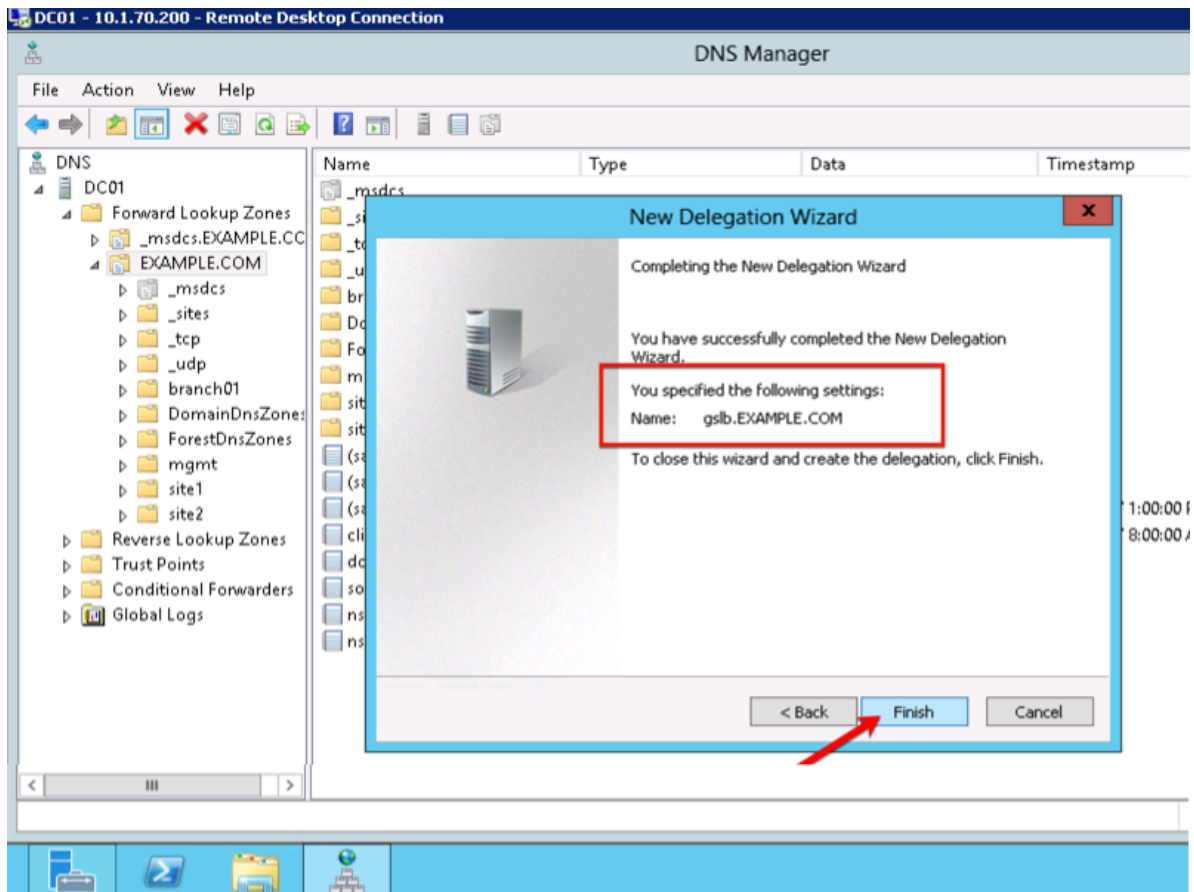


5. Make sure both ns1.example.com and ns2.example.com are added



6. Click "Finish"

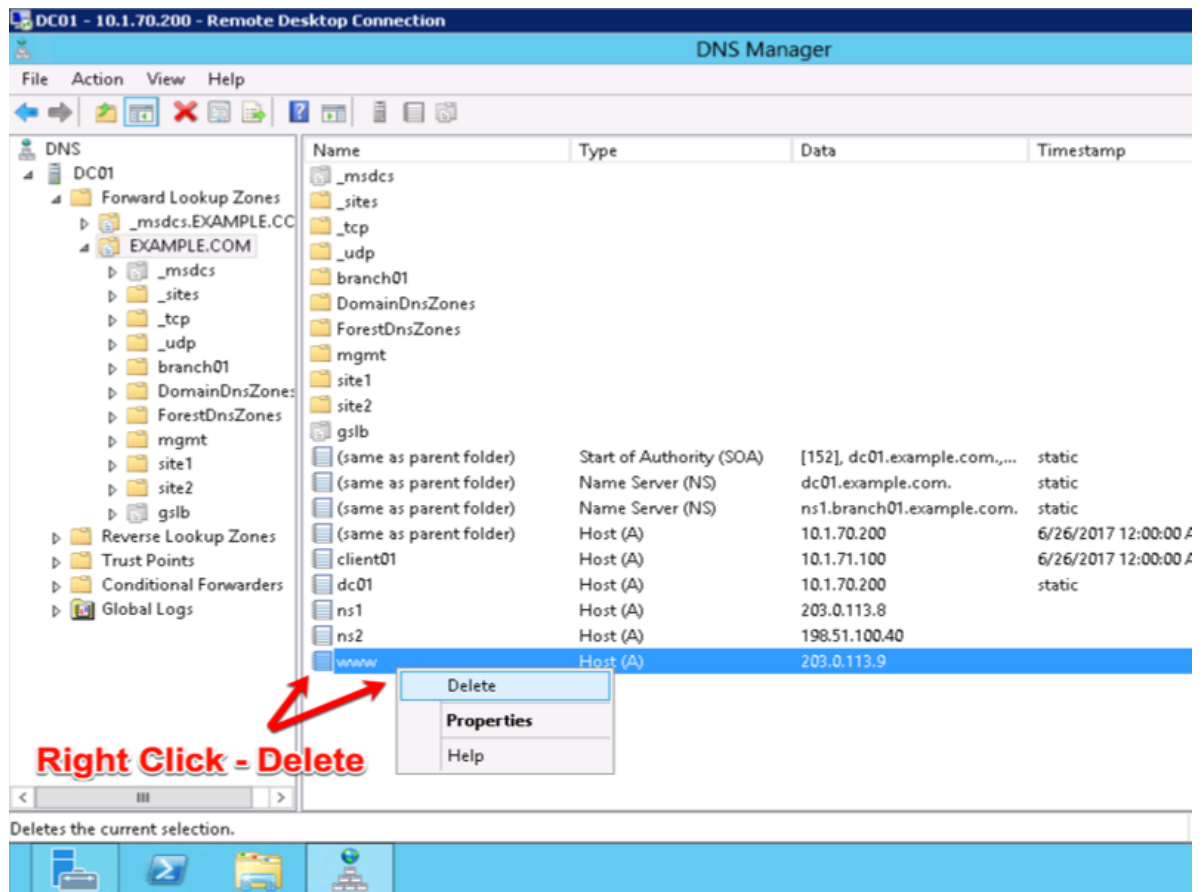




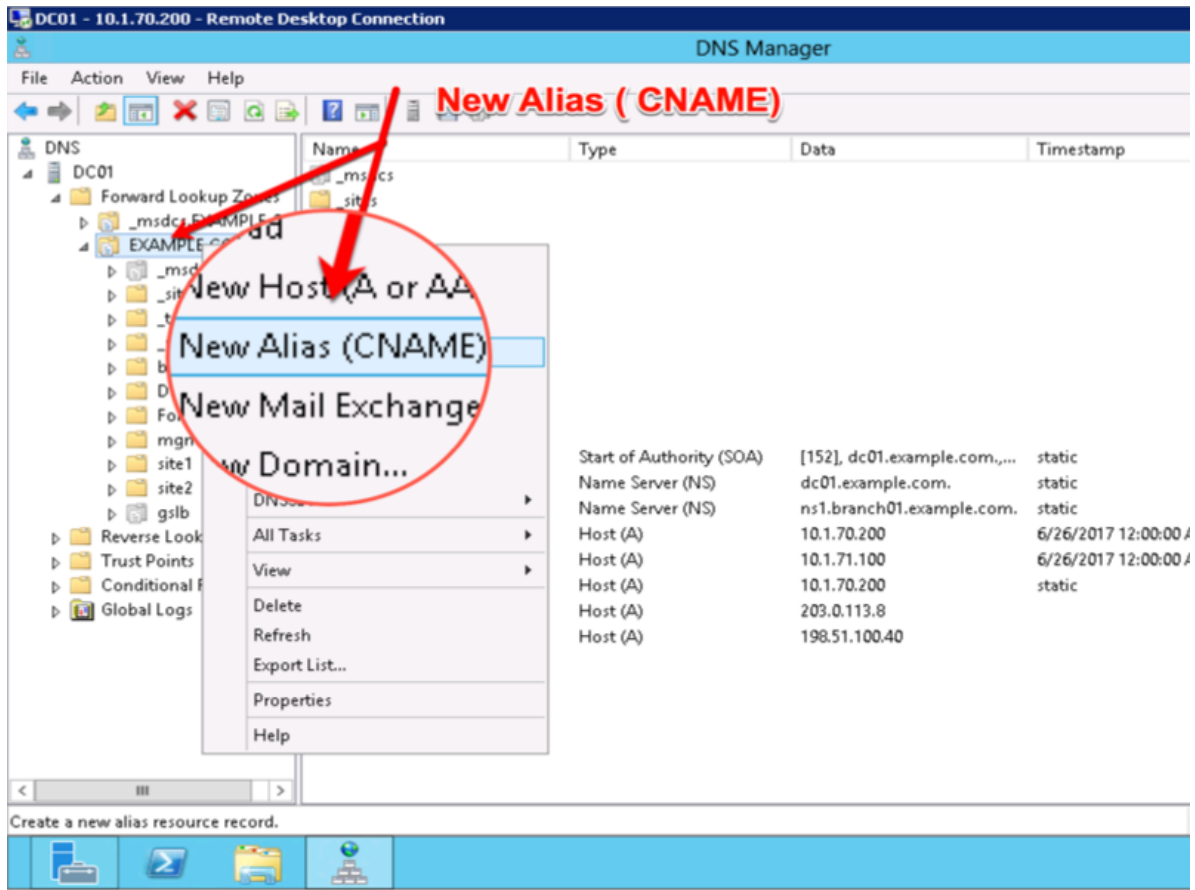
### 4.8.3 CNAME

A CNAME (Canonical name record) functions as an alias for another domain name. Create a CNAME for “www” as an 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.

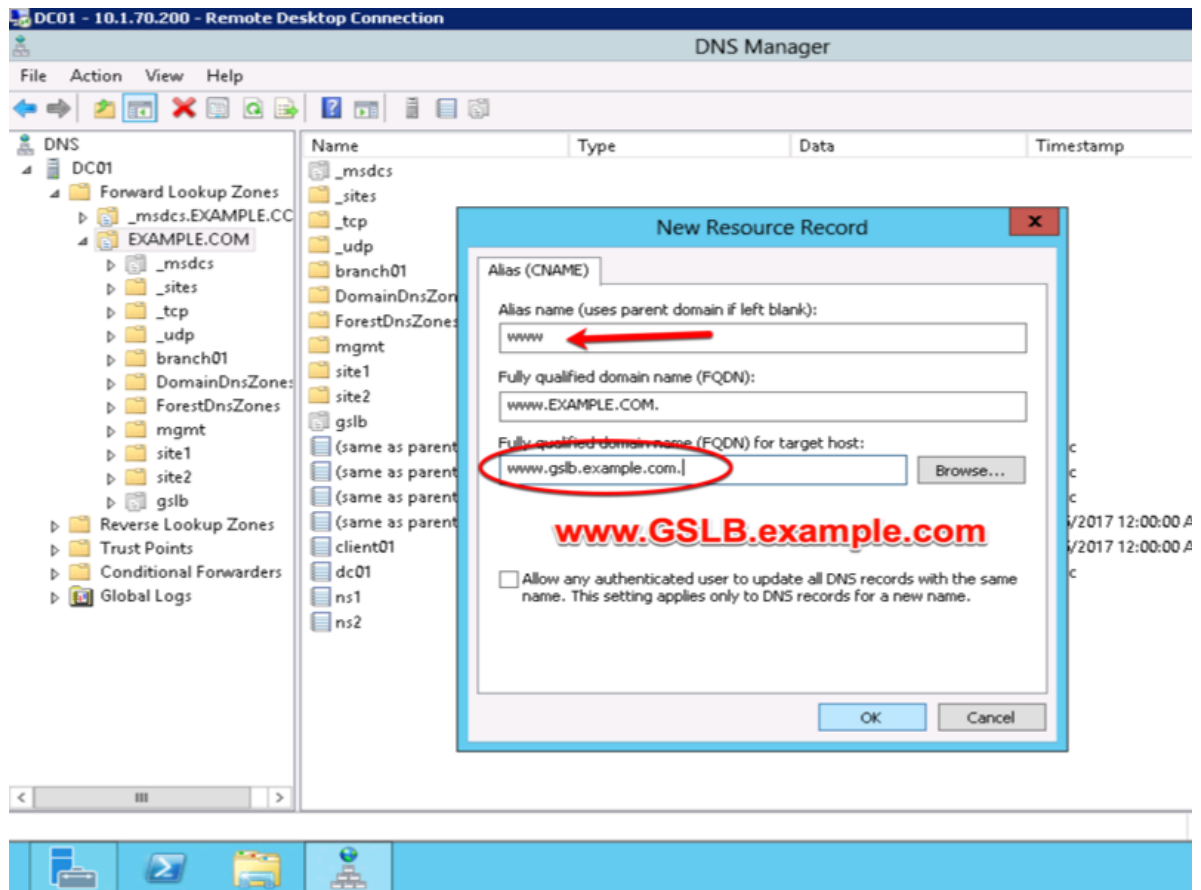
1. Make sure “Forward Lookup Zones” and “EXAMPLE.COM” is expanded. Right click on “www”, and select delete.



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



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



#### 4.8.4 Results

From the Jumpbox use "dig" from the CMD prompt

Do not specifying 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.

```

C:\Users\user.EXAMPLE>dig www.example.com

;; <<>> DiG 9.3.2 <<>> www.example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 687
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.example.com.                IN      A

;; ANSWER SECTION:
www.example.com.                 3600    IN      CNAME   www.gslb.example.com.
www.gslb.example.com.           29      IN      A       203.0.113.9

;; Query time: 46 msec
;; SERVER: 10.1.70.200#53(10.1.70.200)
;; WHEN: Mon Jul 30 11:17:00 2018
;; MSG SIZE rcvd: 72

C:\Users\user.EXAMPLE>dig www.example.com

;; <<>> DiG 9.3.2 <<>> www.example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 593
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

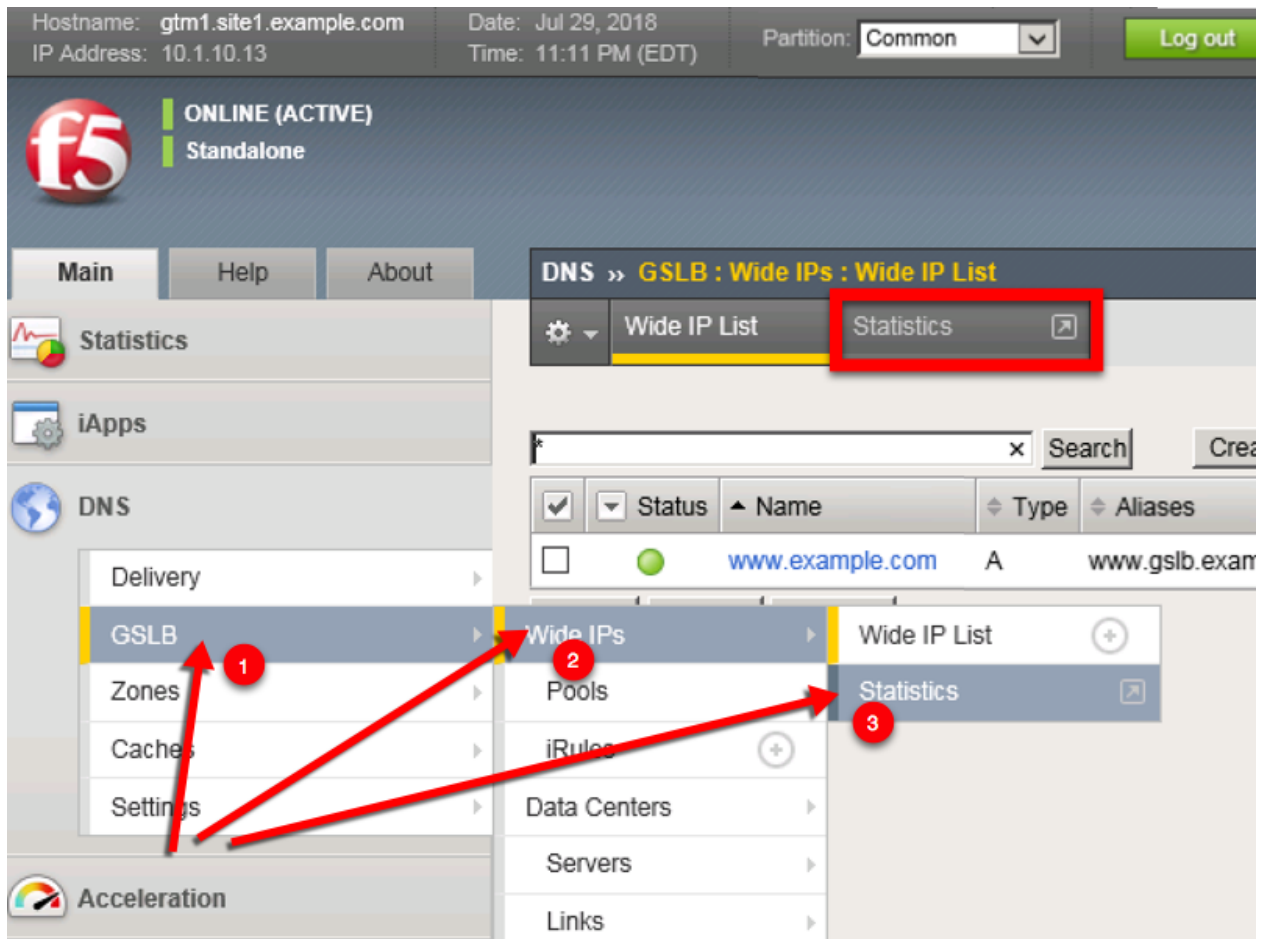
;; QUESTION SECTION:
;www.example.com.                IN      A

;; ANSWER SECTION:
www.example.com.                 3600    IN      CNAME   www.gslb.example.com.
www.gslb.example.com.           29      IN      A       198.51.100.41

;; Query time: 31 msec
;; SERVER: 10.1.70.200#53(10.1.70.200)
;; WHEN: Mon Jul 30 11:19:35 2018
;; MSG SIZE rcvd: 72

C:\Users\user.EXAMPLE>

```



Hostname: gtm1.site1.example.com    Date: Jul 29, 2018    User: admin    Partition:  
IP Address: 10.1.10.13    Time: 11:21 PM (EDT)    Role: Administrator

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

Statistics » **Module Statistics : DNS : GSLB**

Statistics Traffic Summary DNS Subscriber Management Network

Statistics  
Dashboard  
Module Statistics  
Analytics  
Performance

iApps  
DNS  
Acceleration  
Device Management  
Network  
System

**Display Options**

Statistics Type: Wide IPs  
Data Format: Normalized  
Auto Refresh: Disabled Refresh

\* Search

	Status	Wide IP	Type	Partition / Path	Details	Pools	Total	Resolved	Rel
<input type="checkbox"/>		www.example.com	A	Common	<a href="#">View...</a>	<a href="#">View...</a>	44	44	0

Reset

**For more details click**

**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

```

gtm1.SITE1
[root@gtm1: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
  Persisted   0
  Resolved    44
  Dropped     0

Load Balancing
  Preferred    44
  Alternate    0
  Fallback     0
  CNAME Resolutions 0
  Returned from DNS 0
  Returned to DNS 0
  Failures with RCODE 0

-----
| Gtm::Pool::A www.example.com_pool
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Available
|
| Load Balancing
|   Preferred    44
|   Alternate    0
|   Fallback     0
|   Returned from DNS 0
|   Returned to DNS 0
|   Dropped     0
|
-----
| Gtm::Pool Member: www.example.com_pool:A isp1_site1_www.example.com_tcp_https_virtual:site1_ha-pair
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Available
|
| Load Balancing
|   Preferred    35
|   Alternate    0
|   Fallback     0
|
-----
| Gtm::Virtual Server: isp1_site1_www.example.com_tcp_https_virtual
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Monitor /Common/bigip from 203.0.113.5 : UP
|   Destination : 203.0.113.9:443
|   Up Time     : 10:18
|
| Link Name      203.0.113.1
|
| Global
|   Picks        35
|   Connections   0
|   Virtual Server Score 1
|
| Throughput
|   In  Out
|   Bits/sec  0  0
|   Packets/sec 0  0
|
-----
| Gtm::Pool Member: www.example.com_pool:A isp2_site1_www.example.com_tcp_https_virtual:site1_ha-pair
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Available

```



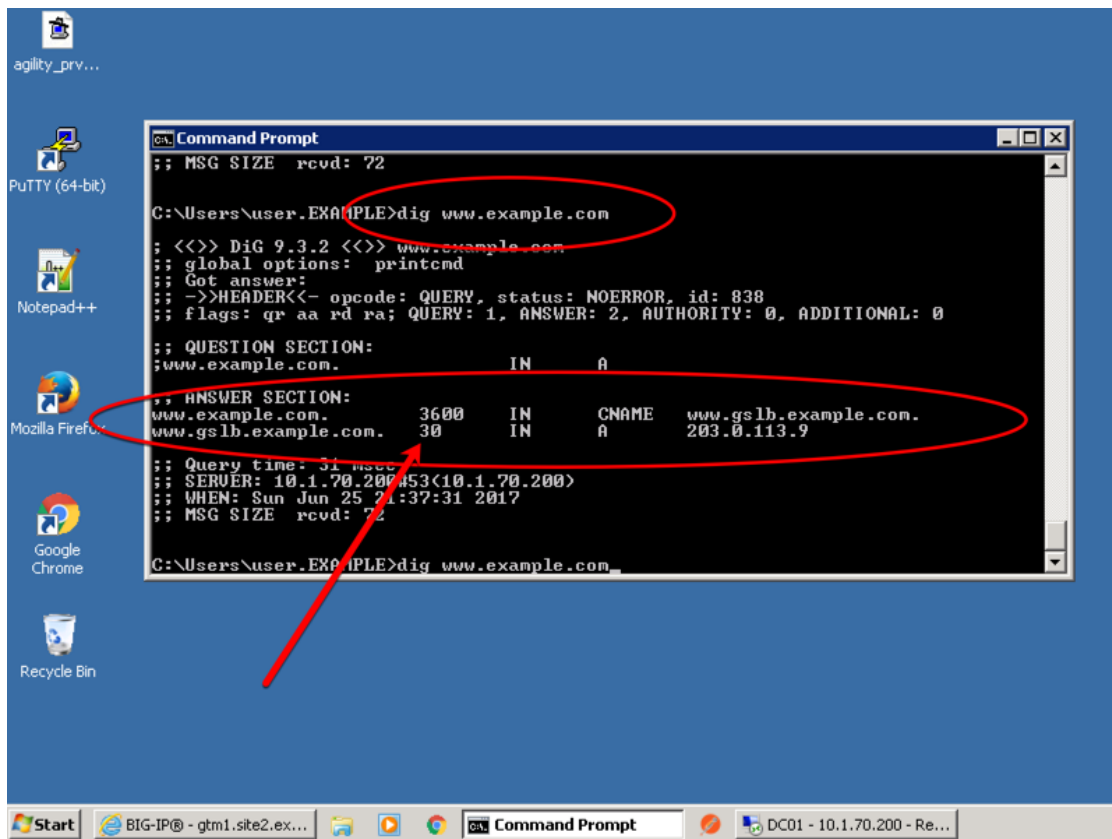
## TMSH

```
tail -f /var/log/ltm
```

```
gtm1.SITE1
[root@gtm1:Active:Standalone] config # tail -f -n 12 /var/log/ltm
Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com qid 991 from 198
.51.100.68#64119: view none: query: www.gslb.example.com IN A + (203.0.113.8%0)
Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com qid 991 from 198
.51.100.68#64119 [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 00:19:49 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 A 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 A + (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 A 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 A + (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 gtm1 info tmm[11966]: 2018-07-30 00:23:43 gtm1.site1.example.com qid 261 to 203.0
.113.68#64121: [NOERROR qr,aa,rd] response: www.example.com. 30 IN A 198.51.100.41;
Jul 30 00:23:50 gtm1 info tmm[11966]: 2018-07-30 00:23:50 gtm1.site1.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 gtm1 info tmm[11966]: 2018-07-30 00:23:50 gtm1.site1.example.com qid 97 from 203.
0.113.68#64122 [www.example.com A] [round robin selected pool (www.example.com_pool)] [pool membe
r 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_https_vir
tual:203.0.113.9)]
Jul 30 00:23:50 gtm1 info tmm[11966]: 2018-07-30 00:23:50 gtm1.site1.example.com qid 97 to 203.0.
```

## 4.9 Failure Condition

Having followed the exercises 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.



```
Command Prompt
C:\Users\user.EXAMPLE>dig www.example.com

;; <<>> DiG 9.3.2 <<>> www.example.com
;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 838
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.example.com.          IN      A

;; ANSWER SECTION:
www.example.com.          3600    IN      CNAME   www.gslb.example.com.
www.gslb.example.com.     30      IN      A       203.0.113.9

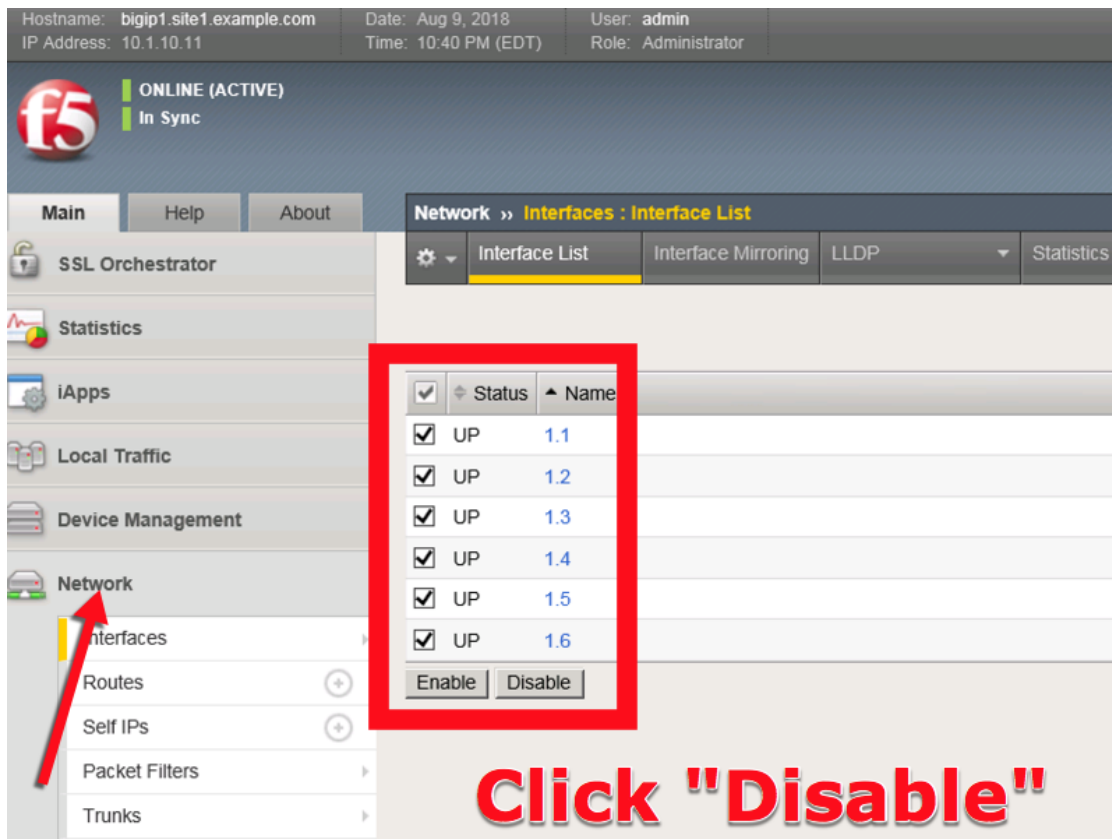
;; Query time: 31 msec
;; SERVER: 10.1.70.200#53(10.1.70.200)
;; WHEN: Sun Jun 25 21:37:31 2017
;; MSG SIZE rcvd: 72

C:\Users\user.EXAMPLE>dig www.example.com
```

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>



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 Date: Aug 9, 2018 User: admin  
IP Address: 10.1.10.13 Time: 11:01 PM (EDT) Role: Administrator

ONLINE (ACTIVE)  
Standalone

Main Help About **DNS » GSLB : Servers : Server List**

Statistics iApps DNS Delivery **GSLB** Zones Caches Settings Acceleration Device Management Network

Server List Trusted Server Certificates Statistics

Search

<input checked="" type="checkbox"/>	Status	Name	Devices	Age
<input type="checkbox"/>	<span style="color: green;">●</span>	gtm1.site1_server	1	20
<input type="checkbox"/>	<span style="color: green;">●</span>	gtm1.site2_server	1	19
<input type="checkbox"/>	<span style="color: red;">◆</span>	site1_ha-pair	2	20
<input type="checkbox"/>	<span style="color: green;">●</span>	site2_ha-pair	2	19

Enable Disable Delete...

**Site1 HA pair is Down**

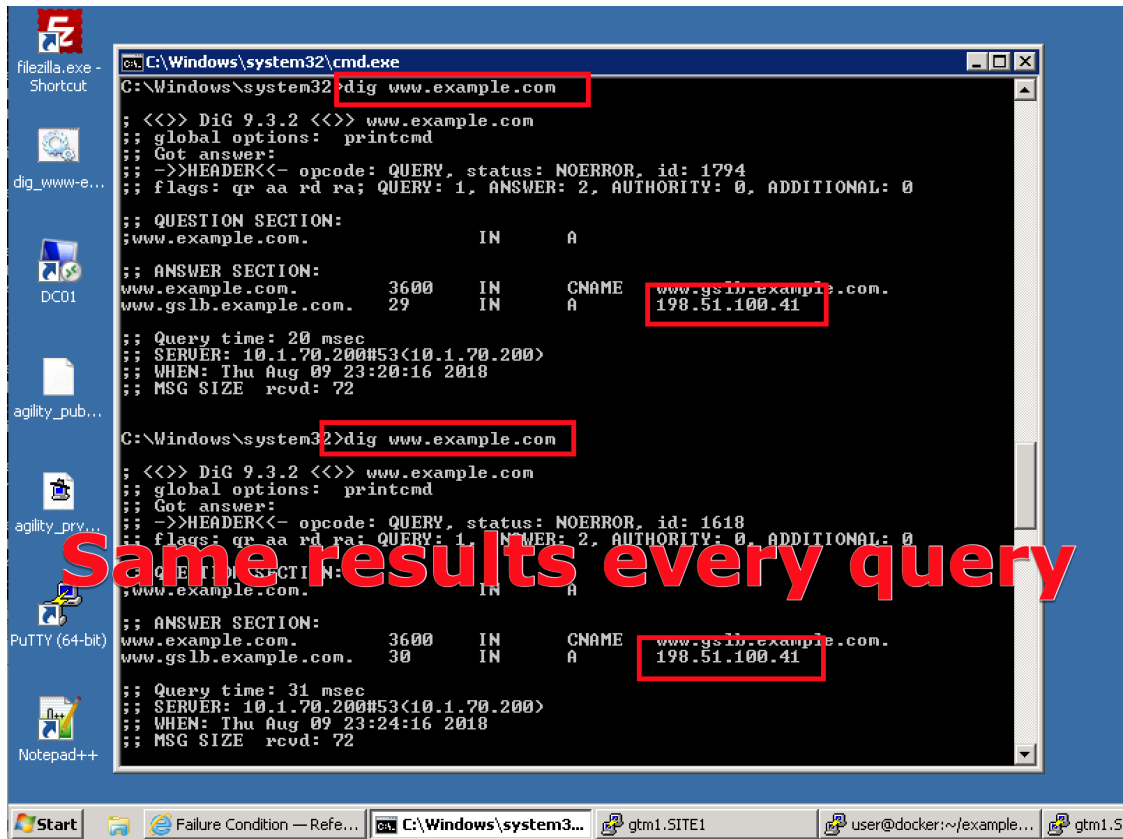
<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/server/list.jsp>

---

### 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

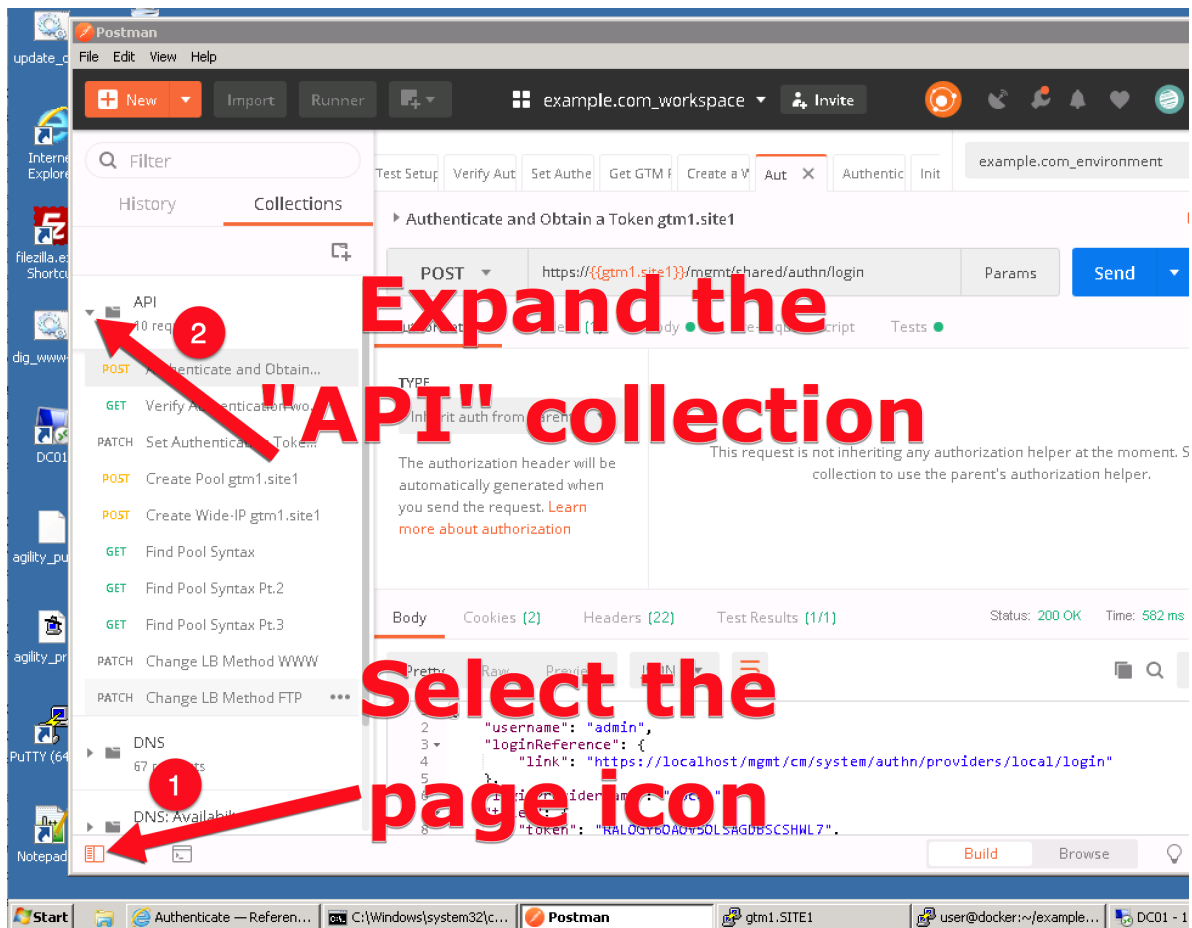
## 4.10 Rest API

### 4.10.1 Authenticate

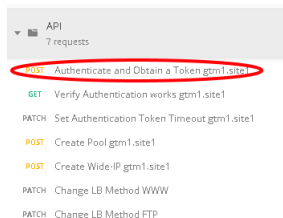
From the Jumpbox using the Postman application navigate to the “API” section under the Collections on the left.

**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 be synchronized to gtm1.site2

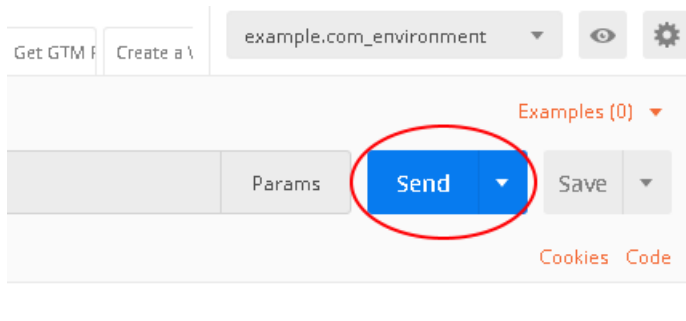
1. Reveal the navigation panel in Postman



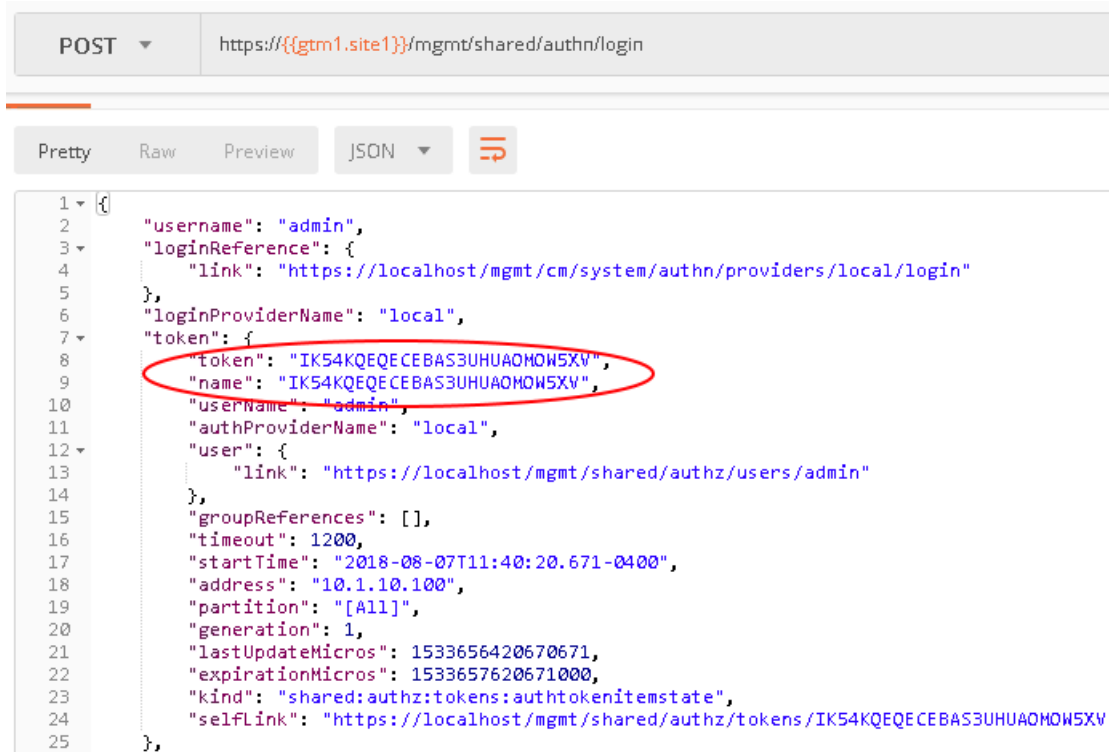
2. Click on “Authenticate and Obtain Token from gtm1.site1”.



3. Click on the “Send” button in the top right.



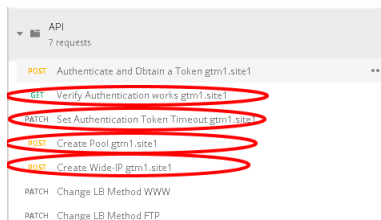
4. Open the response body and observe the received token. The token value is dynamic and your result will not be the same as illustrated below. The token received will be used for all subsequent authenticated actions with the BIG-IP DNS.



### 4.10.2 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.

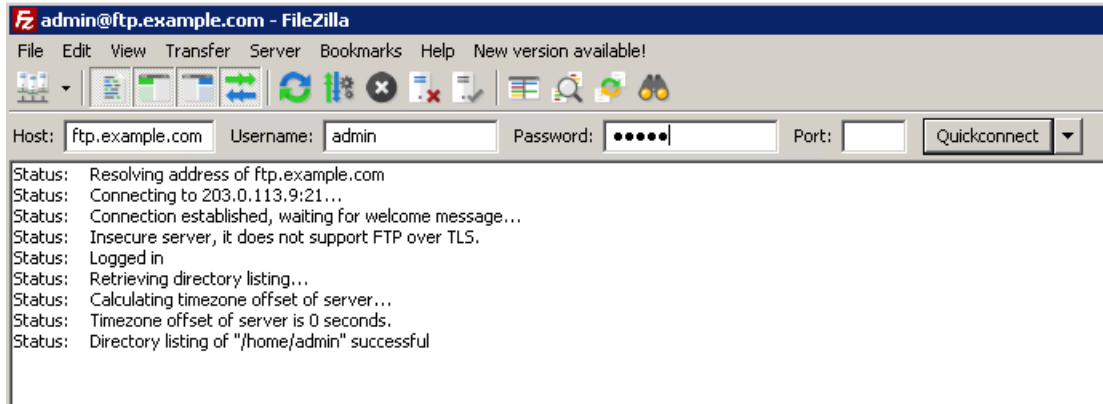


Once complete, login to gtm1.site1 via Web interface and look for the new configuration elements to confirm that they were successfully created. Do the same on gtm1.site2.

### 4.10.3 Results

Now let's 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



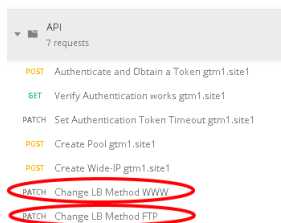
You've just successfully created a new highly available service on BIG-IP DNS all with only a few very simple API commands.

### 4.10.4 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 response when querying either ftp.example.com or www.example.com instead of the round robin behavior.

### 4.10.5 API Extras (Optional)

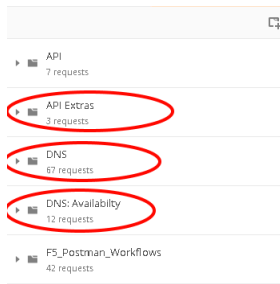
In Postman, feel free to browse the other collections and experiment with additional REST commands.

---

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

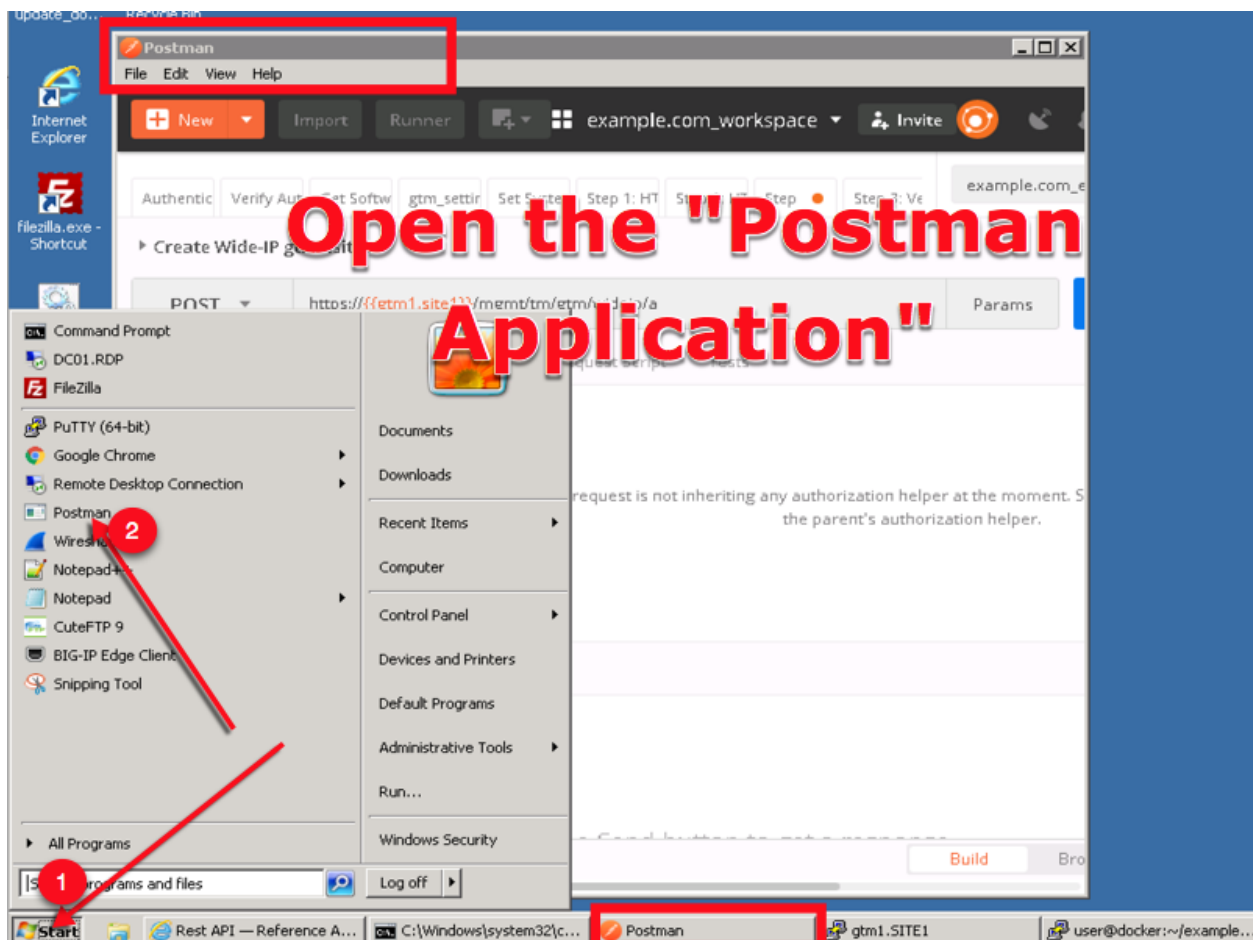
---





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.



## 4.11 Congratulations

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



## Class 4 - EDNS0 client subnet

This class covers the following topics:

- Understanding edns0 as implemented by f5
- Configuring edns0 client subnet on a listener
- Configure a wide-ip with topology resolution to allow for edns0 resolution
- Reviewing the different edns0 setting and the logs created for any differences in the new release.

Expected time to complete: **2 hours**

### 5.1 Getting Started

Please follow the instructions provided by the instructor to start your lab and access your jump host.

---

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

---

#### 5.1.1 Lab Topology

The following components have been included in your lab environment:

- 2 x F5 BIG-IP VE (v14.0) DNS GSLB engines
- 1 x F5 BIG-IP VE (v13.1) central Router
- 1 x Linux server (ubuntu)
- 1 x Linux Jumphost

#### Lab Components

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

Component	VLAN/IP Address(es)	Credentials
bigip-dc1	<ul style="list-style-type: none"> <li>• <b>Management:</b> 10.0.1.245</li> <li>• <b>External:</b> 10.1.0.245</li> </ul>	admin/f5edns0
bigip-dc2	<ul style="list-style-type: none"> <li>• <b>Management:</b> 10.0.1.246</li> <li>• <b>External:</b> 10.2.0.245</li> </ul>	admin/f5edns0
bigip-router	<ul style="list-style-type: none"> <li>• <b>Management:</b> 10.0.1.240</li> </ul>	admin/f5edns0
Linux Jumphost	<ul style="list-style-type: none"> <li>• <b>Management:</b> 10.0.1.50</li> </ul>	ubuntu/supernetops
ubuntu server	<ul style="list-style-type: none"> <li>• <b>Management:</b> 10.0.1.253</li> </ul>	ubuntu/ubuntu

Follow these steps to get your lab started:

1. Open a browser and visit <http://training.f5agility.com>
2. Enter your class number (instructor will provide this) and your student number.
3. You should now be seeing the class portal and can now access the RDP and lab resources.

**AGILITY** Attend Learn Speakers Network Sponsors

**WELCOME TO THE AGILITY 2018 LABS.**

Enter your class number and your student number.

Class #:  Student #:

ABOUT F5  
 Corporate Information  
 Newsroom  
 Investor Relations  
 Careers  
 Contact Information  
 Marketing Guidelines

EDUCATION  
 Training  
 Certification  
 F5 University  
 Free Online Training

F5 SITES  
 F5.com  
 DevCentral  
 Support Portal  
 Partner Central  
 F5 Labs

PREFERENCES  
 Sign Out  
 Update Profile  
 Email Preferences

CONNECT WITH US  
 Twitter  
 LinkedIn  
 Facebook  
 YouTube  
 DevCentral

© 2018 F5 Networks, Inc. All rights reserved | Policies | Privacy | Trademarks

## Welcome

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

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

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

Bugs and Requests for enhancements are handled in two ways:

- Fork the Github Repo, fix or enhance as required and submit a Pull Request
  - <https://help.github.com/articles/creating-a-pull-request-from-a-fork/>
- Open an issue

For more information, visit <https://github.com/f5devcentral/f5-automation-labs/issues> within the F5 DevCentral portal.

Stopping in: 02:43 (hr:min)
 

All VMs: [Start](#) / [Stop](#) [Help](#)

Started

BIG-IP B

SERVICES

TMUI

SSH: 129.146.151.219  
Port: 22

CONSOLE

INFO

Started

Linux Jumpbox

SERVICES

RDP

SSH: 129.146.91.23  
Port: 22

CONSOLE

INFO

Started

iWorkflow

SERVICES

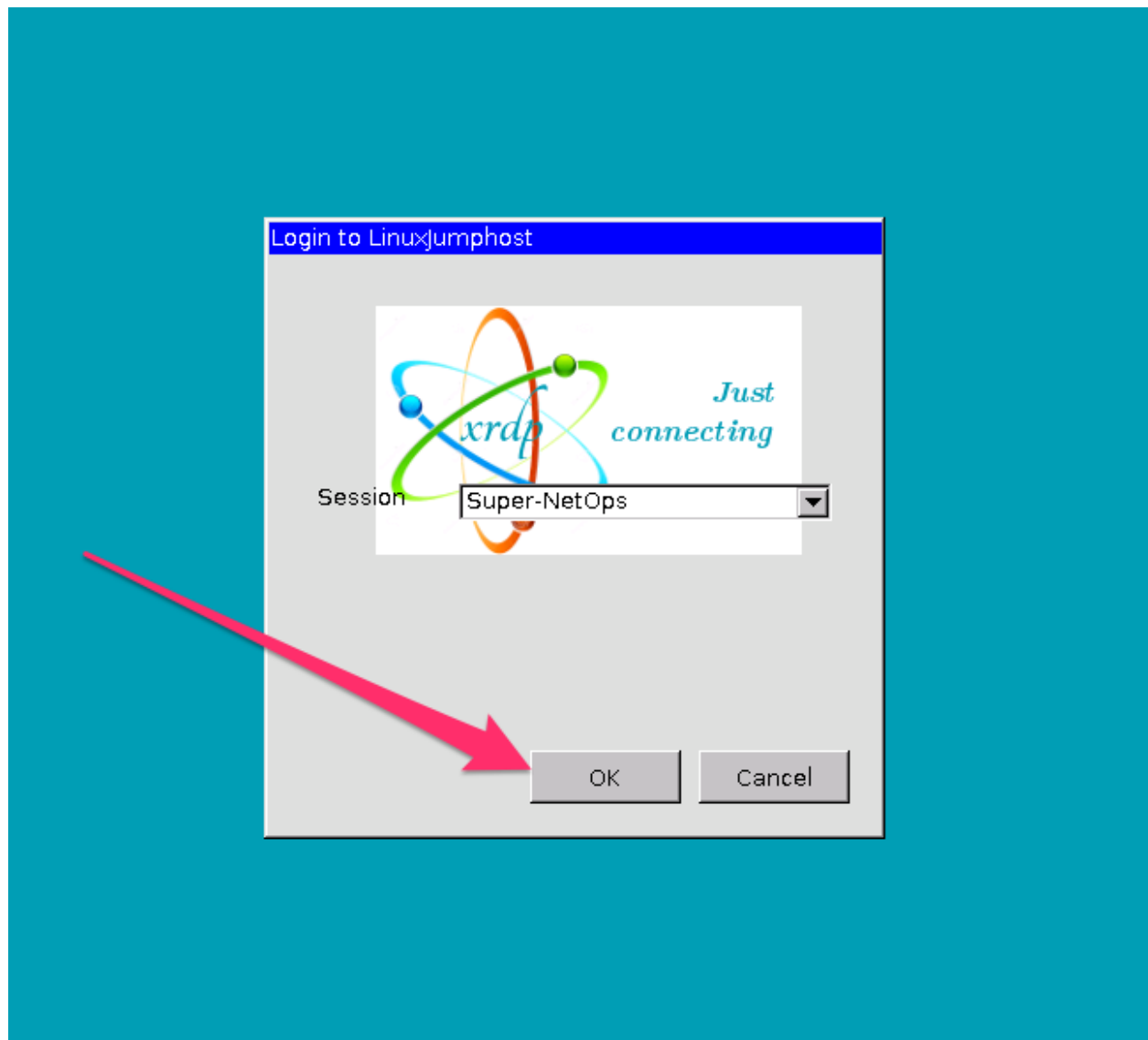
TMUI

SSH: 129.146.147.110  
Port: 22

CONSOLE

INFO

To start your lab you will want to log into the linux jumpbox. From this you can then do all of the exercises in the lab. To log into the jump box for the lab start your session and access the jumpbox via RDP. Once the RDP window is open then just click to log in the “supernetops” user. You should not need a password.



## 5.2 Module – EDNS0 and client subnet

### EDNS0 client subnet - RFC 7871

**Problem:** With the GSLB solution from f5 it is possible to use DNS to determine the geographical location of the user. We can't use the IP address of the client for this, because it is masked by the DNS resolver, and so the dns engine uses the IP address of the DNS resolver instead. In case of the Google DNS or OpenDNS servers, for many end users those servers are not close to them, simply because these providers don't have servers in every country and every ISP's network. For example, OpenDNS does not have DNS servers in South-America. Someone in Brazil using OpenDNS will likely hit their resolver in Florida. The F5 will then think the user is in Florida and as a result it will serve content to the user from a server far away (Florida, not Brazil) resulting in a slow, high latency experience.

**Solution:** To mitigate the problem of DNS based geo-targetting, Google proposed a technical solution to the issue in an IETF draft Client subnet information in DNS requests. This is an experimental DNS extension that allows DNS resolvers to pass the client's IP address (or part of) to compatible authoritative DNS servers.

The F5 DNS server can then use this information to better determine where the end user is. Google DNS and OpenDNS implemented this solution as part of the Global Internet Speedup initiative in August 2011.

The drawback is the experimental nature of the spec and limited support in existing DNS server software. Only OpenDNS and Google Public DNS seems to support it on the resolver side, but NOW with v14 of TMOS F5's DNS GSLB solution can use the Client-subnet options for decision making!

### 5.2.1 Lab – Setup lab and get logged into the components

This lab you will log into the jumpbox and then log into the east and west f5 dns nodes and inspect.

#### Task – Review basic configurations

In this task you will open a web browser and navigate east and west nodes.

Follow these steps to complete this task:

1. Log into the jumphost with the credentials provided in the setup section.
2. Open your web browser in the jumphost window.
3. Navigate to the east DC F5 and open another tab for the west DC.
4. Login with the username and password from the setup section.
5. After logging in take a look at the different settings for the interfaces and ip addresses and examine things to become comfortable with the environment and the two devices.

#### Task – Review the DNS profile

In this task you will review the dns profile used on the listeners and take note of any non-default configuration options. You will see three major changes. One of them is very important to EDNS0 client subnet operation, make sure that you understand that there is no button labeled “EDNS0” of any sort.

Follow these steps to complete this task:

1. Navigate to “DNS : Delivery : Profiles : DNS “
2. Click the dns\_nobind\_edns0 profile and examine the options set.

Hostname: gtm\_west.f5demo.com IP Address: 10.0.1.245 Date: Jun 19, 2018 Time: 2:58 PM (PDT) User: admin Role: Administrator Partition: Common Log out

**f5** ONLINE (ACTIVE) Standalone

Main Help About

DNS » Delivery : Profiles : DNS » Properties : dns\_nobind\_edns0

Statistics IApps DNS Delivery GSLB Zones Caches Settings Local Traffic Acceleration Device Management Shared Objects Network System

**General Properties**

Name	dns_nobind_edns0
Partition / Path	Common
Parent Profile	dns

**Denial of Service Protection** Custom ☒

Rapid Response Mode	Disabled	<input checked="" type="checkbox"/>
Rapid Response Last Action	Drop	<input checked="" type="checkbox"/>

**Hardware Acceleration**

Protocol Validation	Disabled	<input checked="" type="checkbox"/>
Response Cache	Disabled	<input checked="" type="checkbox"/>

**DNS Features**

DNSSEC	Enabled	<input checked="" type="checkbox"/>
GSLB	Enabled	<input checked="" type="checkbox"/>
DNS Express	Enabled	<input checked="" type="checkbox"/>
DNS Cache	Disabled	<input checked="" type="checkbox"/>
DNS Cache Name	Select...	<input checked="" type="checkbox"/>
DNS IPv6 to IPv4	Disabled	<input checked="" type="checkbox"/>
Unhandled Query Actions	Allow	<input checked="" type="checkbox"/>
Use BIND Server on BIG-IP	Disabled	<input checked="" type="checkbox"/>
Insert Source Address into Client Subnet Option	Enabled	<input checked="" type="checkbox"/>

**DNS Traffic**

Zone Transfer	Disabled	<input checked="" type="checkbox"/>
DNS Security	Disabled	<input checked="" type="checkbox"/>
DNS Security Profile Name	Select...	<input checked="" type="checkbox"/>
Process Recursion Desired	Enabled	<input checked="" type="checkbox"/>

**Logging and Reporting**

Logging	Enabled	<input checked="" type="checkbox"/>
Logging Profile	dnslog_profile	<input checked="" type="checkbox"/>
AVR Statistics Sample Rate	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Update Delete...

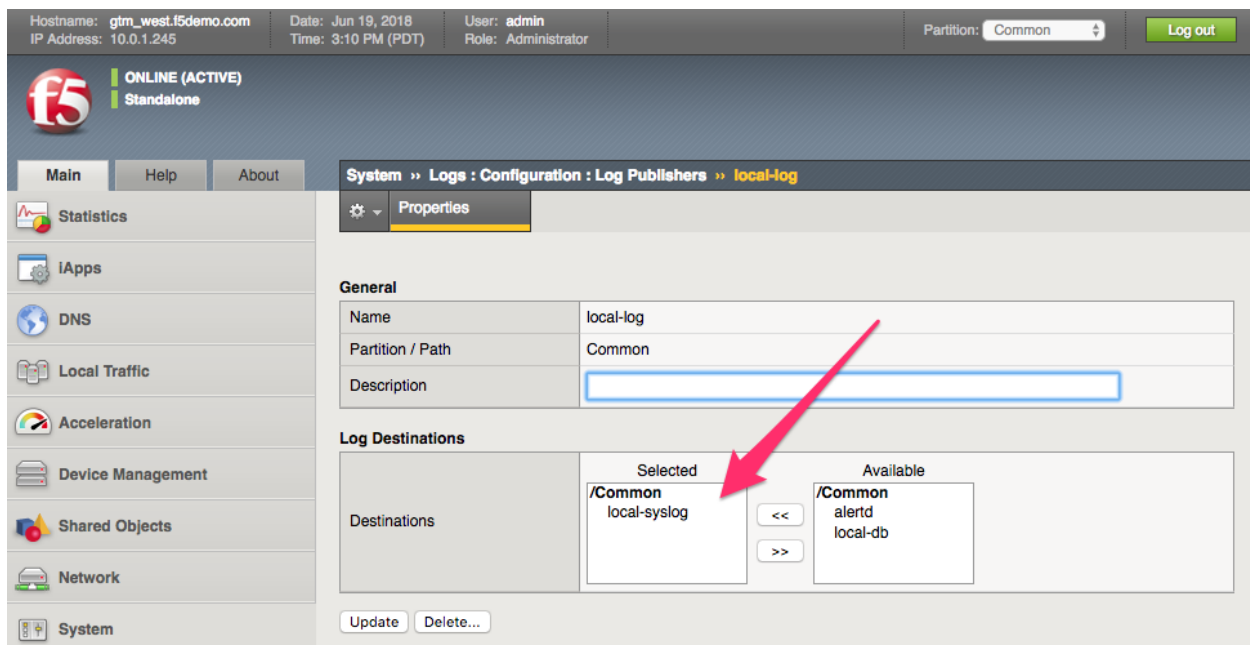
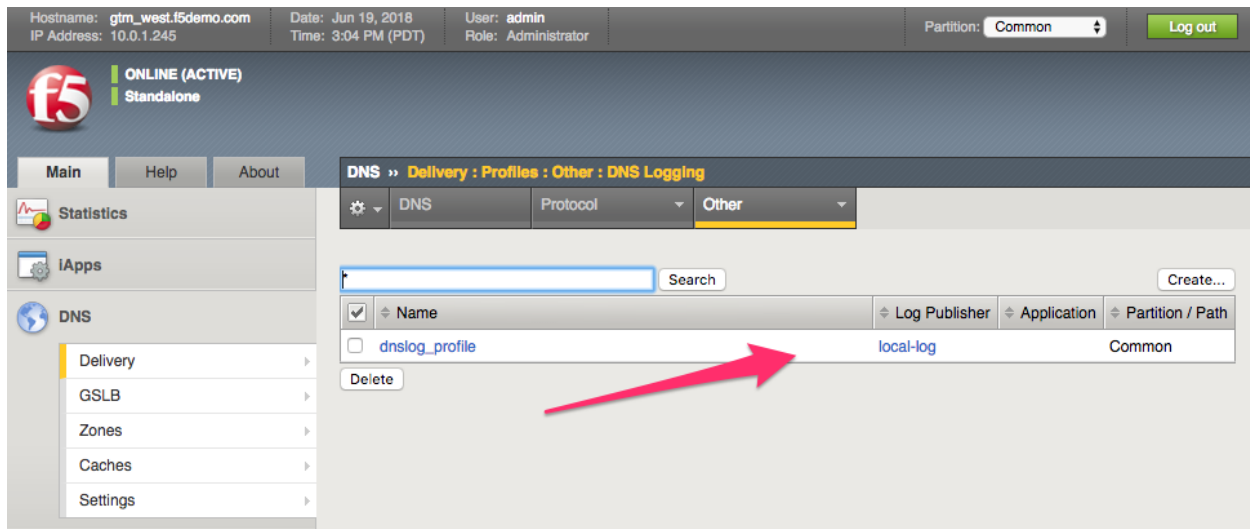
### Task – Review the DNS Logging profile

Follow these steps to complete this task:

1. Navigate to “DNS : Delivery : Profiles : Other : DNS Logging “
2. Click the dnslog\_profile profile and examine the options set.



- Examine the log publisher by navigating to “System: Logs: Configuration: Log Publishers” and click on “local-log”

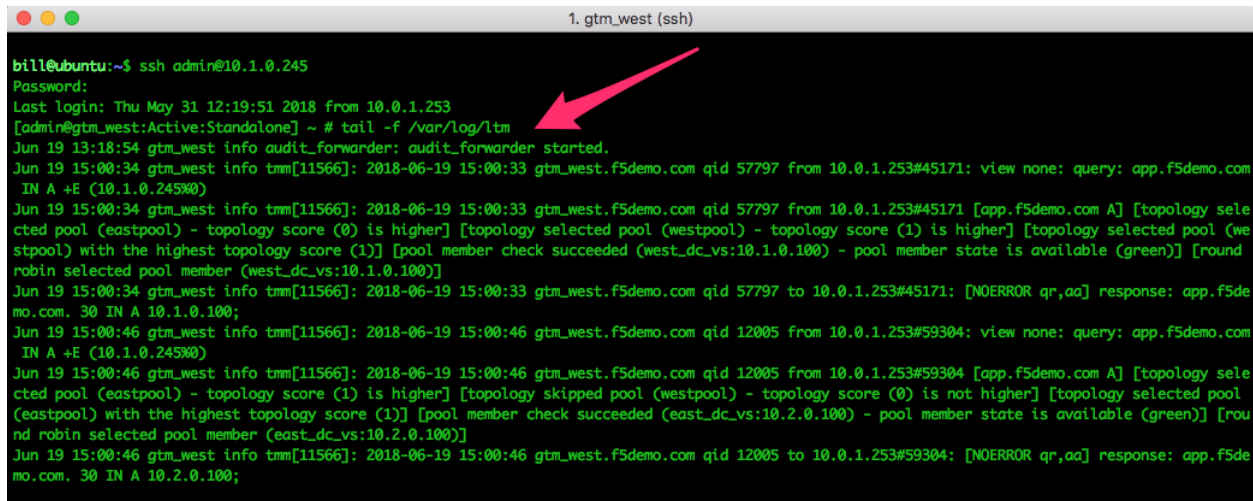


### Task - Open a terminal session to view the log output

Follow these steps to complete this task:

- Open the terminal application on the jump host
- Log into the GTM east and west in different windows via ssh using the admin login and use the following command to tail the log file.

```
tail -f /var/log/ltn
```



```

1. gtm_west (ssh)

bill@ubuntu:~$ ssh admin@10.1.0.245
Password:
Last login: Thu May 31 12:19:51 2018 from 10.0.1.253
[admin@gtm_west:Active:Standalone] ~ # tail -f /var/log/ltn
Jun 19 13:18:54 gtm_west info audit_forwarder: audit_forwarder started.
Jun 19 15:00:34 gtm_west info tmm[11566]: 2018-06-19 15:00:33 gtm_west.f5demo.com qid 57797 from 10.0.1.253#45171: view none: query: app.f5demo.com
IN A +E (10.1.0.245%)
Jun 19 15:00:34 gtm_west info tmm[11566]: 2018-06-19 15:00:33 gtm_west.f5demo.com qid 57797 from 10.0.1.253#45171 [app.f5demo.com A] [topology selected pool (eastpool) - topology score (0) is higher] [topology selected pool (westpool) - topology score (1) is higher] [topology selected pool (westpool) with the highest topology score (1)] [pool member check succeeded (west_dc_vs:10.1.0.100) - pool member state is available (green)] [round robin selected pool member (west_dc_vs:10.1.0.100)]
Jun 19 15:00:34 gtm_west info tmm[11566]: 2018-06-19 15:00:33 gtm_west.f5demo.com qid 57797 to 10.0.1.253#45171: [NOERROR qr,aa] response: app.f5demo.com. 30 IN A 10.1.0.100;
Jun 19 15:00:46 gtm_west info tmm[11566]: 2018-06-19 15:00:46 gtm_west.f5demo.com qid 12005 from 10.0.1.253#59304: view none: query: app.f5demo.com
IN A +E (10.1.0.245%)
Jun 19 15:00:46 gtm_west info tmm[11566]: 2018-06-19 15:00:46 gtm_west.f5demo.com qid 12005 from 10.0.1.253#59304 [app.f5demo.com A] [topology selected pool (eastpool) - topology score (0) is higher] [topology skipped pool (westpool) - topology score (0) is not higher] [topology selected pool (eastpool) with the highest topology score (1)] [pool member check succeeded (east_dc_vs:10.2.0.100) - pool member state is available (green)] [round robin selected pool member (east_dc_vs:10.2.0.100)]
Jun 19 15:00:46 gtm_west info tmm[11566]: 2018-06-19 15:00:46 gtm_west.f5demo.com qid 12005 to 10.0.1.253#59304: [NOERROR qr,aa] response: app.f5demo.com. 30 IN A 10.2.0.100;

```

## 5.2.2 Lab – Examine GSLB objects

In the previous lab we reviewed the basic config and then set up a couple of terminal sessions to watch the dns logs. In this lab we will move forward and examine the GSLB objects that are set up, inspect listeners pool members and other GSLB objects

### Task – Examine the DNS listeners and their profiles

In this task we will examine the listeners set up and make sure the dns profiles are set up correctly.

Follow these steps to complete this task:

1. On both east and west F5s take a look at the listeners and remember the IPs as you will need them..
2. Navigate to **DNS >> Delivery: Listeners: Listener List** and select the listener your interested in viewing.
3. Make sure that the right dns profile is selected for the listeners. Also are there two listeners?

Hostname: gtm\_west.f5demo.com Date: Jun 19, 2018 User: admin  
IP Address: 10.0.1.245 Time: 3:23 PM (PDT) Role: Administrator Partition: Common Log out

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

**DNS » Delivery : Listeners : Listener List » Properties : udp\_listener**

Statistics IApps DNS Delivery GSLB Zones Caches Settings Local Traffic Acceleration Device Management Shared Objects Network System

**General**

Name	udp_listener
Partition	Common
Description	
State	Enabled

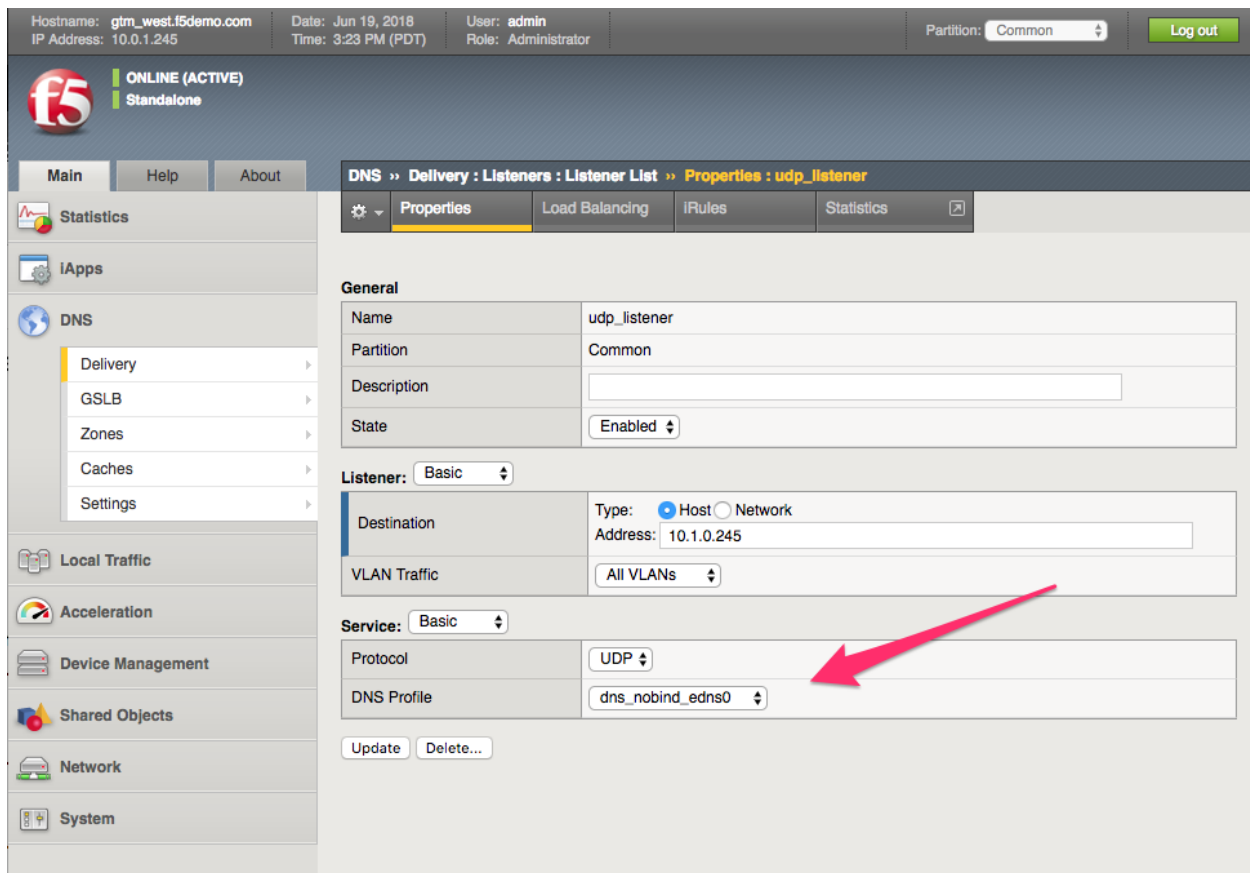
**Listener:** Basic

Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.1.0.245
VLAN Traffic	All VLANs

**Service:** Basic

Protocol	UDP
DNS Profile	dns_nobind_edns0

Update Delete...



### Task – Review the DNS GSLB server objects

In this task we will review the servers used in the GSLB configuration.

Follow these steps to complete this task:

1. Navigate your browser to **DNS >> GSLB : Servers**
2. Inspect the servers. Identify the servers and the underlying objects associated with them.
3. What is the state of the servers , green?

Hostname: gtm\_west.f5demo.com Date: Jun 19, 2018 User: admin  
IP Address: 10.0.1.245 Time: 3:24 PM (PDT) Role: Administrator Partition: Common Log out

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings

**DNS » GSLB : Servers : Server List**

Server List Trusted Server Certificates Statistics

Search Create...

<input checked="" type="checkbox"/>	Status	Name	Devices	Address	Data Center	Virtual Servers	Product	Partition / Path
<input type="checkbox"/>		gtm_east	1	10.2.0.245	east_dc	1	BIG-IP System	Common
<input type="checkbox"/>		gtm_west	1	10.1.0.245	west_dc	1	BIG-IP System	Common

Enable Disable Delete...

### Task – Review the DNS GSLB Data Center objects

In this task we will review the data centers used in the GSLB configuration.

Follow these steps to complete this task:

1. Navigate your browser to **DNS >> GSLB : Data Centers**
2. Inspect the data centers.
3. What is the what happens when you disable a DC? Discuss.

Hostname: gtm\_west.f5demo.com Date: Jun 19, 2018 User: admin  
IP Address: 10.0.1.245 Time: 3:25 PM (PDT) Role: Administrator Partition: Common Log out

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches

**DNS » GSLB : Data Centers : Data Center List**

Data Center List Statistics

Search Create...

<input checked="" type="checkbox"/>	Availability	Name	Location	Links	Servers	Partition / Path
<input type="checkbox"/>		east_dc		0	1	Common
<input type="checkbox"/>		west_dc		0	1	Common

Enable Disable Delete...

### Task – Review the DNS Pools and examine the LB algorithm

In this task we will review the pools used in the GSLB configuration.

Follow these steps to complete this task:

1. Navigate your browser to **DNS >> GSLB : Pools**
2. Inspect the Pools and understand their algorithm.
3. What is the what happens If you changed this ? would it make a difference? Discuss.

Hostname: gtm\_west.f5demo.com Date: Jun 19, 2018 User: admin  
IP Address: 10.0.1.245 Time: 3:28 PM (PDT) Role: Administrator Partition: Common Log out

**f5** ONLINE (ACTIVE)  
Standalone

Main Help About

DNS >> GSLB : Wide IPs : Wide IP List >> Members : app.f5demo.com : A

Statistics  
iApps  
DNS  
Delivery  
GSLB  
Zones  
Caches  
Settings  
Local Traffic  
Acceleration

Properties iRules Pools Statistics

**Pools**

Load Balancing Method: Topology  
Persistence: Disabled  
Last Resort Pool: None  
Update

**Pools** Manage...

<input checked="" type="checkbox"/>	Order	Status	Pool Name	Type	Ratio	Members
<input type="checkbox"/>	0	<span style="color: green;">●</span>	eastpool	A	1	1
<input type="checkbox"/>	1	<span style="color: green;">●</span>	westpool	A	1	1

Delete...

### Task – Review the GSLB WideIP and its configuration

In this task we will review the WideIP used in the GSLB configuration.

Follow these steps to complete this task:

1. Navigate your browser to **DNS >> GSLB : WideIP**
2. Inspect the WideIP and understand the configuration settings, LB algorithm, logging settings.
3. Do you notice anything new here? Use the built in help for the explanation.

The screenshot shows the F5 DNS configuration interface. The top status bar displays: Hostname: gtm\_west.f5demo.com, Date: Jun 19, 2018, Time: 3:28 PM (PDT), User: admin, Role: Administrator, Partition: Common, and a Log out button. The left sidebar contains navigation links: Main, Help, About, Statistics, IApps, DNS (selected), Local Traffic, Acceleration, Device Management, Shared Objects, Network, and System. The DNS section is expanded, showing Delivery, GSLB (selected), Zones, Caches, and Settings. The main content area shows the 'Properties' tab for the service 'app.f5demo.com : A'. The 'General Properties' section is expanded, showing a table of properties:

General Properties: Advanced	
Name	app.f5demo.com
Partition / Path	Common
Type	A
Description	
Alias List	<div>Alias: <input type="text"/></div> <div>Add</div> <div></div> <div>Delete</div>
Availability	Available (Enabled) - Available
State	Enabled
Minimal Response	Disabled
Return Code On Failure	Disabled
Prefer Client Subnet	<input checked="" type="checkbox"/>
Load-Balancing Decision Log	<div><input checked="" type="checkbox"/> Pool Selection</div> <div><input checked="" type="checkbox"/> Pool Traversal</div> <div><input checked="" type="checkbox"/> Pool Member Selection</div> <div><input checked="" type="checkbox"/> Pool Member Traversal</div>

At the bottom of the configuration area are 'Update' and 'Delete...' buttons. A red arrow points to the 'Prefer Client Subnet' checkbox, which is checked.

### Task – Review the Global GSLB settings for Client Subnet

In this task we will review the Global client subnet settings used in the GSLB configuration.

Follow these steps to complete this task:

1. Navigate your browser to **DNS >> Settings : GSLB: Load Balancing**
2. Under Topology, take a look at the “Prefer Client Subnet” option. . .
3. Open the help tab and take a look at the included documentation.

Hostname: gtm\_west.f5demo.com


IP Address: 10.0.1.245

Date: Jun 19, 2018

Time: 3:31 PM (PDT)

User: admin

Role: Administrator



ONLINE (ACTIVE)

Standalone

Main

Help

About

DNS » Settings : GSLB : Load Balancing

⚙️

Delivery

GSLB

Zones

Launch

Print

Expand

Load Balancing Defaults

+ Static Persist CIDR (IPv4)

+ Static Persist CIDR (IPv6)

+ Respect Fallback Dependency

+ Ignore Path TTL

+ Verify Virtual Server Availability

Topology

Note: These settings apply only if you are using the Topology load balancing mode.

+ Longest Match

- Prefer Client Subnet

Specifies, when checked (enabled), that the system uses the edns0 client subnet option (if one exists) instead of the source address, when using topology load balancing. When disabled, or if the query does not contain a client subnet option, the system falls back to the source address. The default is disabled.

When this option is disabled, the **Prefer Client Subnet** option on the Wide IP create or properties page overrides the global setting.

Load Balancing Defaults

Static Persist CIDR (IPv4)	32
Static Persist CIDR (IPv6)	128
Respect Fallback Dependency	<input type="checkbox"/>
Ignore Path TTL	<input type="checkbox"/>
Verify Virtual Server Availability	<input checked="" type="checkbox"/>

Topology

Longest Match	<input checked="" type="checkbox"/>
Prefer Client Subnet	<input checked="" type="checkbox"/>

Update

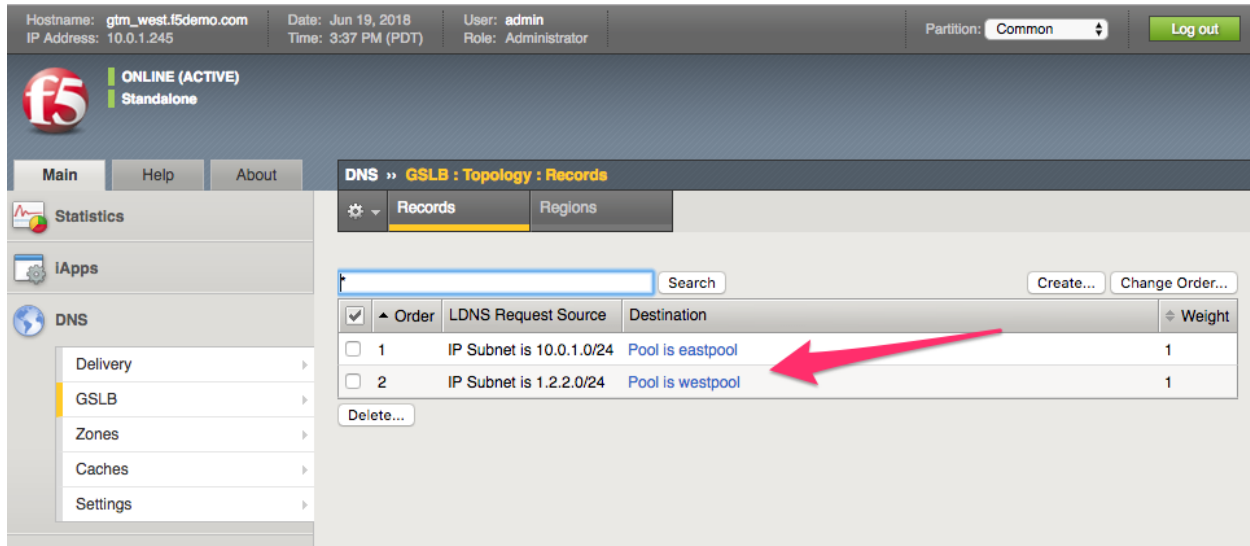
### Task – Review the GSLB Topology records

In this task we will review the GSLB topology records used in the configuration.

Follow these steps to complete this task:

1. Navigate your browser to **DNS >> GSLB : Topology: Records**
2. Review the records and understand their use.

when you check out the topology records you will see that we have created a topology record that matches the local subnet coming from the querier and then another record was added to simulate a different client subnet sent by the dig query with edns0.



### 5.2.3 Lab – Use DIG command to query with client subnet GSLB objects

In this lab, we will utilize the dig command on a linux machine to query the F5 dns engines and observe the responses sent. We will change the options on the dig command to use the new client subnet option.

We will be using a new version of the dig command. My hope is you should be familiar with the general use of the dig command from your previous work with DNS.

The new version of Dig is version 9.10 and it includes an option called the “edns-client-subnet” which allows us to insert the client subnet in the query.

As the client itself cannot insert the client subnet in the query we use the dig command to simulate a query coming from a LDNS which has already inserted the client subnet.

Due to the restrictions on lab resources we have tried to keep this lab of such a size not to be too large or cumbersome, for this reason we will use the dig command instead of a LDNS.

### Task – Log into the linux server and check out the new dig command

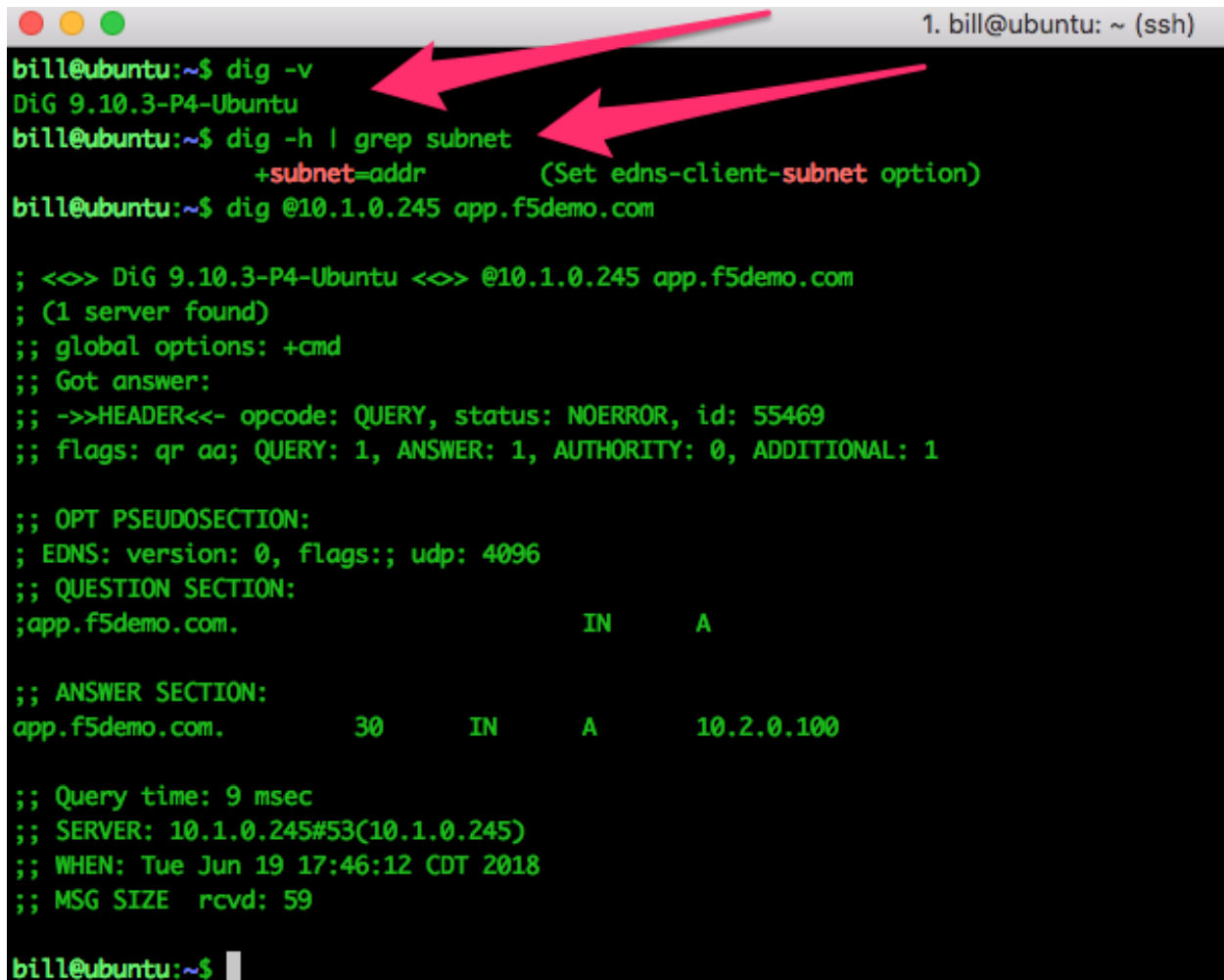
In this task you will open a terminal session and ssh to the linux server to use the local new version of dig.

Follow these steps to complete this task:

1. Log into the linux server at 10.0.1.253 using the user named ubuntu and the password ubuntu
2. Once logged into the linux server check out the linux dig command by typing `dig -v`



3. Take a look at the following output `dig -h | grep subnet`
4. Now do a simple query for the wideip that is configured on one of the east or west DC listener IPs `dig @listener_IP app.f5demo.com`



```

1. bill@ubuntu: ~ (ssh)
bill@ubuntu:~$ dig -v
DiG 9.10.3-P4-Ubuntu
bill@ubuntu:~$ dig -h | grep subnet
      +subnet=addr      (Set edns-client-subnet option)
bill@ubuntu:~$ dig @10.1.0.245 app.f5demo.com

; <=> DiG 9.10.3-P4-Ubuntu <=> @10.1.0.245 app.f5demo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 55469
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;app.f5demo.com.                IN      A

;; ANSWER SECTION:
app.f5demo.com.                 30      IN      A      10.2.0.100

;; Query time: 9 msec
;; SERVER: 10.1.0.245#53(10.1.0.245)
;; WHEN: Tue Jun 19 17:46:12 CDT 2018
;; MSG SIZE rcvd: 59

bill@ubuntu:~$

```

### Task – View the query logs and observe the dig query

Now that we have the new dig command we are almost ready to do some queries but it would be nice to see the query and decision logs that we are looking for just to make sure things are going correctly and we see any output that might be different than we might expect.

1. Open two new terminal windows if you do not have them open from previous sessions, logging into both the East and West DC BigIPs.
2. Once you have logged in as admin you can then `tail -f /var/log/ltn` in both windows to view the logs for the listeners.

```
1. gtm_west (ssh)

;; SERVER: 10.1.0.245#53(10.1.0.245)
;; WHEN: Tue Jun 19 17:46:12 CDT 2018
;; MSG SIZE rcvd: 59

bill@ubuntu:~$ ssh admin@10.1.0.245
Password:
Last login: Tue Jun 19 15:15:22 2018 from 10.0.1.253
[admin@gtm_west:Active:Standalone] ~ # tail -20 /var/log/ltm
Jun 19 13:18:54 gtm_west info audit_forwarder: audit_forwarder started.
Jun 19 15:00:34 gtm_west info tmm[11566]: 2018-06-19 15:00:33 gtm_west.f5demo.com qid 57797 from 10.0.1.253#45171: view none: query: app.f5demo.com IN A +E (10.1.0.245#0)
Jun 19 15:00:34 gtm_west info tmm[11566]: 2018-06-19 15:00:33 gtm_west.f5demo.com qid 57797 from 10.0.1.253#45171 [app.f5demo.com A] [topology selected pool (eastpool) - topology score (0) is higher] [topology selected pool (westpool) - topology score (1) is higher] [topology selected pool (westpool) with the highest topology score (1)] [pool member check succeeded (west_dc_vs:10.1.0.100) - pool member state is available (green)] [round robin selected pool member (west_dc_vs:10.1.0.100)]
Jun 19 15:00:34 gtm_west info tmm[11566]: 2018-06-19 15:00:33 gtm_west.f5demo.com qid 57797 to 10.0.1.253#45171: [NOERROR qr,aa] response: app.f5demo.com. 30 IN A 10.1.0.100;
Jun 19 15:00:46 gtm_west info tmm[11566]: 2018-06-19 15:00:46 gtm_west.f5demo.com qid 12005 from 10.0.1.253#59304: view none: query: app.f5demo.com IN A +E (10.1.0.245#0)
Jun 19 15:00:46 gtm_west info tmm[11566]: 2018-06-19 15:00:46 gtm_west.f5demo.com qid 12005 from 10.0.1.253#59304 [app.f5demo.com A] [topology selected pool (eastpool) - topology score (1) is higher] [topology skipped pool (westpool) - topology score (0) is not higher] [topology selected pool (eastpool) with the highest topology score (1)] [pool member check succeeded (east_dc_vs:10.2.0.100) - pool member state is available (green)] [round robin selected pool member (east_dc_vs:10.2.0.100)]
Jun 19 15:00:46 gtm_west info tmm[11566]: 2018-06-19 15:00:46 gtm_west.f5demo.com qid 12005 to 10.0.1.253#59304: [NOERROR qr,aa] response: app.f5demo.com. 30 IN A 10.2.0.100;
Jun 19 15:32:05 gtm_west notice mcpd[4509]: 0107168c:5: Incremental sync complete: This system is updating the configuration on device group /Common/gtm device %big3d-for-igsys ncer-:ffff:10.0.1.246:47478 from commit id { 1 6568446412398328879 /Common/bigip02.f5demo.com } to commit id { 110 6568927096578804119 /Common/bigip01.f5demo.com }.
Jun 19 15:46:12 gtm_west info tmm[11566]: 2018-06-19 15:46:11 gtm_west.f5demo.com qid 55469 from 10.0.1.253#56518: view none: query: app.f5demo.com IN A +E (10.1.0.245#0)
Jun 19 15:46:12 gtm_west info tmm[11566]: 2018-06-19 15:46:11 gtm_west.f5demo.com qid 55469 from 10.0.1.253#56518 [app.f5demo.com A] [topology selected pool (eastpool) - topology score (1) is higher] [topology skipped pool (westpool) - topology score (0) is not higher] [topology selected pool (eastpool) with the highest topology score (1)] [pool member check succeeded (east_dc_vs:10.2.0.100) - pool member state is available (green)] [round robin selected pool member (east_dc_vs:10.2.0.100)]
Jun 19 15:46:12 gtm_west info tmm[11566]: 2018-06-19 15:46:11 gtm_west.f5demo.com qid 55469 to 10.0.1.253#56518: [NOERROR qr,aa] response: app.f5demo.com. 30 IN A 10.2.0.100;
```

### Task – Use the +subnet option in dig to change the client subnet

Lets test to see if the client subnet affects the response given by the topology records in our GSLB configuration. To do this we will be using our friend dig.

1. Use the dig command to hit your favorite listener and query the wideip app.f5demo.com
2. dig @10.1.0.245 app.f5demo.com
3. Change the client subnet using dig @10.1.0.245 app.f5demo.com +subnet=9.9.9.0/24
4. Examine the response and the logs to see what decision was made ... why?
5. Change your query request to include a matching client subnet for a topology record that matches the configuration. dig @10.1.0.245 app.f5demo.com=1.2.2.0/24 .

```

1. bill@ubuntu: ~ (ssh)
bill@ubuntu:~$ dig @10.1.0.245 app.f5demo.com +subnet=1.2.2.0/24

; <=> DiG 9.10.3-P4-Ubuntu <=> @10.1.0.245 app.f5demo.com +subnet=1.2.2.0/24
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11666
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; CLIENT-SUBNET: 1.2.2.0/24/24
;; QUESTION SECTION:
;app.f5demo.com.                IN      A

;; ANSWER SECTION:
app.f5demo.com.                30      IN      A      10.1.0.100

;; Query time: 3 msec
;; SERVER: 10.1.0.245#53(10.1.0.245)
;; WHEN: Tue Jun 19 17:52:42 CDT 2018
;; MSG SIZE rcvd: 70

bill@ubuntu:~$

```

### 5.2.4 Lab – Use TCPdump and Wireshark to analyze DNS ends0 client subnet transactions

In this lab, we will utilize the tcpdump utility to capture DNS queries to the F5 BIGIP DNS listeners.

Next we will use wireshark on the jumphost to examine the queries and responses edns0 information to see the ECS (client subnet) information.

Last, we will change our query to the BIND server and use tcpdump/wireshark to examine the LDNS behavior of BIND.

As in the previous lab, we will be using a new version of the dig command. You should be familiar with the general use of the dig command from your previous labs and work with DNS.

#### Task – Use tcpdump to capture dns queries from the linux jumphost

Follow these steps to complete this task:

1. Log into the BIGIP DNS via ssh `admin@10.0.1.245` and use the command `tcpdump -nnni 0.0.0.0 port 53 -w /tmp/edns0.pcap`
2. Use the jumphost to query the listener with a edns0 query: `dig @10.1.0.245 app.f5demo.com +subnet=9.9.9.0/24`
3. Once the query and response are complete stop the capture with a ctrl-c.

- Copy the file from the BIGIP to the jumphost using the scp command `scp admin@10.1.0.245:/tmp/edns0.pcap .`
- Start wireshark by typing the following into a terminal `wireshark &`
- Once wireshark is open, choose file->open and open the edns0.pcap file in wireshark.
- Open up the DNS query and examine the ends0 section. It is under the “Additional Records” arrow. What is the client subnet set to?

edns0.pcap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.1.50	10.0.1.253	DNS	96	Standard query 0x505e A app.f5demo.com OPT
2	0.004906	10.0.1.253	10.1.0.245	DNS	85	Standard query 0x0e1a A app.f5demo.com OPT
3	0.006608	10.0.1.253	8.8.4.4	DNS	70	Standard query 0xe312 NS <Root> OPT
4	0.008378	10.1.0.245	10.0.1.253	DNS	101	Standard query response 0x0e1a A app.f5demo
5	0.011993	10.0.1.253	10.0.1.50	DNS	312	Standard query response 0x505e A app.f5demo
6	0.014684	8.8.4.4	10.0.1.253	DNS	567	Standard query response 0xe312 NS <Root> NS
7	41.522261	10.0.1.50	10.0.1.253	DNS	96	Standard query 0x7581 A app.f5demo.com OPT
8	41.526264	10.0.1.253	10.1.0.245	DNS	85	Standard query 0xe6ab A app.f5demo.com OPT
9	41.527981	10.0.1.253	8.8.4.4	DNS	70	Standard query 0x2ab4 NS <Root> OPT
10	41.528879	10.1.0.245	10.0.1.253	DNS	101	Standard query response 0xe6ab A app.f5demo
11	41.530973	10.0.1.253	10.0.1.50	DNS	312	Standard query response 0x7581 A app.f5demo
12	41.536152	8.8.4.4	10.0.1.253	DNS	567	Standard query response 0x2ab4 NS <Root> NS

Answer RRs: 0  
 Authority RRs: 0  
 Additional RRs: 1  
 Queries  
 Additional records  
 - <Root>: type OPT  
   Name: <Root>  
   Type: OPT (41)  
   UDP payload size: 4096  
   Higher bits in extended RCODE: 0x00  
   EDNS0 version: 0  
   Z: 0x0000  
   Data length: 11  
   Option: CSUBNET - Client subnet

0000 2c c2 60 7c 12 63 2c c2 60 2b 59 a5 08 00 45 00 . . | . c . . + Y . . E .  
 0010 00 52 5e 38 00 00 40 11 05 35 0a 00 01 32 0a 00 . R ^ 8 . . @ . . 5 . . 2 . .  
 0020 01 fd 87 79 00 35 00 3e 4f 48 75 81 01 20 00 01 . . . y . 5 . > 0 H u . . .  
 0030 00 00 00 00 00 01 03 61 70 70 06 66 35 64 65 6d . . . . . a p p . f 5 d e m  
 0040 6f 03 63 6f 6d 00 00 01 00 01 00 00 29 10 00 00 o . c o m . . . . . ) . . .  
 0050 00 00 00 00 0b 00 08 00 07 00 01 18 00 01 02 02 . . . . . . . . . . .

Task - Use wireshark to view a client dns request from the linux jumphost


This task is pretty simple but looking at the client request should in theory look just like the request captured at the DNS listener.

- Start wireshark and start a new capture on the ethernet interface of the jumphost.
- Filter for DNS packets (port 53)
- Use a terminal window to send a `dig @10.1.0.245 app.f5demo.com=9.9.9.0/24`
- send a new dig command to 8.8.8.8 and look at the response... `dig @8.8.8.8 www.microsoft.com +subnet=8.7.6.0/24`
- Inspect the dns request and the response packets, and look to see if you can see any difference between the last tasks output.
- Notice the difference in the dig output between the query to the BIGIP DNS listener and 8.8.8.8.

```
FLD-ML-BWESTER1:agility_edns0_docs_18 bwester$ dig @8.8.8.8 www.microsoft.com +subnet=8.7.6.0/24

; <=> DiG 9.10.3-P4 <=> @8.8.8.8 www.microsoft.com +subnet=8.7.6.0/24
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20923
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 512
; CLIENT-SUBNET: 8.7.6.0/24/0
;; QUESTION SECTION:
;www.microsoft.com.      IN      A
```





## Class 5 - DNS over HTTPS/DNS over TLS

### 6.1 Introduction

In this lab, you will see DNS over HTTPS (DoH) and DNS over TLS (DoT) queries proxied in both directions. That is, traditional DNS queries will be proxied to backend DoT/DoH servers, as well as DoH/DoT queries being proxied to traditional DNS servers.

DoT is “simpler” to proxy as the original DNS protocol is simply encapsulated in TLS using client-SSL (DoT-to-DNS) or server-ssl (DNS-to-DoT) profiles.

DoH is a bit more complex as we must take the DNS request and encapsulate it into a binary HTTPS payload (DNS-to-DoH) or extract the binary payload and convert it into a traditional DNS query (DoH-to-DNS).

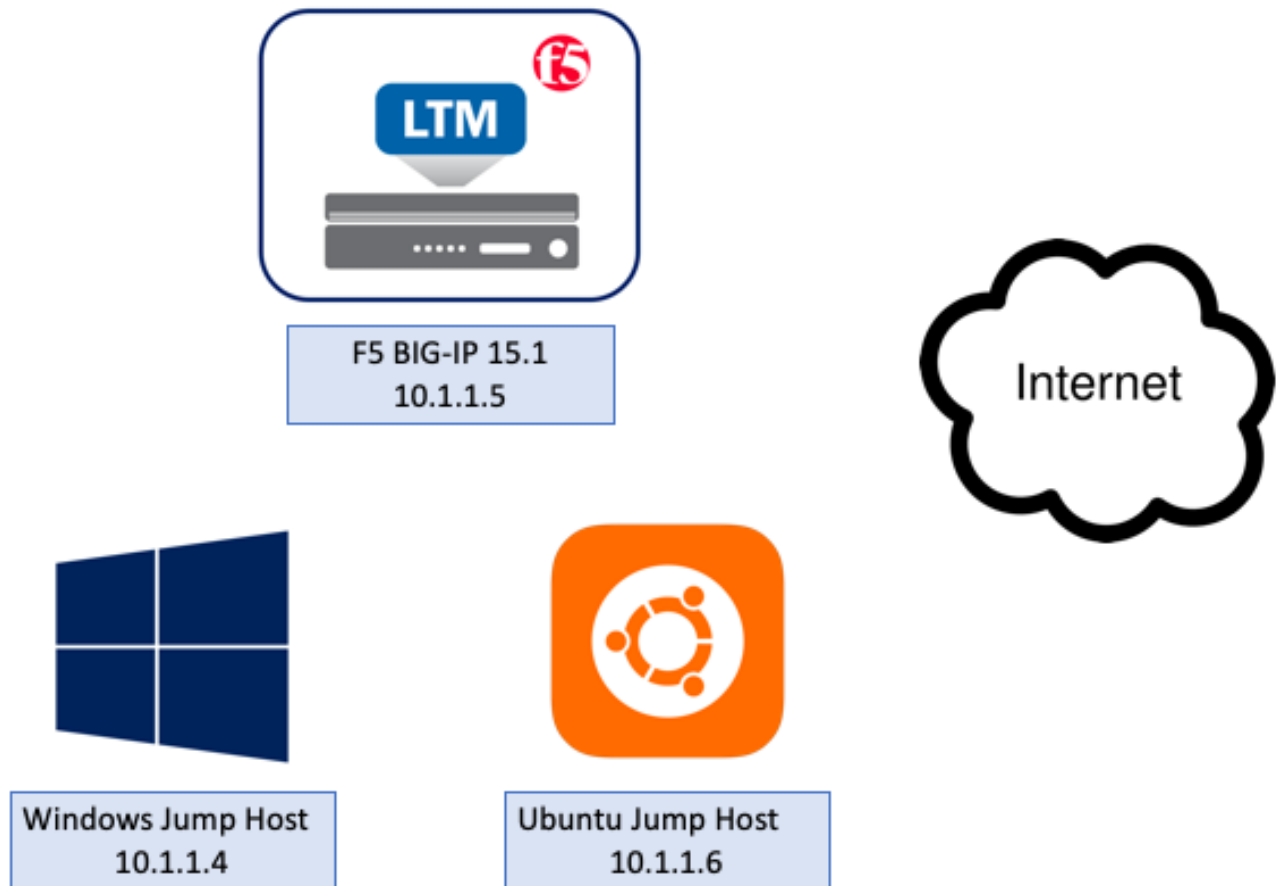
We will use the power of iRulesLX to handle this advanced task. Native functionality will be available in a near-future release of TMOS so that the iRules will not be necessary.

The lab consists of four sections:

- Proxying DNS over HTTPS queries to traditional DNS servers
  - In this section, you will use Mozilla Firefox as a DoH client to browse the web using encrypted DNS through the BIG-IP using DNS over HTTPS
- Proxying DNS over TLS queries to traditional DNS servers
  - In this section, you will use the `kdig` utility as a DoT client to perform queries through the BIG-IP using DNS over TLS
- Proxying traditional DNS queries to DNS over HTTPS servers
  - In this section, you will use the `nslookup`/`dig` utilities to send traditional DNS queries through the BIG-IP to Google’s DoH service
- Proxying traditional DNS queries to DNS over TLS servers
  - In this section, you will use the `nslookup`/`dig` utilities to send traditional DNS queries through the BIG-IP to Google’s DoT service

### 6.1.1 Topology

This lab consists of a single BIG-IP that is proxying the various DNS packet types. A single Windows jump host sits in the client segment while an Ubuntu jump server sits in the server segment.



### 6.1.2 Components

The lab consists of the following items:

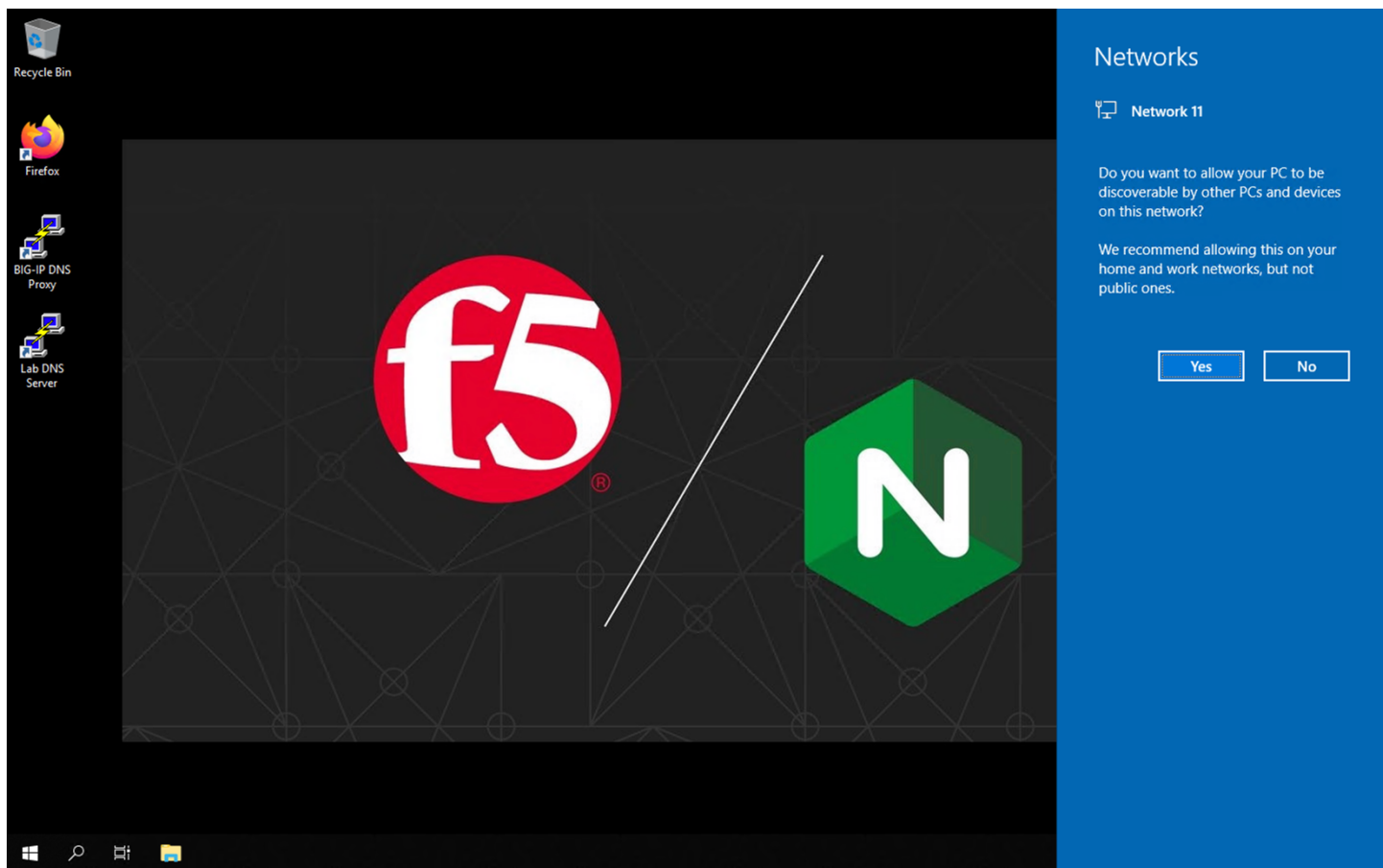
- Subnets
  - Management: 10.1.1.0/24
  - DNS VIPs: 10.1.10.0/24
  - DNS Servers: 10.1.20.0/24
- Hosts
  - Windows Jump Host
    - \* Credentials: user / f5agility2020
    - \* Management IP: 10.1.1.4



- Ubuntu Jump Host
  - \* Credentials: user / f5agility2020
  - \* Management IP: 10.1.1.6
- F5 BIG-IP Proxy:
  - \* Credentials: admin / f5agility2020 | root / f5agility2020
  - \* Management IP: 10.1.1.5
  - \* Client Subnet IP: 10.1.10.10
  - \* Server Subnet IP: 10.1.20.10
  - \* DNS VIPs
    - DoT-to-DNS: 10.1.10.100 (TCP/853)
    - DoH-to-DNS: 10.1.10.100 (TCP/443)
    - DNS-to-DoT: 10.1.10.101 (TCP/53 and UDP/53)
    - DNS-to-DoH: 10.1.10.102 (TCP/53)

### 6.1.3 BIG-IP Configuration Review

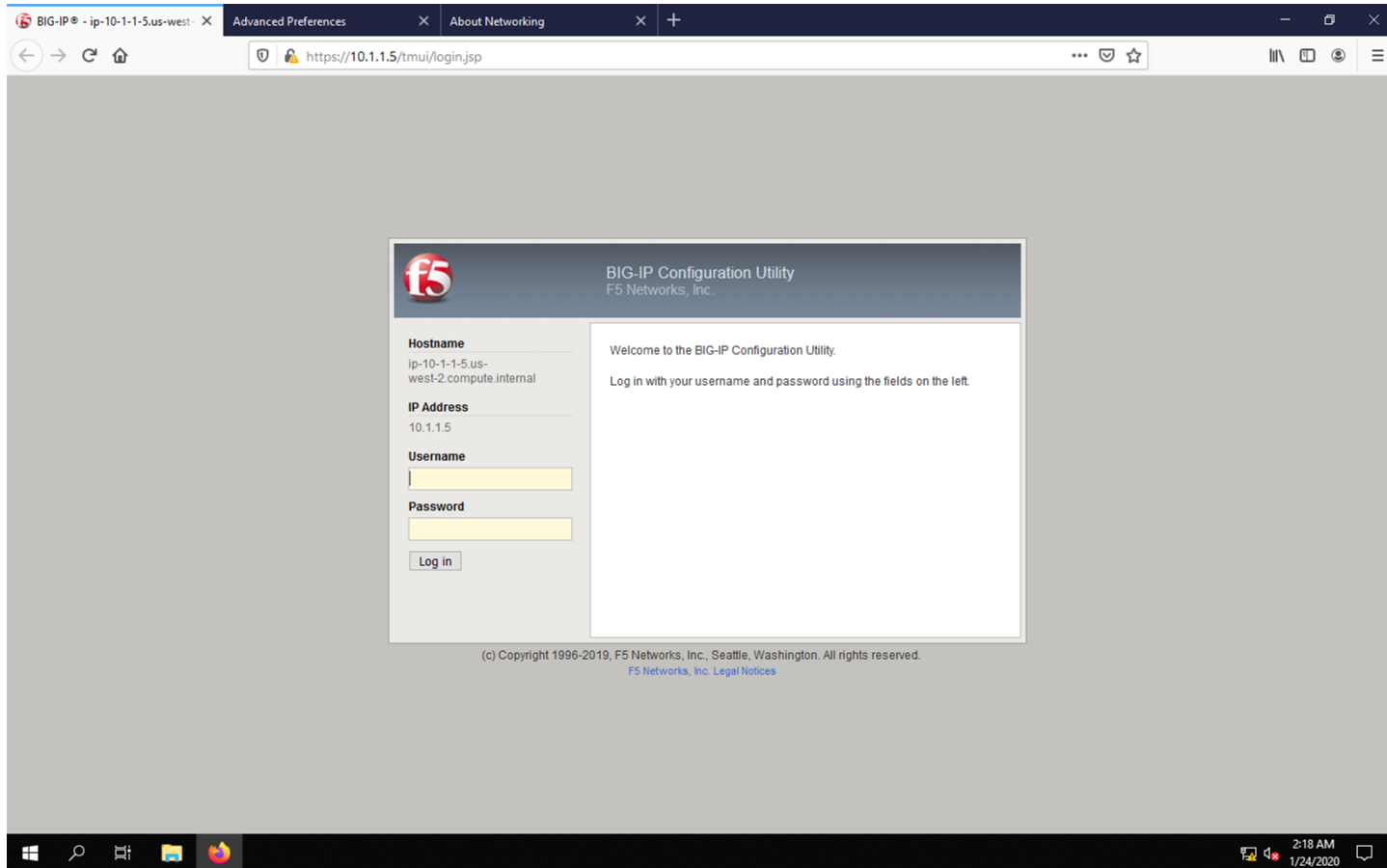
Launch your RDP client and connect to the Windows Jump Host.



Click “No” to close the network discovery prompt.

Click on the Firefox icon to launch the browser.

Three tabs will open up. The first tab is the UI of the BIG-IP. Let's login using **admin** for our username and **f5agility2020** as our password.



You should see the license screen initially. Let's take a look at the configuration before we proceed with testing the proxy.

## System Configuration

### Resource Provisioning

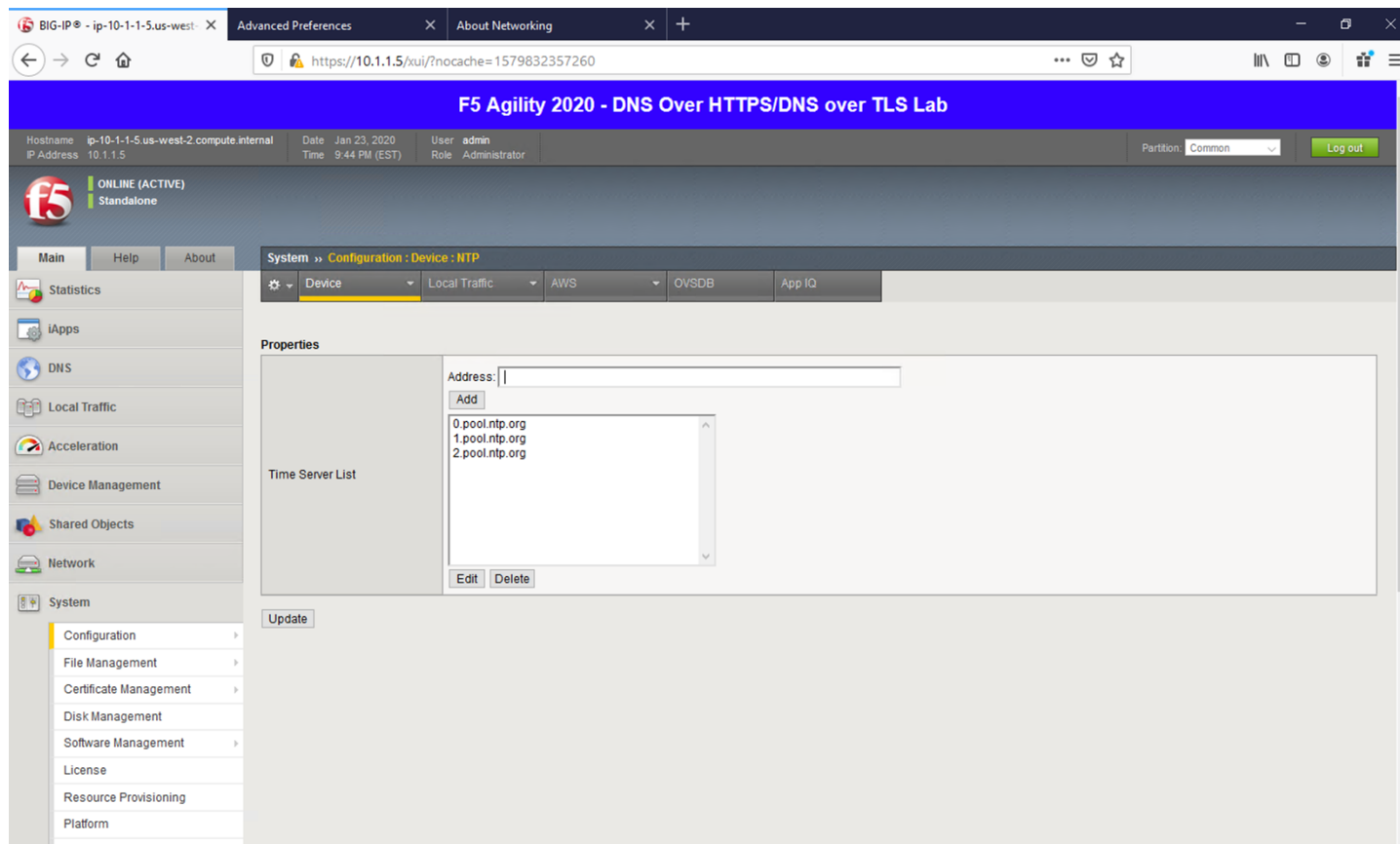
First, let's look at how the platform's modules are provisioned. Navigate to **System -> Resource Provisioning** in the menu. You will see that we have LTM and iRulesLX provisioned. We'll need both of these modules for handling DNS connections and translating between DNS and HTTPS.

System Configuration Table:

Module	Provisioning	License Status	Required Disk (GB)	Required Memory (MB)
Management (MGMT)	Small	N/A	0	1264
Local Traffic (LTM)	<input checked="" type="checkbox"/> Nominal	Licensed	0	1504
Application Security (ASM)	<input type="checkbox"/> None	Unlicensed	20	1492
Fraud Protection Service (FPS)	<input type="checkbox"/> None	N/A	12	544
Global Traffic (DNS)	<input type="checkbox"/> None	Licensed	0	148
Link Controller (LC)	<input type="checkbox"/> None	Unlicensed	0	148
Access Policy (APM)	<input type="checkbox"/> None	Limited	12	494
Application Visibility and Reporting (A/R)	<input type="checkbox"/> None	Licensed	16	576
Policy Enforcement (PEM)	<input type="checkbox"/> None	Unlicensed	16	1223
Advanced Firewall (AFM)	<input type="checkbox"/> None	Unlicensed	16	1058
Application Acceleration Manager (AAM)	<input type="checkbox"/> None	Unlicensed	32	2050
Secure Web Gateway (SWG)	<input type="checkbox"/> None	Unlicensed	24	4096
iRules Language Extensions (iRulesLX)	<input checked="" type="checkbox"/> Nominal	Licensed	0	748
URLDB Minimal (URLDB)	<input type="checkbox"/> None	Unlicensed	36	2048
SSL Orchestrator (SSLO)	<input type="checkbox"/> None	Unlicensed	0	128
Carrier Grade NAT (CGNAT)	<input type="checkbox"/> None	Unlicensed	16	336

## NTP

Next, let's look at a few key system settings necessary for overall system health. Navigate to **System** -> **Configuration** -> **Device** -> **NTP**. It's important that NTP is configured and working properly on all BIG-IPs, especially when deployed in a cluster and/or when managed by BIG-IQ.

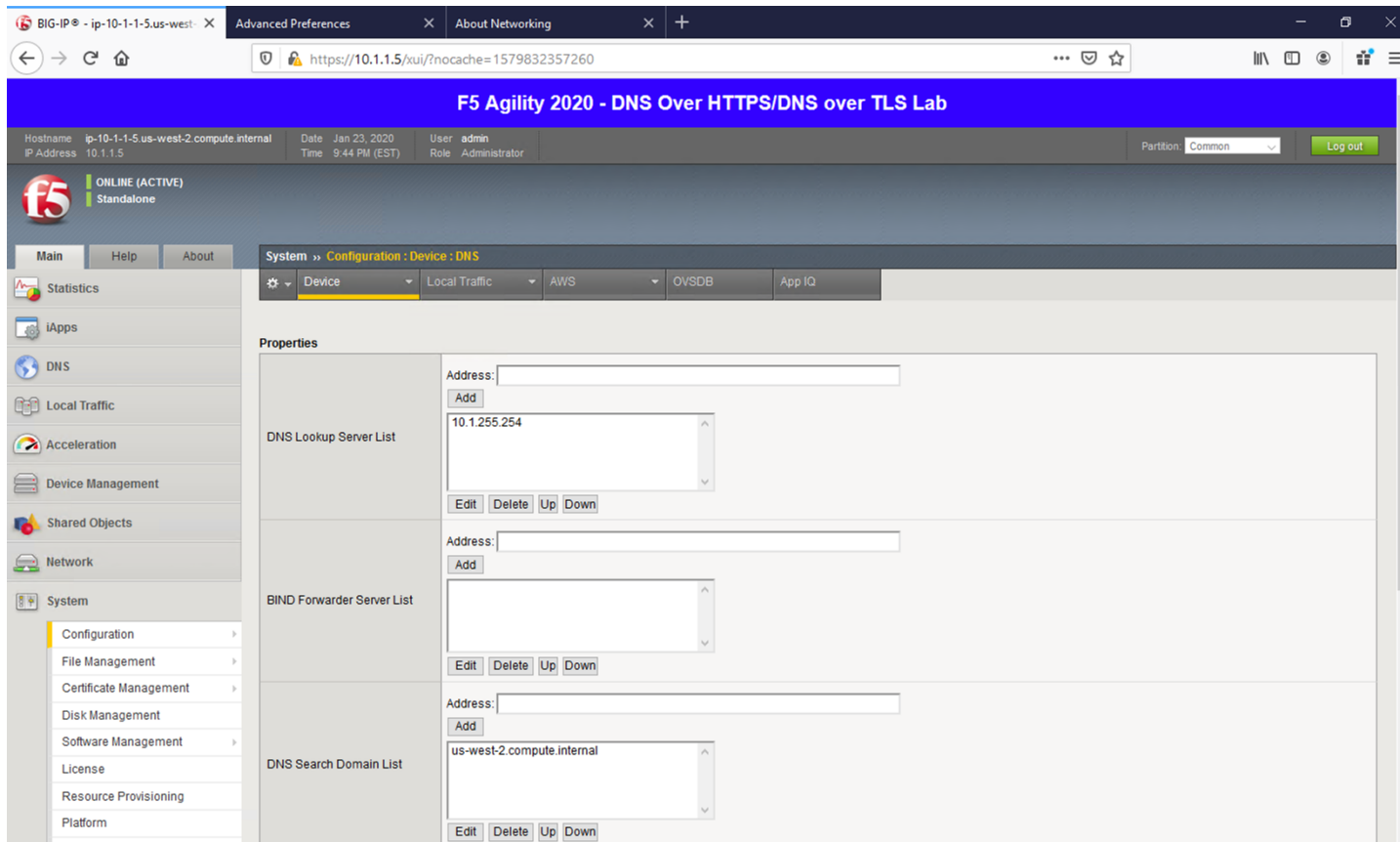


## DNS

Navigate to **System -> Configuration -> Device -> DNS**

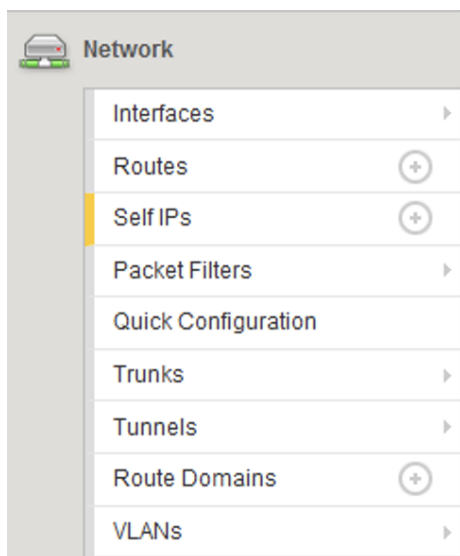
Because we're using FQDNs in our iRules and DNS pools, we'll need a DNS resolver(s) that the BIG-IP can use to resolve them.

**If avoid specifying DNS servers in a your environment, you can simply assign static pool members addresses and specify resolvers by IP address in the iRules to alleviate this requirement. If this doesn't make sense now, it will shortly.**



## Network Configuration

The BIG-IP sits in two VLANs with self-IPs in each. One side serves up the DNS VIPs and the other is used to reach DNS servers. If you wish to view this portion of the config, you can click on the respective sections under the Network menu. Please do not make any changes.



### Local Traffic Manager (LTM)

Let's now look at the portion of the configuration that is performing the heavy lifting – the LTM configuration.

### Nodes

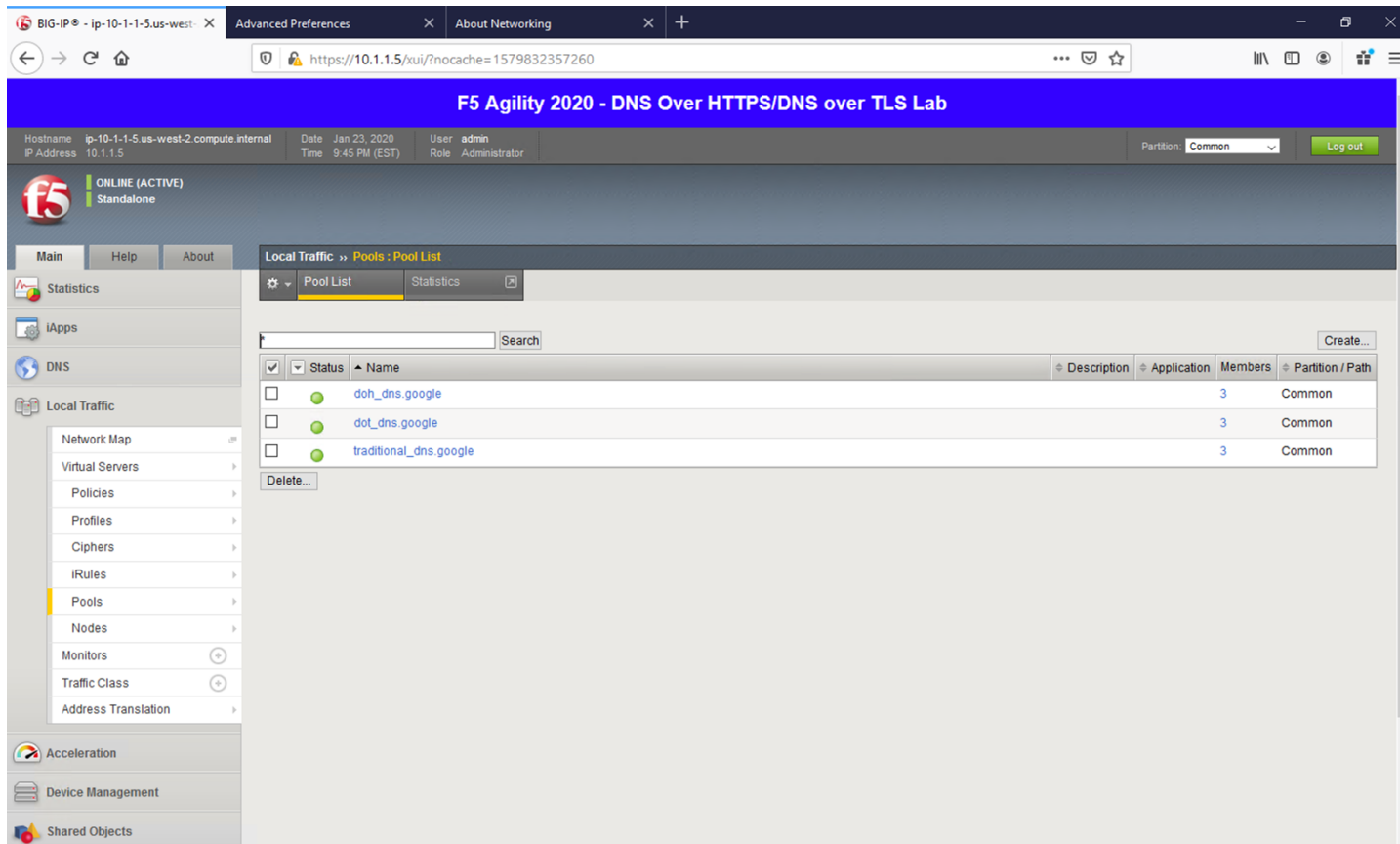
Navigate to **Local Traffic** -> **Nodes** and look at the node list. Here, we're resolving dns.google and automatically creating pool members based on the records returned.

The screenshot shows the F5 Agility 2020 web interface for the 'DNS Over HTTPS/DNS over TLS Lab'. The browser address bar shows the URL <https://10.1.1.5/xui/?nocache=1579832357260>. The interface includes a top navigation bar with 'Main', 'Help', and 'About' tabs. A left sidebar contains a tree view with categories like 'Statistics', 'iApps', 'DNS', 'Local Traffic', 'Acceleration', 'Device Management', and 'Shared Objects'. The 'Local Traffic' category is expanded, showing sub-items like 'Network Map', 'Virtual Servers', 'Policies', 'Profiles', 'Ciphers', 'iRules', 'Pools', 'Nodes', 'Monitors', 'Traffic Class', and 'Address Translation'. The 'Nodes' item is selected, displaying the 'Node List' table. The table has columns for 'Status', 'Name', 'Description', 'Application', 'Address', 'FQDN', 'Ephemeral', and 'Partition / Path'. It lists three nodes: '\_auto\_8.8.4.4', '\_auto\_8.8.8.8', and 'dns.google'. Below the table are buttons for 'Enable', 'Disable', 'Force Offline', and 'Delete...'. A 'Create...' button is located at the top right of the table area.

Status	Name	Description	Application	Address	FQDN	Ephemeral	Partition / Path
<input type="checkbox"/>	_auto_8.8.4.4			8.8.4.4	dns.google	Yes	Common
<input type="checkbox"/>	_auto_8.8.8.8			8.8.8.8	dns.google	Yes	Common
<input type="checkbox"/>	dns.google			::	dns.google	No	Common

### Pools

If you'll kindly navigate to **Local Traffic** -> **Pools**, you will see three pools. While the backend nodes are identical between them, the ports used for each are not. You'll see a pool for DNS over HTTPS (doh\_dns.google) that uses port 443, a pool for DNS over TLS (dot\_dns.google) that utilizes port 853 and finally a pool that uses port 53 for traditional DNS services (traditional\_dns.google). If you're not familiar with LTM pools, click through each pool to see how the service ports are specified.

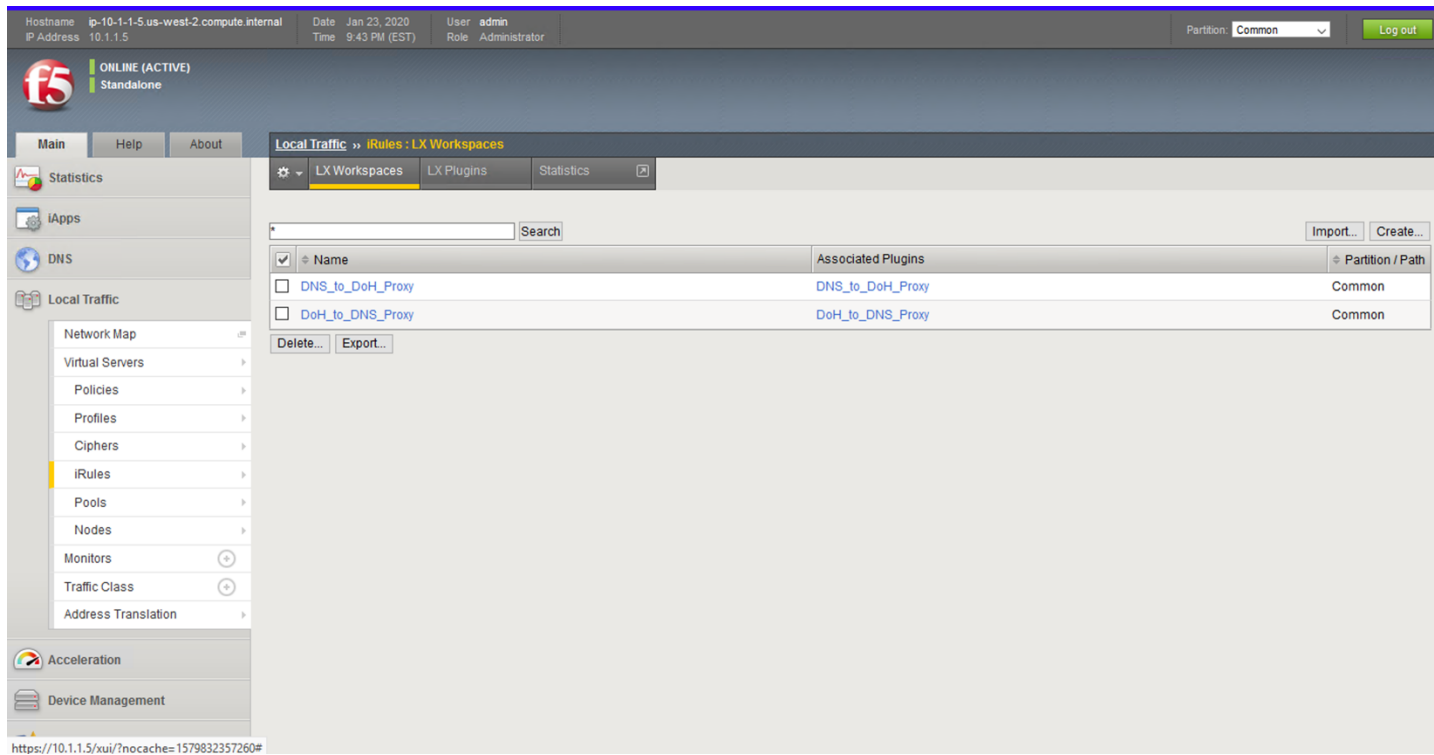


## iRulesLX

iRulesLX engine based on Node.js is the mechanism that we will leverage to handle DNS over HTTPS translations. DoH requests either arrive at the BIG-IP in an HTTPS POST with a binary payload or a base64url- encoded GET request parameter. We'll need to transpose the data from these requests and translate into a traditional DNS request (DoH-to-DNS). We can also take a traditional DNS request and encapsulate it into a DoH request using iRulesLX.

## Workspaces

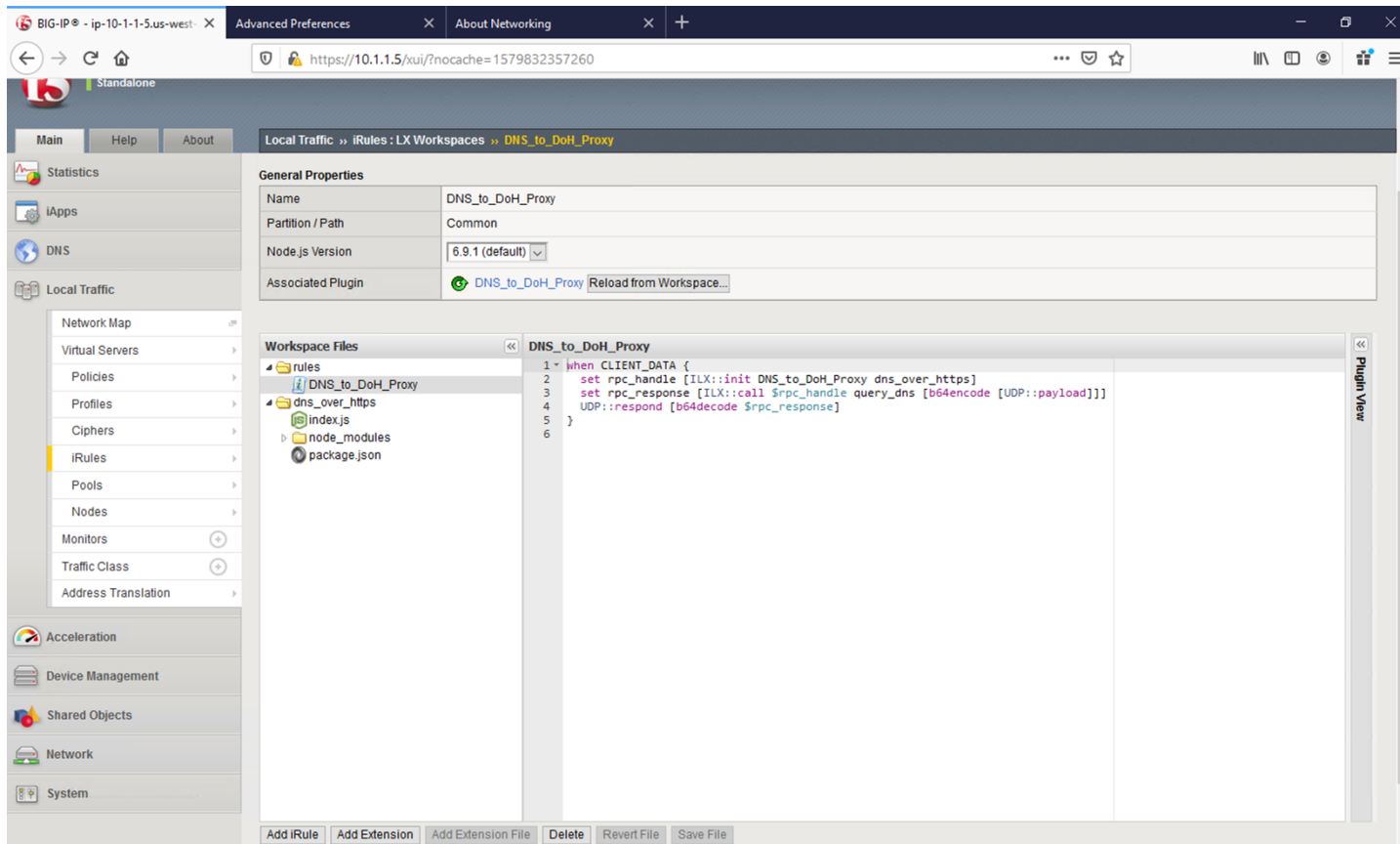
If you'll navigate to **Local Traffic -> iRules -> LX Workspaces**, you can see the two rules for handling conversions in their respective direction. Click on the rule titled *DNS\_to\_DoH\_Proxy*.



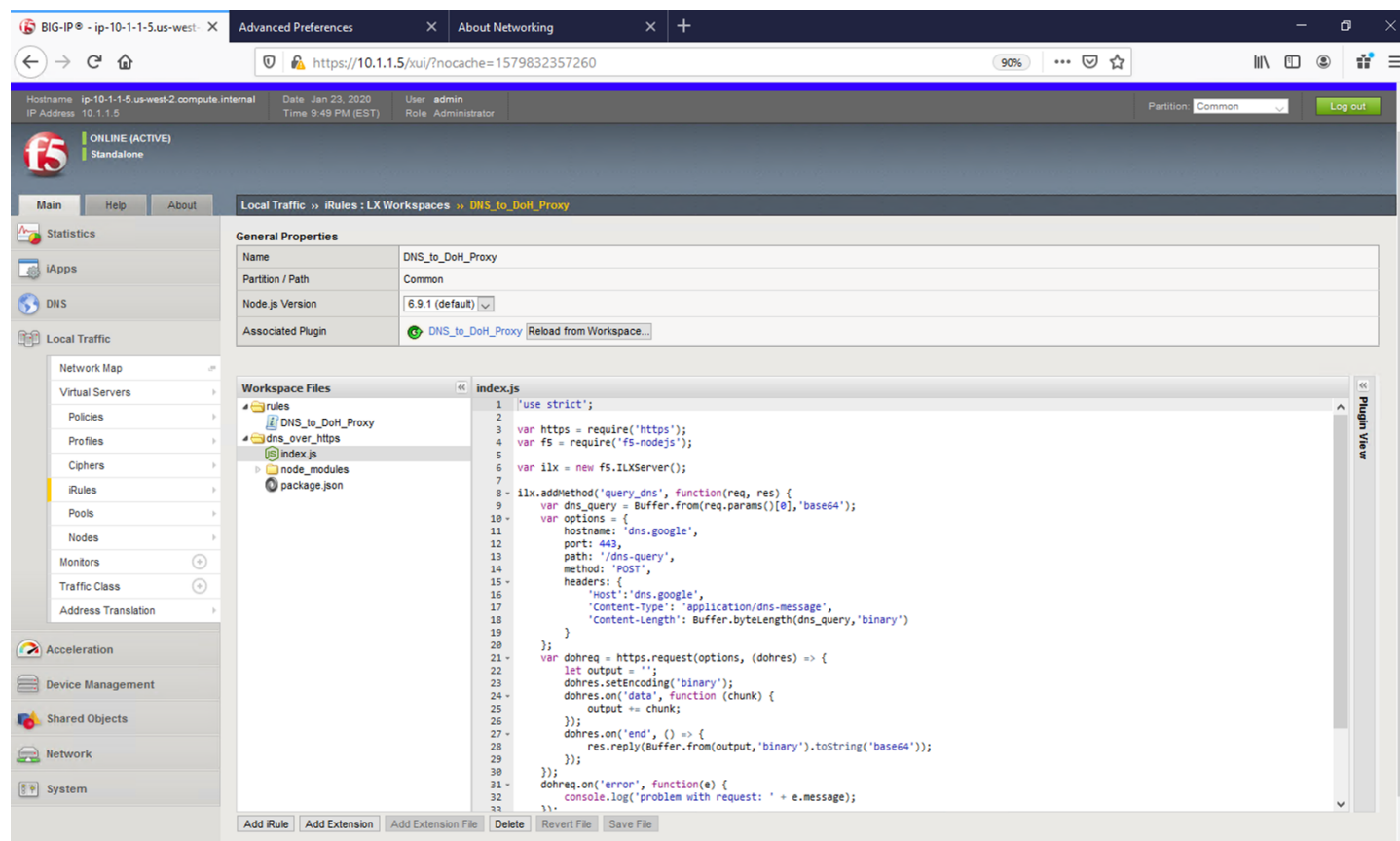
### DNS to DoH Proxy

Click on the *DNS\_to\_DoH\_Proxy* item under the *rules* section of **Workspace Files**. The first rule, *DNS\_to\_DoH\_Proxy*, has two components. The classic iRule, which is written in TCL, is used to nab data from the incoming payload and pass it off to iRulesLX. The `ILX::init` function is called and the entire UDP payload is simply passed to iRulesLX using base64 encoding. Once the request is processed, the response will be returned to this iRule, which will be base64 decoded and passed to the client.





Click on the `index.js` file under the `dns_over_https` section of **Workspace Files**. The iRulesLX portion takes the DNS packet's payload and sends it to a remote DoH server as a binary payload using the HTTP POST method. The response, which will also be binary, gets base64 encoded and passed back to the TCL portion of the iRule, which then sends the request back to the client.



## DoH to DNS Proxy

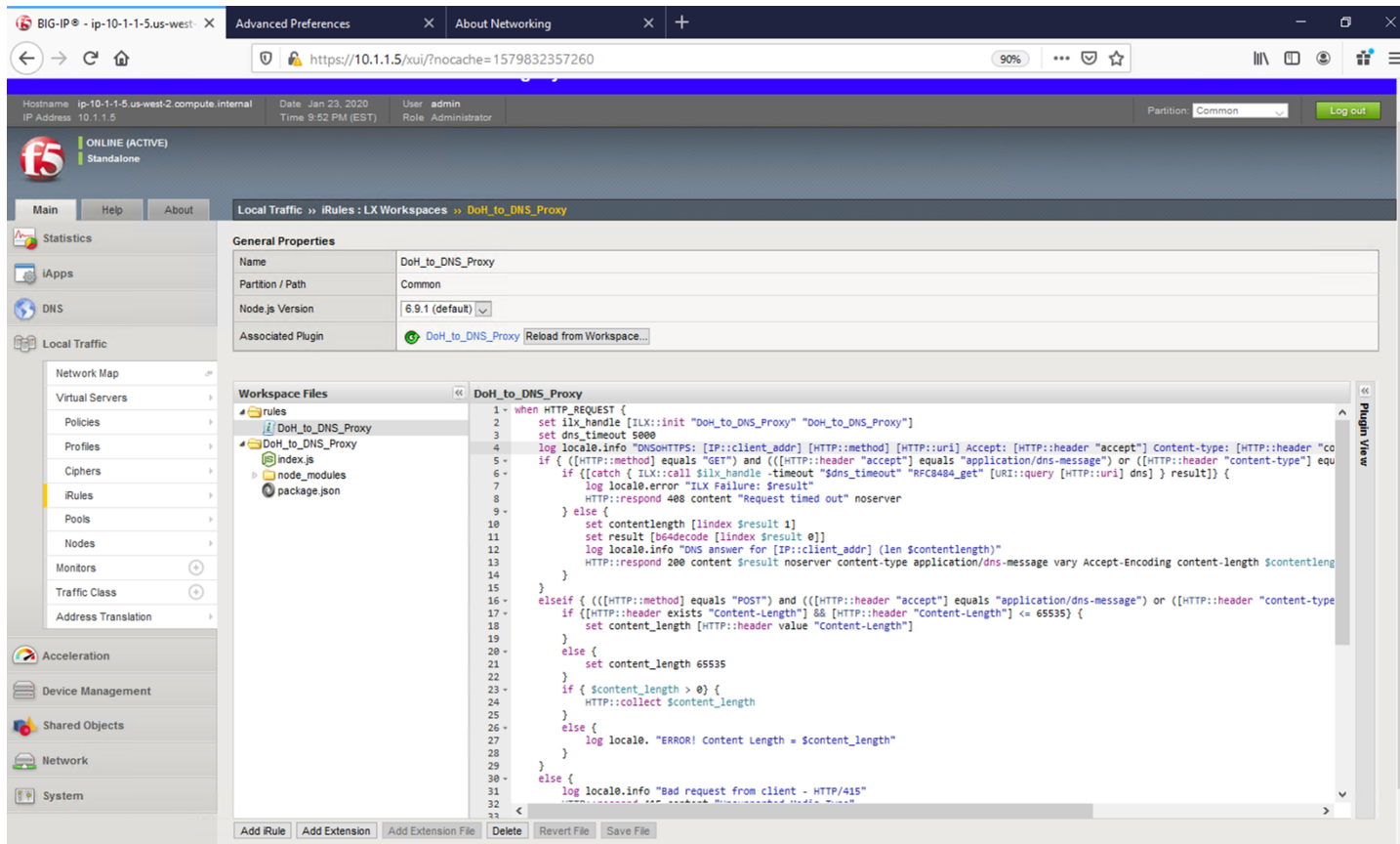
Navigate back to the iRulesLX Workspace list (**Local Traffic -> iRules -> iRulesLX Workspaces**) and view the *DoH\_to\_DNS\_Proxy* iRule. Click on the *DoH\_to\_DNS\_Proxy* item under the *rules* section of **Workspace Files**. This conversion is a more intensive task.

First, POST and GET are both valid DoH request methods, but have different payloads. POST payloads are binary and GET requests are base64url encoded in the URI request, so we need to treat them separately.

Since POST has the request in the actual HTTP payload, we'll have to grab that information, perform base64 encoding and pass it along to iRulesLX to process.

For GET requests, we can simply send the base64url-encoded GET parameter. In both cases, we'll also have to wait for a response from the iRulesLX engine, which is handled in this portion of the iRule as well.

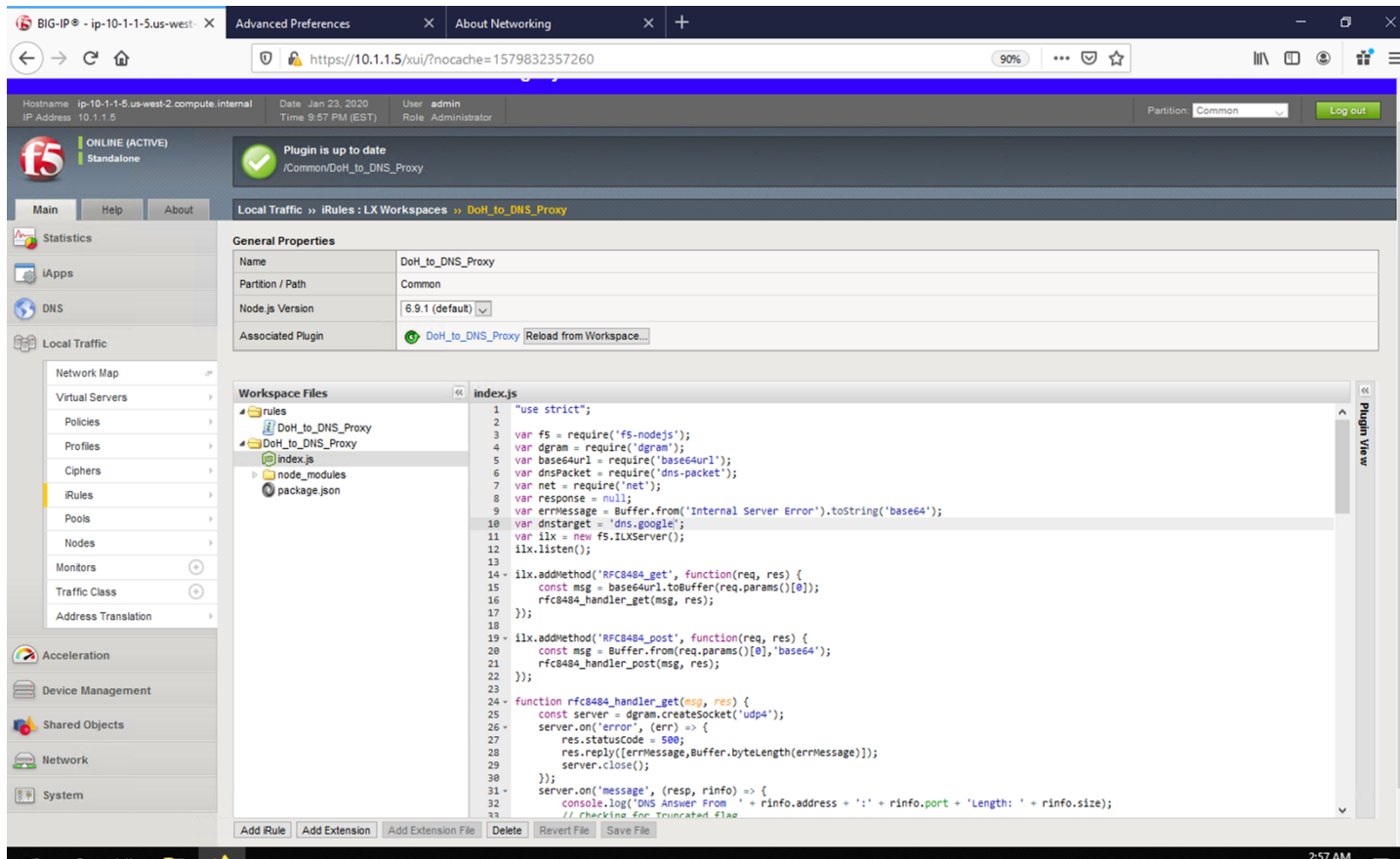
There is a slight distinction between base64 and base64url encoding! For more information, see <https://en.wikipedia.org/wiki/Base64>.



Click on the *index.js* item under *DoH\_to\_DNS\_Proxy* section of **Workspace Files**. For the iRulesLX portion, the script has several steps it must perform.

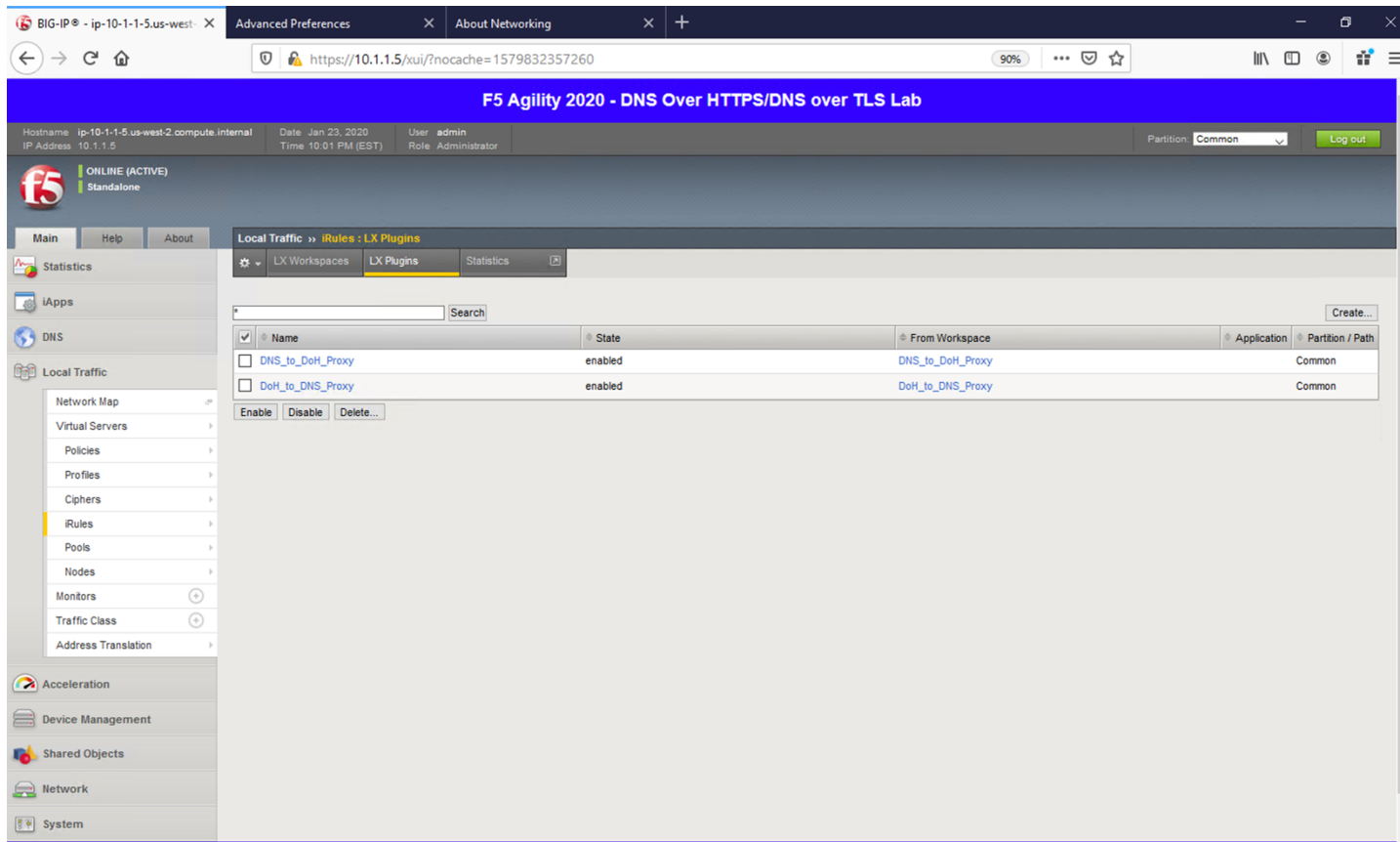
First, we need to get the DoH request into a traditional DNS request packet. Not only that, but we need check for truncated responses from UDP requests and resend them as TCP requests. Once we have a response from the DNS server, we'll need to encode it to pass back to TCL so the final response can be returned to the server.

The process intensive iRule can take advantage of the BIG-IPs native SSL and TCP protocol accelerations, greatly increasing the volume of requests that can be handled.



## Plugins

Navigate to **Local Traffic** -> **iRules** -> **LX Plugins**. This is where a workspace is mapped to a plug-in. This allows you to make changes to the workspace without committing those changes immediately.



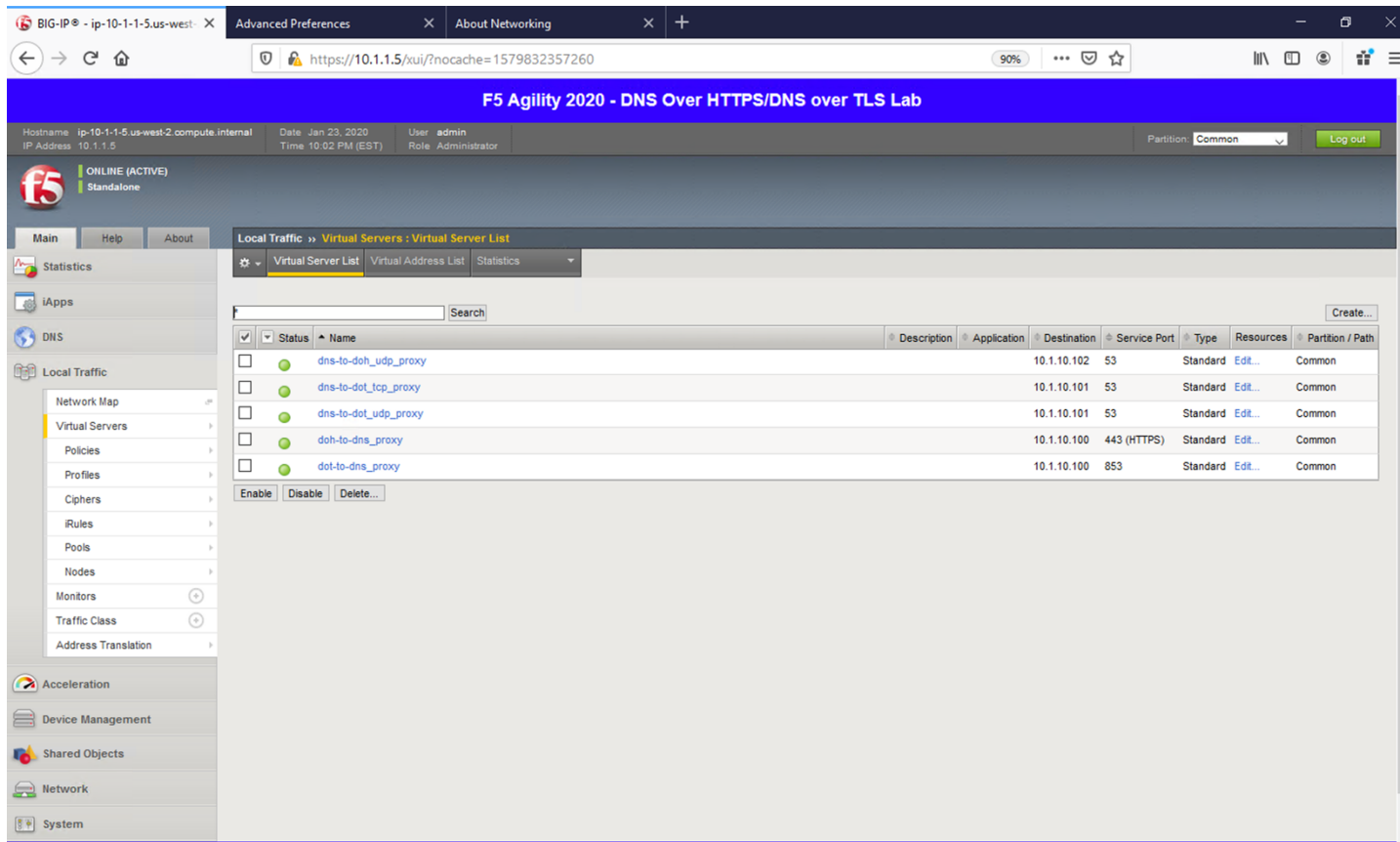
## Virtual Servers

Finally, let's take a look at the virtual servers handling incoming requests. Navigating to **Local Traffic** -> **Virtual Servers** will bring up the list.

Notice that we have 5 scenarios to cover in order to handle DNS translations in either direction.

First, the DNS-to-DoH virtual server handles incoming traditional DNS requests and encapsulates them to a backend DoH server. The next two rules handle DNS-to-DoT for both inbound TCP and UDP requests. An example use case for these proxies would be offering encrypted DNS services to client software/hardware that doesn't support DoH/DoT.

The next two rules handle inbound DoH and DoT requests, respectively. An example use case for these proxies would be for offering DoH/DoT to clients/customers/etc. without the need for modifying existing DNS infrastructure.



### 6.1.4 Proxying DNS over HTTPS Queries to Traditional DNS

#### Certificate Requirements for DoH/DoT Virtual Servers

**NOTICE** DNS over HTTPS requires a valid server-side certificate. In our lab, we created a self-signed CA certificate as well as a self-signed certificate for the server. We loaded those certificates in your Firefox browser so that the browser will trust the BIG-IP DoH resolver.

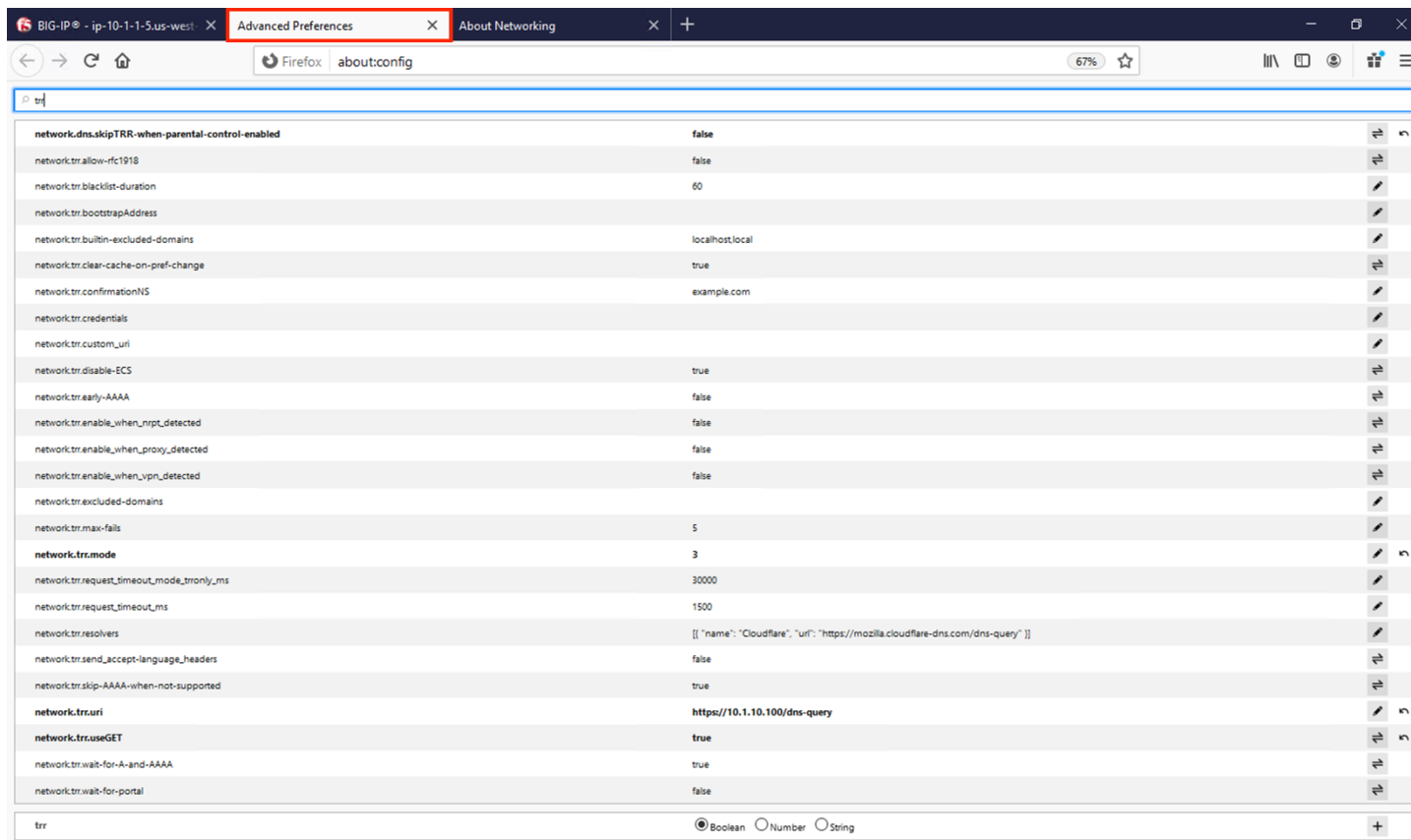
In a real-world scenario, you would need a certificate signed by a well-known certificate authority and loaded into the BIG-IP and attached to the client-ssl profile in use for DoH/DoT listeners. Most DoH clients, including Firefox, will not trust a DoH server if the certificate is not signed by a known certificate authority.

#### Test Driving DNS over HTTPS to Traditional DNS

Now, let's generate some traffic and see the translations in real-time.

#### Firefox Configuration

For this test, we're going to use Firefox as our DoH client. Click the second tab in Firefox to view the [about:config](#) page. On the top of that page, you'll see a search box. Enter *trr* and press enter to see the DoH (trusted recursive resolver) configuration.

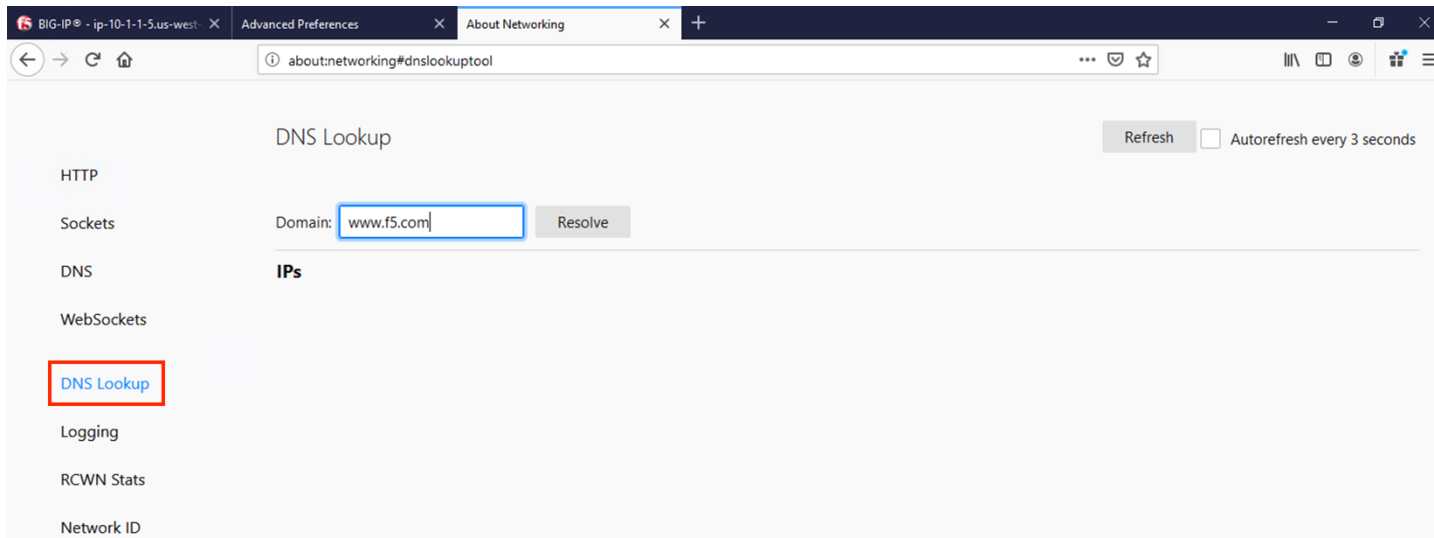


We've pre-configured a few things for you. First, we set *network.trr.uri* to our custom virtual server URL. We also enabled *network.trr.useGET* as it's a bit faster than using POST, but you're welcome to test using POST as well. We set *network.trr.mode* to 3, which means we want Firefox to **only** use DoH. This will not be a typical configuration as Firefox defaults to traditional DNS when a DoH request fails. That explains the differing timeout values just below that setting. The *network.dns.skipTRR-when-parental-control-enabled* disables Firefox's feature that disables DoH when parental control via DNS is sensed on the network.

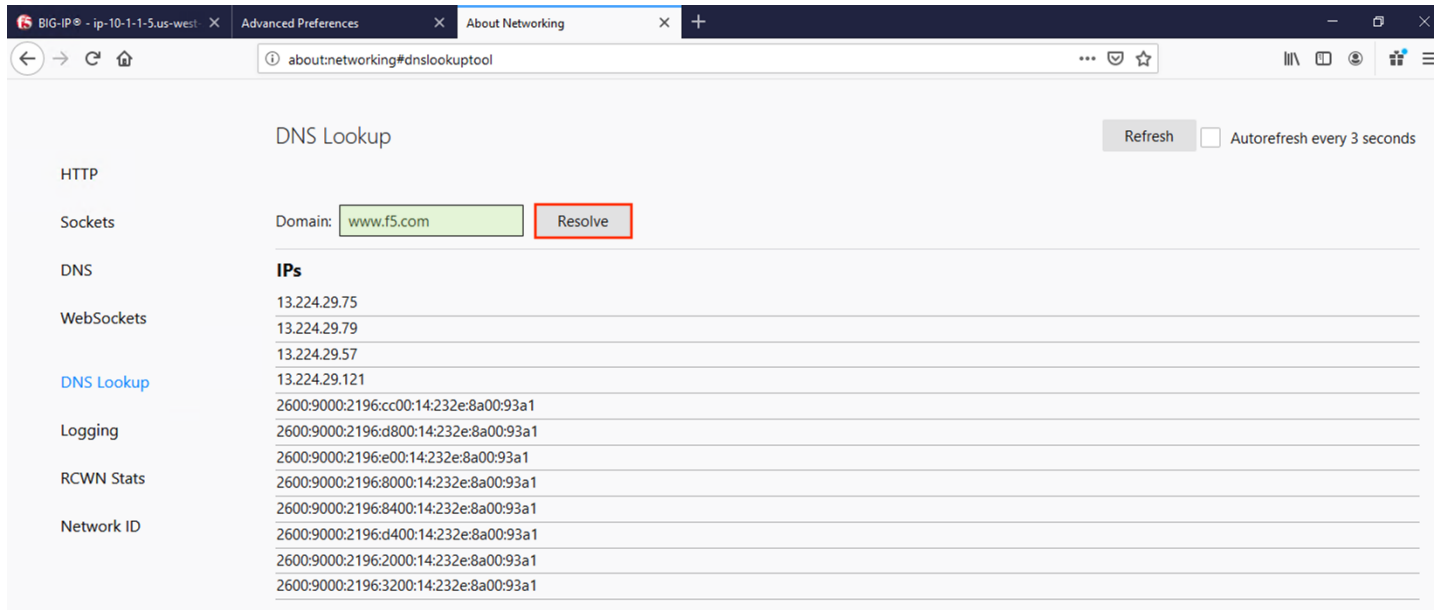
**Please keep in mind that these settings are changing as Firefox continues testing DoH. The ink on the RFC is still wet, technically, and those heavily involved in encrypted DNS are still working out the nuances.**

## Firefox Network Utilities

Clicking on the third tab in Firefox will open the networking tools page within the browser. This is a great way to see if DoH (TRR in Mozilla-speak) is working. Click on *DNS Lookup* to bring up the DNS query tool.



Entering a URL and clicking *Resolve* will show the A/AAAA records returned for that FQDN.



If you then click on *DNS*, you'll be presented with a table of the current in-browser DNS cache. Click on *Refresh* to update the view. You can see in the output below that TRR was *true* for the queries sent, meaning DoH was used to resolve those hostnames.



**DNS** Refresh ☐ Autorefresh every 3 seconds

HTTP

Sockets

**DNS**

WebSockets

DNS Lookup

Logging

RCWN Stats

Network ID

**DNS suffix**

- us-west-2.compute.internal
- us-west-2.ec2-utilities.amazonaws.com
- us-east-1.ec2-utilities.amazonaws.com
- us-west-2.compute.internal

Hostname	Family	TRR	Addresses	Expires (Seconds)
ocsp.digicert.com	ipv4	true	72.21.91.29	2051
ocsp.digicert.com	ipv4	true	72.21.91.29	2928
			13.224.29.75	
			13.224.29.79	
			13.224.29.57	
			13.224.29.121	
			2600:9000:2196:cc00:14:232e:8a00:93a1	
			2600:9000:2196:d800:14:232e:8a00:93a1	
			2600:9000:2196:e00:14:232e:8a00:93a1	
			2600:9000:2196:8000:14:232e:8a00:93a1	
			2600:9000:2196:8400:14:232e:8a00:93a1	
			2600:9000:2196:d400:14:232e:8a00:93a1	
			2600:9000:2196:2000:14:232e:8a00:93a1	
			2600:9000:2196:3200:14:232e:8a00:93a1	
www.f5.com	ipv4	true		17

## DoH in Action

Open a new tab and browse to a website. Return to the third tab and click *Refresh* to see the updated DNS cache table.

**DNS** Refresh ☐ Autorefresh every 3 seconds

HTTP

Sockets

**DNS**

WebSockets

DNS Lookup

Logging

RCWN Stats

Network ID

**DNS suffix**

- us-west-2.compute.internal
- us-west-2.ec2-utilities.amazonaws.com
- us-east-1.ec2-utilities.amazonaws.com
- us-west-2.compute.internal

Hostname	Family	TRR	Addresses	Expires (Seconds)
ocsp.digicert.com	ipv4	true	72.21.91.29	1906
ocsp.digicert.com	ipv4	true	72.21.91.29	2783
www.paypal.com	ipv4	true	184.26.82.215	52
ak1s.abmr.net	ipv4	true	104.81.179.236	54
www.paypalobjects.com	ipv4	true	184.51.50.36	53

## BIG-IP Statistics and Logging

Back in the first tab on the F5 web UI, navigate to **Statistics -> Module Statistics -> Local Traffic**. Make sure that *Virtual Servers* is selected in the *Statistics Type* drop-down. Observe the traffic statistics on the DoH-to-DNS virtual server.

The screenshot shows the F5 Agility 2020 - DNS Over HTTPS/DNS over TLS Lab interface. The browser address bar shows `https://10.1.1.5/xui/?nocache=1579832357260`. The interface includes a top navigation bar with tabs for Advanced Preferences, About Networking, and a plus sign. Below this is a status bar showing Hostname: `ip-10-1-1-5.us-west-2.compute.internal`, IP Address: `10.1.1.5`, Date: Jan 23, 2020, Time: 10:27 PM (EST), User: admin, Role: Administrator, Partition: Common, and a Log out button.

The main content area is titled "Statistics » Module Statistics : Local Traffic » Virtual Servers". The left sidebar shows a navigation menu with options: Main, Help, About, Statistics, iApps, DNS, Local Traffic, Acceleration, Device Management, Shared Objects, Network, and System. The "Statistics" section is expanded, showing "Module Statistics" selected.

The "Display Options" section shows "Statistics Type" set to "Virtual Servers", "Data Format" set to "Normalized", and "Auto Refresh" set to "9 seconds". Below this is a table with columns for Status, Virtual Server, Partition / Path, Details, Bits (In, Out), Packets (In, Out), Connections (Current, Maximum, Total), Requests (Total), CPU Utilization Avg. (5 Sec, 1 Min, 5 Min), and Message Routing Framework (Msg. In, Msg. Out, Req. In, Req. Out, Resp. In, Resp. Out).

Status	Virtual Server	Partition / Path	Details	Bits In	Bits Out	Packets In	Packets Out	Connections Current	Connections Maximum	Connections Total	Requests Total	CPU Utilization Avg. 5 Sec	CPU Utilization Avg. 1 Min	CPU Utilization Avg. 5 Min	Msg. In	Msg. Out	Req. In	Req. Out	Resp. In	Resp. Out
<input type="checkbox"/>	dns-to-doh_udp_proxy	Common	View...	0	0	0	0	0	0	0	0	0%	0%	0%	0	0	0	0	0	0
<input type="checkbox"/>	dns-to-dot_tcp_proxy	Common	View...	0	0	0	0	0	0	0	0	0%	0%	0%	0	0	0	0	0	
<input type="checkbox"/>	dns-to-dot_udp_proxy	Common	View...	0	0	0	0	0	0	0	0	0%	0%	0%	0	0	0	0	0	
<input type="checkbox"/>	doh-to-dns_proxy	Common	View...	622.8K	545.9K	707	798	2	3	33	0	0%	0%	0%	0	0	0	0	0	
<input type="checkbox"/>	dot-to-dns_proxy	Common	View...	0	0	0	0	0	0	0	0	0%	0%	0%	0	0	0	0	0	

Change the *Statistics Type* to iRulesLX and you can see how many RPC connections have been made.

The screenshot shows the F5 Agility 2020 - DNS Over HTTPS/DNS over TLS Lab interface. The browser address bar shows `https://10.1.1.5/xui/?nocache=1579832357260`. The interface includes a top navigation bar with tabs for Advanced Preferences, About Networking, and a plus sign. Below this is a status bar showing Hostname: `ip-10-1-1-5.us-west-2.compute.internal`, IP Address: `10.1.1.5`, Date: Jan 23, 2020, Time: 10:29 PM (EST), User: admin, Role: Administrator, Partition: Common, and a Log out button.

The main content area is titled "Statistics » Module Statistics : Local Traffic » iRules LX". The left sidebar shows a navigation menu with options: Main, Help, About, Statistics, iApps, DNS, Local Traffic, Acceleration, Device Management, Shared Objects, Network, and System. The "Statistics" section is expanded, showing "Module Statistics" selected.

The "Display Options" section shows "Statistics Type" set to "iRules LX", "Data Format" set to "Normalized", and "Auto Refresh" set to "1 seconds". Below this is a table with columns for Status, Plugin : Extension, Partition / Path, Details, Restarts, CPU (%), Total Virtual Size, RPC Info (Total Connections, Total Calls), and Streaming Info (Clientside Total, Serverside Total).

Status	Plugin : Extension	Partition / Path	Details	Restarts	CPU (%)	Total Virtual Size	RPC Info Total Connections	RPC Info Total Calls	Streaming Info Clientside Total	Streaming Info Serverside Total
<input type="checkbox"/>	DNS_to_DoH_Proxy : dns_over_https	Common	View...	0	0	1.8G	0	0	0	0
<input type="checkbox"/>	DoH_to_DNS_Proxy : DoH_to_DNS_Proxy	Common	View...	0	0	2.1G	54	54	0	0

Change the drop-down to *Pools*. You should notice that the back-end pools show 0 connections. Why? Because iRulesLX is talking to the back-end DoH resolvers directly.

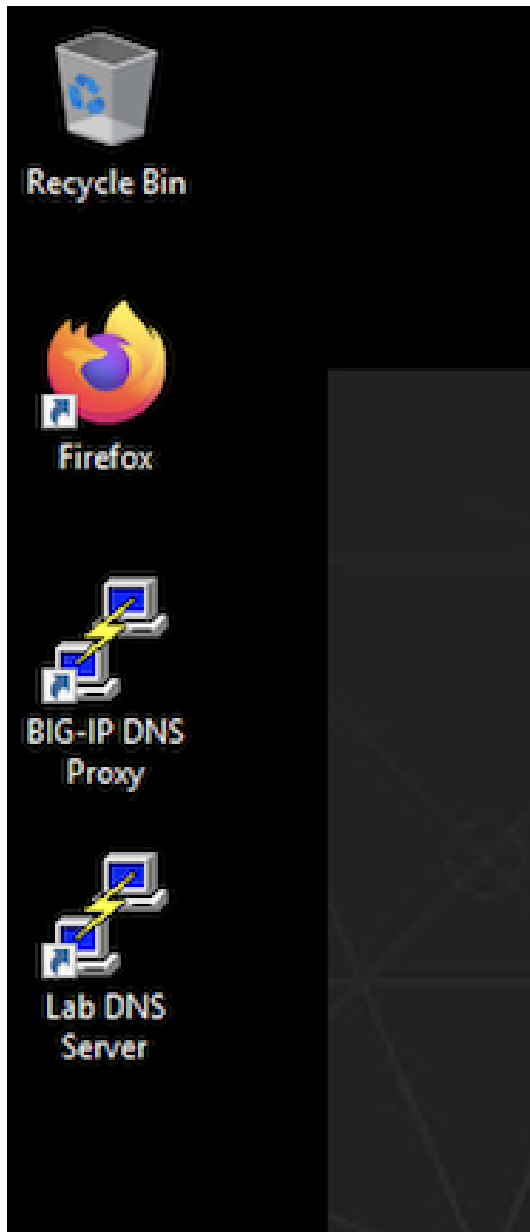
The screenshot shows the F5 Agility 2020 interface for DNS Over HTTPS/DNS over TLS Lab. The top navigation bar includes 'Main', 'Help', and 'About'. The left sidebar lists various modules: Statistics, iApps, DNS, Local Traffic, Acceleration, Device Management, Shared Objects, Network, and System. The main content area is titled 'Statistics >> Module Statistics : Local Traffic >> Pools'. It features a 'Display Options' section with a 'Statistics Type' dropdown set to 'Pools', a 'Data Format' dropdown set to 'Normalized', and an 'Auto Refresh' section set to '2 seconds'. Below this is a table with columns for Status, Pool, Pool Member, Partition / Path, In/Out, Current, Maximum, Total, Requests, Request Queue, and Message Routing Framework. The table lists three pools: 'doh\_dns.google', 'dot\_dns.google', and 'traditional\_dns.google', all with a 'Common' partition and zero activity across all metrics.

Navigate to **System -> Logs -> Local Traffic**. Notice that some useful information is being logged to help show the parsing and querying that is taking place behind the scenes.

The screenshot shows the F5 Agility 2020 interface for DNS Over HTTPS/DNS over TLS Lab, specifically the 'System >> Logs : Local Traffic' section. The left sidebar is expanded to show the 'System' module, with sub-items like Configuration, File Management, Certificate Management, Disk Management, Software Management, License, Resource Provisioning, Platform, High Availability, Archives, Services, and Preferences. The main content area displays a log table with columns for Timestamp, Log Level, Host, Service, Status Code, and Event. The log entries show various system events, including 'audit\_forwarder started', 'src=127.0.0.1, user=' (repeated multiple times), and 'Rule /Common/DoH\_to\_DNS\_Proxy/DoH\_to\_DNS\_Proxy <HTTP\_REQUEST>: DNSoHTTPS: 10.1.1.4 GET /dns-query?dns=AAABAAABAAAAABCHNuaXBwZXRzA2NkbGdtb3ppbGxhA25idAAAAHAAABAApEAAAAAAAAAq Content-type:'. The log also shows 'pid[14179] plugin[/Common/DoH\_to\_DNS\_Proxy/DoH\_to\_DNS\_Proxy] DNS Answer From 10.1.20.101:53Length: 196' and 'Answer is NOT truncated. Flag is 0.Returning D'.

### Capturing DNS over HTTPS Queries to Traditional DNS Traffic

Finally, minimize *Firefox* to reveal the CLI shortcuts on the desktop:



Let's open the BIG-IP DNS Proxy link to bring up the BIG-IP's CLI. Once running, let's start a capture that will show us both sides of the DoH proxy:

```
tcpdump -nni 0.0 (host 10.1.1.4 and host 10.1.10.100 and port 443) or (host 8.8.4.4 or host 8.8.8.8 and port 53)
```

Once running, maximize *Firefox* and perform another DNS lookup. View the HTTPS and DNS traffic in the packet capture output. The output below shows my queries to f5.com, f5agility.com and disney.com.

```

22:43:43.205722 IP 10.1.20.10.44868 > 10.1.255.254.53: 25033+ A? dns.google. (28) out slot1/tmm1 lis=
22:43:43.206697 IP 10.1.255.254.53 > 10.1.20.10.4773: 51509 2/0/0 A 8.8.8.8, A 8.8.4.4 (60) in slot1/tmm0 lis=
22:43:43.208032 IP 10.1.255.254.53 > 10.1.20.10.44868: 25033 2/0/0 A 8.8.8.8, A 8.8.4.4 (60) in slot1/tmm1 lis=
22:43:43.208304 IP 10.1.20.10.62107 > 8.8.8.8.53: 0+ [lau] A? f5.com. (43) out slot1/tmm1 lis=
22:43:43.208328 IP 10.1.20.10.44736 > 8.8.8.8.53: 0+ [lau] AAAA? f5.com. (43) out slot1/tmm1 lis=
22:43:43.223391 IP 8.8.8.8.53 > 10.1.20.10.62107: 0 1/0/1 A 104.219.111.168 (59) in slot1/tmm1 lis=
22:43:43.224514 IP 10.1.10.100.443 > 10.1.1.4.50205: Flags [P.], seq 528741, ack 980, win 25987, length 213 out slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:43.236659 IP 8.8.8.8.53 > 10.1.20.10.44736: 0 1/0/1 AAAA 2620:0:c14:f5f5:1::e8 (71) in slot1/tmm1 lis=
22:43:43.241877 IP 10.1.10.100.443 > 10.1.1.4.50169: Flags [P.], seq 1:226, ack 324, win 22902, length 225 out slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:43.245281 IP 10.1.1.4.50205 > 10.1.10.100.443: Flags [.], ack 741, win 64027, length 0 in slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:43.260985 IP 10.1.1.4.50169 > 10.1.10.100.443: Flags [.], ack 226, win 62890, length 0 in slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:47.191992 IP 10.1.1.4.50205 > 10.1.10.100.443: Flags [P.], seq 980:1312, ack 741, win 64027, length 332 in slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:47.192043 IP 10.1.10.100.443 > 10.1.1.4.50205: Flags [.], ack 1312, win 26319, length 0 out slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:47.193530 IP 10.1.20.10.54189 > 10.1.255.254.53: 53724+ A? dns.google. (28) out slot1/tmm0 lis=
22:43:47.193775 IP 10.1.1.4.50169 > 10.1.10.100.443: Flags [P.], seq 324:656, ack 226, win 62890, length 332 in slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:47.193802 IP 10.1.10.100.443 > 10.1.1.4.50169: Flags [.], ack 656, win 23234, length 0 out slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:47.194745 IP 10.1.20.10.33036 > 10.1.255.254.53: 55740+ A? dns.google. (28) out slot1/tmm1 lis=
22:43:47.195441 IP 10.1.255.254.53 > 10.1.20.10.54189: 53724 2/0/0 A 8.8.4.4, A 8.8.8.8 (60) in slot1/tmm0 lis=
22:43:47.195443 IP 10.1.255.254.53 > 10.1.20.10.33036: 55740 2/0/0 A 8.8.8.8, A 8.8.4.4 (60) in slot1/tmm1 lis=
22:43:47.195814 IP 10.1.20.10.57523 > 8.8.8.8.53: 0+ [lau] AAAA? fsagility.com. (50) out slot1/tmm1 lis=
22:43:47.195837 IP 10.1.20.10.17635 > 8.8.4.4.53: 0+ [lau] A? fsagility.com. (50) out slot1/tmm1 lis=
22:43:47.235274 IP 8.8.8.8.53 > 10.1.20.10.57523: 0 0/1/1 (112) in slot1/tmm1 lis=
22:43:47.236298 IP 10.1.10.100.443 > 10.1.1.4.50169: Flags [P.], seq 226:493, ack 656, win 23234, length 267 out slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:47.252153 IP 8.8.4.4.53 > 10.1.20.10.17635: 0 1/0/1 A 104.219.111.169 (66) in slot1/tmm1 lis=
22:43:47.253645 IP 10.1.10.100.443 > 10.1.1.4.50205: Flags [P.], seq 741:961, ack 1312, win 26319, length 220 out slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:47.260989 IP 10.1.1.4.50169 > 10.1.10.100.443: Flags [.], ack 493, win 64240, length 0 in slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:47.276625 IP 10.1.1.4.50205 > 10.1.10.100.443: Flags [.], ack 961, win 63807, length 0 in slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:52.889023 IP 10.1.1.4.50205 > 10.1.10.100.443: Flags [P.], seq 1312:1640, ack 961, win 63807, length 328 in slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:52.889068 IP 10.1.10.100.443 > 10.1.1.4.50205: Flags [.], ack 1640, win 26647, length 0 out slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:52.890484 IP 10.1.20.10.39184 > 10.1.255.254.53: 2788+ A? dns.google. (28) out slot1/tmm1 lis=
22:43:52.890679 IP 10.1.1.4.50169 > 10.1.10.100.443: Flags [P.], seq 656:984, ack 493, win 64240, length 328 in slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:52.890704 IP 10.1.10.100.443 > 10.1.1.4.50169: Flags [.], ack 984, win 23562, length 0 out slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:52.891491 IP 10.1.20.10.59922 > 10.1.255.254.53: 44568+ A? dns.google. (28) out slot1/tmm0 lis=
22:43:52.891722 IP 10.1.255.254.53 > 10.1.20.10.39184: 2788 2/0/0 A 8.8.4.4, A 8.8.8.8 (60) in slot1/tmm1 lis=
22:43:52.892041 IP 10.1.20.10.9521 > 8.8.4.4.53: 0+ [lau] A? disney.com. (47) out slot1/tmm0 lis=
22:43:52.892060 IP 10.1.255.254.53 > 10.1.20.10.59922: 44568 2/0/0 A 8.8.8.8, A 8.8.4.4 (60) in slot1/tmm0 lis=
22:43:52.892264 IP 10.1.20.10.57149 > 8.8.8.8.53: 0+ [lau] AAAA? disney.com. (47) out slot1/tmm0 lis=
22:43:52.907463 IP 8.8.4.4.53 > 10.1.20.10.9521: 0 1/0/1 A 130.211.198.204 (63) in slot1/tmm0 lis=
22:43:52.908418 IP 10.1.10.100.443 > 10.1.1.4.50205: Flags [P.], seq 961:1178, ack 1640, win 26647, length 217 out slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:52.932880 IP 10.1.1.4.50205 > 10.1.10.100.443: Flags [.], ack 1178, win 63590, length 0 in slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:52.981019 IP 8.8.8.8.53 > 10.1.20.10.57149: 0 0/1/1 (93) in slot1/tmm0 lis=
22:43:52.981571 IP 10.1.10.100.443 > 10.1.1.4.50169: Flags [P.], seq 493:740, ack 984, win 23562, length 247 out slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:43:52.995339 IP 10.1.1.4.50169 > 10.1.10.100.443: Flags [.], ack 740, win 63993, length 0 in slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:44:02.122484 IP 10.1.1.4.65193 > 10.1.10.100.53: 36886+ A? wpad.us-west-2.ec2-utilities.amazonaws.com. (60) in slot1/tmm0 lis=
22:44:02.917184 IP 10.1.1.4.50205 > 10.1.10.100.443: Flags [.], seq 1639:1640, ack 1178, win 63590, length 1 in slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:44:02.917245 IP 10.1.10.100.443 > 10.1.1.4.50205: Flags [.], ack 1640, win 26647, length 0 out slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:44:02.995431 IP 10.1.1.4.50169 > 10.1.10.100.443: Flags [.], seq 983:984, ack 740, win 63993, length 1 in slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:44:02.995467 IP 10.1.10.100.443 > 10.1.1.4.50169: Flags [P.], ack 984, win 23562, length 0 out slot1/tmm1 lis=/Common/doh-to-dns_proxy
22:44:03.136523 IP 10.1.1.4.65193 > 10.1.10.100.53: 36886+ A? wpad.us-west-2.ec2-utilities.amazonaws.com. (60) in slot1/tmm0 lis=
22:44:04.136219 IP 10.1.1.4.65193 > 10.1.10.100.53: 36886+ A? wpad.us-west-2.ec2-utilities.amazonaws.com. (60) in slot1/tmm0 lis=
22:44:06.151615 IP 10.1.1.4.65193 > 10.1.10.100.53: 36886+ A? wpad.us-west-2.ec2-utilities.amazonaws.com. (60) in slot1/tmm0 lis=

```

Stop your capture before moving to the next section. This concludes the DoH-to-DNS proxy portion of the lab.

## 6.1.5 Proxying DNS over TLS Queries to Traditional DNS

DoT-to-DNS is a bit more simplistic. We're simply taking the existing DNS request and encapsulating it in TLS. No iRule magic needed here; just classic BIG-IP high-performance SSL offloading.

**The client-SSL profile on this virtual server specifies that SSL/TLS termination should occur on the client side of the connection.**

### Virtual Server Configuration

Maximize *Firefox*. Click on the first tab to return to the BIG-IP web UI. Navigate to **Local Traffic -> Virtual Servers**. If you review the virtual server configuration, you'll notice that we're simply using a client-SSL profile and a backend pool. The client-SSL profile utilizes a self-signed certificate in this lab, you'll need a certificate from a certificate authority that your clients' browsers trust in a production deployment.



## General Properties



Name	dot-to-dns_proxy		
Partition / Path	Common		
Description	<input type="text"/>		
Type	Standard <input type="button" value="v"/>		
Source Address	<input checked="" type="radio"/> Host <input type="radio"/> Address List <input type="text" value="0.0.0.0/0"/>		
Destination Address/Mask	<input checked="" type="radio"/> Host <input type="radio"/> Address List <input type="text" value="10.1.10.100"/>		
Service Port	<input checked="" type="radio"/> Port <input type="radio"/> Port List <input type="text" value="853"/> Other: <input type="button" value="v"/>		
Notify Status to Virtual Address	<input checked="" type="checkbox"/>		
Availability	Available (Enabled) - The virtual server is available		
Syncookie Status	Inactive		
State	Enabled <input type="button" value="v"/>		

Configuration: Basic 

Protocol	TCP <input type="button" value="v"/>		
Protocol Profile (Client)	f5-tcp-lan <input type="button" value="v"/>		
Protocol Profile (Server)	f5-tcp-wan <input type="button" value="v"/>		
HTTP Profile (Client)	None <input type="button" value="v"/>		
HTTP Profile (Server)	(Use Client Profile) <input type="button" value="v"/>		
HTTP Proxy Connect Profile	None <input type="button" value="v"/>		
FTP Profile	None <input type="button" value="v"/>		
RTSP Profile	None <input type="button" value="v"/>		
SSL Profile (Client)	<div>Selected</div> <div> <input type="text" value="/Common"/>              agility_selfsigned           </div>	<div>Available</div> <div> <input type="text" value="/Common"/>              clientssl              clientssl-insecure-compatible              clientssl-secure              crypto-server-default-clientssl              session-default-clientssl              wom-default-clientssl           </div>	<div>&lt;&lt;</div> <div>&gt;&gt;</div>

Clicking on **Resources** tab on the top navigation bar will show that the virtual server has a simple pool and no iRules attached.

Local Traffic » Virtual Servers : Virtual Server List » dot-to-dns\_proxy


Properties
Resources
Statistics


### Load Balancing

Default Pool	traditional_dns.google
Default Persistence Profile	None
Fallback Persistence Profile	None

Update

### iRules

Name
No records to display.

### Policies

Name
No records to display.

### Test Driving DNS over TLS to Traditional DNS

Minimize Firefox to view the desktop shortcuts and launch the Lab DNS Server client. You'll be automatically logged in. Let's run a DNS over TLS query:

```
kdig +tls @10.1.10.100 www.f5.com
```

You should see a response similar to the output below. Run a few more queries against other domains to generate statistics.

```
user@ip-10-1-1-6: ~  
user@ip-10-1-1-6:~$ man dig  
user@ip-10-1-1-6:~$  
user@ip-10-1-1-6:~$ kdig +tls @10.1.10.100 www.f5.com  
;; TLS session (TLS1.2)-(ECDHE-RSA-SECP256R1)-(AES-128-GCM)  
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 15427  
;; Flags: qr rd ra; QUERY: 1; ANSWER: 5; AUTHORITY: 0; ADDITIONAL: 1  
  
;; EDNS PSEUDOSECTION:  
;; Version: 0; flags: ; UDP size: 512 B; ext-rcode: NOERROR  
  
;; QUESTION SECTION:  
;; www.f5.com.                IN      A  
  
;; ANSWER SECTION:  
www.f5.com.                29      IN      CNAME   dwbfwz8xncgm.cloudfront.net.  
dwbfwz8xncgm.cloudfront.net. 59      IN      A       13.224.2.97  
dwbfwz8xncgm.cloudfront.net. 59      IN      A       13.224.2.74  
dwbfwz8xncgm.cloudfront.net. 59      IN      A       13.224.2.75  
dwbfwz8xncgm.cloudfront.net. 59      IN      A       13.224.2.91  
  
;; Received 145 B  
;; Time 2020-01-24 03:52:48 UTC  
;; From 10.1.10.100@853(TCP) in 59.2 ms  
user@ip-10-1-1-6:~$
```

### Viewing Statistics for DoT-to-DNS

You can then see statistics on the virtual server by navigating to **Statistics -> Module Statistics -> Local Traffic** and selecting *Virtual Servers* in the drop-down list.



The screenshot shows the F5 Agility 2020 - DNS Over HTTPS/DNS over TLS Lab interface. The left sidebar contains navigation links: Main, Help, About, Statistics, iApps, DNS, Local Traffic, Acceleration, Device Management, Shared Objects, Network, and System. The main content area is titled "Statistics >> Module Statistics : Local Traffic >> Virtual Servers". Below this, there are tabs for Traffic Summary, DNS, Local Traffic (selected), Subscriber Management, Network, Memory, and System. The "Display Options" section shows "Statistics Type" set to "Virtual Servers" (highlighted with a red box), "Data Format" set to "Normalized", and "Auto Refresh" set to "9 seconds". The main table displays statistics for various virtual servers, including dns-to-doh\_udp\_proxy, dns-to-dot\_tcp\_proxy, dns-to-dot\_udp\_proxy, doh-to-dns\_proxy, and dot-to-dns\_proxy. The table columns include Status, Virtual Server, Partition / Path, Details, Bits (In, Out), Packets (In, Out), Connections (Current, Maximum, Total), Requests (Total), CPU Utilization Avg. (5 Sec, 1 Min, 5 Min), and Message Routing Framework (Msg. In, Msg. Out, Req. In, Req. Out, Resp. In, Resp. Out).

Because this virtual server is taking advantage of backend pools, you will see statistics under the *Pools* statistics type as well.

The screenshot shows the F5 Agility 2020 - DNS Over HTTPS/DNS over TLS Lab interface. The left sidebar is the same as the previous screenshot. The main content area is titled "Statistics >> Module Statistics : Local Traffic >> Pools". Below this, there are tabs for Traffic Summary, DNS, Local Traffic (selected), Subscriber Management, Network, Memory, and System. The "Display Options" section shows "Statistics Type" set to "Pools" (highlighted with a red box), "Data Format" set to "Normalized", and "Auto Refresh" set to "6 seconds". The main table displays statistics for various pools, including doh\_dns.google, dot\_dns.google, and traditional\_dns.google. The table columns include Status, Pool, Pool Member, Partition / Path, Bits (In, Out), Packets (In, Out), Connections (Current, Maximum, Total), Requests (Total), Request Queue (Depth, Maximum Age), and Message Routing Framework (Msg. In, Msg. Out, Req. In, Req. Out, Resp. In, Resp. Out).

Because we don't have any type of logging configured for that virtual server, you won't see any information in **System -> Logs** for this traffic. If you'd desire logging in your environment, general LTM F5 logging/statistics practices can be used.

### Capturing DNS over TLS to Traditional DNS Traffic

Minimize Firefox and return to the BIG-IP DNS Proxy session from the first section of this lab, or open a new session by clicking on the BIG-IP DNS Proxy icon on the desktop. Execute the follow tcpdump command:

```
tcpdump -nni 0.0 port 53 or port 853
```

Pull the Lab DNS Server session window up and re-run the **kdig** command. Observe the front and back-end connections using port 853 and 53, respectively, shown in the packet capture output.

```
23:07:21.434497 IP 10.1.10.100.853 > 10.1.1.6.49992: Flags [P.], seq
is=/Common/dot-to-dns_proxy
23:07:21.434520 IP 10.1.20.10.49992 > 8.8.4.4.53: Flags [S], seq 2784
is=/Common/dot-to-dns_proxy
23:07:21.434536 IP 10.1.10.100.853 > 10.1.1.6.49992: Flags [P.], seq
lis=/Common/dot-to-dns_proxy
23:07:21.434889 IP 10.1.1.6.49992 > 10.1.10.100.853: Flags [P.], seq
is=/Common/dot-to-dns_proxy
23:07:21.434913 IP 10.1.10.100.853 > 10.1.1.6.49992: Flags [.], ack 4
o-dns_proxy
23:07:21.441472 IP 8.8.4.4.53 > 10.1.20.10.49992: Flags [S.], seq 128
length 0 in slot1/tmml lis=/Common/dot-to-dns_proxy
23:07:21.441494 IP 10.1.20.10.49992 > 8.8.4.4.53: Flags [.], ack 1, w
proxy
23:07:21.441506 IP 10.1.20.10.49992 > 8.8.4.4.53: Flags [P.], seq 1:1
m. (128) out slot1/tmml lis=/Common/dot-to-dns_proxy
23:07:21.448194 IP 8.8.4.4.53 > 10.1.20.10.49992: Flags [.], ack 131,
proxy
23:07:21.485209 IP 8.8.4.4.53 > 10.1.20.10.49992: Flags [P.], seq 1:1
8xncgmg.cloudfront.net., A 13.224.2.91, A 13.224.2.97, A 13.224.2.75,
23:07:21.485256 IP 10.1.20.10.49992 > 8.8.4.4.53: Flags [.], ack 148,
s_proxy
23:07:21.485373 IP 10.1.10.100.853 > 10.1.1.6.49992: Flags [P.], seq
lis=/Common/dot-to-dns_proxy
23:07:21.488839 IP 10.1.1.6.49992 > 10.1.10.100.853: Flags [P.], seq
```

Stop your capture before moving on to the next section. This concludes the DoT-to-DNS portion of the lab.

### 6.1.6 Proxying Traditional DNS to DNS over TLS

In this section of the lab, we're going to run DoT in the opposite direction, taking traditional DNS requests and translating them into DoT requests. This is done as simply as the DoT-to-DNS; we simply take the incoming DNS connection (UDP or TCP) and encapsulate it in TLS using a server-side SSL profile.

#### Test Driving Traditional DNS to DNS over TLS

On the Lab DNS Server, issue the following command:

```
kdig @10.1.10.101 www.yahoo.com
```

You should receive a successful response as shown below:

```

user@ip-10-1-1-6:~$ dig @10.1.10.101 www.yahoo.com

; <<>> DiG 9.11.3-lubuntul.11-Ubuntu <<>> @10.1.10.101 www.yahoo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7629
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::; udp: 4096
;; QUESTION SECTION:
;www.yahoo.com.                IN      A

;; ANSWER SECTION:
www.yahoo.com.                1185    IN      CNAME   atsv2-fp-shed.wgl.b.yahoo.com.
atsv2-fp-shed.wgl.b.yahoo.com. 18 IN      A       98.137.246.8
atsv2-fp-shed.wgl.b.yahoo.com. 18 IN      A       98.137.246.7

;; Query time: 38 msec
;; SERVER: 10.1.10.101#53(10.1.10.101)
;; WHEN: Fri Jan 24 04:12:36 UTC 2020
;; MSG SIZE rcvd: 108

```

## Viewing Statistics for DNS-to-DoT

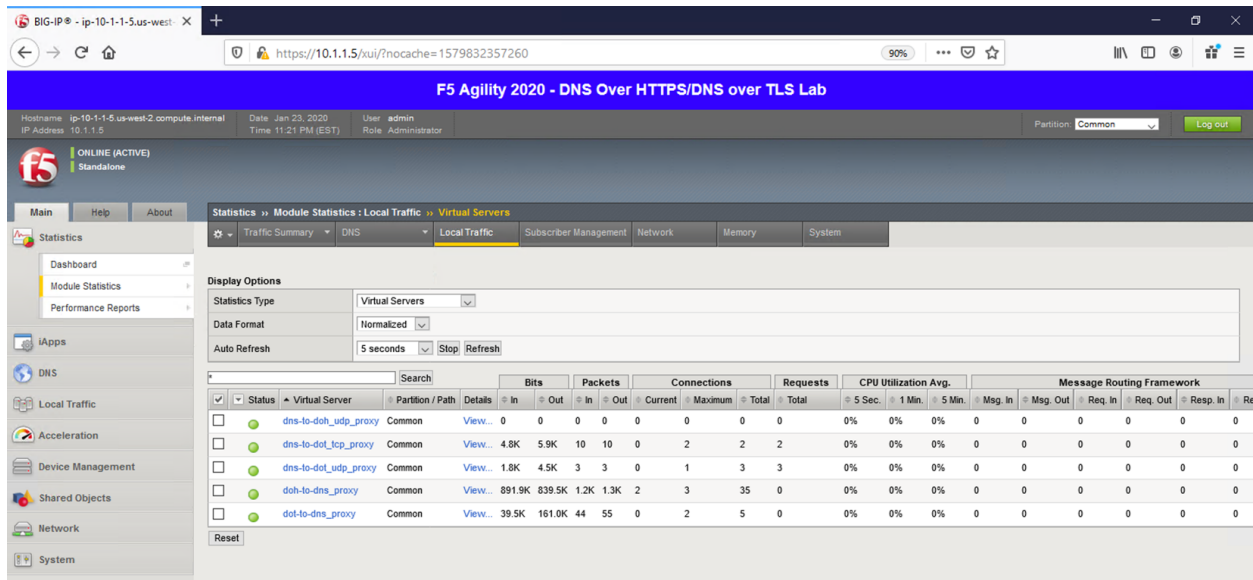
Restore Firefox and click on the first tab to return to the BIG-IP web UI. You can then see statistics on the virtual server by navigating to Statistics -> Module Statistics -> Local Traffic and selecting Virtual Servers in the drop-down list.

The screenshot shows the F5 Agility 2020 web interface for the 'DNS Over HTTPS/DNS over TLS Lab'. The left sidebar contains navigation links: Main, Statistics, iApps, DNS, Local Traffic, Acceleration, Device Management, Shared Objects, Network, and System. The main panel is titled 'F5 Agility 2020 - DNS Over HTTPS/DNS over TLS Lab' and shows system information like Hostname, Date, User, and Role. Below this, there's a 'Statistics' section with a breadcrumb trail: 'Statistics > Module Statistics > Local Traffic > Virtual Servers'. A table displays statistics for various virtual servers. The table has columns for Status, Virtual Server, Partition/Path, Details, Bits, Packets, Connections, Requests, CPU Utilization Avg., and Message Routing Framework. The data rows show different proxy configurations and their associated traffic metrics.

Status	Virtual Server	Partition/Path	Details	Bits	Packets	Connections	Requests	CPU Utilization Avg.	Message Routing Framework									
<input checked="" type="checkbox"/>	dns-to-doh_udp_proxy	Common	View...	0	0	0	0	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
<input checked="" type="checkbox"/>	dns-to-dot_tcp_proxy	Common	View...	0	0	0	0	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	
<input checked="" type="checkbox"/>	dns-to-dot_udp_proxy	Common	View...	1.2K	3.2K	2	2	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	
<input checked="" type="checkbox"/>	doh-to-dns_proxy	Common	View...	832.4K	742.4K	1.1K	1.2K	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	
<input checked="" type="checkbox"/>	dot-to-dns_proxy	Common	View...	39.5K	161.0K	44	55	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	

Back on the Lab DNS Server, issue the same `kdig` command with the `TCP` option to increment the counters on the corresponding virtual server:

```
kdig +tcp @10.1.10.101 www.f5.com
```



Since this is basic LTM functionality, general LTM logging practices can be used if you wish to log traffic in your environment.

### Capturing Traditional DNS to DNS over TLS Traffic

On the BIG-IP CLI, we can see the 53/853 exchange on a packet capture using the same **tcpdump** command we used in the DoT-to-DNS section, as the IP/ports are simply being switched around. In the BIG-IP DNS Proxy session, issue the following command:

```
tcpdump -nni 0.0 (host 10.1.20.10 or 10.1.1.6) and (port 53 or port 853)
```

When running **kdig** commands on the Lab DNS Server, you will see the port 53 and port 853 connections in the output, as shown below.

```

length 0 in slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.118037 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [.], ack 1, win 3650, options [nop,nop,TS val 3587003485 ecr 3183768418], length 0 out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.118067 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [P.], seq 1:163, ack 1, win 3650, options [nop,nop,TS val 3587003485 ecr 3183768418], length 162 out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.125491 IP 8.8.8.8.853 > 10.1.20.10.39332: Flags [.], ack 163, win 240, options [nop,nop,TS val 3183768426 ecr 3587003485], length 0 in slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.133447 IP 8.8.8.8.853 > 10.1.20.10.39332: Flags [.], seq 1:1419, ack 163, win 240, options [nop,nop,TS val 3183768433 ecr 3587003485], length 1418 in slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.133463 IP 8.8.8.8.853 > 10.1.20.10.39332: Flags [.], seq 1419:2837, ack 163, win 240, options [nop,nop,TS val 3183768433 ecr 3587003485], length 1418 in slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.133472 IP 8.8.8.8.853 > 10.1.20.10.39332: Flags [P.], seq 2837:3098, ack 163, win 240, options [nop,nop,TS val 3183768433 ecr 3587003485], length 261 in slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.133982 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [.], ack 3098, win 4424, options [nop,nop,TS val 3587003501 ecr 3183768433], length 0 out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.134429 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [P.], seq 163:211, ack 3098, win 4424, options [nop,nop,TS val 3587003501 ecr 3183768433], length 48 out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.134461 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [P.], seq 211:256, ack 3098, win 4424, options [nop,nop,TS val 3587003501 ecr 3183768433], length 45 out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.142284 IP 8.8.8.8.853 > 10.1.20.10.39332: Flags [P.], seq 3098:3149, ack 256, win 240, options [nop,nop,TS val 3183768442 ecr 3587003501], length 51 in slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.142314 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [.], ack 3149, win 4437, options [nop,nop,TS val 3587003510 ecr 3183768442], length 0 out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.142852 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [P.], seq 256:322, ack 3149, win 4437, options [nop,nop,TS val 3587003510 ecr 3183768442], length 66 out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.142911 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [P.], seq 322, win 240, options [nop,nop,TS val 3183768454 ecr 3587003510], length 0 in slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.153855 IP 8.8.8.8.853 > 10.1.20.10.39332: Flags [P.], seq 3149:3257, ack 322, win 240, options [nop,nop,TS val 3183768563 ecr 3587003510], length 108 in slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.162697 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [.], ack 3257, win 4464, options [nop,nop,TS val 3587003630 ecr 3183768563], length 0 out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.263229 IP 10.1.10.101.53 > 10.1.1.6.39332: Flags [P.], seq 1:80, ack 39, win 12341, options [nop,nop,TS val 3587003630 ecr 1324775930], length 7931166 2/0/0 CNAME redirec.f5.com., A 104.219.111.169 (77) out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.263587 IP 10.1.1.6.39332 > 10.1.10.101.53: Flags [.], ack 80, win 62648, options [nop,nop,TS val 1324776083 ecr 3587003630], length 0 in slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.265299 IP 10.1.1.6.39332 > 10.1.10.101.53: Flags [F.], seq 38, ack 80, win 62648, options [nop,nop,TS val 1324776085 ecr 3587003630], length 0 in slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.265322 IP 10.1.10.101.53 > 10.1.1.6.39332: Flags [.], ack 39, win 12341, options [nop,nop,TS val 3587003633 ecr 1324776085], length 0 out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.265334 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [F.], seq 322, ack 3257, win 4464, options [nop,nop,TS val 3587003633 ecr 3183768563], length 0 out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.273102 IP 8.8.8.8.853 > 10.1.20.10.39332: Flags [F.], seq 3257, ack 323, win 240, options [nop,nop,TS val 3183768573 ecr 3587003633], length 0 in slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.273161 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [.], ack 3258, win 4464, options [nop,nop,TS val 3587003640 ecr 3183768573], length 0 out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.273184 IP 10.1.10.101.53 > 10.1.1.6.39332: Flags [F.], seq 80, ack 39, win 12341, options [nop,nop,TS val 3587003640 ecr 1324776085], length 0 out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:26:41.273546 IP 10.1.1.6.39332 > 10.1.10.101.53: Flags [.], ack 81, win 62648, options [nop,nop,TS val 1324776093 ecr 3587003640], length 0 in slot1/tmml lis=/Common/dns-to-dot_tcp_proxy

```

Stop your capture before moving on to the next section. This concludes the DNS-to-DoT section.

## 6.1.7 Proxying Traditional DNS queries to DNS over HTTPS

Finally, let's look at converting a DNS query to a DoH request.

### Test Driving Traditional DNS to DNS over HTTPS

Minimize Firefox and bring both CLI session windows up. On the Lab DNS Server, once again use **kdig** to simply generate a traditional DNS request. Notice that this section of the lab uses a different VIP, the 10.1.10.102 address.

```
kdig @10.1.10.102 www.f5agility.com
```

You'll get a response as shown below:



```

user@ip-10-1-1-6:~$ kdig @10.1.10.102 www.f5agility.com
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 25887
;; Flags: qr rd ra; QUERY: 1; ANSWER: 2; AUTHORITY: 0; ADDITIONAL: 0

;; QUESTION SECTION:
;; www.f5agility.com.                IN      A

;; ANSWER SECTION:
www.f5agility.com.      299     IN      CNAME   redirect.f5.com.
redirect.f5.com.        29      IN      A       104.219.111.169

;; Received 77 B
;; Time 2020-01-24 04:31:03 UTC
;; From 10.1.10.102@53 (UDP) in 134.3 ms

```

## Viewing Statistics for DNS-to-DoH

Back on the BIG-IP, we'll see connections on the DNS-to-DoH virtual server in the Local Traffic module statistics:

The screenshot shows the F5 Agility 2020 - DNS Over HTTPS/DNS over TLS Lab interface. The left sidebar contains a navigation menu with items like Statistics, iApps, DNS, Local Traffic, Acceleration, Device Management, Shared Objects, Network, and System. The 'Statistics' menu item is highlighted, and a sub-menu is open showing 'Dashboard', 'Module Statistics' (which is highlighted with a red box), and 'Performance Reports'. The main content area displays 'Module Statistics : Local Traffic' with a 'Virtual Servers' tab selected. Below this, there are 'Display Options' for 'Statistics Type' (set to 'Virtual Servers'), 'Data Format' (set to 'Normalized'), and 'Auto Refresh' (set to '4 seconds'). A table of statistics is shown with columns for Status, Virtual Server, Partition / Path, Details, Bits (In, Out), Packets (In, Out), Connections (Current, Maximum, Total), Requests (Total), CPU Utilization Avg. (5 Sec, 1 Min, 5 Min), and Message Routing Framework (Msg. In, Msg. Out, Req. In, Req. Out, Resp. In, Resp. Out). The table lists four virtual servers: dns-to-doh\_udp\_proxy, dns-to-dot\_tcp\_proxy, dns-to-dot\_udp\_proxy, and doh-to-dns\_proxy, each with its respective statistics.

Status	Virtual Server	Partition / Path	Details	Bits In	Bits Out	Packets In	Packets Out	Connections Current	Connections Maximum	Connections Total	Requests Total	CPU Utilization Avg. 5 Sec	CPU Utilization Avg. 1 Min	CPU Utilization Avg. 5 Min	Msg. In	Msg. Out	Req. In	Req. Out	Resp. In	Resp. Out
<input type="checkbox"/>	dns-to-doh_udp_proxy	Common	View...	504	840	1	1	0	1	1	0	0%	0%	0%	0	0	0	0	0	0
<input type="checkbox"/>	dns-to-dot_tcp_proxy	Common	View...	14.5K	16.9K	30	30	0	2	6	3	0%	0%	0%	0	0	0	0	0	
<input type="checkbox"/>	dns-to-dot_udp_proxy	Common	View...	1.8K	4.5K	3	3	0	1	3	3	0%	0%	0%	0	0	0	0	0	
<input type="checkbox"/>	doh-to-dns_proxy	Common	View...	930.6K	877.3K	1.4K	1.4K	2	3	35	0	0%	0%	0%	0	0	0	0	0	
<input type="checkbox"/>	dot-to-dns_proxy	Common	View...	39.5K	161.0K	44	55	0	2	5	0	0%	0%	0%	0	0	0	0	0	

If we set the statistics type to *iRulesLX*, we'll see RPC connections on the iRule for this translation:

## Capturing Traditional DNS to DNS over HTTPS Traffic

Running a packet capture on the BIG-IP DNS Proxy, we can view the front-end udp/53 requests being translated to DoH requests:

`tcpdump -nni 0.0 (host 10.1.10.102 and port 53) or (host 8.8.4.4 or host 8.8.8.8 and port 443)`

Run **kdig** queries on the Lab DNS Server to generate traffic.

**NOTICE** If your packet capture is “noisy,” remember that you’re also capturing the HTTPS monitor traffic as the “doh\_google.dns” pool performing regular queries.

Notice that a port 53 request comes in, a HTTPS connection is set up and the query is passed, then the port 53 response is sent to the client before the HTTPS connection is torn down.

```
13:24:31.414842 IP 10.1.1.6.44657 > 10.1.10.102.53: 39939+ A? www.f5agility.com. (35) in slot1/tmm0 lis=
13:24:31.492130 IP 10.1.20.10.21881 > 8.8.8.8.443: Flags [S], seq 3145906949, win 29200, options [mes 146
13:24:31.500689 IP 10.1.20.10.21881 > 8.8.8.8.443: Flags [S.], seq 3232513395, ack 3145906950, win 60192,
13:24:31.501173 IP 10.1.20.10.21881 > 8.8.8.8.443: Flags [P.], seq 1:510, ack 1, win 229, options [nop,nop,TS val 363
13:24:31.509805 IP 8.8.8.8.443 > 10.1.20.10.21881: Flags [.], ack 510, win 240, options [nop,nop,TS val 4
13:24:31.510181 IP 8.8.8.8.443 > 10.1.20.10.21881: Flags [P.], seq 1:169, ack 510, win 240, options [nop,
13:24:31.510230 IP 10.1.20.10.21881 > 8.8.8.8.443: Flags [.], ack 169, win 237, options [nop,nop,TS val 3
13:24:31.510516 IP 10.1.20.10.21881 > 8.8.8.8.443: Flags [P.], seq 510:814, ack 169, win 237, options [nop
13:24:31.523172 IP 8.8.8.8.443 > 10.1.20.10.21881: Flags [.], ack 814, win 244, options [nop,nop,TS val 4
13:24:31.587284 IP 8.8.8.8.443 > 10.1.20.10.21881: Flags [P.], seq 169:819, ack 814, win 244, options [no
13:24:31.587701 IP 10.1.20.10.21881 > 8.8.8.8.443: Flags [P.], seq 814:845, ack 819, win 247, options [no
13:24:31.587835 IP 10.1.10.102.53 > 10.1.1.6.44657: 39939 2/0/0 CNAME redirect.f5.com., A 104.219.111.169
13:24:31.587902 IP 10.1.20.10.21881 > 8.8.8.8.443: Flags [F.], seq 845, ack 819, win 247, options [nop,no
13:24:31.587917 IP 8.8.8.8.443 > 10.1.20.10.21881: Flags [F.], seq 819, ack 814, win 244, options [nop,no
13:24:31.588120 IP 10.1.20.10.21881 > 8.8.8.8.443: Flags [.], ack 820, win 247, options [nop,nop,TS val 3
13:24:31.586160 IP 8.8.8.8.443 > 10.1.20.10.21881: Flags [.], ack 845, win 244, options [nop,nop,TS val 4
13:24:31.596328 IP 8.8.8.8.443 > 10.1.20.10.21881: Flags [.], ack 846, win 244, options [nop,nop,TS val 4
13:24:31.596546 IP 8.8.8.8.443 > 10.1.20.10.21881: Flags [R.], seq 820, ack 846, win 244, options [nop,no
13:24:31.596562 IP 8.8.8.8.443 > 10.1.20.10.21881: Flags [R], seq 3232514215, win 0, length 0 in slot1/tm
```

This concludes the hands-on portion of the lab.

## 6.1.8 Additional Resources

The following resources will allow you to explore DoH and DoT more, and setup this functionality in your own environment.

- RFC8484: DNS over HTTPS: <https://tools.ietf.org/html/rfc8484>
- RFC7858: DNS over TLS: <https://tools.ietf.org/html/rfc7858>
- Github repository with iRules and sample configuration: <https://github.com/grf5/DoHDoTIRulesLX>



## LAB: F5 DNS Cloud Service & F5 DNS Load Balancer Cloud Service

### Table of Contents

- *LAB: F5 DNS Cloud Service & F5 DNS Load Balancer Cloud Service*
  - *Introduction*
  - *Pre-Requisites*
  - *Lab Environment Overview*
    - \* *1. APIs and Services*
    - \* *2. Application Scenario*
  - *Lab Environment Setup / Validation*
    - \* *1. F5 Cloud Services Portal*
    - \* *2. Opera with VPN to Test Geo Services*
    - \* *3. Postman Configuration*
    - \* *4. Zone Name*
  - *F5 DNS Cloud Service - UI*
    - \* *1. Create Secondary DNS Zone*
    - \* *2. Query via Browser*
    - \* *3. Delete Zone*
  - *F5 DNS Cloud Service - API*
    - \* *1. Create Zone*
    - \* *2. Get Zone File*
    - \* *3. Query via Browser*
    - \* *4. Review the JSON*
    - \* *5. Delete Zone*
  - *F5 DNS Load Balancer Cloud Service - UI*

- \* *1. Create F5 DNS Load Balancer Cloud Service*
- \* *2. Add Single Endpoint, Health Monitor, Pool and Default Geoproximity Rule*
- \* *3. Add Multiple Endpoints to Load Balanced Pool & Test*
- \* *4. Add Europe Region & EU Endpoint with Corresponding Geoproximity Record*
- \* *5. Duplicate Load Balanced Record using JSON through the UI*
- \* *6. Delete DNS Load Balancer Service*
- *F5 DNS Load Balancer Cloud Service - API*
  - \* *1. Create DNS Load Balancer Subscription*
  - \* *2. Activate DNS Load Balancer Subscription*
  - \* *3. Test NA Pool*
  - \* *4. Add Endpoints & Pool Members*
  - \* *5. Test Round Robin (lab)*
  - \* *6. Update Proximity Rule*
  - \* *7. Test Proximity Rules (lab)*
  - \* *8. Review the JSON*
  - \* *9. Delete DNS Load Balancer Service*
- *Clean Up*

## 7.1 Introduction

Welcome to the F5 Cloud Services lab that covers DNS and DNS Load Balancer services. This lab will take you through the setting up, configuration, updates, and removal of the F5 Cloud Services that provide DNS capabilities. You will be using both browser-based UI of the F5 Cloud Services platform, as well as the declarative API, which is available to do all of the things the UI does, and more!

In the process of this lab you will learn how to:

- Set up a DDoS-protected secondary DNS service
- Retrieve and review the zone file retrieved from the primary DNS (we will provide you with a primary DNS and a zone just for you!)
- Set up Anycast network-backed load balanced DNS record
- Add and update application endpoints and a load-balancer pool
- Configure, update, and test geoproximity rules, and
- Have fun working with UI and APIs!

## 7.2 Pre-Requisites

- Any modern browser: for working with the UI (and this document)
- Postman: for working with the API of the F5 Cloud Services

- Opera browser: for simulating geo-location specific traffic
- Any text editor: for duplicating Load Balanced Record

**IMPORTANT NOTE:** If you originally signed up for F5 Cloud Services through a Limited User invitation (such as an email invite from another lab or from a different account owner), then it is possible that you haven't yet completed a full registration.

You can quickly tell if you have a full account by looking at your account(s) in the [F5 Cloud Services Portal](#). If you do now see any "Accounts you own:" and only see "Accounts you've been granted access to" as a "**Limited User**", then you will need to create a full account / update user info before you can proceed with this lab. You can do so in the step 4(c) below via the F5 Cloud Services API using the Postman request titled "Set User Info (optional)", the details of which are outlined below after the Login.

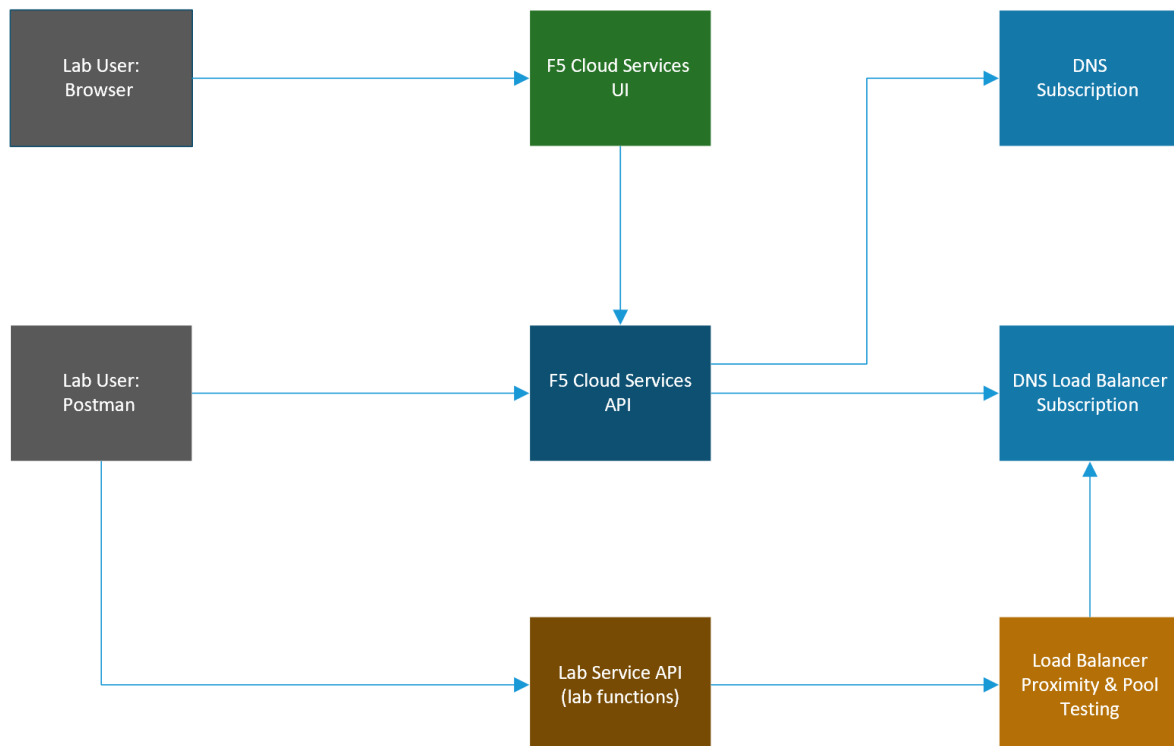
## 7.3 Lab Environment Overview

### 7.3.1 1. APIs and Services

This Lab utilizes standard *F5 Cloud Services API*, as well as a *Lab Service API*, which was custom-built just for executing this lab:

- **F5 Cloud Services API:** create, use, and remove the services in the scope of this lab
- **Lab service API:** facilitates auxiliary functions for the lab only: creating DNS entries, sending targeted requests & traffic to the apps/services, etc.

The following diagram captures the core components of this Lab:



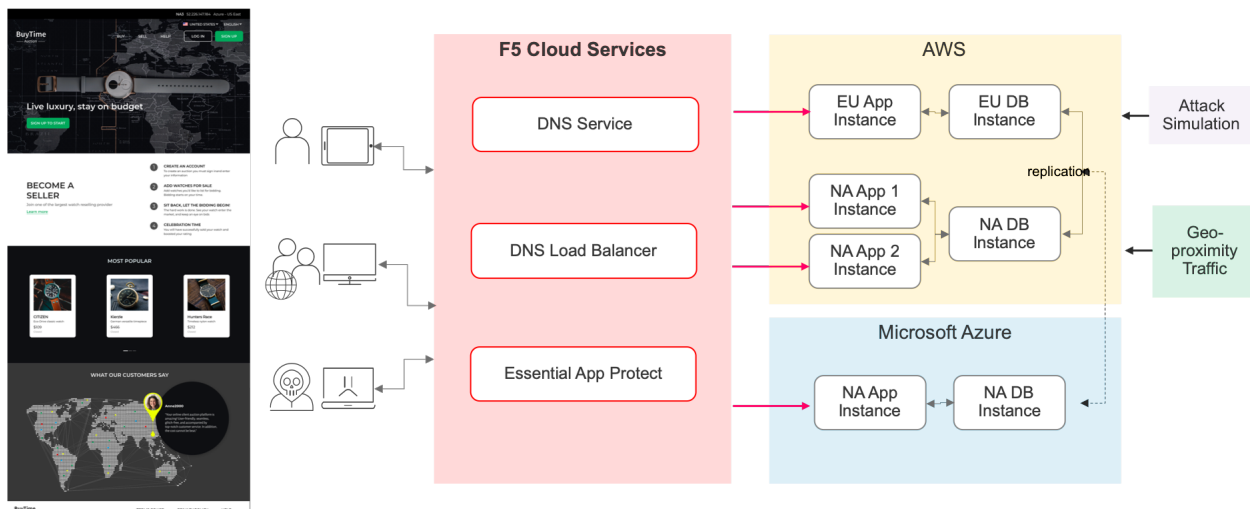
## 7.3.2 2. Application Scenario

In order to fully explore the capabilities of F5 Cloud Services, you will be able to use an existing application with a set of live instances across different clouds and geographic locations. This app is “[BuyTime Auction](#)”, a fictitious multi-instance deployment that helps to simulate a globally deployed app topology. Unsurprisingly, performance, global availability, zero downtime, and security are critical for this application, while the app Developers & DevOps are used to consuming app infrastructure as-a-Service.

The following are the demo application instances, some of which will be utilized in the scope of this lab:

Name	Geography	Cloud/Region	IP	URI
NA1	North America	AWS - US East (N. Virginia)	34.229.48.248	<a href="http://na1-auction.cloudservicesdemo.net/">http://na1-auction.cloudservicesdemo.net/</a>
NA2	North America	AWS – US East (N. Virginia)	318.232.64.254	<a href="http://na2-auction.cloudservicesdemo.net/">http://na2-auction.cloudservicesdemo.net/</a>
NA3	North America	Azure – US East	13.82.106.211	<a href="http://na3-auction.cloudservicesdemo.net/">http://na3-auction.cloudservicesdemo.net/</a>
EU	Europe	AWS – Europe (Frankfurt)	3.122.191.227	<a href="http://eu-auction.cloudservicesdemo.net/">http://eu-auction.cloudservicesdemo.net/</a>

The following diagram is a simplified architecture of the Auction application:



## 7.4 Lab Environment Setup / Validation

### 7.4.1 1. F5 Cloud Services Portal

#### a) Login

In order to use F5 Cloud Services, you need to be logged in with a valid user account. If you need to sign up, or if you already have one, proceed to the [F5 Cloud Services portal](#).

Once you’ve logged in with an account, you will be using the user name and password values in the lab to authenticate with the F5 Cloud Services and the API.

#### b) Subscribe to Catalogs

In order to access specific F5 Cloud Services, you need to subscribe to the corresponding service catalogs.

## LOG IN

Email

Password
Show

Log In

Forgot your password?

Don't have an account yet? [Create One!](#)Or if you prefer to use your AWS account, start at [AWS Marketplace](#)

DELIVER EVERY APP.  
ANYWHERE.  
WITH CONFIDENCE.

Copyright F5 Networks, Inc. All Rights Reserved. [F5 Cloud Services Legal](#) | [Privacy](#) | [Trademarks](#)

1. Click on the **Your F5 Cloud** tab in the left navigation panel and you will see the available service catalogs, as well as the services you have subscribed to, if any. For this lab you will need to click **Subscribe** to **DNS** and **DNS Load Balancer** services.



R&amp;R



## NO SUBSCRIBED SERVICES.

To get started, subscribe to one of the available services below.



Users

1

Active in this service

## ADD F5 CLOUD SERVICES



## DNS

Map and manage your domains and zone files with secondary authoritative DNS.

[See pricing information](#)

Available

[Subscribe](#)

## DNS Load Balancer

Load balance your traffic across servers and regions.

[See pricing information](#)

Available

[Subscribe](#)

## Essential App Protect

Secure your apps and protect your assets.

[See pricing information](#)

Available

[Try it free \(10 days\)](#)

## Beacon

Gain full visibility and insights across your application landscape.

[See pricing information](#)

Available

[Subscribe](#)

## Bot Protect

Manage your bot traffic and secure your apps from malicious bots.

Available

[Start free preview](#)

## NEED SUPPORT?



## F5 Cloud Services Support

For technical assistance and other questions please visit our [support pages](#).

## Looking for API documentation?

To get help with portal services, hit the "Help" button in the masthead above. To learn about our API, read the [API Reference](#) or [API Guidelines](#).

## Don't forget to whitelist us!

Add F5 Cloud services IP addresses to your DNS provider whitelist if you're using us as secondary DNS. [Here's the list](#).

## Legal Terms and Policies

Review the terms of your subscription, privacy policy, and relevant [F5 legal documents](#).If you have feedback, suggestions, or feature requests, [send us an email](#). We want to hear from you!

## Take our 5-minute survey!

Let us know how the portal is working for you and how we can make it better. [Start the survey here](#).

## Found a bug?

Tell us about it [here](#) so we can fix it.

2. For the purposes of the lab you can utilize the Free Tier for both the DNS and DNS Load Balancer services. **NOTE:** you will be asked to add your payment card even for the free tier, however you will not be charged if you follow the Free Tier guidelines outlined here:

- [F5 DNS Cloud Service Pricing](#)
- [F5 DNS Load Balancer Service Pricing](#)

Should you decide to add additional zones or LBR records beyond the Free Tier, you will only pay for what you use.

You may also choose to not use a credit card, and instead subscribe through **AWS Marketplace**.

- [AWS Marketplace: F5 DNS Cloud Service](#)
- [AWS Marketplace: F5 DNS Load Balancer Service](#)

**SUBSCRIBE TO DNS SERVICE?** ×

- Standard service pricing applies.
- A valid payment method must be present and will be charged for applicable usage at the end of each billing period
- Unsubscribe from the service at any time to cancel.

Use this payment method:

☒ Credit card

☐ Subscribe through AWS Marketplace

Cancel Yes, subscribe now

Add payment card to pay by credit card:

Or initiate the subscription from AWS Marketplace to subscribe through it:

After successfully subscribing, your services will appear in the **Your F5 Cloud** tab. You will also see their current status.

If you need to check your payment information, it is available in the **Accounts** tab, **Payment** section.

## 7.4.2 2. Opera with VPN to Test Geo Services

You will need the Opera browser to test proximity rules we will set later.

Open the Opera browser, click **Settings**, **Advanced**, **Features** and then **Enable VPN**.

## ADD PAYMENT CARD



Card Type



Card Number

Expiration Date (YYYY)

- Select One - ▼

 / 

- Select One - ▼

CW



Cardholder Name

Street Address

City

State/Province/Region

Zip/Postal Code


Country

- Select One - ▼

aws marketplace

Categories ▾ Delivery Methods ▾ Solutions ▾ Migration Mapping Assistant Your Saved List

Partners Sell In AWS Marketplace Amazon Web Services Home Help



## F5 DNS Load Balancer Cloud Service

Sold by: [F5 Networks](#)

Set up global load-balancing across clouds in minutes

Continue to Subscribe

Save to list

Overview

Pricing

Usage

Support

Reviews

### Product Overview

Set-up global load balancing across clouds or on-prem in minutes with F5 DNS Load Balancer Cloud Service. This SaaS offer is built to allow customers to leverage F5's 20+ years of load balancing experience in a pre-configured, cloud native solution that can be provisioned and configured with just a few clicks. You can easily perform intelligent load balancing, geolocation-based routing, and app health checks through an intuitive user interface. Move even faster by automating everything using APIs.

Optimize your app delivery using F5 Cloud Services.

Sold by	F5 Networks
Fulfillment Method	Software as a Service (SaaS)

#### Highlights

- Advanced security:** Protect applications from DNS vectored DDoS attacks
- High availability:** Ensure application performance and availability within minutes of activation
- Location-based routing on a global network:** Clients can be directed to the nearest application instance with geolocation-based load balancing for the best user experience
- Move Faster:** Automate everything across your hybrid app environment through a single API for quick and easy integration into your DevOps toolchain or use the simple, modern web interface.

### Pricing Information


This software is priced along a consumption dimension. Your bill will be determined by the number of units you use. Additional taxes or fees may apply.


CLOUD SERVICES

Help


YOUR F5 CLOUD

YOUR SERVICES - Current status


**DNS**  
**HEALTHY**  
3 Healthy / 0 Degraded

**DNS LOAD BALANCER**  
**HEALTHY**  
2 Healthy / 0 Degraded


ADD F5 CLOUD SERVICES

**DNS**  
Map and manage your domains and zone files with secondary authoritative DNS.  
[See pricing information](#)  

Subscribed Unsubscribe


**DNS Load Balancer**  
Load balance your traffic across servers and regions.  
[See pricing information](#)  


Subscribed Unsubscribe

**Essential App Protect**  
Secure your apps and protect your assets.  
[See pricing information](#)  

Subscribed Unsubscribe

USAGE - Last 90 Days

**TOTAL REQUESTS**  
**4,130**

**TOTAL REQUESTS**  
**7**


**TOTAL ZONES**  
**3**  
3 Active / 0 Inactive


**TOTAL SERVICES**  
**2**  
2 Active / 0 Inactive


ORGANIZATION & USERS


**Users**  
**5**  
Active in this service


NEED SUPPORT?


**F5 Cloud Services Support**  
For technical assistance and other questions please visit our [support pages](#).

**Looking for API documentation?**  
To get help with portal services, hit the "Help" button in the masthead above. To learn about our API, read the [API Reference](#) or [API Guidelines](#).

**Don't forget to whitelist us!**  
Add F5 Cloud services IP addresses to your DNS provider whitelist if you're using us as secondary DNS. [Here's the list](#).

**Legal Terms and Policies**  
Review the terms of your subscription, privacy policy, and [relevant F5 legal documents](#).

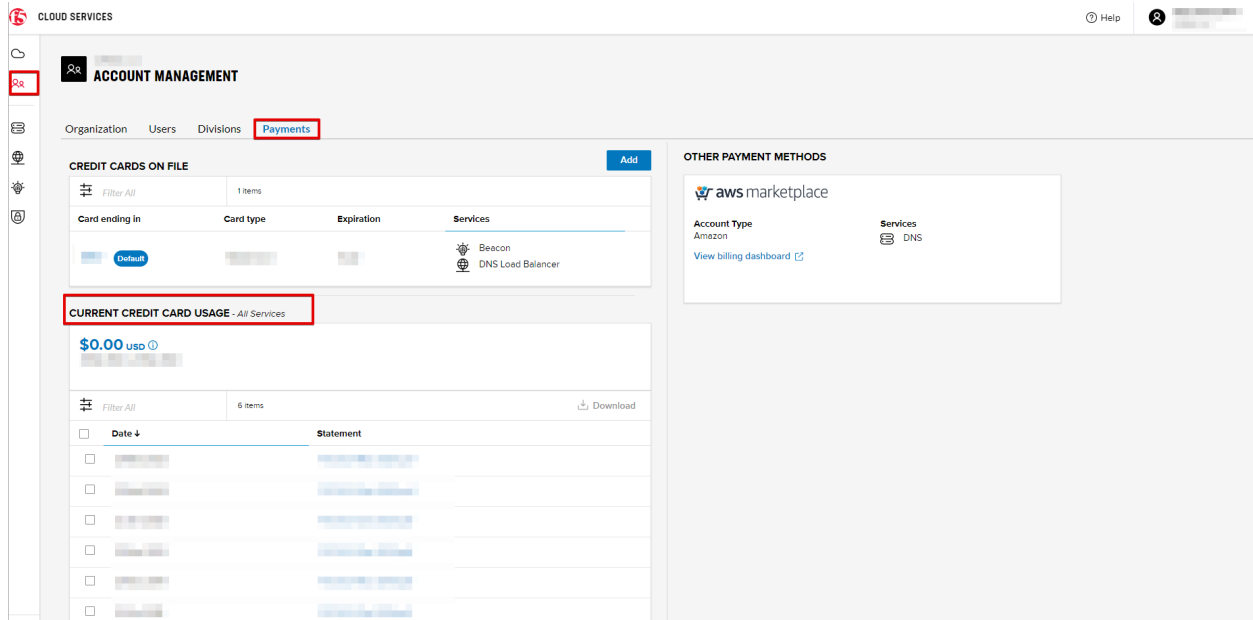
**If you have feedback, suggestions, or feature requests, send us an email.** We want to hear from you!

**Take our 5-minute survey!**  
Let us know how the portal is working for you and

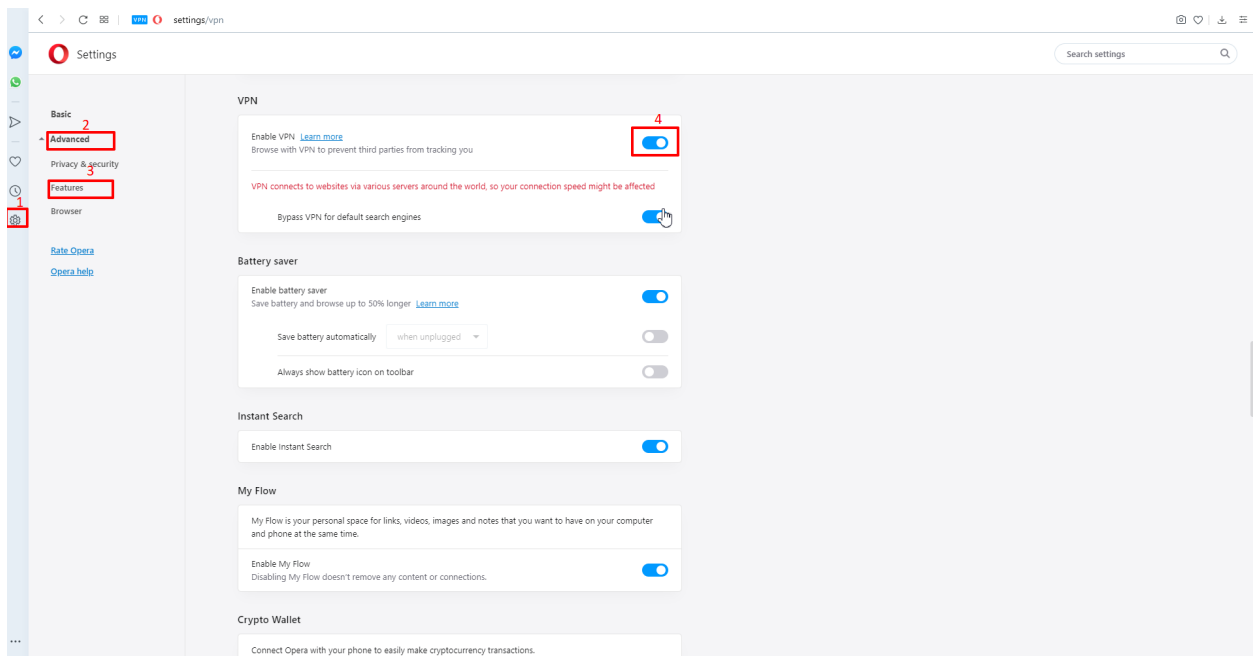
296

Chapter 7. LAB: F5 DNS Cloud Service & F5 DNS Load Balancer Cloud Service





The screenshot shows the AWS Cloud Services Account Management interface. The left sidebar contains navigation icons, with the 'Payments' icon highlighted. The main header shows 'ACCOUNT MANAGEMENT' with tabs for 'Organization', 'Users', 'Divisions', and 'Payments'. The 'Payments' tab is active. The main content area is divided into two sections: 'CREDIT CARDS ON FILE' and 'CURRENT CREDIT CARD USAGE - All Services'. The 'CREDIT CARDS ON FILE' section shows a table with one card ending in '0000', card type 'Default', and services 'Beacon' and 'DNS Load Balancer'. The 'CURRENT CREDIT CARD USAGE - All Services' section shows a balance of '\$0.00 usd'. The right sidebar shows 'OTHER PAYMENT METHODS' with 'aws marketplace' and 'Account Type: Amazon'.

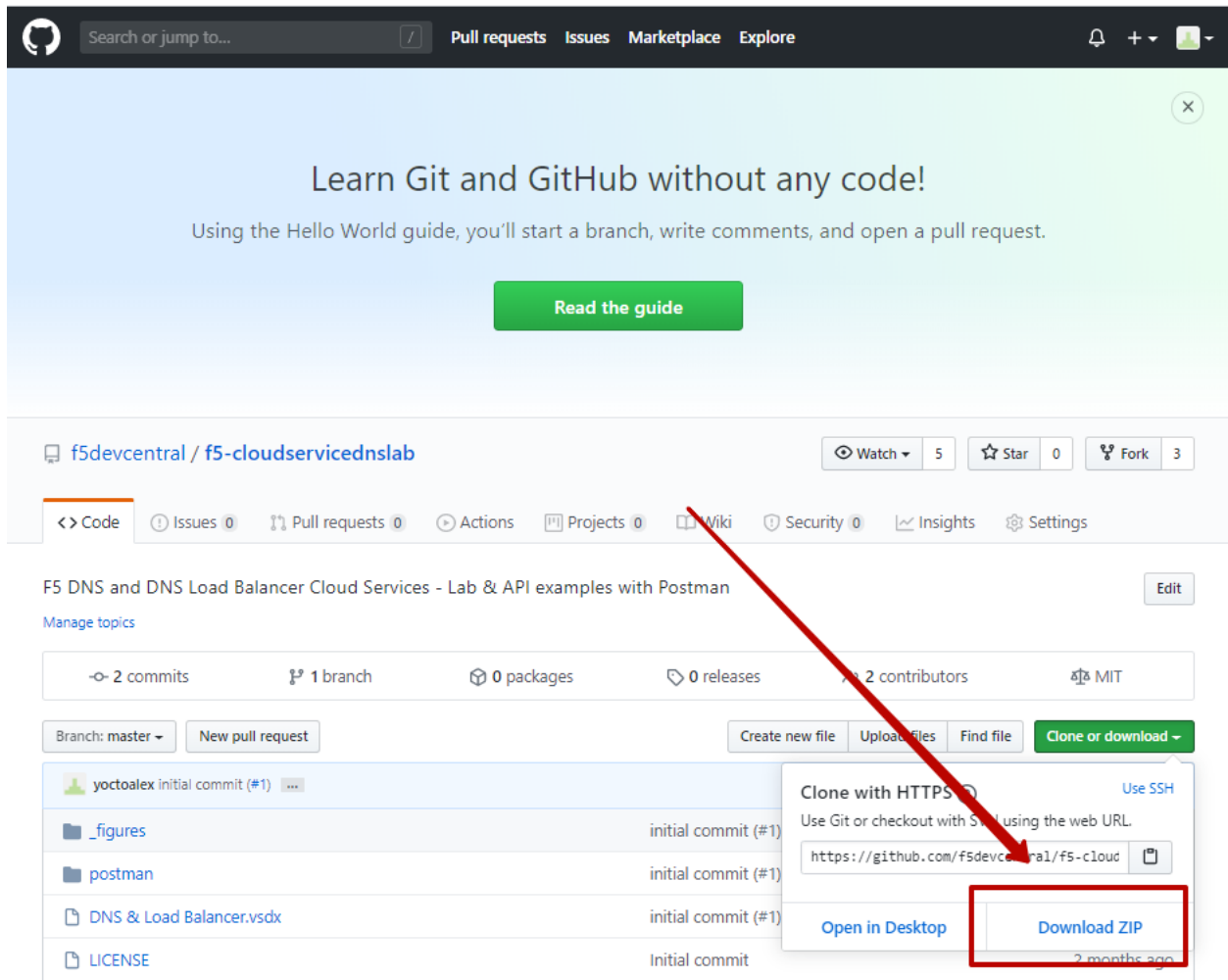


The screenshot shows the Opera Settings application. The left sidebar contains navigation icons, with the 'Settings' icon highlighted. The main header shows 'Settings' with a search bar. The main content area is divided into two sections: 'VPN' and 'Battery saver'. The 'VPN' section has a toggle switch for 'Enable VPN' which is turned on. The 'Battery saver' section has a toggle switch for 'Enable battery saver' which is turned on. The 'Instant Search' section has a toggle switch for 'Enable Instant Search' which is turned on. The 'My Flow' section has a toggle switch for 'Enable My Flow' which is turned on. The 'Crypto Wallet' section has a toggle switch for 'Connect Opera with your phone to easily make cryptocurrency transactions' which is turned on.

### 7.4.3 3. Postman Configuration

a) Download Postman [here](#), open it, create a Postman account if you don't have one and choose to do so, and sign in.

b) Clone or download and extract the repository



c) Import collection – **/postman/F5 Cloud Services DNS LAB.postman\_collection.json** and environment – **/postman/F5 Cloud Services DNS LAB.postman\_environment.json**.

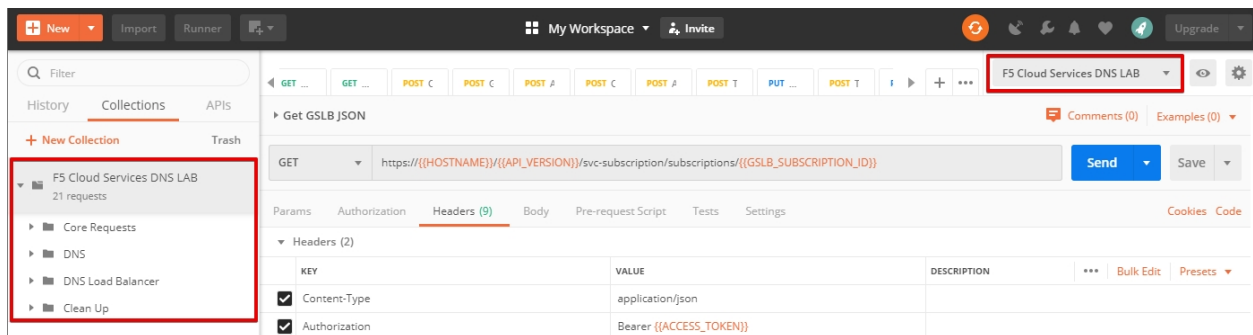
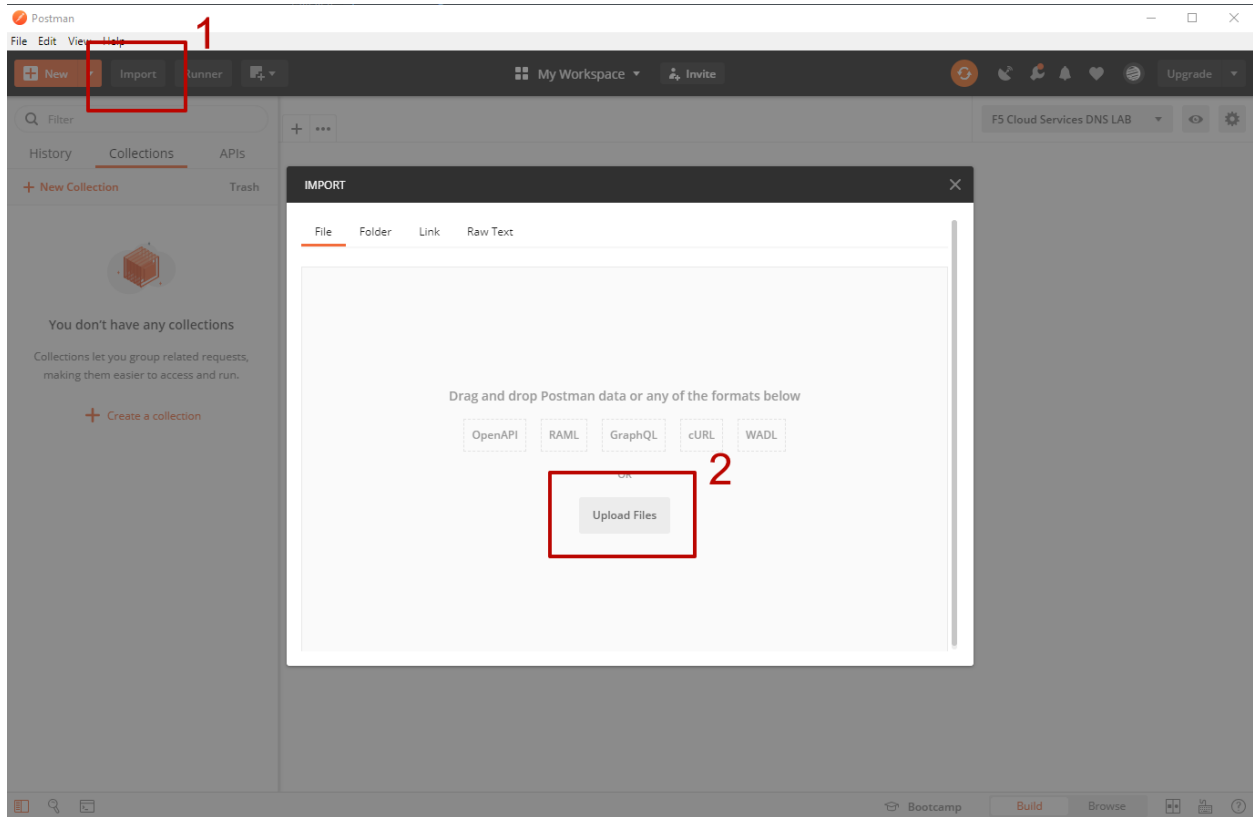
You will now see the imported collection (left side) with the calls that you will be utilizing grouped into several categories, as well as the environment variables (top right) used to store and pass data between Postman and the API.

You are now ready to interface with the F5 Cloud Services using Postman.

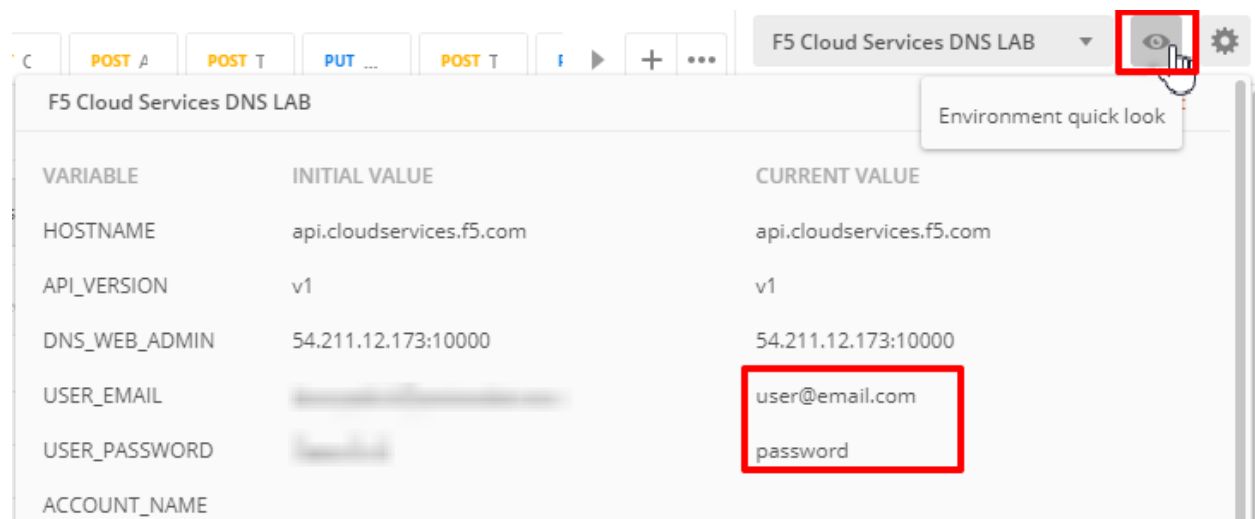
### 7.4.4 4. Zone Name

In order to create secondary DNS zone in the F5 Cloud Services portal, you need to have a zone name. Use Postman and follow the steps below to get the Zone name from the Lab service API.

a) Open the “F5 Cloud Services DNS LAB” environment variables by clicking the “Environment Quick Look”, click into the field of the corresponding variable, and type the value of user email in the variable

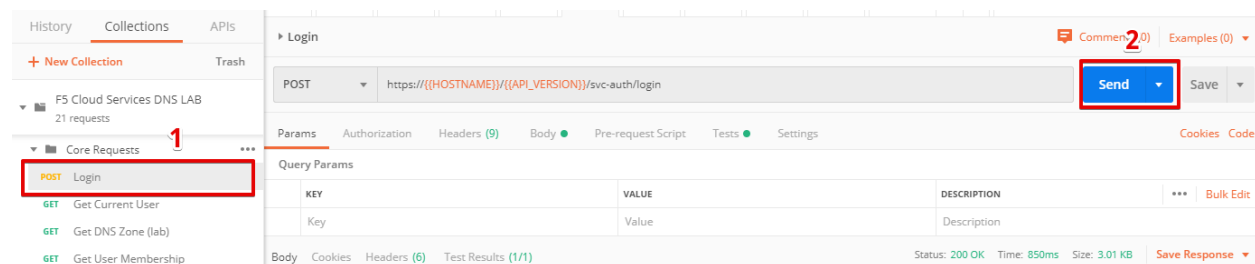


“USER\_EMAIL” (click **Enter** after typing the values).

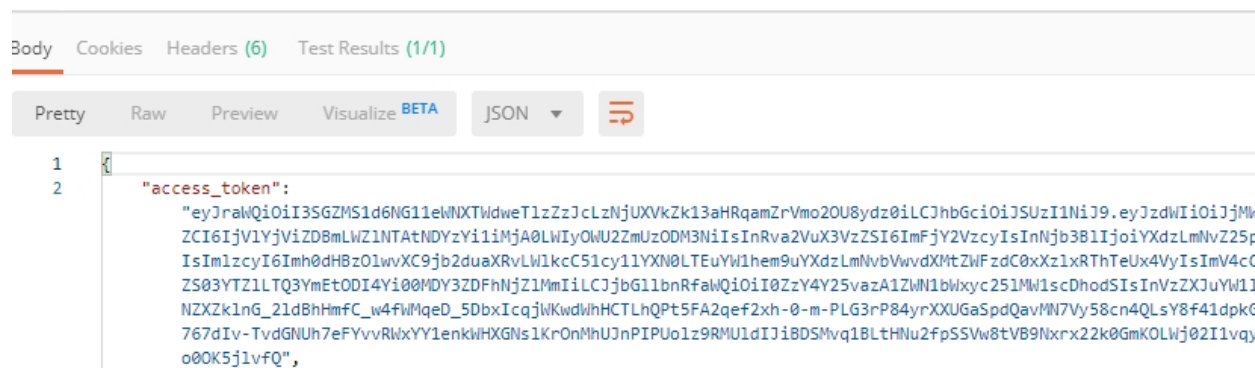


Repeat the same for the "USER\_PASSWORD".

b) Select the **Login** request in the sidebar to login to your F5 Cloud Services profile and click **Send** to get the authorization token. More detailed information on this API request can be found [here](#).



A successful login will result in Postman returning the tokens from the API, shown in the response body below:



These tokens are then stored for subsequent calls using a function inside Postman to set environment variables. You can see the test function in the **Tests** tab:

**NOTE:** If any of the subsequent Postman calls return a blank response or “**status**”: “**unauthorized**” response (see the screenshot below), it means your user token has expired and you will need to re-login. To do that you just need to re-send the **Login** request.

The screenshot shows a REST client interface with a POST request to `https://{{HOSTNAME}}/{{API_VERSION}}/svc-auth/login`. The **Tests** tab is active, displaying a test script:

```
1 pm.test("Set token variable", function() {
2   var jsonData = pm.response.json();
3   pm.environment.set("ACCESS_TOKEN", jsonData.access_token);
4 })
5
```

The **Body** tab is also active, showing the response in JSON format:

```
1 {
2   "status": "unauthorized",
3   "message": "access denied"
4 }
```

#### c) OPTIONAL: Set User ID & Account Info

**IMPORTANT NOTE:** If you originally signed up for F5 Cloud Services through a Limited User invitation (such as an email invite from another lab or from a different account owner), then it is possible that you haven't yet completed a full registration. You can quickly tell if you have by looking at your account(s) in the [F5 Cloud Services Portal](#). If you do now see any "Accounts you own:" and only see "Accounts you've been granted access to" as a **"Limited User"**, then you need to create a full account & update user info before you can proceed with this lab.

You can do this by running the following **Set User Info** API call, after you've updated the Body of the request with your own organization & address information:

The response returns the following detail, including your own organization account ID (id):

More information on this API request can be found [here](#).

At this point you should be a full user with an "Owned Account" and a primary organization account id, which can also be confirmed in the [F5 Cloud Services Portal](#) in the drop-down under your user name (top right), where you should see "Accounts you own:" and the Organization Account you created with **"Owner"** defined.

#### d) Retrieve User ID & Account ID

Select the **Get Current User** request and click **Send** to retrieve User ID and Account ID to be used in the further requests.

The response returns the following detail:

The retrieved User ID and Account ID are then stored for subsequent calls.

More detailed information on this API request can be found [here](#).

e) Let's now retrieve DNS Zone Name with the **Get DNS Zone (lab)** API call. Click **Send**. This call will pass your "ACCESS\_TOKEN" in the header of the request to the Labs API in order to validate existence of your F5 account & return back a Zone name unique to your lab.

► Set User Info (optional)


POST ▼ https://{{HOSTNAME}}/{{API\_VERSION}}/svc-account/accounts

Params Authorization Headers (10) **Body** ● Pre-request Script Tests ● Settings

● none ● form-data ● x-www-form-urlencoded ● **raw** ● binary ● GraphQL **JSON** ▼

```
1 {  
2   "name": "Demo Account",  
3   "address": {  
4     "street_1": "801 5th Ave",  
5     "city": "Seattle",  
6     "state": "WA",  
7     "postal_code": "98104",  
8     "country": "US"  
9   }  
10 }
```

Body Cookies Headers (6) Test Results (1/1)

Pretty Raw Preview Visualize JSON ▼ 


```
1 {  
2   "id": "a-aaDYQhrBca",  
3   "name": "Demo Account",  
4   "parent_account_id": "",  
5   "status": "active",  
6   "level": "0",  
7   "signup_provider": "standard",  
8   "address": {  
9     "street_1": "801 5th Ave",  
10    "street_2": "",  
11    "city": "Seattle",  
12    "state": "WA",  
13    "country": "US",  
14    "postal_code": "98104-1663"  
}
```

GET ▼ https://{{HOSTNAME}}/{{API\_VERSION}}/svc-account/user


Params Authorization Headers (8) **Body** Pre-request Script Tests ● Settings

▼ Headers (1)

	KEY	VALUE
<input checked="" type="checkbox"/>	Authorization	Bearer {{ACCESS_TOKEN}}
	Key	Value

► Temporary Headers (7) 


Body Cookies Headers (6) Test Results (1/1)


Pretty Raw Preview Visualize BETA JSON 

```

1  {
2    "id": " ",
3    "email": " ",
4    "first_name": " ",
5    "last_name": " ",
6    "phone": "",
7    "primary_account_id": " ":,
8    "status": "active",
9    "email_confirmed": true,
10   "phone_confirmed": false,
11   "unconfirmed_email": "",
12   "time_zone": "",
13   "preferred_language": "",
14   "user_email_history": [],
15   "current_password": "",
16   "create_time": "2019-07-22T14:54:39.998412Z",
17   "update_time": "2019-07-22T14:54:39.998412Z",
18   "activate_time": null,
19   "delete_time": null,
20   "reset_password_sent_time": null,
21   "reset_password_time": null,
22   "email_confirmation_sent_time": "2019-07-22T14:54:57.906915Z",
23   "email_confirmation_time": "2019-07-22T14:54:57.906915Z",
24   "phone_confirmation_sent_time": null,
25   "phone_confirmation_time": null
  }

```

GET  https://{{HOSTNAME}}/{{API\_VERSION}}/svc-account/user

Params Authorization Headers (8) Body Pre-request Script Tests  Settings

```

1  pm.test("Set account_id and user_id variables", function() {
2    var jsonData = pm.response.json();
3    pm.environment.set("ACCOUNT_ID", jsonData.primary_account_id);
4    pm.environment.set("USER_ID", jsonData.id);
5  })
6

```

Request:

GEThttp://{{DNS\_WEB\_ADMIN}}/zone

Params

Authorization

Headers (2)

Body

Pre-request Script

Tests

Settings

▼ Headers (2)

	KEY	VALUE
<input checked="" type="checkbox"/>	Content-Type	application/json
<input checked="" type="checkbox"/>	Authorization	Bearer {{ACCESS_TOKEN}}

The response will return your test DNS zone name and the status.

Body	Cookies	Headers (6)	Test Results (1/1)	Status: 200 OK
Pretty Raw Preview Visualize JSON ▼				
1	{			
2	"status": "ok",			
3	"zone": "user-n1h0si.securelab.online",			
4	"zone2": "user-n1h0si-2.securelab.online"			
5	}			

Sending this request will automatically capture of the Zone variables:

GET

▼

http://{{DNS\_WEB\_ADMIN}}/zone

Params

Authorization

Headers (9)

Body

Pre-request Script

Tests ●

Settings

1

2

3

4

5

```
pm.test("Get User's DNS Zone Name", function() {  
    var jsonData = pm.response.json();  
    pm.environment.set("ZONE_NAME", jsonData.zone);  
})
```

This Zone Name will be used for creating Secondary DNS Zone in the F5 Cloud Services portal, as well as throughout the lab as the domain name for your test applications.

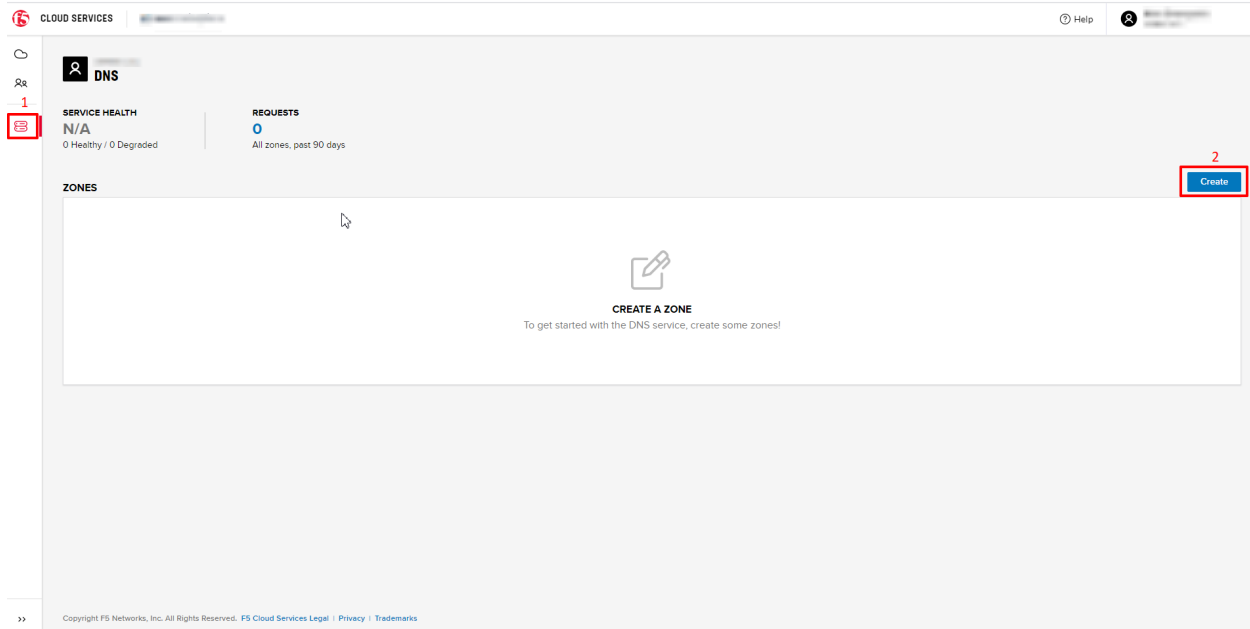
## 7.5 F5 DNS Cloud Service - UI

### 7.5.1 1. Create Secondary DNS Zone

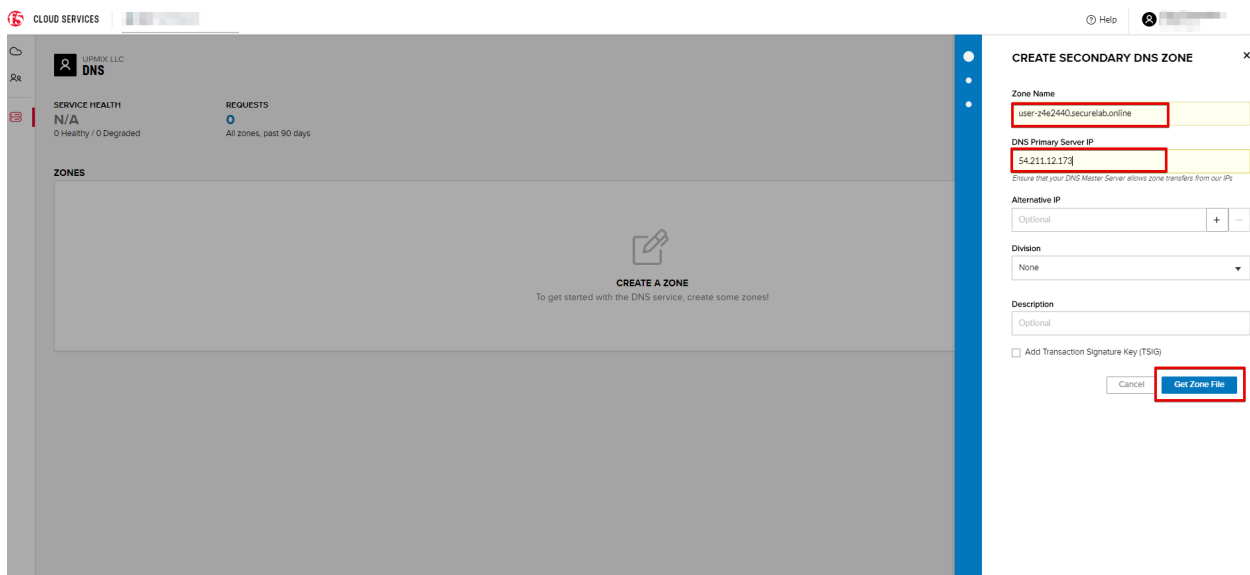
Let's now return to the F5 Cloud Services portal and create Secondary DNS Zone using the UI. We will repeat the same flow through the API in the subsequent section.

a) Go to the **DNS** tab and click **Create**.





b) Paste **Zone name** retrieved in step 4.e) above and indicate the following DNS IP: **54.211.12.173** as the DNS Primary Server IP. Other values are optional. Then click **Get Zone File**.



c) This will retrieve the zone file from your primary DNS server. Click **Deploy** and then **Done**. This will create Secondary DNS Zone.

## 7.5.2 2. Query via Browser

Let's now see how the created Secondary DNS works.

a) Click on your zone in the **DNS** tab and scroll down to see **ZONE FILE**, where you need to copy "na1-auction.user-your\_zone\_name".

b) Paste the address into your browser and you'll get to the website:

CLOUD SERVICES

UPMXX, LLC

DNS

SERVICE HEALTH

HEALTHY

2 Healthy / 0 Degraded

REQUESTS

178

All zones, past 90 days

ZONES

Filter All

3 items

Zone Name	Health	Primary IP	Division	Last Updated
user-3e95yl.securelab.online	Healthy	54.211.12.173		Jan 31, 2020 / 10:47
user-n1h0sl.securelab.online	N/A	54.211.12.173		Feb 13, 2020 / 10:51
user-z4e2440.securelab.online	Healthy	54.211.12.173		Feb 7, 2020 / 16:26

Help

Alex Shemyakin

UPMXX, LLC

Zone File

A copy of the raw zone file is displayed below for your verification

```

user-n1h0sl.securelab.online. 30 IN SOA ns1.user-
n1h0sl.securelab.online. info user-n1h0sl.securelab.online.
2020010101 30 30 30 30
user-n1h0sl.securelab.online. 30 IN NS
ns1.f5cloudservices.com
user-n1h0sl.securelab.online. 30 IN NS
ns2.f5cloudservices.com
auction.user-n1h0sl.securelab.online. 30 IN NS
ns91.dns.cloudservices.f5.com.
eu-auction.user-n1h0sl.securelab.online. 30 IN A
3.122.191.227
ns3-auction.user-n1h0sl.securelab.online. 30 IN A
34.229.48.248
ns3-auction.user-n1h0sl.securelab.online. 30 IN A
52.226.147.184
ns1.user-n1h0sl.securelab.online. 30 IN A
54.211.12.173
user-n1h0sl.securelab.online. 30 IN SOA ns1.user-
n1h0sl.securelab.online. info user-n1h0sl.securelab.online.
2020010101 30 30 30 30

```

Back

Cancel

Deploy

CLOUD SERVICES

Help

ZONE PROPERTIES

Name and location of your zone file.

Zone Name

user-z4e2440.securelab.online

Description

Optional

DNS Primary Server IP

54.211.12.173

Add Transaction Signature Key (TSIG)

Alternative IP

Optional

+

-

Division

None

ZONE FILE

Here is the zone file we're using.

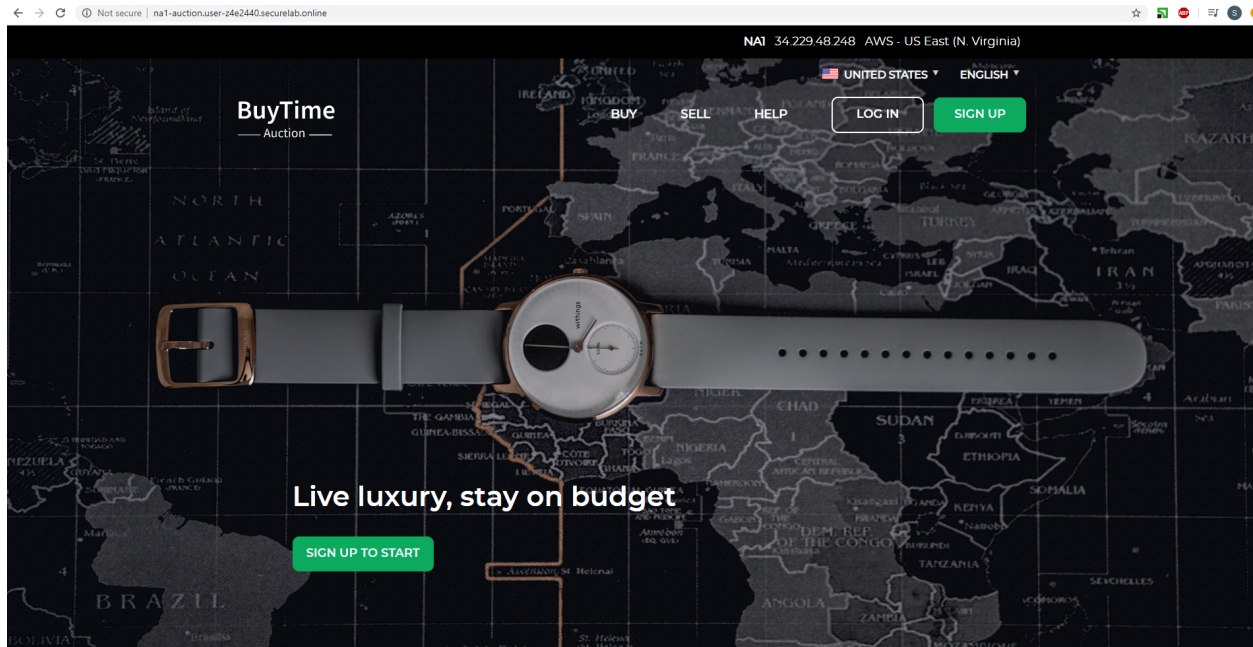
```

user-z4e2440.securelab.online. 10 IN SOA 8180256742b8.info user-z4e2440.securelab.online. 2020020537 10 10 10 10
user-z4e2440.securelab.online. 10 IN NS ns1.f5cloudservices.com.
user-z4e2440.securelab.online. 10 IN NS ns2.f5cloudservices.com.
auction.user-z4e2440.securelab.online. 10 IN NS ns91.dns.cloudservices.f5.com.
eu-auction.user-z4e2440.securelab.online. 10 IN A 3.122.191.227
ns1-auction.user-z4e2440.securelab.online. 10 IN A 34.229.48.248
ns3-auction.user-z4e2440.securelab.online. 10 IN A 52.226.147.184
ns3-auction.user-z4e2440.securelab.online. 10 IN CNAME waf-aa5ckbg1x.waf.prd.f5aas.com.
user-z4e2440.securelab.online. 10 IN SOA 8180256742b8.info user-z4e2440.securelab.online. 2020020537 10 10 10 10

```

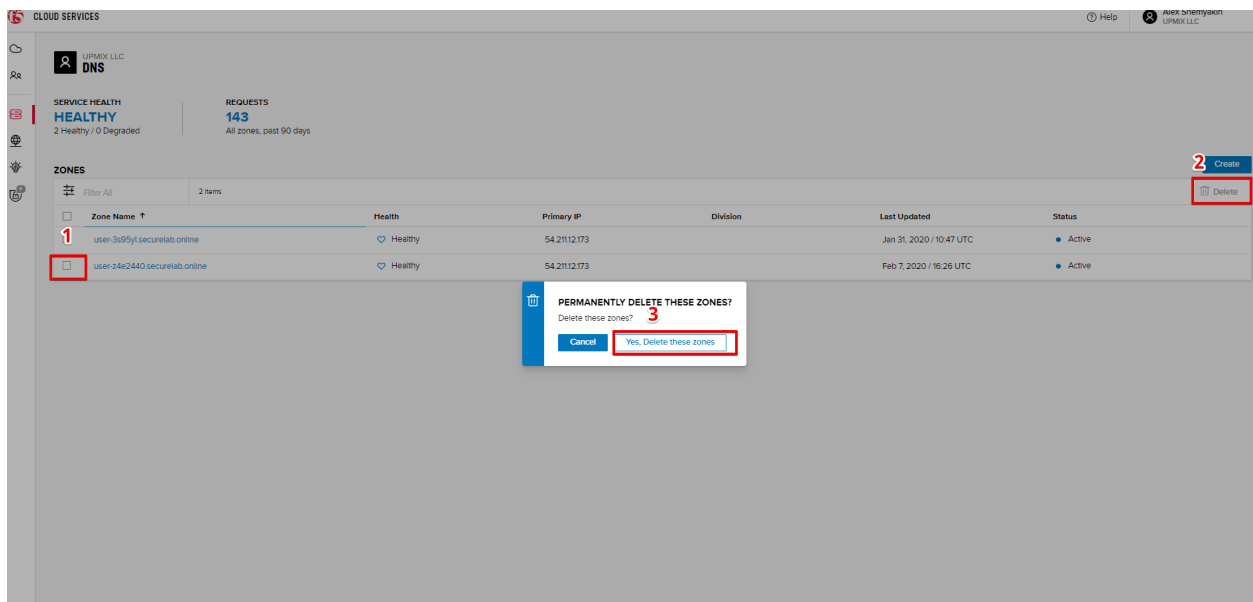
306

Chapter 7. LAB: F5 DNS Cloud Service & F5 DNS Load Balancer Cloud Service



### 7.5.3 3. Delete Zone

In case you need to delete the zone, tick your zone, click **Delete** and then confirm your choice.



## 7.6 F5 DNS Cloud Service - API

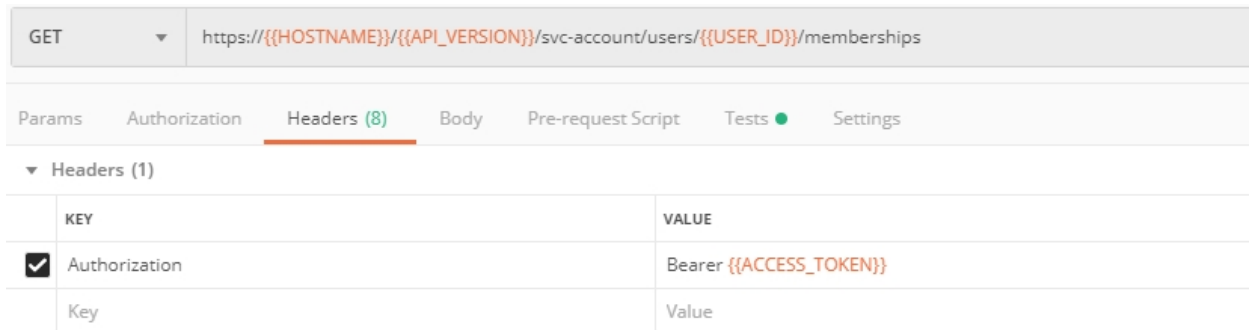
In this section we will repeat the flow of the preceding section by using the F5 Cloud Services APIs with the help of Postman.

## 7.6.1 1. Create Zone

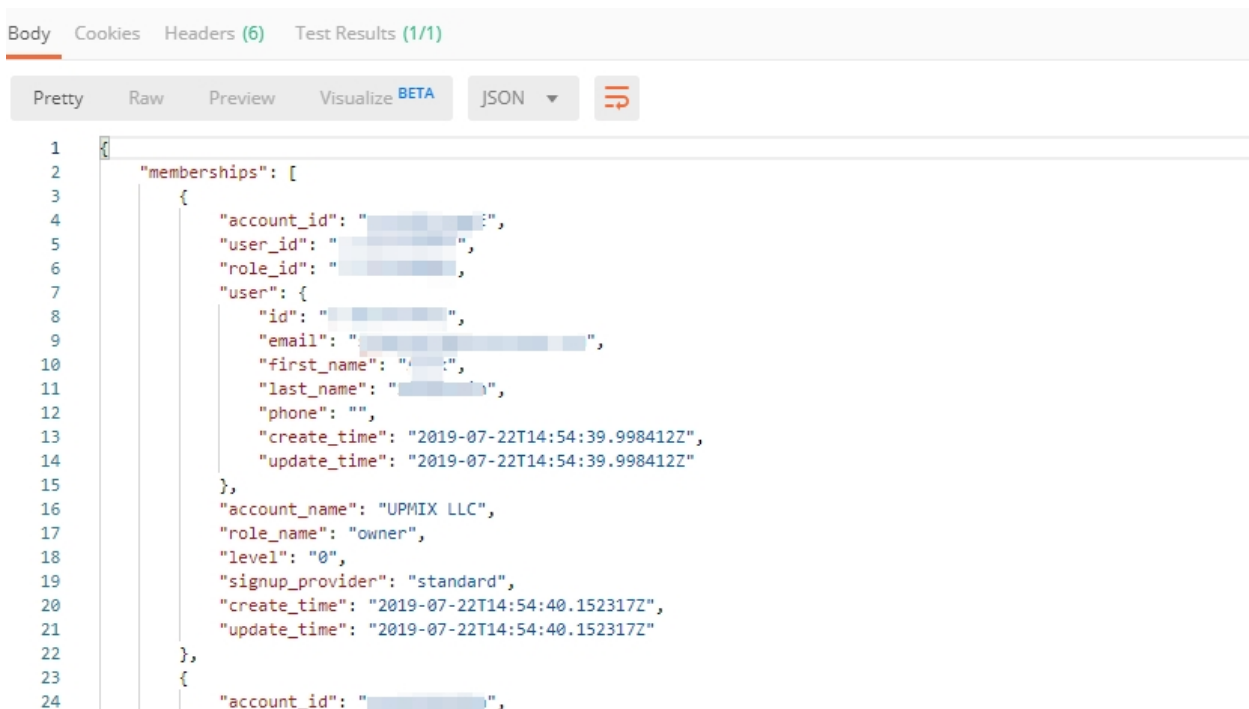
In order to create your zone using API, you will first need to get your account details - membership and catalogs.

a) Get User Membership to F5 Cloud Services accounts

In Postman, send the **Get User Membership** request which returns info on your user's access to Cloud Services accounts.



You will see account ids, names, roles and other information in the body of response.



Your "account\_id" will be retrieved using "account\_name" and used for creating user's instances.

More detailed information on this API request can be found [here](#).

b) Retrieve information on available catalogs and their IDs

Select the **Get Catalogs** request and click **Send** to retrieve data about the available Catalogs and their IDs.

As you see there are a number of catalogs available:

The retrieved IDs are then stored for subsequent calls using a function inside Postman to set environment variables. You can see the test function in the **Tests** tab:

GET ▼ `https://{{HOSTNAME}}/{{API_VERSION}}/svc-account/users/{{USER_ID}}/memberships`

Params Authorization Headers (8) Body Pre-request Script Tests ● Settings

```

1 pm.test("Switch account", function() {
2   var jsonData = pm.response.json();
3   for(var i=0; i<jsonData.memberships.length; i++) {
4     if (jsonData.memberships[i].account_name === "{{ACCOUNT_NAME}}") {
5       pm.environment.set("ACCOUNT_ID", jsonData.memberships[i].account_id);
6     }
7   }
8 })

```

GET ▼ `https://{{HOSTNAME}}/{{API_VERSION}}/svc-catalog/catalogs`

Params Authorization Headers (8) Body Pre-request Script Tests ● Settings

▼ Headers (1)

KEY	VALUE
<input checked="" type="checkbox"/> Authorization	Bearer <code>{{ACCESS_TOKEN}}</code>
Key	Value

► Temporary Headers (7) ⓘ

Body Cookies Headers (6) Test Results (1/1)

Pretty Raw Preview Visualize BETA JSON ▼ ≡

```

/1      ],
72      "create_time": "2019-07-22T21:21:49.494932Z",
73      "update_time": "2019-07-22T21:21:49.494932Z",
74      "delete_time": null,
75      "preview_end_time": null
76    },
77    {
78      "catalog_id": "c-aaQn0rPjGu",
79      "name": "DNS Load Balancer",
80      "description": "Load balance your traffic across servers and regions.",
81      "status": "STATUS_ACTIVE",
82      "logo_url": "https://staging-ui.srv.f5aas.com/static/media/logo.6a1ab75a.svg",
83      "info_url": "https://www.f5.com/products/ways-to-deploy/cloud-services/dns-load-balancer-cloud-service",
84      "service_type": "gslb",
85      "deleted": false,
86      "preview": false,
87      "providers": [
88        {
89          "name": "aws",
90          "preview": false,
91          "status": "STATUS_ACTIVE",
92          "info_url": "https://aws.amazon.com/marketplace/pp/B07W3P8HM4",

```

```

1 pm.test("Set Catalog variables", function() {
2   var jsonData = pm.response.json();
3   for(var i=0; i<jsonData.Catalogs.length; i++) {
4     if (jsonData.Catalogs[i].service_type === "waf") {
5       pm.environment.set("WAF_CATALOG_ID", jsonData.Catalogs[i].catalog_id);
6     }
7
8     if (jsonData.Catalogs[i].service_type === "adns") {
9       pm.environment.set("DNS_CATALOG_ID", jsonData.Catalogs[i].catalog_id);
10    }
11
12    if (jsonData.Catalogs[i].service_type === "gslb") {
13      pm.environment.set("GSLB_CATALOG_ID", jsonData.Catalogs[i].catalog_id);
14    }
15  }

```

More detailed information on this API request can be found [here](#).

c) Select the **Create DNS Subscription** request and click **Send** to create a new service instance of Secondary Authoritative DNS using “account\_id” and “catalog\_id” retrieved a few steps above.

```

1 {
2   "account_id": "{{ACCOUNT_ID}}",
3   "catalog_id": "{{DNS_CATALOG_ID}}",
4   "service_instance_name": "{{ZONE_NAME}}",
5   "configuration": {
6     "adns_service": {
7       "zone": "{{ZONE_NAME}}",
8       "master_servers": [
9         "54.211.12.173"
10      ]
11    }
12  },
13   "service_type": "adns"
14 }

```

You will see “subscription\_id” and created “service\_instance\_id” in the body.

The retrieved “subscription\_id” is then stored for subsequent calls.

You can change its status from “DISABLED” to “ACTIVE” sending the **Activate DNS Subscription** request below. More detailed information on this API request can be found [here](#).

d) Select the **Activate DNS Subscription** request and click **Send**. This will deploy the secondary DNS using “subscription\_id” captured in one of the steps above.

You will see “active” subscription status.

Note that it takes some time to deploy the service, so you can just re-send the same request after a few minutes to see “service\_state”: “DEPLOYED”.

More detailed information on this API request can be found [here](#).

Body Cookies Headers (6) Test Results (1/1)

```

1 {
2   "subscription_id": " ",
3   "account_id": " ",
4   "user_id": " ",
5   "catalog_id": "c-aax8Jkfg8u",
6   "service_instance_id": " ",
7   "status": "DISABLED",
8   "service_instance_name": "user-z4e2440.securelab.online",
9   "deleted": false,
10  "service_type": "adns",
11  "configuration": {
12    "adns_service": {
13      "master_servers": [
14        "54.211.12.173"
15      ],
16      "zone": " "
17    },
18    "nameservers": [
19      {
20        "ipv4": " ",
21        "ipv6": " ",
22        "name": " "
23      },
24      {
25        "ipv4": " "

```

POST https://{{HOSTNAME}}/{{API\_VERSION}}/svc-subscription/subscriptions

Params Authorization Headers (10) Body Pre-request Script Tests Settings

```

1 pm.test("Set DNS subscription id variable", function() {
2   var jsonData = pm.response.json();
3   pm.environment.set("DNS_SUBSCRIPTION_ID", jsonData.subscription_id);
4 })
5

```

POST https://{{HOSTNAME}}/{{API\_VERSION}}/svc-subscription/subscriptions/{{DNS\_SUBSCRIPTION\_ID}}/activate

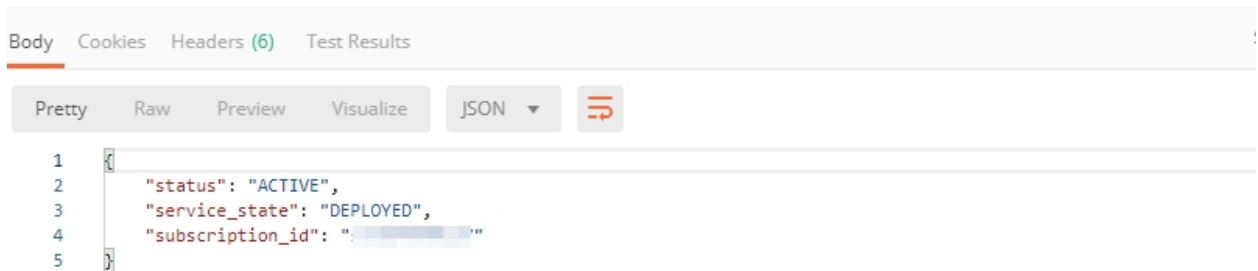
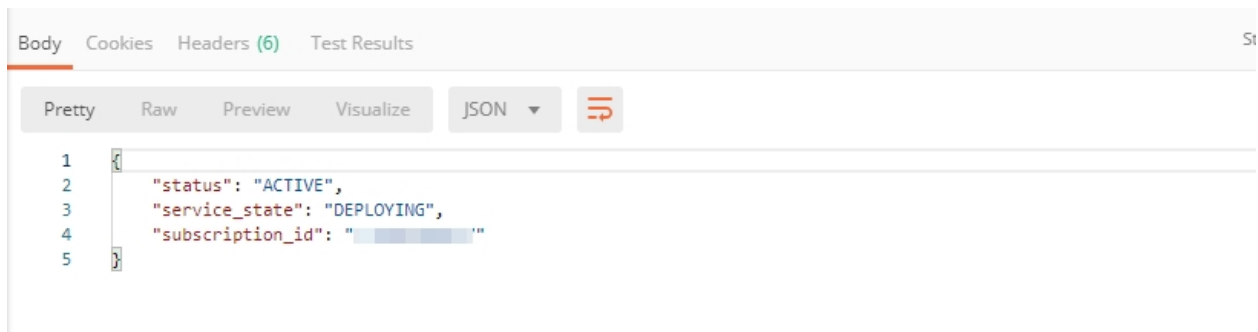
Params Authorization Headers (10) Body Pre-request Script Tests Settings

☐ none
☐ form-data
☐ x-www-form-urlencoded
☒ raw
☐ binary
☐ GraphQL BETA
JSON

```

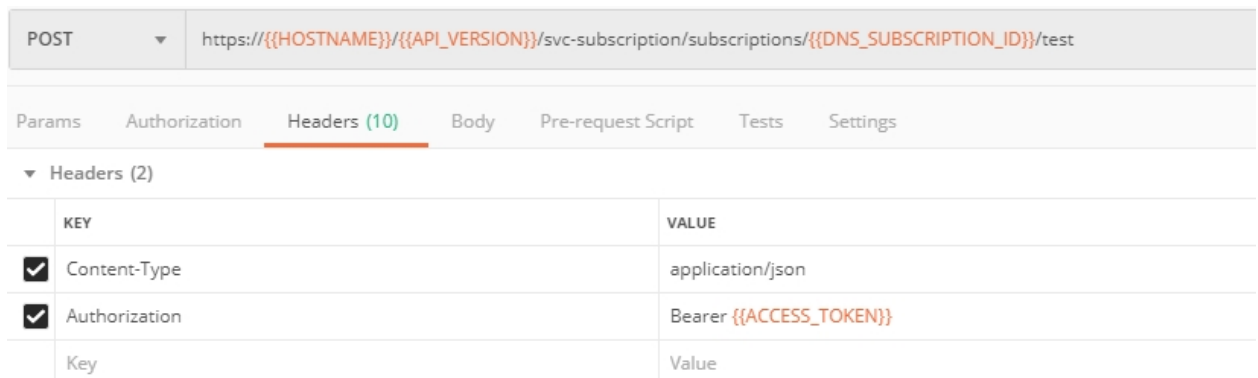
1 {
2   "subscription_id": "{{DNS_SUBSCRIPTION_ID}}",
3   "omit_config": true
4 }

```



### 7.6.2 2. Get Zone File

Send the **Get DNS Subscription Zones** request which uses DNS “subscription\_id” created a few steps above. This will retrieve a zone file from your primary DNS server.



As a result, you will get the zone file describing your DNS zone and containing mappings between domain names and IP addresses.

### 7.6.3 3. Query via Browser

Let's now check the created DNS service via browser.

a) Copy NA1 address from the Zone file retrieved in the step above:

b) Paste the copied address into your browser and you will get to the created secondary DNS instance:



Body Cookies Headers (6) Test Results Status: 200 OK Time: 186ms

Pretty Raw Preview Visualize JSON ↺

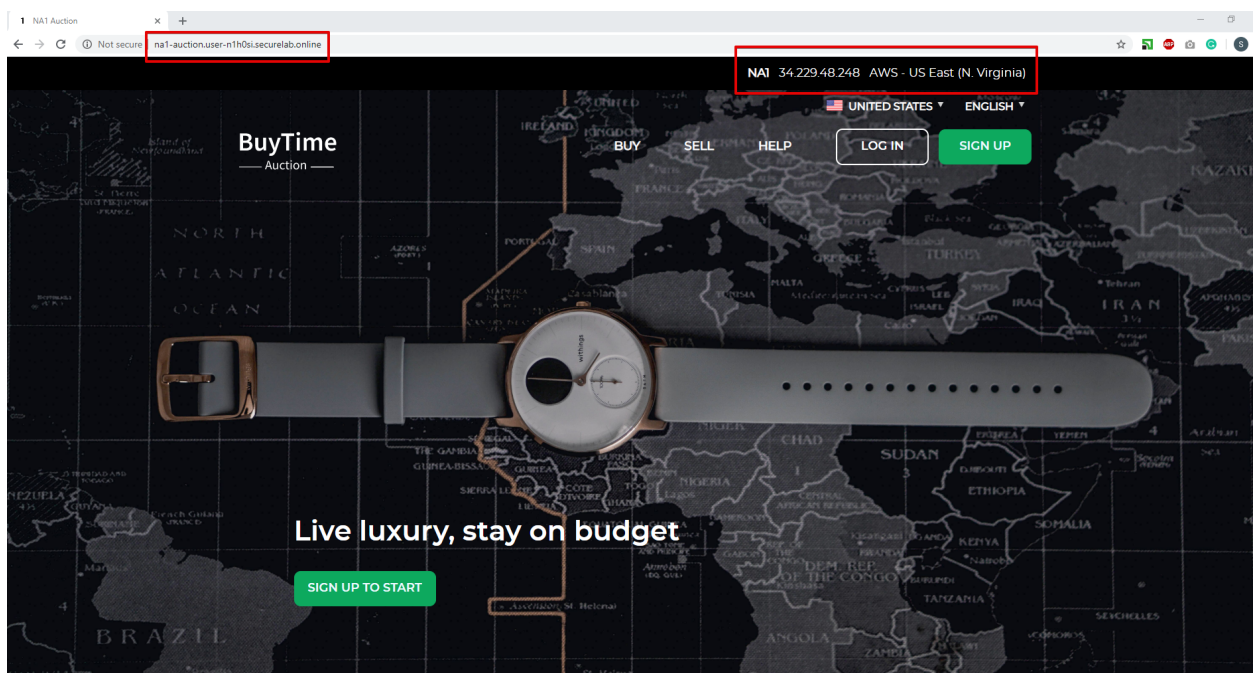
```
1 {
2   "configuration": {
3     "zone_field": "user-n1h0si.securelab.online.\t30\tIN\tSOA\tns1.user-n1h0si.securelab.online. info.user-n1h
      2020021809 30 30 30
      30\tuser-n1h0si.securelab.online.\t30\tIN\tNS\tns1.f5cloudservices.com.\tuser-n1h0si.securelab.online.
      f5cloudservices.com.\tnauction.user-n1h0si.securelab.online.\t30\tIN\tNS\tns91.dns.cloudservices.f5.com
      securelab.online.\t30\tIN\tA\t3.122.191.227\tna1-auction.user-n1h0si.securelab.online.\t30\tIN\tA\t34.
      user-n1h0si.securelab.online.\t30\tIN\tCNAME\twaf-aagr4igerk.waf.prd.f5aas.com.\tna3-auction.user-n1h0
      \t30\tIN\tA\t52.226.147.184\tnns1.user-n1h0si.securelab.online.\t30\tIN\tA\t54.211.12.173\tuser-n1h0si.
      \t30\tIN\tSOA\tns1.user-n1h0si.securelab.online. info.user-n1h0si.securelab.online. 2020021809 30 30 30
4   }
5 }
```

Body Cookies Headers (6) Test Results Status: 200 OK Time: 186ms

Pretty Raw Preview Visualize JSON ↺

na1 Aa Abi

```
1 {
2   "configuration": {
3     "zone_field": "user-n1h0si.securelab.online.\t30\tIN\tSOA\tns1.user-n1h0si.securelab.online. info.user-n1h
      2020021809 30 30 30
      30\tuser-n1h0si.securelab.online.\t30\tIN\tNS\tns1.f5cloudservices.com.\tuser-n1h0si.securelab.online.
      f5cloudservices.com.\tnauction.user-n1h0si.securelab.online.\t30\tIN\tNS\tns91.dns.cloudservices.f5.com
      securelab.online.\t30\tIN\tA\t3.122.191.227\tna1-auction.user-n1h0si.securelab.online.\t30\tIN\tA\t34.
      user-n1h0si.securelab.online.\t30\tIN\tCNAME\twaf-aagr4igerk.waf.prd.f5aas.com.\tna3-auction.user-n1h0
      \t30\tIN\tA\t52.226.147.184\tnns1.user-n1h0si.securelab.online.\t30\tIN\tA\t54.211.12.173\tuser-n1h0si.
      \t30\tIN\tSOA\tns1.user-n1h0si.securelab.online. info.user-n1h0si.securelab.online. 2020021809 30 30 30
```



## 7.6.4 4. Review the JSON

Let's now see the structure of the JSON. In order to get the JSON, go back to Postman and send the **Get DNS JSON** request which uses your ACCESS\_TOKEN to retrieve the JSON:

GET	https://{{HOSTNAME}}/{{API_VERSION}}/svc-subscription/subscriptions/{{DNS_SUBSCRIPTION_ID}}	
Params	Authorization	Headers (9)
▼ Headers (2)		
<input checked="" type="checkbox"/>	Content-Type	application/json
<input checked="" type="checkbox"/>	Authorization	Bearer {{ACCESS_TOKEN}}
	Key	Value

The response will retrieve the JSON containing all the DNS instance information:

As you can see, the JSON provides some general information on subscription\_id, user\_id, and instance name, as well as all configuration details (service IP, zone name, etc).

## 7.6.5 5. Delete Zone

In order to delete your Zone using Postman, send the **Retire DNS Subscription** request which uses the relevant "subscription\_id".

You will see "retired" status in the response body which means that it's not available on the F5 Cloud Services portal anymore.

More detailed information on these API requests can be found [here](#).

## 7.7 F5 DNS Load Balancer Cloud Service - UI

In this section we will use the F5 Cloud Services UI to set up the Load Balancer DNS record, add endpoints for our Auction app, add health checks, load balanced pools, and run through a few configuration options.

### 7.7.1 1. Create F5 DNS Load Balancer Cloud Service

Let's now create DNS Load Balancer Service to be able to balance loads across multiple clouds (Azure & AWS) and provide global availability and performance with health-check and built-in DDoS protection.

a) Go to the **DNS Load Balancer** tab and click **Create**.

b) Enter name of the zone we [created before](#) and click **Create**.

Your DNS Load Balancer instance will appear on the list but in **Inactive** status. You can change the status after creating load balanced record and pool.

Pretty Raw Preview Visualize JSON

```

1 {
2   "subscription_id": " ",
3   "account_id": " ",
4   "user_id": " ",
5   "catalog_id": "c-aax8Jkfg8u",
6   "service_instance_id": " ",
7   "status": "ACTIVE",
8   "service_instance_name": "user-nlh0si.securelab.online",
9   "deleted": false,
10  "service_type": "adns",
11  "configuration": {
12    "adns_service": {
13      "master_servers": [
14        "54.211.12.173"
15      ],
16      "zone": "user-nlh0si.securelab.online"
17    },
18    "details": {
19      "latest_axfr": "2020-02-28T07:26:42Z",
20      "zone_count": 9
21    },
22    "nameservers": [
23      {
24        "ipv4": " ",
25        "ipv6": " ",
26        "name": " "
27      },
28      {
29        "ipv4": " ",
30        "ipv6": " ",
31        "name": " "
32      }
33    ]
34  },
35  "create_time": "2020-02-28T07:26:28.668432Z",
36  "update_time": "2020-02-28T07:26:35.457966Z",
37  "cancel_time": null,
38  "end_time": null
39 }

```

POST https://{{HOSTNAME}}/{{API\_VERSION}}/svc-subscription/subscriptions/{{DNS\_SUBSCRIPTION\_ID}}/retire

Params Authorization Headers (10) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL BETA JSON

```

1 {
2   "subscription_id": "{{DNS_SUBSCRIPTION_ID}}",
3   "omit_config": true
4 }

```

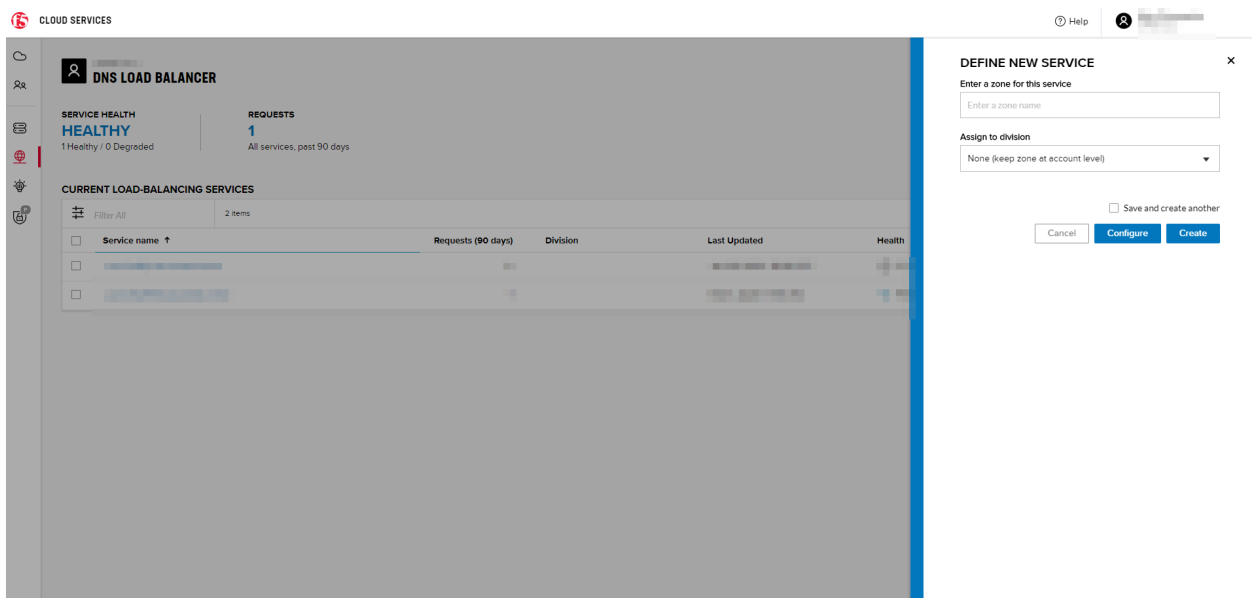
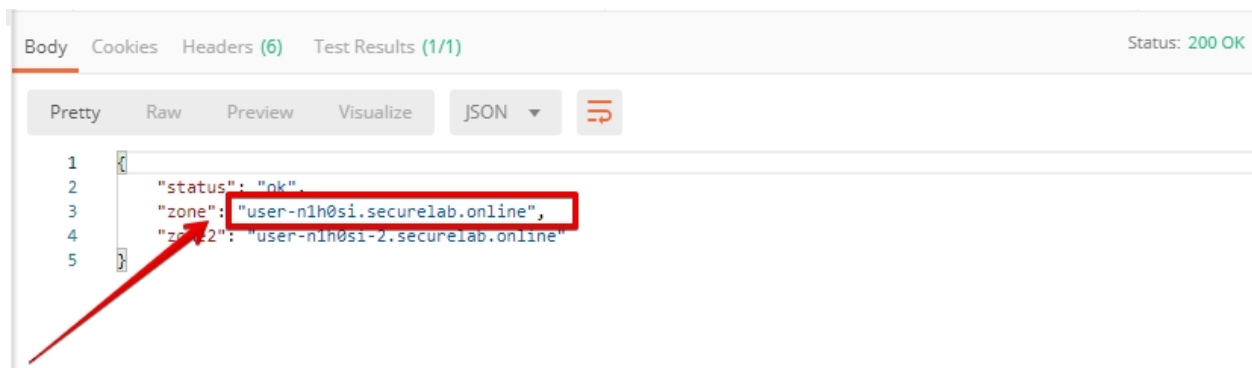
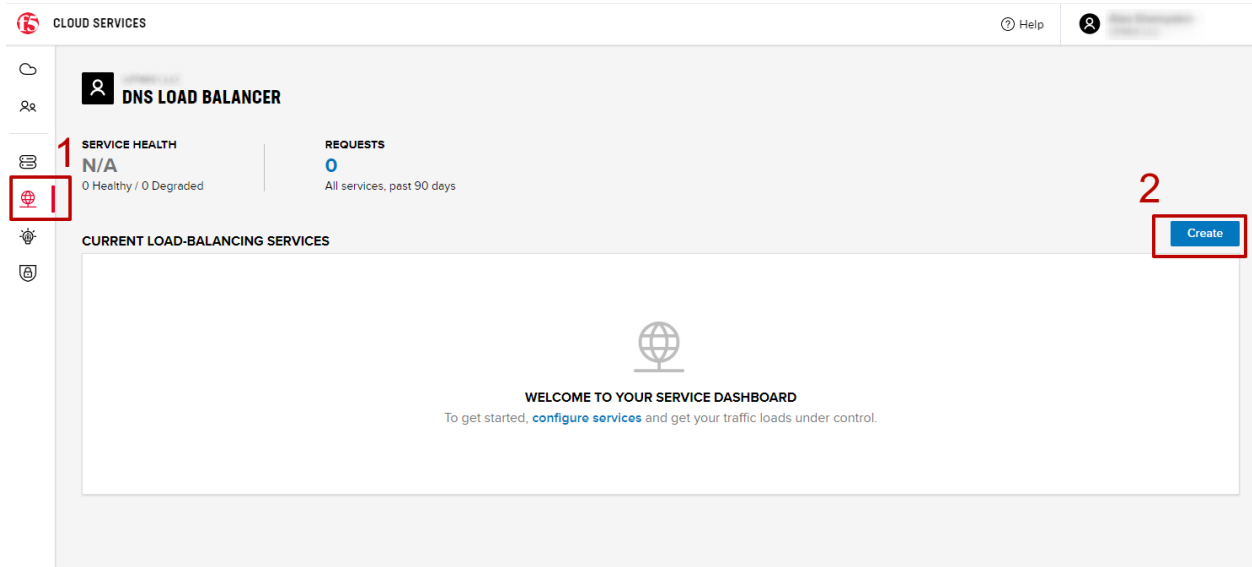
Body Cookies Headers (6) Test Results

Pretty Raw Preview Visualize BETA JSON

```

1 {
2   "status": "RETIRED",
3   "service_state": "UNDEPLOYING",
4   "subscription_id": " "
5 }

```

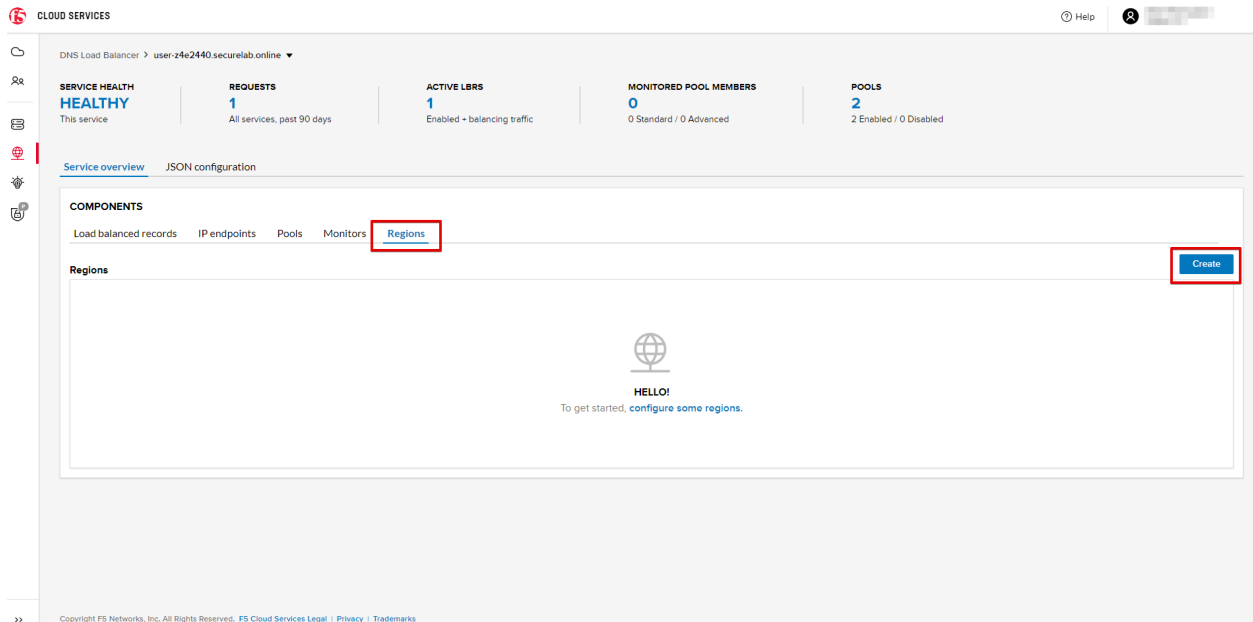


## 7.7.2 2. Add Single Endpoint, Health Monitor, Pool and Default Geoproximity Rule

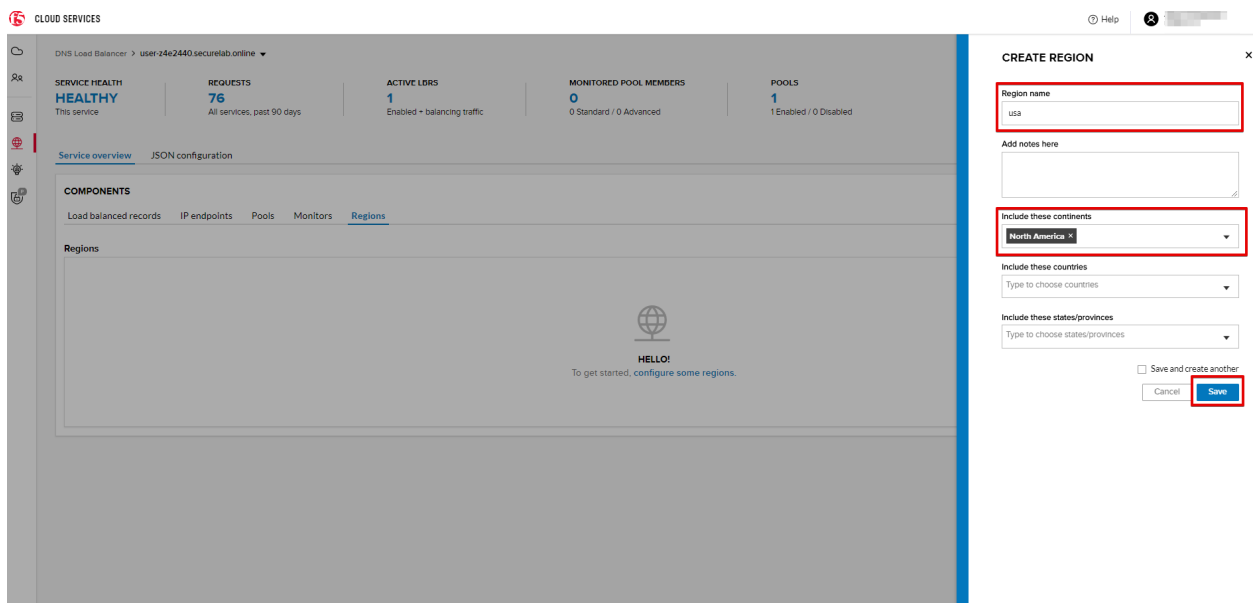
### a) Create a Region

Creating regions will allow grouping incoming requests by geographic areas and directing them to specific pools.

1. Click on DNS Load Balancer instance which we have just created and go to the **Regions** tab. Click **Create**.



2. Fill “usa” as “Region name” and select “North America” in “Include these continents”. **Save** the created region.

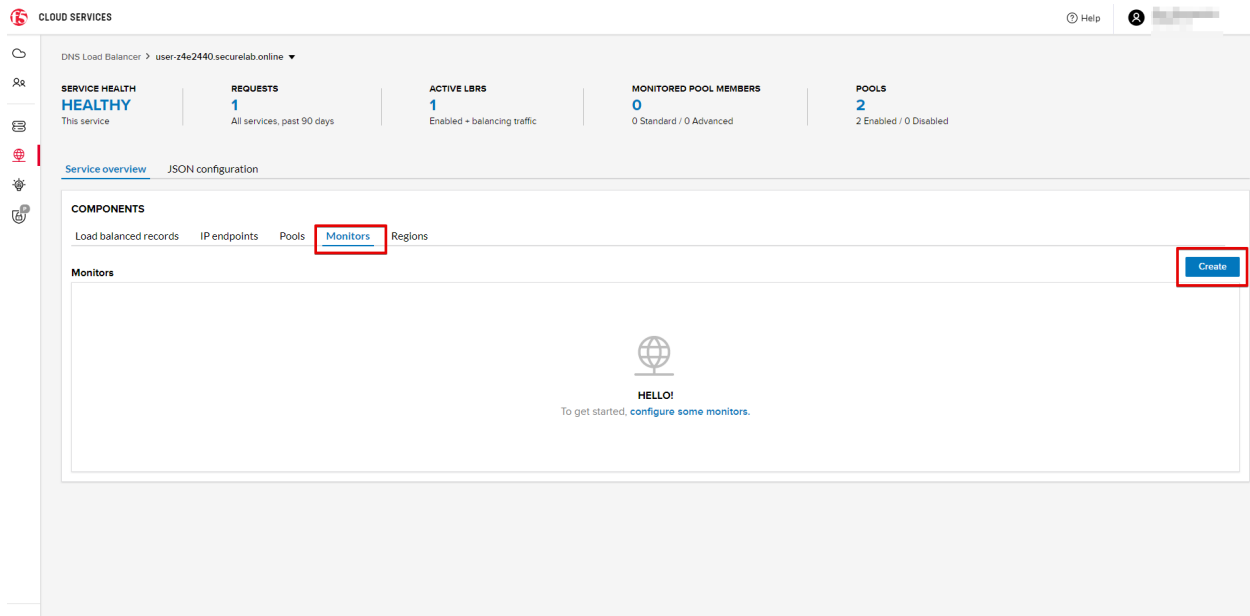


Now all requests from North America will be covered by the “usa” region.

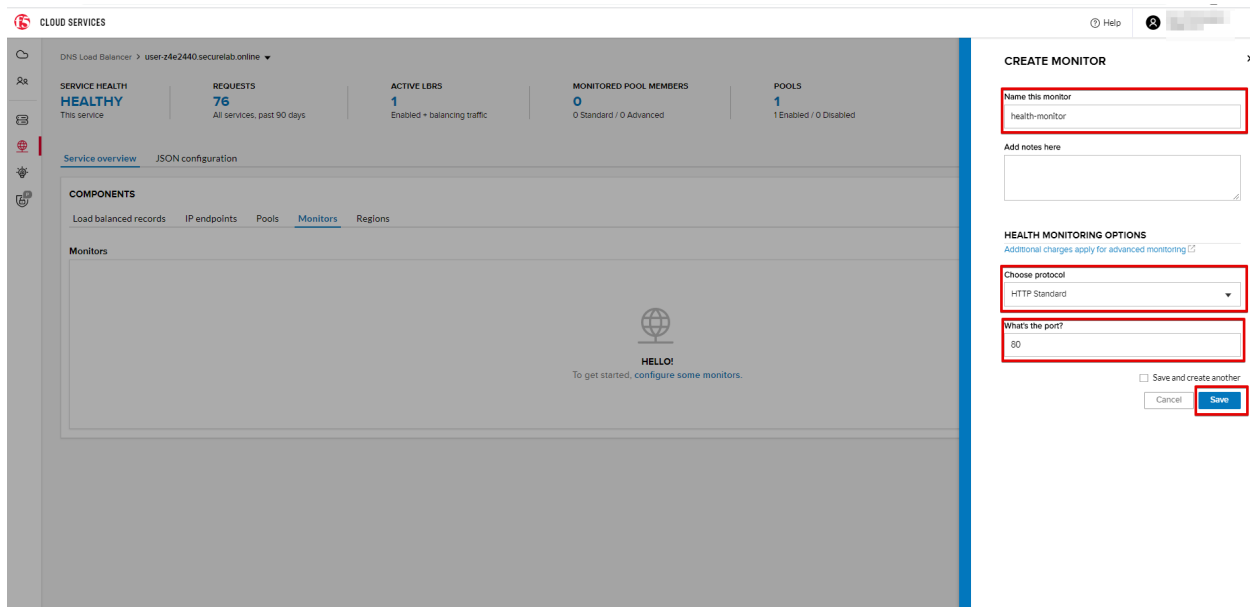
### b) Add A Health Monitor

To distribute the load, DNS Load Balancer will need to monitor health of each IP Endpoint. So, let's create a monitor.

1. Go to the **Monitors** tab and then click **Create**.



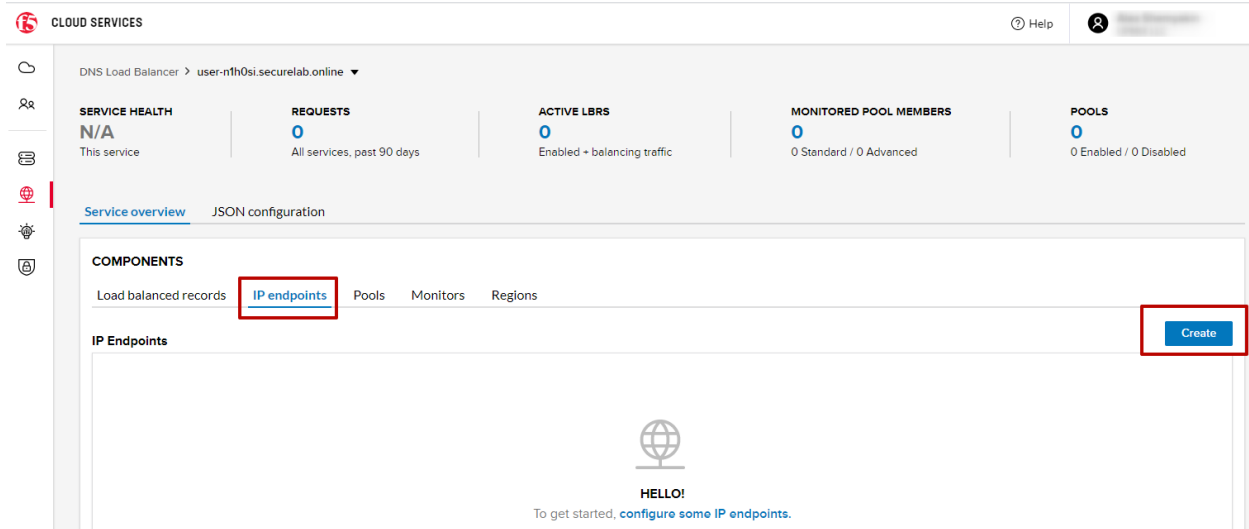
2. Fill in "health-monitor" name, choose "HTTP Standard" protocol, indicate "80" port and click **Save**.



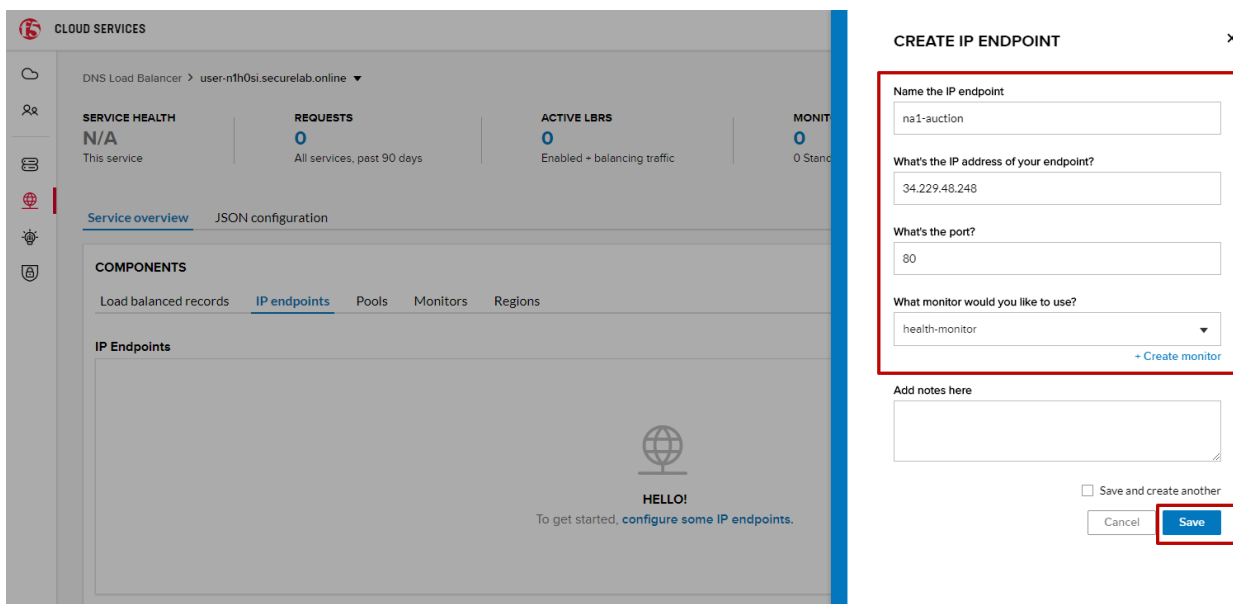
- c) Add an IP Endpoint (NA) with Health Check

Let's now create an IP endpoint that will currently service all incoming requests. DNS Load Balancer chooses an IP endpoint based on request origin and configuration of IP endpoints, as well as IP Endpoint health.

1. Go to the **IP endpoints** tab and then click **Create**.



2. Fill in name (“na1-auction”), IP address (“34.229.48.248”), port (“80”) and select the monitor we created above.



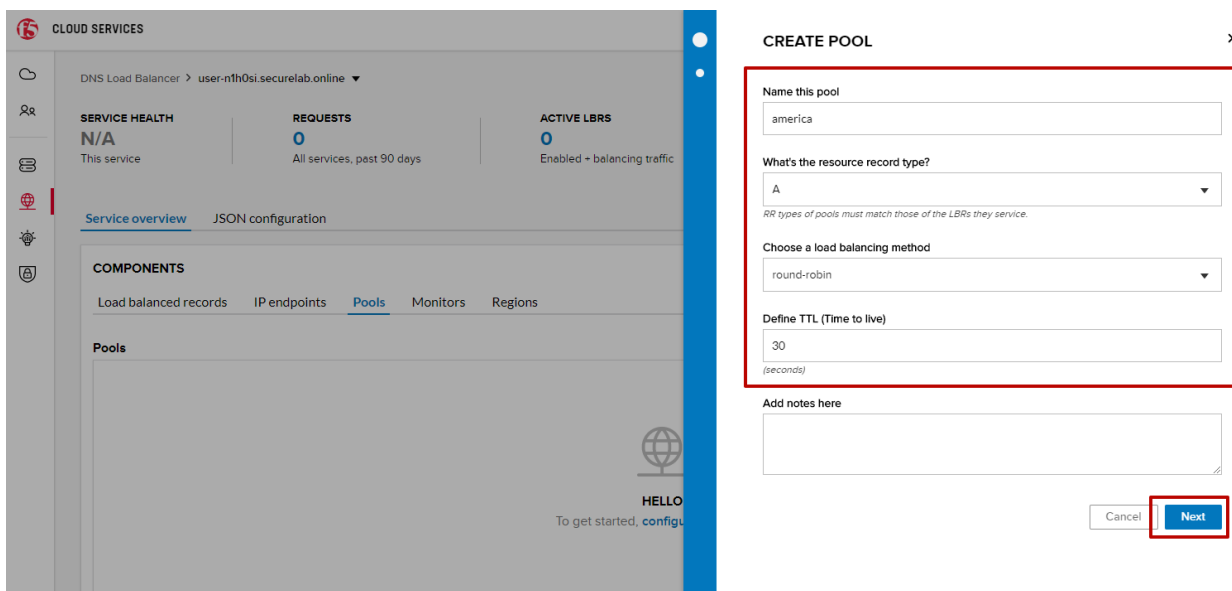
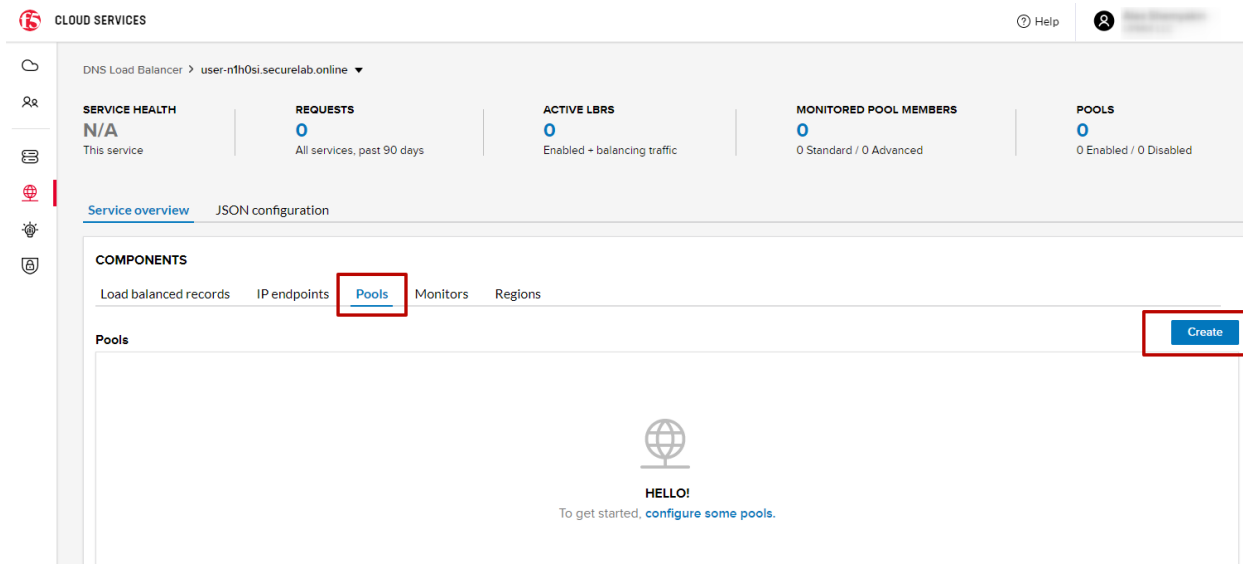
#### d) Create a Pool

Let's now create a pool and add a member to it.

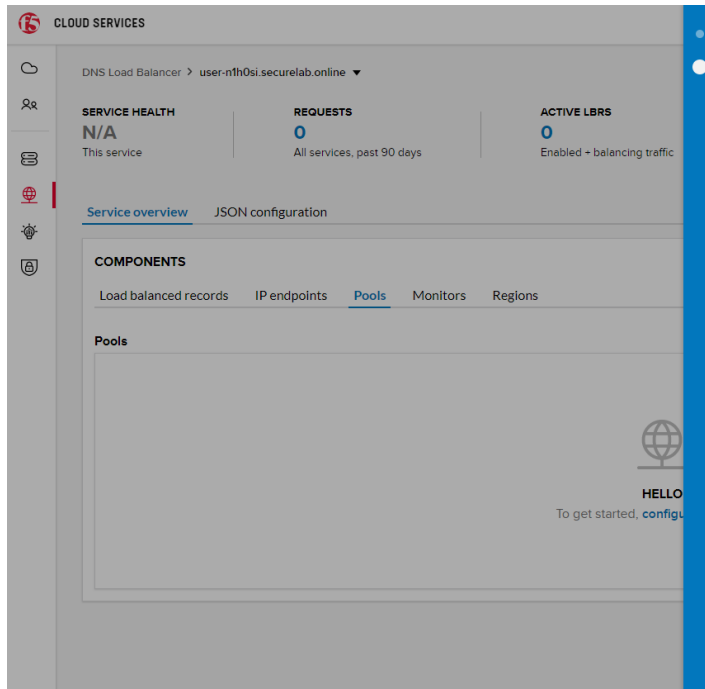
1. Go to the **Pools** tab and then click **Create**.
2. Fill in “america” name, choose “round-robin” method and define TTL “30”. Then click **Next**.
3. Click **Add Member** to add an IP Endpoint to the pool.
4. Select the endpoint we've just created, as well as the monitor. Click **Add** and **Create**.

A newly created pool with the one NA endpoint will appear on the list.

#### e) Add a Load Balanced Record








## CREATE POOL

Pool **america** RR Type **A**

**LOAD BALANCING SETTINGS**  
Add at least one pool member to use a pool in an active service. For optimal load balancing, add at least two pool members.

☐ Enabled

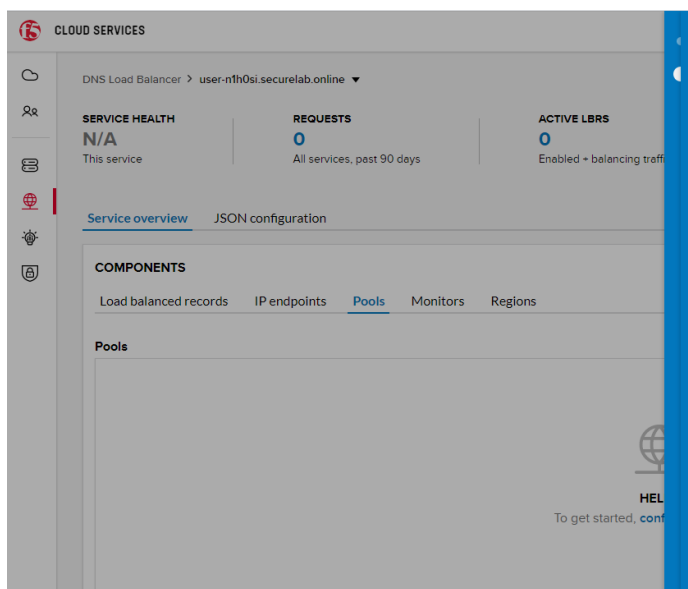
**0 MEMBERS** **Add Member**

  
**MEMBERS APPEAR HERE**  
As you add them above

Specify the maximum IP endpoints returned per response  
1

☐ Save and create another

Back Cancel Create



## ADD MEMBER TO POOL

Pool **america** RR Type **A**

**IP endpoint**  
nel-euction (34.229.48.248) + Create IP endpoint

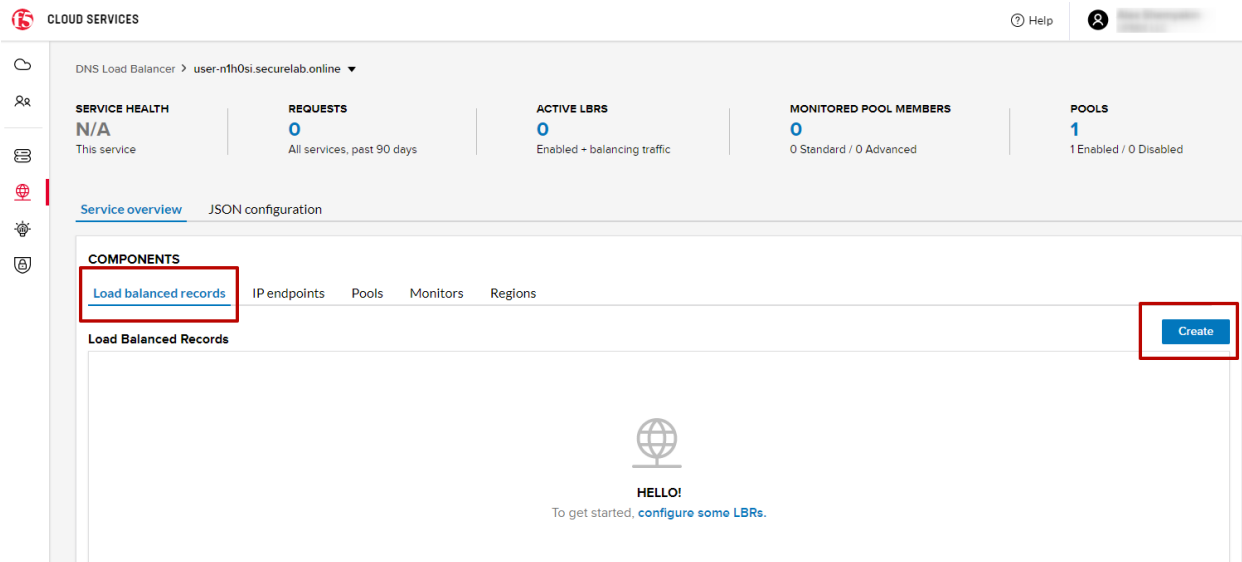
**Monitor**  
health-monitor + Create monitor

☐ Save and create another

Cancel **Add**

After creating all the components (IP endpoint, Pool, Region and Monitor), we can create a DNS Load Balancer record and its proximity rule.

1. Go to the **Load balanced records** tab and then click **Create**.



2. Fill in LBR name "auction", host "auction", select "A" as "Resource Record Type" and set a proximity rule ("Anywhere" -> "america" pool) to direct requests from anywhere to "america" pool with the created NA1 endpoint. Set score of the proximity rule to be "1". This will define the priority of the rule after some more are added.

Click **Add Rule**, then check **\*Enabled\*** tick and **Save** the record.

3. Go back to the DNS Load Balancer tab, click on your service and activate it.

The DNS Load Balancer service is now setup.

### f) Test via Browser

Let's test the created service with the proximity rule via browser.

1. Open FQDN ("auction.{{zone name}}") where {{zone name}} is the value copied from postman in one of the step above) in your browser.
2. You will see that acc to the proximity rule, you joined the endpoint belonging to the "america" pool.

### g) Test via Command Prompt

Another way to test the new proximity rule is via **Command Prompt**.

1. Start **Command Prompt**.
2. Paste the following command to the **Command Prompt**: **nslookup "your FQDN name"** and press **Enter**.

And you will see **34.229.48.248** IP in the response which belongs to **na1-auction** endpoint from **america** pool.

## 7.7.3 3. Add Multiple Ednpoints to Load Balanced Pool & Test

### a) Add More Endpoints (NA2,3)

**CLOUD SERVICES** Help user-n1h0si.securelab.online

DNS Load Balancer > user-n1h0si.securelab.online

Load-Balanced Records > auction

**RECORD STATUS**  
So it can be used in your active service configuration. At least one proximity rule is required.

☒ Enabled **7**

**PROXIMITY RULES**  
How to balance end-user requests across regions and pools

For All End-user Requests Coming From  
Anywhere **4** [+ Create region](#)

Route Requests to This Pool  
america **5** [+ Create pool](#)

Using this Score  
1 **6** [Add Rule](#)

**LOAD-BALANCED RECORD PROPERTIES**  
Which host to load balance

LBR name **1**  
auction

Resource Record Type  
A **3**

Hosts (Wildcards Allowed)  
auction **2** [+](#) [-](#)

Notes

☒ Cache responses so that clients receive persistent answers  
Length of CIDR masks used to group client  
IPv4 Clients (0-32) 24 IPv6 Clients (0-128) 56  
Remember persistence records for (seconds) 3600

**8**

[Delete](#) [Cancel](#) [Save](#)

**CLOUD SERVICES** Help user-n1h0si.securelab.online

**UPMIX LLC**  
**DNS LOAD BALANCER**

**SERVICE HEALTH**  
N/A  
0 Healthy / 0 Degraded

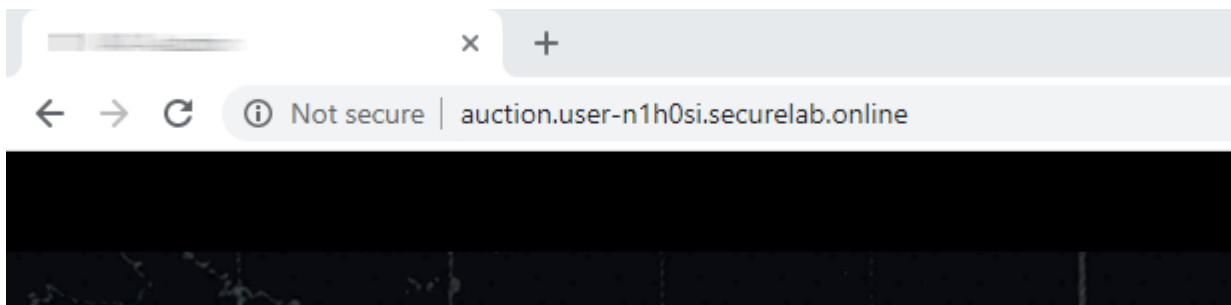
**REQUESTS**  
0  
All services, past 90 days

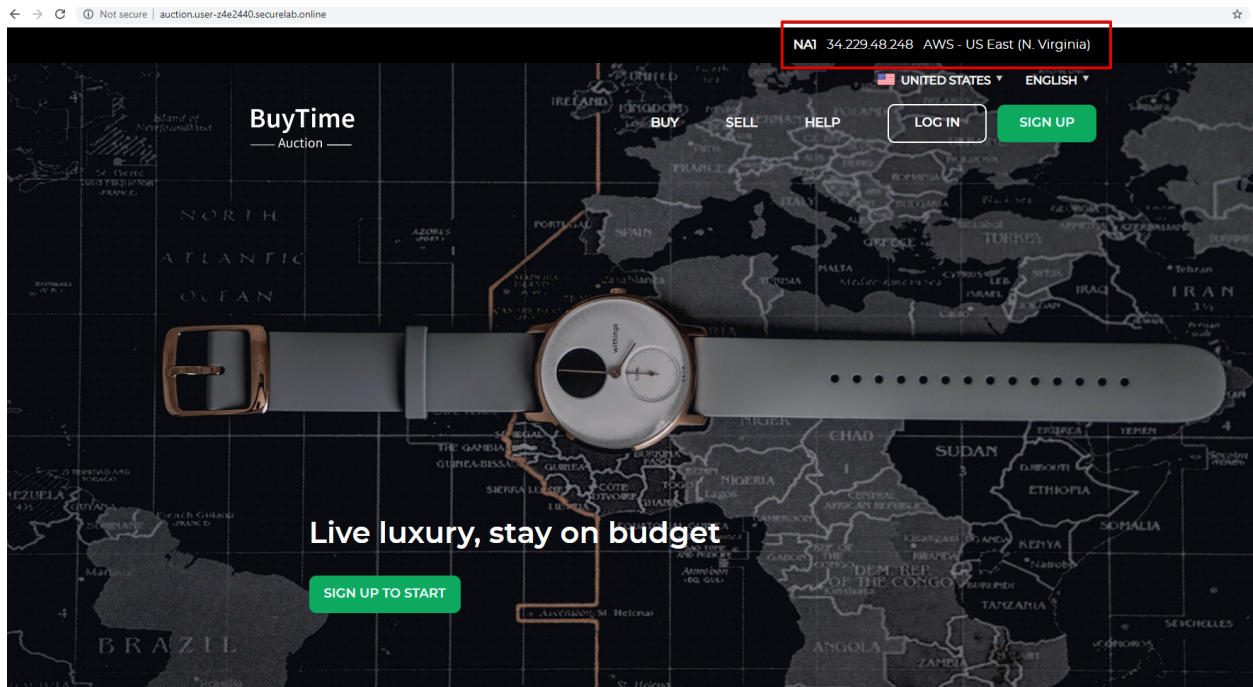
**CURRENT LOAD-BALANCING SERVICES** [Create](#)

[Filter All](#) 1 selected of 1 items

[Activate](#) [Suspend](#) [Delete](#)

<input checked="" type="checkbox"/>	Service name ↑	Requests (90 days)	Division	Last Updated	Health	Status
<input checked="" type="checkbox"/>	user-n1h0si.securelab.online	0		May 28, 2020 / 17:11 UTC	N/A	Inactive





Let's now add a few more endpoints for load balancing of the application. Note that NA2 endpoint is deployed on Amazon AWS, whereas NA3 is running on Microsoft Azure.

1. Go back to the F5 Cloud Services portal, the **DNS Load Balancer** service, the **IP endpoints** tab and select **Create**.
2. Fill in name ("na2-auction"), IP address ("18.232.64.254"), port ("80") and select the monitor we created above.

Create one more endpoint repeating the step above using the following properties: "na3-auction" for name, "13.82.106.211" for IP address, "80" for port. You will have three endpoints as a result.

#### b) Add the Endpoints to the Pool

Let's now add the newly created endpoints to the existing pool.

1. Go to the **Pools** tab and click on the **america** pool.
2. Click **Add Member** and select the endpoint to be added.

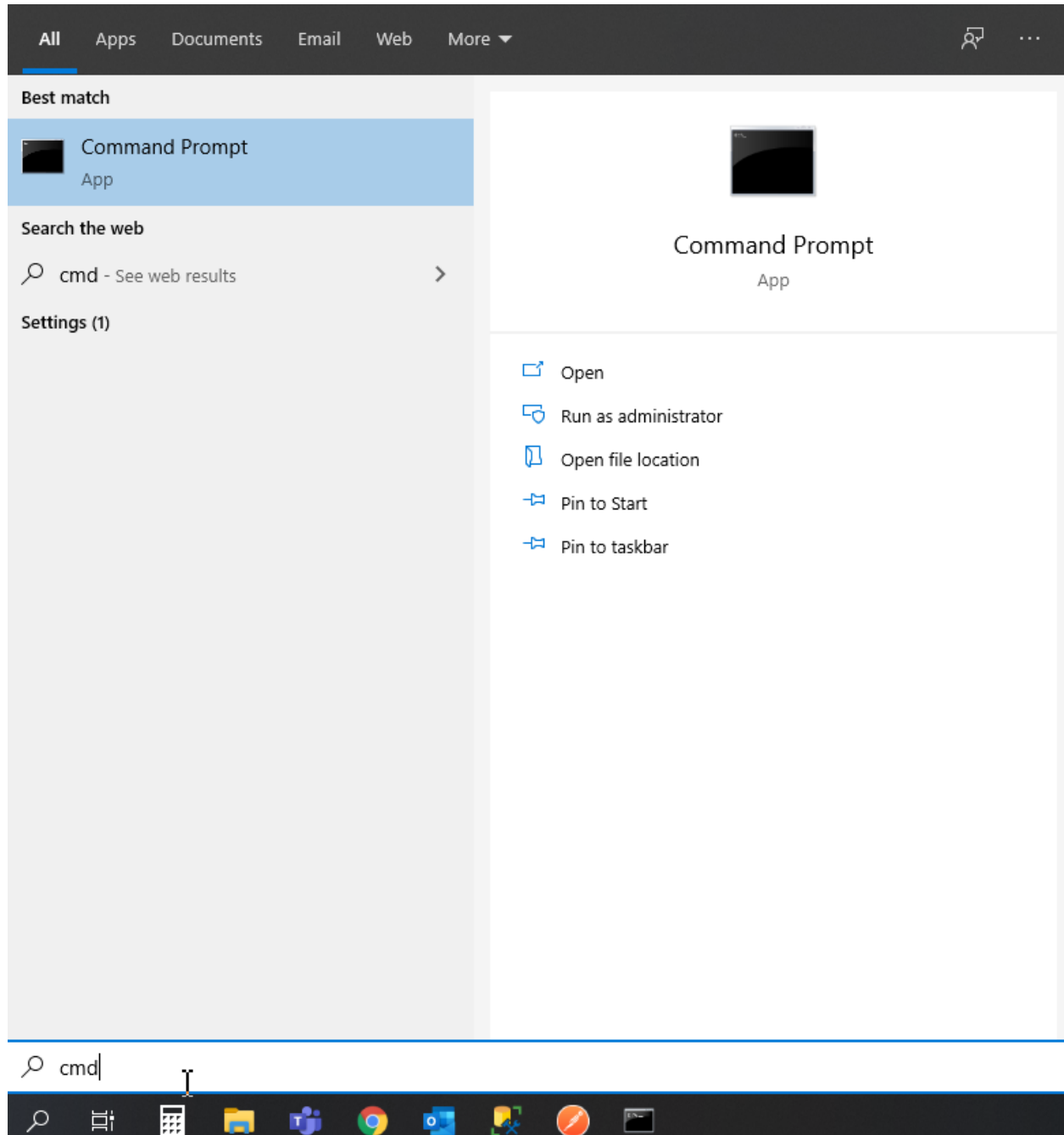
Add one more endpoint and click **Save**. Now all three endpoints belong to one pool:

#### c) Test via Default Browser

Let's test the updated pool with the new endpoints via browser.

1. Open FQDN ("auction.{{zone name}}") where {{zone name}} is the value copied from postman in one of the step above) in your browser.
2. You will see that acc to the proximity rule and pool members, you will get to endpoints belonging to the **america** pool in a round-robin manner.

And let's now update the page:



```
Command Prompt
Microsoft Windows [Version 10.0.18362.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\> nslookup auction.user-n1h0si.securelab.online
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: auction.user-n1h0si.securelab.online
Address: 34.229.48.248

C:\Users\>
```

DNS Load Balancer > user-n1h0si.securelab.online

**SERVICE HEALTH** N/A  
This service

**REQUESTS** 0  
All services, past 90 days

**ACTIVE LBRS** 1  
Enabled - balancing traffic

**MONITORED POOL MEMBERS** 0  
0 Standard / 0 Advanced

**POOLS** 1  
1 Enabled / 0 Disabled

**Service overview** JSON configuration

**COMPONENTS**

Load balanced records **IP endpoints** Pools Monitors Regions

**IP Endpoints** Create

Filter All 3 items Delete

<input type="checkbox"/>	IP endpoint name ↑	LTM VIP? ⓘ	IP Address	Notes
<input type="checkbox"/>	n1-auction		34.229.48.248	
<input type="checkbox"/>				
<input type="checkbox"/>				

Copyright F5 Networks, Inc. All Rights Reserved. F5 Cloud Services Legal | Privacy | Trademarks

The screenshot shows the F5 DNS Load Balancer Cloud Service UI. The main panel displays the 'SERVICE HEALTH' as 'HEALTHY' with 39 requests, 1 active LBR, 1 monitored pool member, and 1 pool. The 'IP Endpoints' section shows 1 item: 'na1-auction' with IP address 34.229.48.248. A modal titled 'CREATE IP ENDPOINT' is open on the right, with fields for 'Name the IP endpoint' (na2-auction), 'What's the IP address of your endpoint?' (18.232.64.254), 'What's the port?' (80), and 'What monitor would you like to use?' (health-monitor). The 'Save' button is highlighted with a red box.

**CREATE IP ENDPOINT**

Name the IP endpoint  
na2-auction

What's the IP address of your endpoint?  
18.232.64.254

What's the port?  
80

What monitor would you like to use?  
health-monitor

+ Create monitor

Add notes here

☐ Save and create another

Cancel Save

The screenshot shows the F5 DNS Load Balancer Cloud Service UI. The main panel displays the 'SERVICE HEALTH' as 'N/A' with 0 requests, 1 active LBR, 0 monitored pool members, and 1 pool. The 'IP Endpoints' section shows 3 items: 'na1-auction', 'na2-auction', and 'na3-auction'. The 'na2-auction' and 'na3-auction' rows are highlighted with a red box. A 'Create' button is visible in the top right corner of the 'IP Endpoints' section.

**IP Endpoints**

Filter All 3 items

IP endpoint name ↑	LTM VIP? ⓘ	IP Address	Notes
na1-auction		34.229.48.248	
na2-auction		18.232.64.254	
na3-auction		52.226.147.184	

Create

CLOUD SERVICES

Help

DNS Load Balancer

user-nth0si.securelab.online

**SERVICE HEALTH**  
 HEALTHY  
 This service

**REQUESTS**  
 3  
 All services, past 90 days

**ACTIVE LBRS**  
 1  
 Enabled + balancing traffic

**MONITORED POOL MEMBERS**  
 1  
 1 Standard / 0 Advanced

**POOLS**  
 1  
 1 Enabled / 0 Disabled

Service overview

JSON configuration

**COMPONENTS**

Load balanced records

IP endpoints

Pools

Monitors

Regions

Filter All

1 items

Disable

Enable

Delete

Pool name ↑	Pool record type	Pool members	Load balancing method	Status
america	A	1	round-robin	Enabled

Create

CLOUD SERVICES

Help

DNS Load Balancer

user-nth0si.securelab.online

**SERVICE HEALTH**  
 HEALTHY  
 This service

**REQUESTS**  
 3  
 All services, past 90 days

**ACTIVE LBRS**  
 1  
 Enabled + balancing traffic

**MONITORED POOL MEMBERS**  
 1  
 1 Standard / 0 Advanced

**POOLS**  
 1  
 1 Enabled / 0 Disabled

Service overview

JSON configuration

**COMPONENTS**

Load balanced records

IP endpoints

Pools

Monitors

Regions

Filter All

1 items

Disable

Enable

Delete

Pool name ↑	Pool record type	Pool members	Load balancing method	Status
america	A	1	round-robin	Enabled

Create

Filter All

1 items

Disable

Enable

Delete

Pool name ↑	Pool record type	Pool members	Load balancing method	Status
america	A	1	round-robin	Enabled

Create



DNS Load Balancer > user-n1h0si.securelab.online

Pools > america

**POOL STATUS**  
At least one pool member is required to enable this pool for use in an active service.

☒ Enabled

**LOAD BALANCING SETTINGS**  
Add at least one pool member to use a pool in an active service. For optimal load balancing, add at least two pool members.

What's the resource record type?  
A

RR types of pools must match those of the LBRs they service.

Choose a load balancing method  
round-robin

Specify the maximum IP endpoints returned per response  
1

**3 MEMBERS** [Add Member](#)

IP endpoint ↑	Health monitor	Member status
na1-auction	health-monitor	N/A
na2-auction	health-monitor	N/A
na3-auction	basic option	N/A

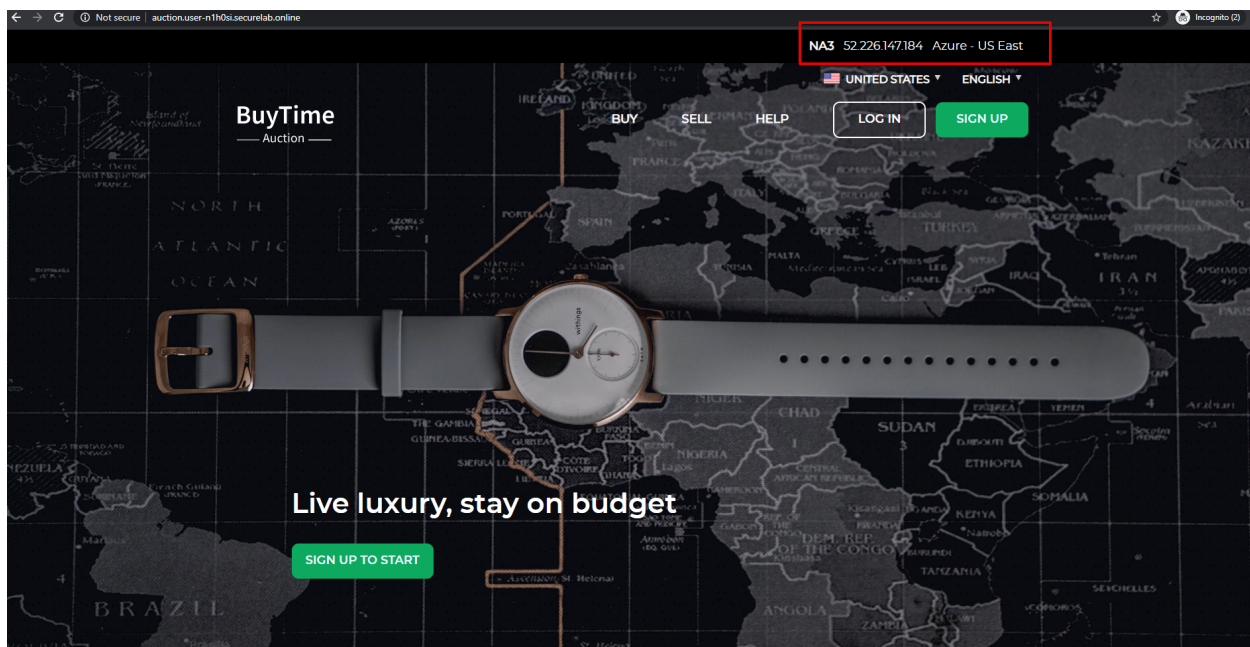
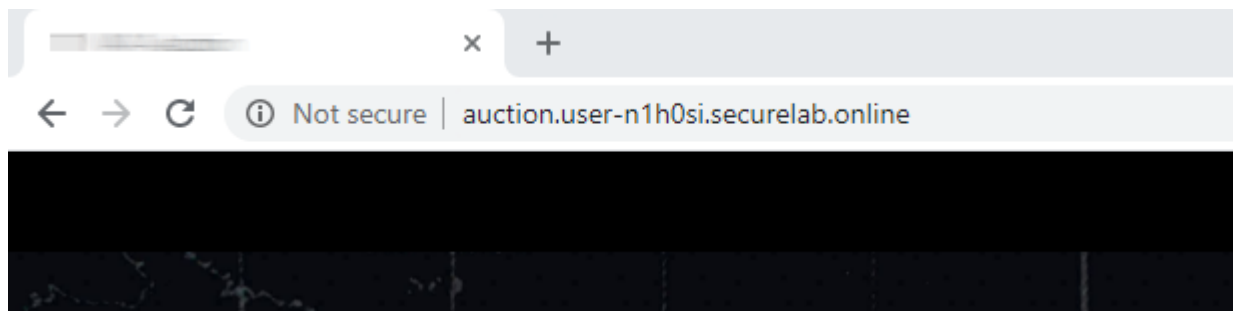
**POOL PROPERTIES**

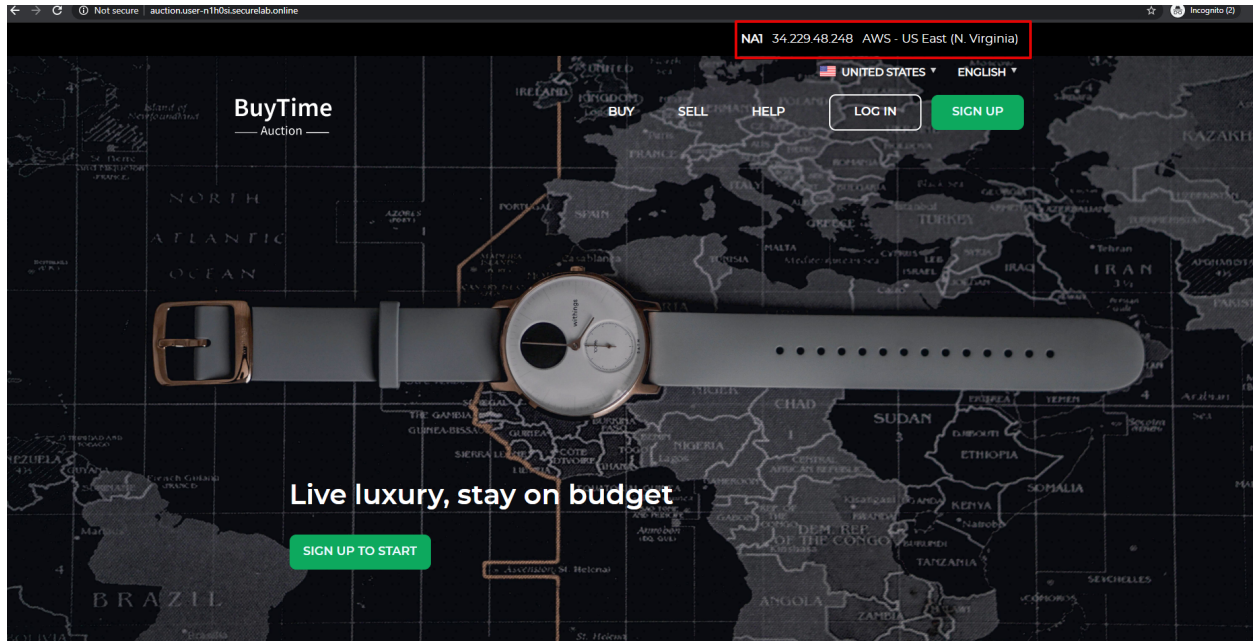
Pool name  
america

Notes

TTL (Time to live)  
30 (seconds)

Delete Cancel Save



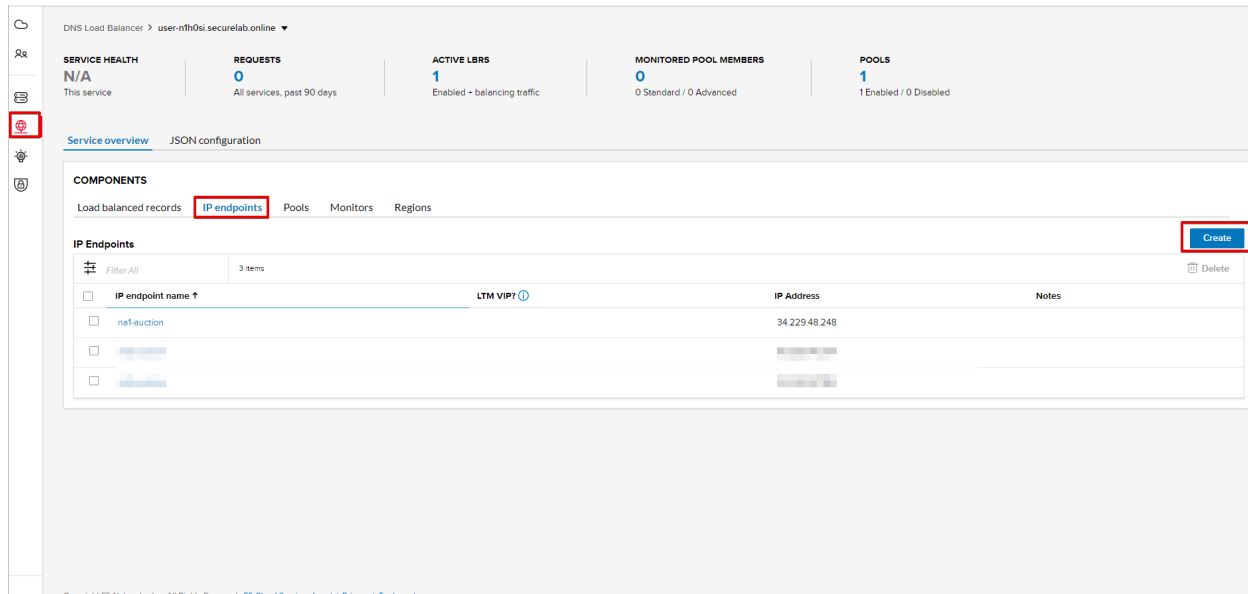


### 7.7.4 4. Add Europe Region & EU Endpoint with Corresponding Geoproximity Record

#### a) Add EU Endpoint

Let's now add a EU endpoint which is deployed on Amazon AWS.

1. Go back to the F5 Cloud Services portal, the **DNS Load Balancer** service, the **IP endpoints** tab and select **Create**.



2. Fill in name ("eu-auction"), IP address ("3.122.191.227"), port ("80") and select the monitor we've created above.

The new endpoint will appear on the list.

### b) Add EU Region

Creating EU region will allow grouping requests coming from the European region and directing them to a specific pool.

1. Go to the **Regions** tab and click **Create**.

Region / group name	Includes continents	Includes countries	Includes states/provinces	Mentioned in rules	Mentioned in LBRs
usa	1	0	0	0	0

2. Fill "europe" as "Region name" and select "Europe" in "Include these continents". Save the created region.

Now you have two regions created.

### c) Add EU Pool

Let's now create a pool and add a member to it.

1. Go to the **Pools** tab and then click **Create**.
2. Fill in "europe" name, choose "round-robin" method and define TTL "30". Then click **Next**.
3. Click **Add Member** to add an IP Endpoint to the pool.

CLOUD SERVICES

DNS Load Balancer > user-nth0si.securelab.online

Help

**SERVICE HEALTH** **HEALTHY** **REQUESTS** 9 All services, past 90 days **ACTIVE LBRS** 1 Enabled + balancing traffic **MONITORED POOL MEMBERS** 3 3 Standard / 0 Advanced **POOLS** 1 1 Enabled / 0 Disabled

Service overview JSON configuration

**COMPONENTS**

Load balanced records IP endpoints Pools Monitors **Regions**

**Regions**

Filter All 1 items

<input type="checkbox"/> Region / group name ↑	Includes continents	Includes countries	Includes states/provinces
<input type="checkbox"/> uss	1	0	0

**CREATE REGION**

Region name  
europe

Add notes here

Include these continents  
Europe x

Include these countries  
Type to choose countries

Include these states/provinces  
Type to choose states/provinces

☐ Save and create another

Cancel Save

CLOUD SERVICES

DNS Load Balancer > user-nth0si.securelab.online

Help

**SERVICE HEALTH** **HEALTHY** **REQUESTS** 195 All services, past 90 days **ACTIVE LBRS** 1 Enabled + balancing traffic **MONITORED POOL MEMBERS** 3 3 Standard / 0 Advanced **POOLS** 1 1 Enabled / 0 Disabled

Service overview JSON configuration

**COMPONENTS**

Load balanced records IP endpoints **Pools** Monitors Regions

**Pools**

Filter All 1 items

<input type="checkbox"/> Pool name ↑	Pool record type	Pool members	Load balancing method	Status
<input type="checkbox"/> america	A	3	round-robin	● Enabled

Disable Enable Delete

Create

CLOUD SERVICES

DNS Load Balancer > user-nth0si.securelab.online

**SERVICE HEALTH**  
HEALTHY  
This service

**REQUESTS**  
9  
All services, past 90 days

**ACTIVE LBRS**  
1  
Enabled + balancing traffic

**MONITORED POOL MEMBERS**  
3  
3 Standard / 0 Advanced

Service overview JSON configuration

**COMPONENTS**

Load balanced records IP endpoints **Pools** Monitors Regions

**Pools**

Filter All 1 items

Pool name ↑	Pool record type	Pool members	Load balancing
america	A	3	round-robin

**CREATE POOL**

Name this pool  
europe

What's the resource record type?  
A  
RR types of pools must match those of the LBRS they service.

Choose a load balancing method  
round-robin

Define TTL (Time to live)  
30  
(seconds)

Add notes here

Cancel **Next**

CLOUD SERVICES

DNS Load Balancer > user-nth0si.securelab.online

**SERVICE HEALTH**  
HEALTHY  
This service

**REQUESTS**  
179  
All services, past 90 days

**ACTIVE LBRS**  
1  
Enabled + balancing traffic

**MONITORED POOL MEM**  
3  
3 Standard / 0 Advanced

Service overview JSON configuration

**COMPONENTS**

Load balanced records IP endpoints **Pools** Monitors Regions

**Pools**

Filter All 1 items

Pool name ↑	Pool record type	Pool members	Load balancing
america	A	3	round-robin

**CREATE POOL**

Pool **europe** RR Type **A**

**LOAD BALANCING SETTINGS**

Add at least one pool member to use a pool in an active service. For optimal load balancing, add at least two pool members.

☐ Enabled

**0 MEMBERS** **Add Member**

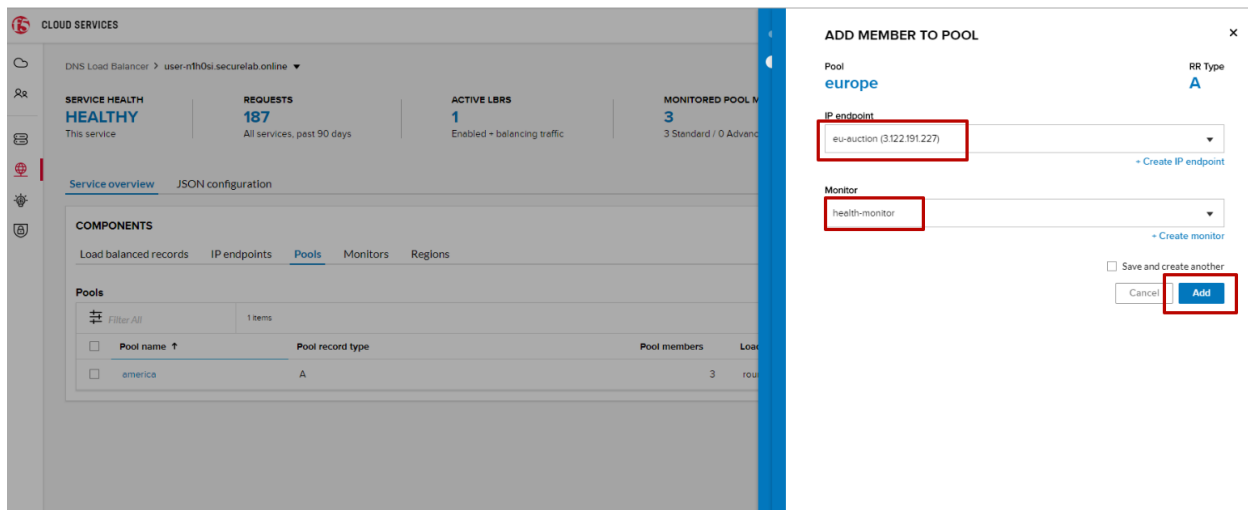
**MEMBERS APPEAR HERE**  
As you add them above

Specify the maximum IP endpoints returned per response  
1

☐ Save and create another

Back Cancel **Create**

4. Select the endpoint we've just created, as well as the monitor. Click **Add** and **Create**.

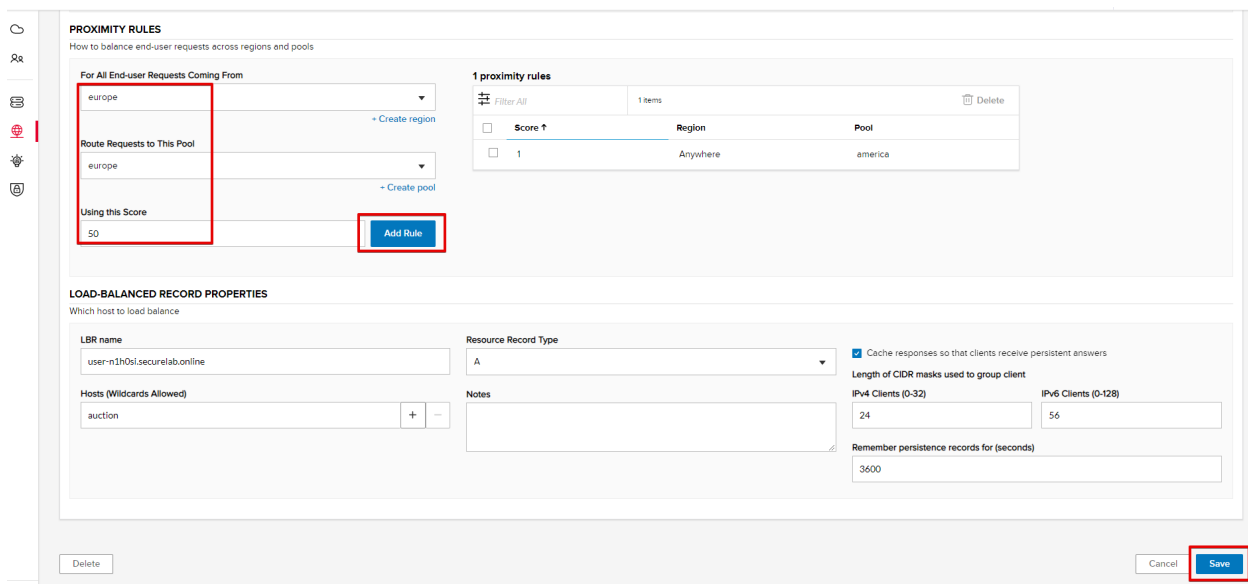


A newly created pool with one EU endpoint will appear on the list.

d) Update LB Record Europe -> "europe"

Now that we have created EU pool, region and endpoint, we can update load balanced record and add a new proximity rule: to send the traffic originating in Europe to the "europe" pool, utilizing a higher relative score than the previous rule of routing traffic from "Anywhere" to the "america" pool. This type of geo-proximity based routing is useful for GDPR compliance.

Go to the **Load balanced records** tab and click on your record. Set a new proximity rule ("europe" -> "europe" pool). Set the score of the proximity rule to be "50".

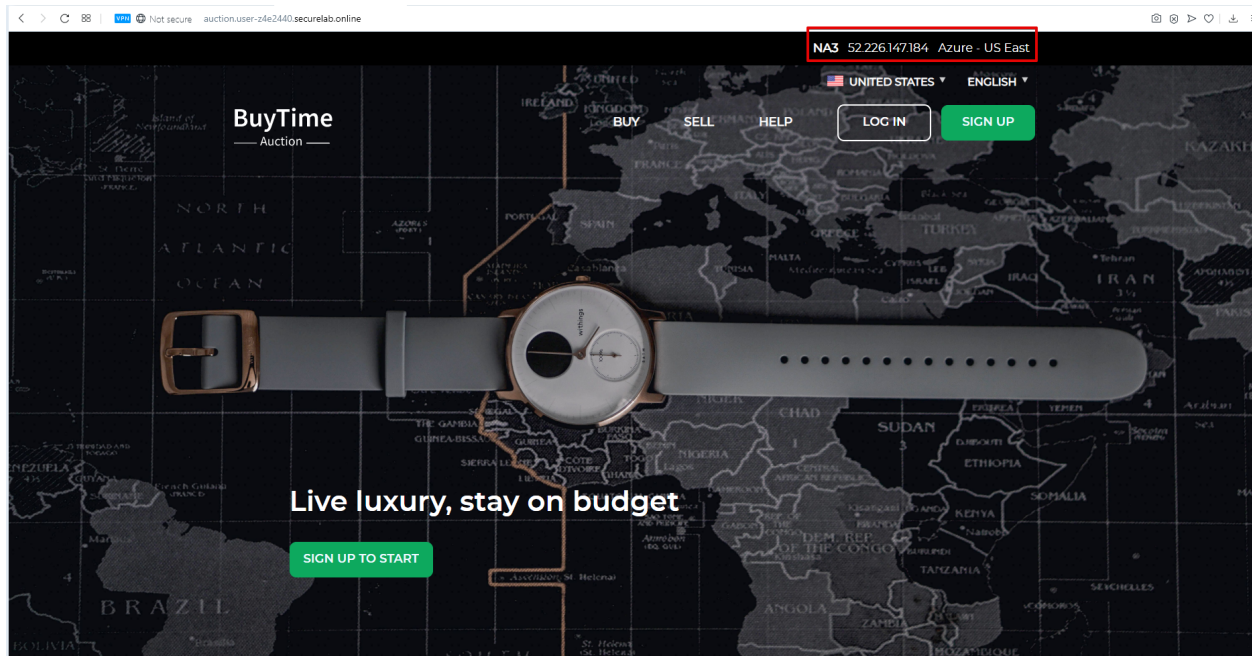


Click **Add Rule** and **Save** the record. The new proximity rule will direct requests from Europe region to **europe** pool.

e) Test using the Opera Browser

Now let's test the new proximity rule. This can be done either via the Opera browser or via your computer's **Command Prompt** (see the next section).

1. Open the Opera browser, copy FQDN name ("auction."your zone name") in **Load balanced record properties** and paste into your browser. You will get to one of three available IP endpoints of the "america" pool.



2. Let's now test the EU proximity rule. Click **VPN** and select **Europe**. This will simulate your entering BuyTime Website from Europe.
3. Update your "auction."zone name"" page to see that acc to the proximity rule, you switched to the European pool.

f) Test via Command Prompt

Another way to test the new proximity rule is via **Command Prompt**.

1. Start **Command Prompt**.
2. Paste the following command to the **Command Prompt**: "nslookup auction.cloudservicesdemo.net 198.6.100.25".  
And you will see **34.229.48.248** IP in the response which belongs to **na1-auction** endpoint from **america** pool.
3. Now let's check the **europa** pool. Paste the following command to the **Command Prompt**: **nslookup auction.cloudservicesdemo.net 158.43.240.3**.  
And you will see **3.122.191.227** IP in the response which belongs to **eu-auction** endpoint from **europa** pool.

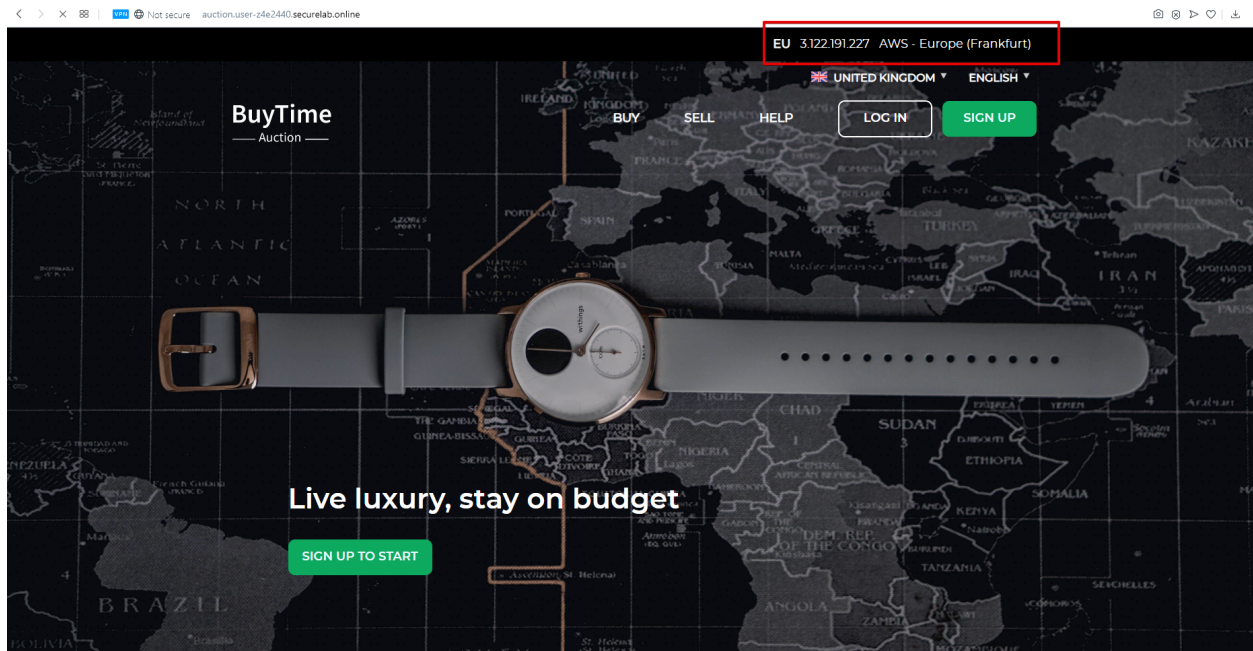
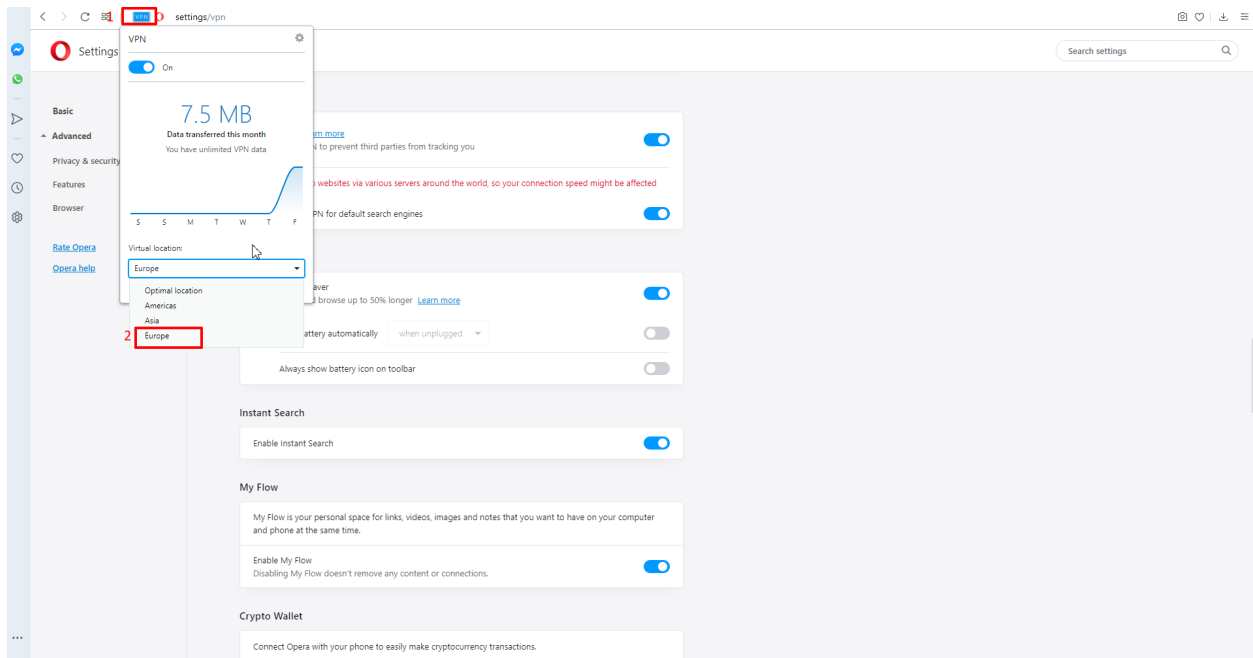
## 7.7.5 5. Duplicate Load Balanced Record using JSON through the UI

Let's now duplicate a load balanced record and its configuration in the existing Load-balancing service via the F5 Cloud Services portal. To do that, follow the step below:

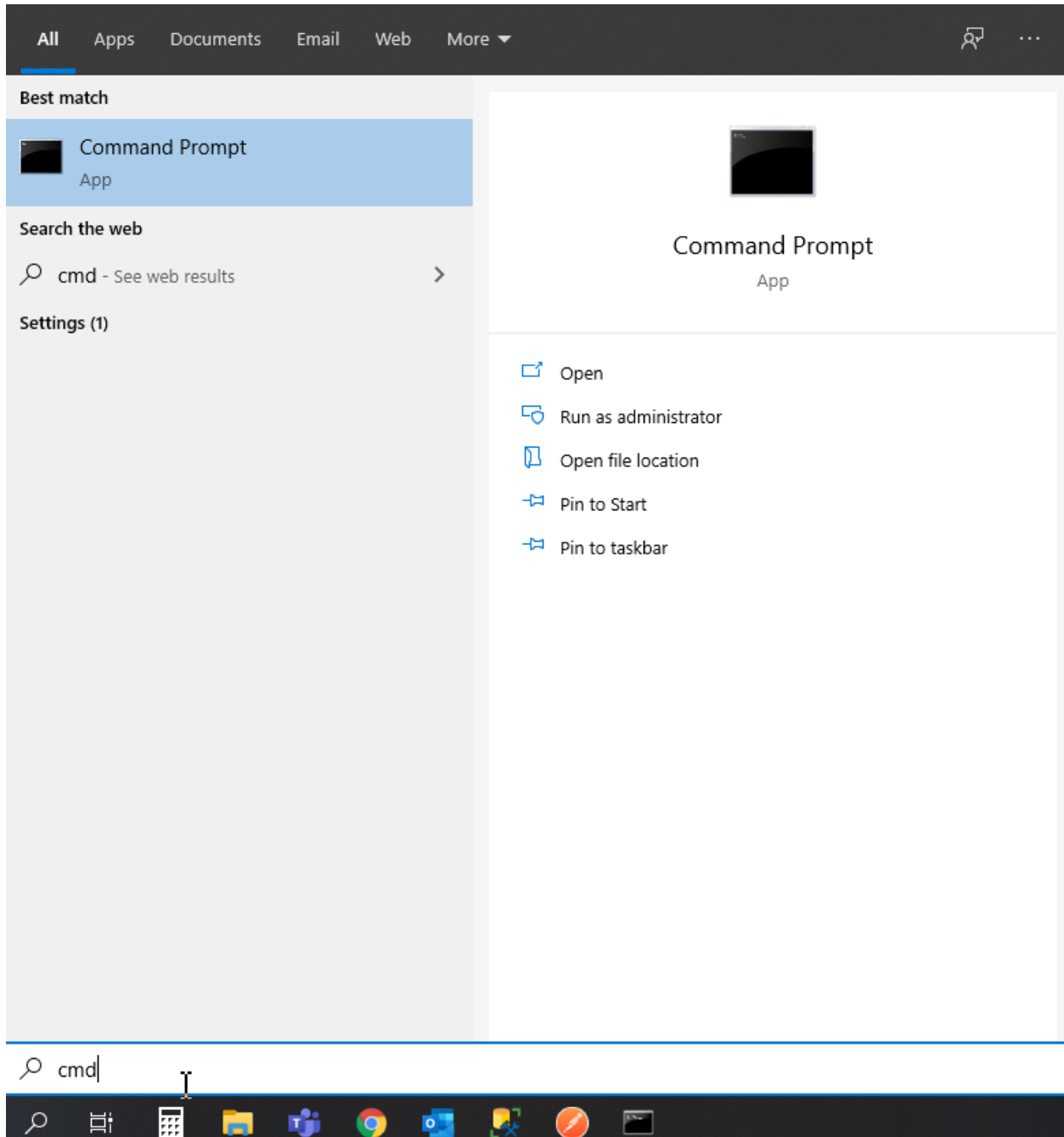
a) Get JSON

Go to the **DNS Load Balancer** tab in the portal and click on your existing Load-balancing service. Open the **JSON configuration** tab and copy it.









```
Command Prompt
Microsoft Windows [Version 10.0.18362.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\> nslookup auction.user-n1h0si.securelab.online
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: auction.user-n1h0si.securelab.online
Address: 34.229.48.248

C:\Users\>
```

```
Command Prompt
Microsoft Windows [Version 10.0.18362.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\> nslookup auction.cloudservicesdemo.net 198.6.100.25
Server: cache00-wcom.uu.net
Address: 198.6.100.25

Non-authoritative answer:
Name: auction.cloudservicesdemo.net
Address: 34.229.48.248

C:\Users\> nslookup auction.cloudservicesdemo.net 158.43.240.3
Server: cache003a.ns.ca.uu.net
Address: 158.43.240.3

Non-authoritative answer:
Name: auction.cloudservicesdemo.net
Address: 3.122.191.227

C:\Users\>
```

The screenshot shows the F5 Cloud Services portal for a DNS Load Balancer service. The top navigation bar includes 'CLOUD SERVICES', 'Help', and a user profile. The main header displays the service name 'user-n1h0si.securelab.online' and its status 'HEALTHY'. Below this, a summary bar shows '22 REQUESTS', '2 ACTIVE LBRS', '0 MONITORED POOL MEMBERS', and '3 POOLS'. The 'JSON configuration' tab is selected, displaying a JSON configuration for a zone named 'user-n1h0si.securelab.online'. The configuration includes load balanced records, a portal, and a pool named 'pools\_usa'.

```

1 {
2   "zone": "user-n1h0si.securelab.online",
3   "load_balanced_records": {
4     "lbrs_id6780c2_8a94_a091_b7d8_970fad339124": {
5       "aliases": [
6         "portal"
7       ],
8       "rr_type": "A",
9       "display_name": "portal.user-n1h0si.securelab.online",
10      "enable": true,
11      "persistence": true,
12      "persist_cidr_ipv6": 24,
13      "persist_cidr_ipv6": 56,
14      "persistence_ttl": 3600,
15      "proximity_rules": {
16        {
17          "region": "global",
18          "pool": "pools_usa",
19          "score": 1
20        }
21      }
22    },
23    "lbrs_auction": {
24      "aliases": [
25        "auction"
26      ],
27      "rr_type": "A",
28      "display_name": "auction.user-n1h0si.securelab.online",
29      "enable": true,
30      "persistence": false,
31      "proximity_rules": {
32        {
33          "region": "regions_usa",
34          "pool": "pools_usa",
35          "score": 1
36        }
37      }
38    },
39    "region": "regions_europe".

```

### b) Create New Load Balanced Service

Let's now create a new Load-balancing service via UI to copy the record to. To do that, you will first need to get "zone2".

1. Go back to Postman and open **Get DNS Zone(lab)** request. Copy "zone2" which is returned in its response.

The screenshot shows the Postman API client interface. The 'Body' tab is selected, displaying the JSON response of a 'Get DNS Zone(lab)' request. The response is a JSON object with a 'status' of 'ok' and two zone names: 'zone' and 'zone2'. The 'zone2' value, 'user-n1h0si-2.securelab.online', is highlighted with a red box.

```

1 {
2   "status": "ok",
3   "zone": "user-n1h0si.securelab.online",
4   "zone2": "user-n1h0si-2.securelab.online"
5 }

```

2. Open any text editor (say, **Notepad**) and paste the **JSON configuration**. Replace the existing zone name with the "zone2" copied from the Postman in the step above:

A new JSON configuration with the properties copied from the existing zone is ready.

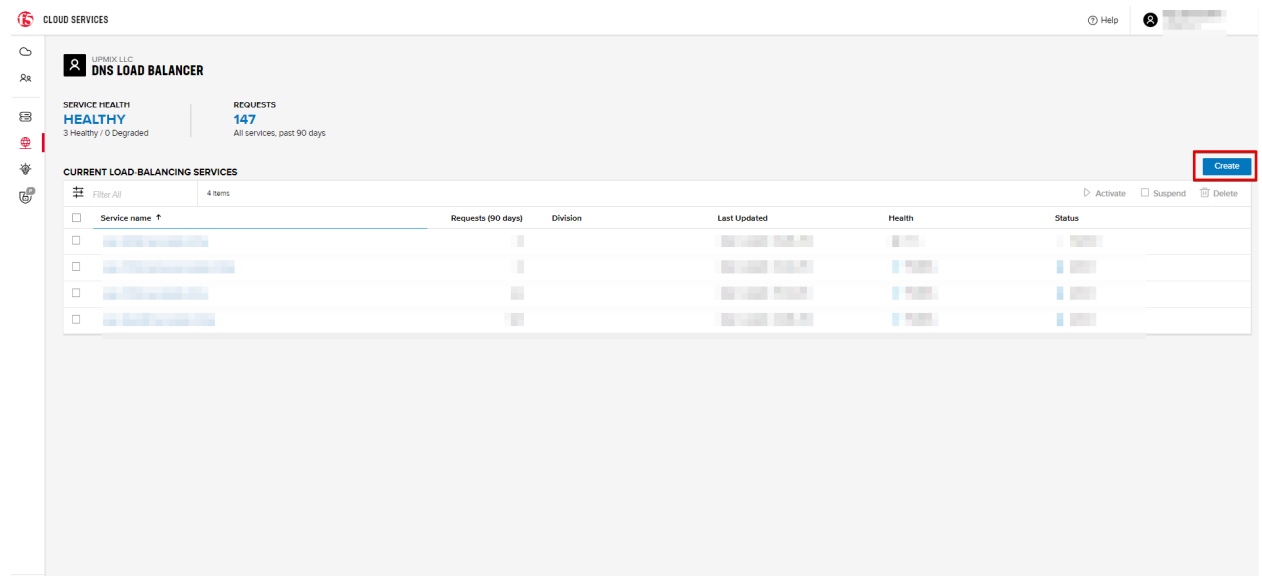
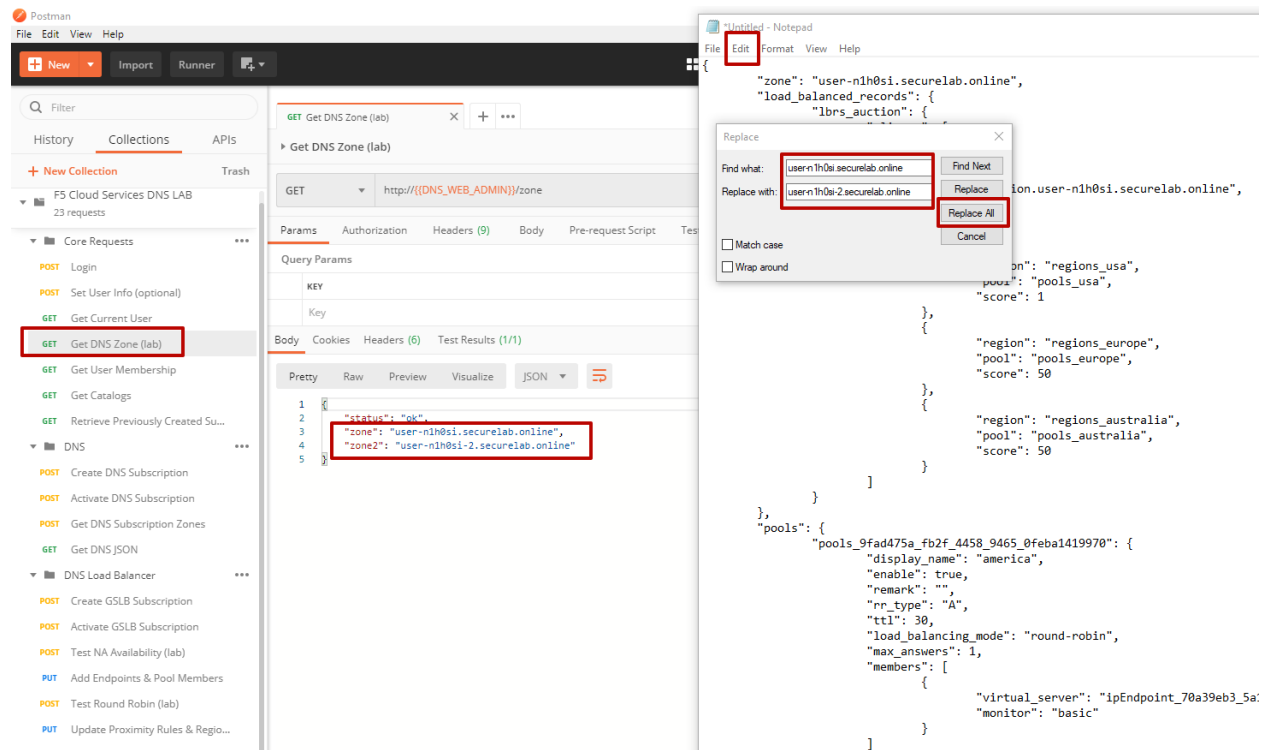
3. Return to the F5 Cloud Services portal and open the **DNS Load Balancer** tab. Click **Create**.

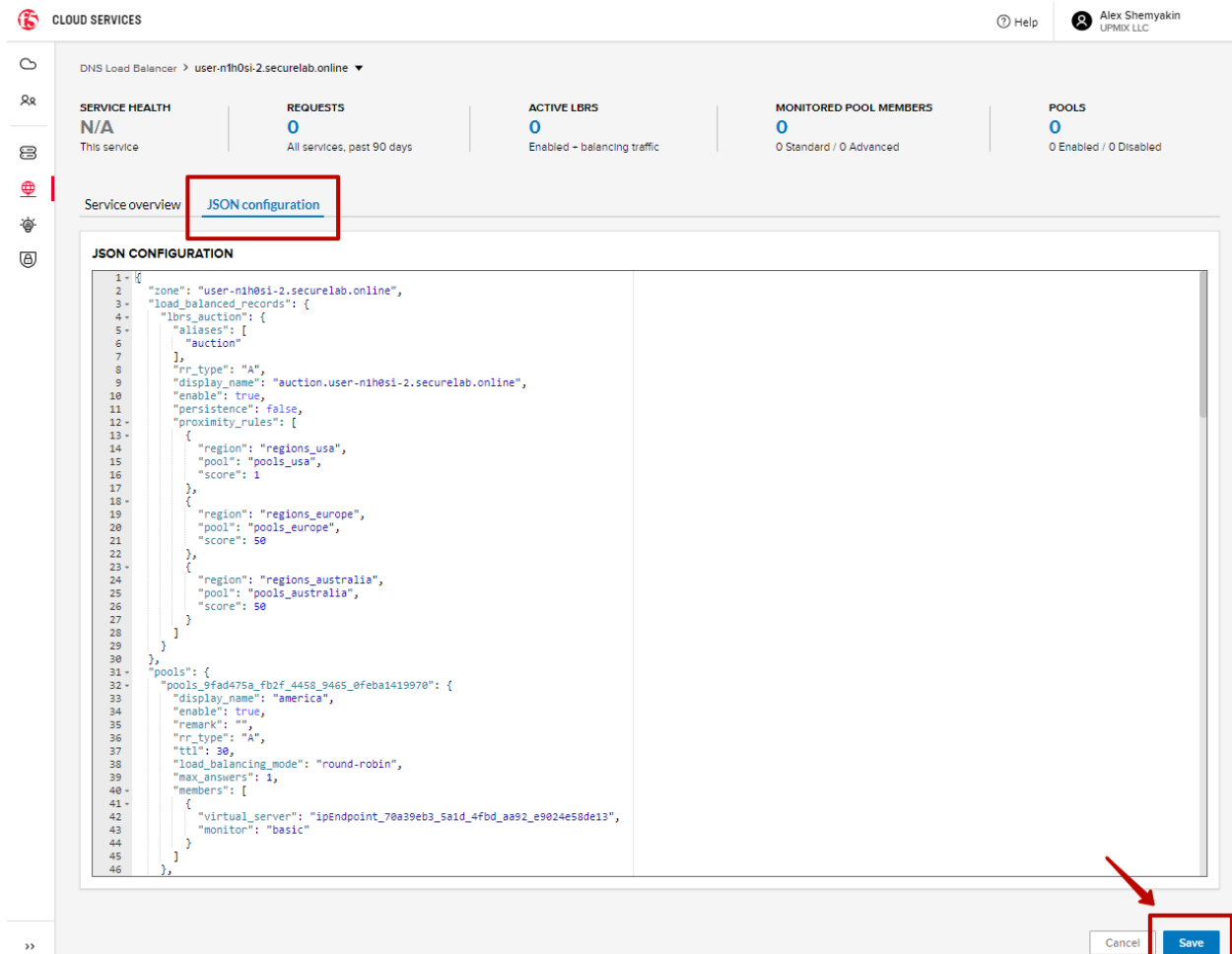
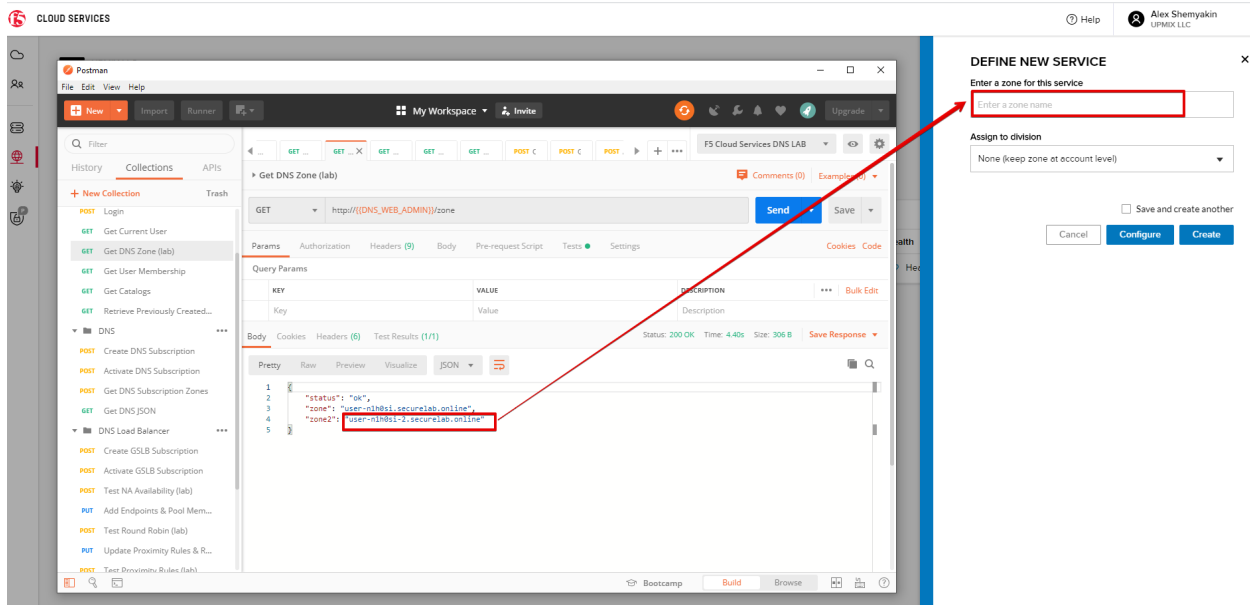
Paste "zone2" name which you copied in step 1 above and click **Create**.

### c) Update JSON

You have just created a new Load-balancing service. Let's configure it by duplicating the Load balanced record from the existing service.

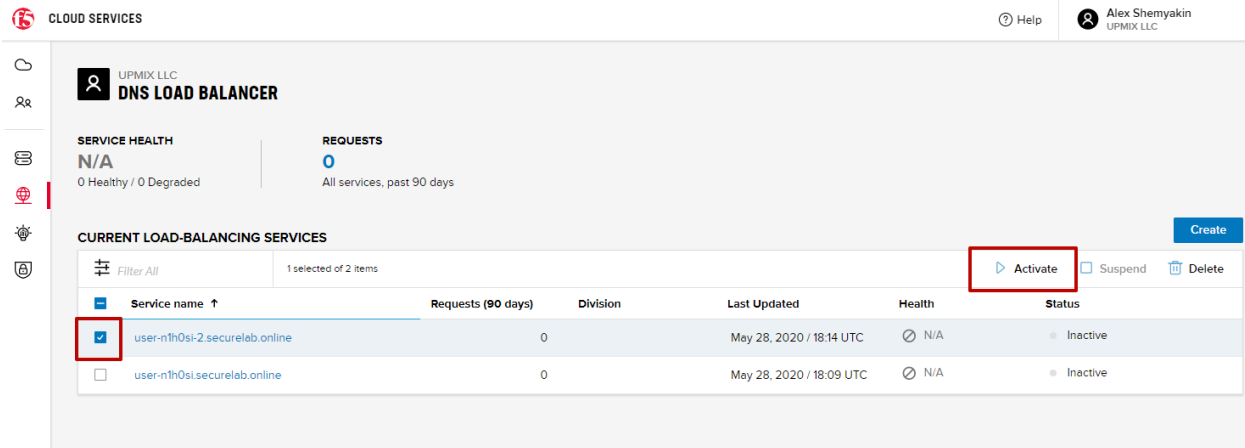
Click on your newly created service and open the **JSON configuration** tab. Paste the JSON which you created in step b) 2. above and click **Save**.





Go back to the newly created Load-balancing service to see the newly created record which is the copy of the original one.

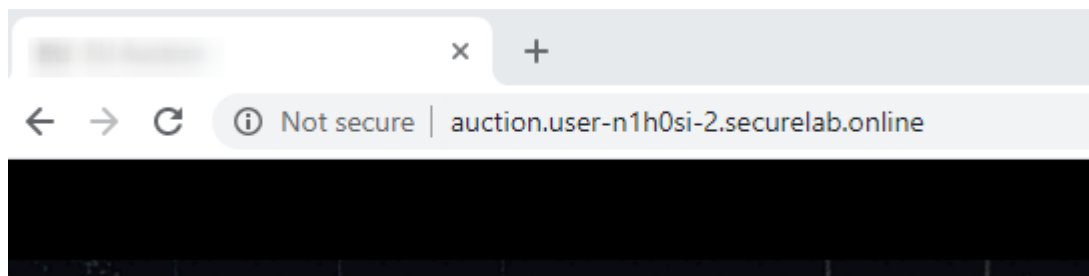
d) Go back to the DNS Load Balancer tab and activate the new DNS Load Balancer service by selecting **Activate** button:



Status will be updated a few seconds later.

e) Test via Browser

1. Open FQDN ("auction.{{zone-2 name}}") where {{zone-2 name}} is the value copied from postman in one of the step above) in your browser.



2. You will see that acc to the proximity rule and pool members, you will get to endpoints belonging to the **closest** pool in a round-robin manner.

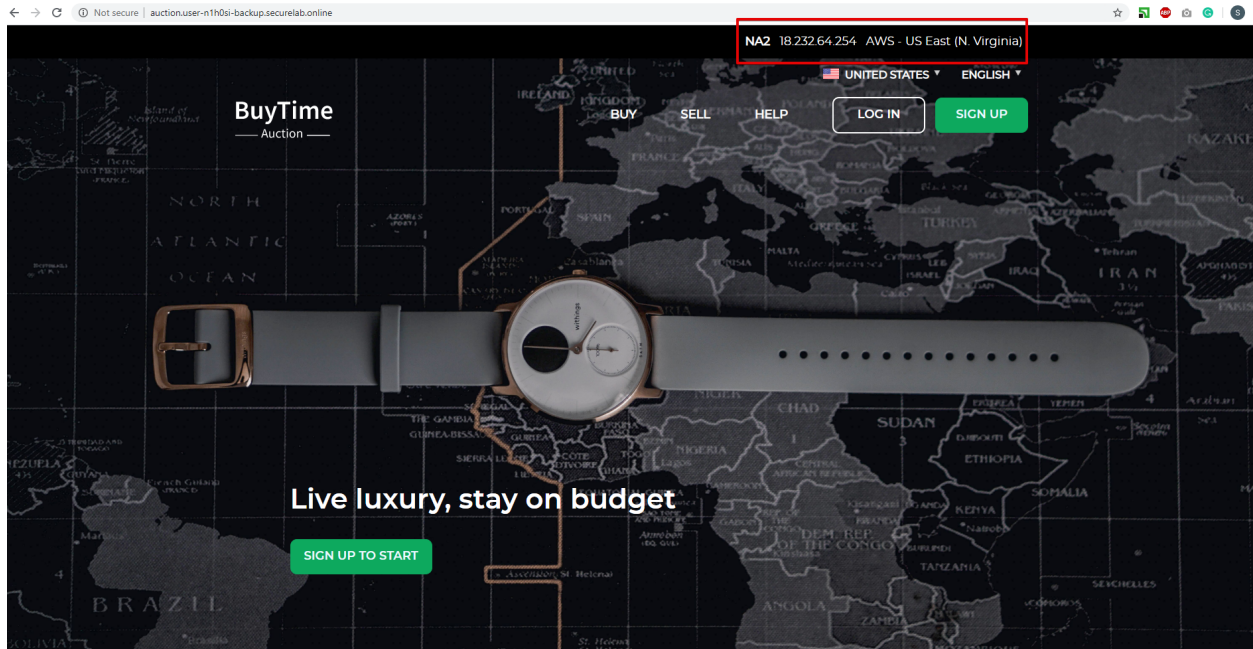
### 7.7.6 6. Delete DNS Load Balancer Service

1. Go back to the F5 Cloud Services portal, the **DNS Load Balancer** tab, and click on your load-balancing service.
2. Tick the records and click **Delete**, then confirm your choice.

## 7.8 F5 DNS Load Balancer Cloud Service - API

### 7.8.1 1. Create DNS Load Balancer Subscription

Select the **Create GSLB Subscription** request and click **Send** to create a new service instance of DNS Load Balancer using "account\_id" and "catalog\_id" retrieved a few steps above.



CLOUD SERVICES

UPMIX LLC  
DNS LOAD BALANCER

SERVICE HEALTH  
**HEALTHY**  
2 Healthy / 0 Degraded

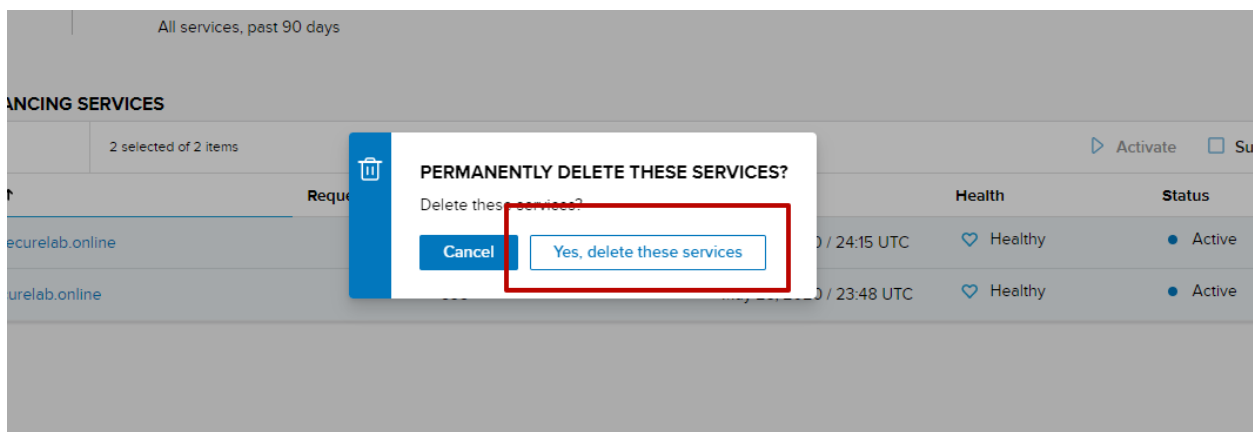
REQUESTS  
**325**  
All services, past 90 days

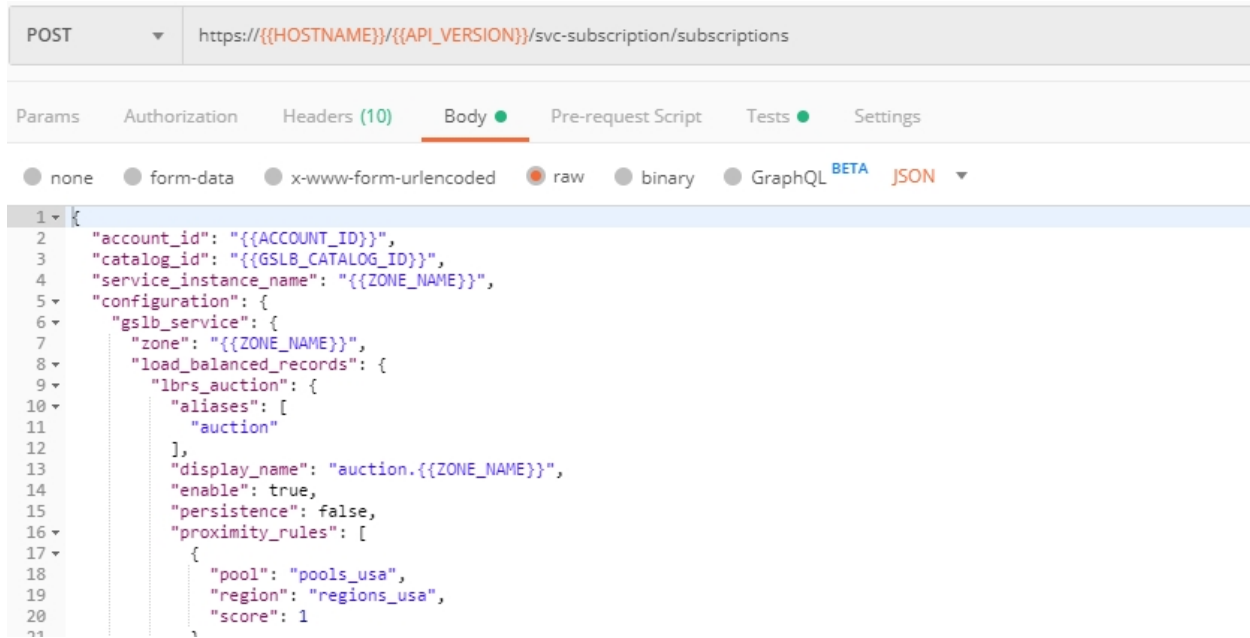
CURRENT LOAD-BALANCING SERVICES

Filter All 2 selected of 2 items

Activate Suspend Delete

Service name	Requests (90 days)	Division	Last Updated	Health	Status
<input checked="" type="checkbox"/> user-n1h0s1-2.securelab.online	0		May 29, 2020 / 24:15 UTC	Healthy	Active
<input checked="" type="checkbox"/> user-n1h0s1.securelab.online	325		May 28, 2020 / 23:48 UTC	Healthy	Active





You will see “subscription\_id” and created “service\_instance\_id” in the body. You may also note that this request will create only NA1 endpoint for now. Some more will be created in the subsequent requests.

You may also notice that the current proximity rule is set to send traffic from: Everyone -> Americas pool. This means that only one endpoint (NA1) will be serving all requests now. We will subsequently configure proper load balancing and geoproximity rules.

The retrieved “subscription\_id” is then stored for subsequent calls.

You can change its status from “DISABLED” to “ACTIVE” sending the **Activate GSLB Subscription** request below.

More detailed information on this API request can be found [here](#).

## 7.8.2 2. Activate DNS Load Balancer Subscription

Select the **Activate GSLB Subscription** request and click **Send**. This will deploy DNS Load Balancer using “subscription\_id” captured in one of the steps above.

You will see “active” subscription status.

More detailed information on this API request can be found [here](#).

## 7.8.3 3. Test NA Pool

Send the **Test NA Availability (lab)** request to execute a call against the Lab service API, which in turn uses an external VM (located in the USA) to run a “wget” to retrieve the response from <http://auction.cloudservicesdemo.net>. This should show the only available instance NA1 in the HTML that is returned.

The response shows that your first instance is available:



```

Pretty Raw Preview Visualize BETA JSON
1 {
2   "subscription_id": "s-aa2ZnQhK0h",
3   "account_id": "a-aaIQLhugvE",
4   "user_id": "u-aaLHtsH4PJ",
5   "catalog_id": "c-aaQnOrPjGu",
6   "service_instance_id": "gslb-aa79ePk7ri",
7   "status": "DISABLED",
8   "service_instance_name": "user-z4e2440.securelab.online",
9   "deleted": false,
10  "service_type": "gslb",
11  "configuration": {
12    "gslb_service": {
13      "load_balanced_records": {
14        "lbrs_auction": {
15          "aliases": [
16            "auction"
17          ],
18          "display_name": "auction.user-z4e2440.securelab.online",
19          "enable": true,
20          "persistence": false,
21          "proximity_rules": [
22            {
23              "pool": "pools_usa",
24              "region": "regions_usa",
25              "score": 1
26            }
27          ],
28          "rr_type": "A"
29        }
30      }
31    }
32  }
33 }

```

POST ▼ https://{{HOSTNAME}}/{{API\_VERSION}}/svc-subscription/subscriptions

Params Authorization Headers (10) Body ● Pre-request Script Tests ● Settings

```

1 pm.test("Set GSLB subscription id variable", function() {
2   var jsonData = pm.response.json();
3   pm.environment.set("GSLB_SUBSCRIPTION_ID", jsonData.subscription_id);
4 })
5

```

POST ▼ https://{{HOSTNAME}}/{{API\_VERSION}}/svc-subscription/subscriptions/{{GSLB\_SUBSCRIPTION\_ID}}/activate

Params Authorization Headers (10) Body ● Pre-request Script Tests Settings

● none ● form-data ● x-www-form-urlencoded ● raw ● binary ● GraphQL **BETA** JSON ▼

```

1 {
2   "subscription_id": "{{GSLB_SUBSCRIPTION_ID}}",
3   "omit_config": true
4 }

```

Body Cookies Headers (6) Test Results

Pretty Raw Preview Visualize BETA

JSON



```

1 {
2   "status": "ACTIVE",
3   "service_state": "DEPLOYING",
4   "subscription_id": " "
5 }

```

POST

http://{{DNS\_WEB\_ADMIN}}/proxy/northamerica

Params Authorization Headers (10) Body Pre-request Script Tests Settings

☐ none ☐ form-data ☐ x-www-form-urlencoded ☒ raw ☐ binary ☐ GraphQL BETA JSON

```

1 {
2   "domain": "auction.{{ZONE_NAME}}"
3 }

```

Body Cookies Headers (6) Test Results

Pretty Raw Preview Visualize BETA

HTML



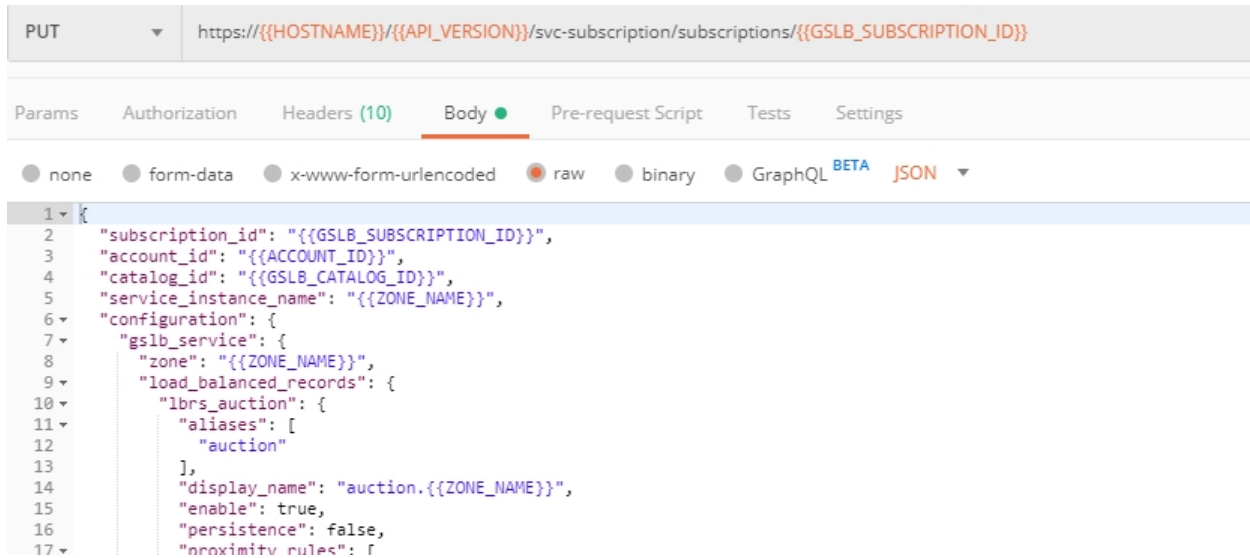
```

1 <!doctype html>
2 <html lang="en">
3
4 <head>
5   <meta charset="utf-8" />
6   <link rel="shortcut icon" href="/favicon.ico" />
7   <meta name="viewport" content="width=device-width,initial-scale=1" />
8   <meta name="theme-color" content="#000000" />
9   <title>NA1 Auction</title>
10  <link href="/static/css/3-66046cc7.chunk.css" rel="stylesheet">
11  <link href="/static/css/main.d2df78d6.chunk.css" rel="stylesheet">
12 </head>
13
14 <body><noscript>You need to enable JavaScript to run this app.</noscript>
15 <div id="root"></div>
16 <script>
17   !function(l){function e(e){for(var r,t,n=e[0],o=e[1],u=e[2],f=0,i=[];f<n.length;f++)t=n[f],p[t]&&i.push(p[t][0]);
    Object.prototype.hasOwnProperty.call(o,r)&&(l[r]=o[r]);for(s&&s(e);i.length;i.shift()){return c.push.apply(c,
    +){for(var t=c[r],n=!0,o=1;o<t.length;o++){var u=t[o];0!==p[u]&&(n=!1)}n&&(c.splice(r--,1),e=f(f.s=t[0]))}
    return t[e].exports;var r=t[e]={i:e,l:!1,exports:{}};return l[e].call(r.exports,r,r.exports,f),r.l=!0,r.e=
    Object.defineProperty(e,r,{enumerable:!0,get:t}}),f.r=function(e){("undefined"!=typeof Symbol&&Symbol.toString
    {value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},f.t=function(r,e){if(1&&(r=f(r)),8&
    return r;var t=Object.create(null);if(f.r(t),Object.defineProperty(t,"default",{enumerable:!0,value:r}),2&
    {return r[e]}.bind(null,n));return t},f.n=function(e){var r=e&&e.__esModule?function(){return e.default}:f
    (e,r){return Object.prototype.hasOwnProperty.call(e,r)},f.p="/";var r=window.webpackJsonp=window.webpackJs

```

## 7.8.4 4. Add Endpoints & Pool Members

Send the **Add Endpoint & Pool Members** request to add a few more endpoints for load balancing of the application. Note that three of the new endpoints (EU and NA2) are deployed on Amazon AWS, and one (NA3) is running on Microsoft Azure. NA1, NA2, and NA3 endpoints are aggregated into a pool “usa”, which demonstrates multi-cloud load balancing.



You will see all the information on the added endpoints:

## 7.8.5 5. Test Round Robin (lab)

Run the **Test Round Robin (lab)** request to check the response from the Lab service API to test what instance is now being returned. This should show a result different from the previous due to the newly-configured round-robin load balancing.

**NOTE:** it's possible that you will still get the same endpoint in the response due to either DNS caching or 1/3 chance of the same endpoint to be pulled from the load-balance pool. Let's try:

And check the response:

You can send the same request to check other instances.

## 7.8.6 6. Update Proximity Rule

Run the **Update Proximity Rules & Regions**. This adds a new region “europe”, and assigns a EU endpoint to it. It also updates the DNS Load Balancer with new proximity rules: to send the traffic originating in Europe to the “europe” pool, utilizing a higher relative score than the previous rule of routing traffic from “Anywhere” to the “usa” pool. This type of geo-proximity based routing is useful for GDPR compliance.

And you will see all the information on available pools and regions:

## 7.8.7 7. Test Proximity Rules (lab)

Send the **Test Proximity Rules (lab)** request, which uses an external VM (located in Europe) to run a “wget” to retrieve the response from <http://auction.cloudservicesdemo.net>. This simulates what an EU-

PrettyRawPreviewVisualize BETA

JSON

```
24         "region": "global",
25         "score": 1
26     },
27 ],
28     "rr_type": "A"
29 },
30 },
31 "pools": {
32     "pools_europe": {
33         "display_name": "europe",
34         "enable": true,
35         "load_balancing_mode": "round-robin",
36         "max_answers": 1,
37         "members": [
38             {
39                 "final": null,
40                 "monitor": "basic",
41                 "virtual_server": "ipEndpoint_eu_auction"
42             }
43         ],
44         "remark": "",
45         "rr_type": "A",
46         "ttl": 30
47     },
48     "pools_usa": {
49         "display_name": "usa",
50         "enable": true,
51         "load_balancing_mode": "round-robin",
52         "max_answers": 1,
53         "members": [
54             {
```

POST

http://{{DNS\_WEB\_ADMIN}}/proxy/northamerica

ParamsAuthorizationHeaders (10)BodyPre-request ScriptTestsSettings

☐ none

☐ form-data

☐ x-www-form-urlencoded

☒ raw

☐ binary

☐ GraphQL BETA

JSON

```
1 {
2     "domain": "auction.{{ZONE_NAME}}"
3 }
```

Body Cookies Headers (6) Test Results

Pretty Raw Preview Visualize BETA

HTML



```

1 <!doctype html>
2 <html lang="en">
3
4 <head>
5   <meta charset="utf-8" />
6   <link rel="shortcut icon" href="/favicon.ico" />
7   <meta name="viewport" content="width=device-width,initial-scale=1" />
8   <meta name="theme-color" content="#000000" />
9   <title>NA3 Auction</title>
10  <link href="/static/css/0.66646cc7.chunk.css" rel="stylesheet">
11  <link href="/static/css/main.d2df78d6.chunk.css" rel="stylesheet">
12 </head>
13
14 <body><noscript>You need to enable JavaScript to run this app.</noscript>
15 <div id="root"></div>
16 <script>
17   !function(l){function e(e){for(var r,t,n=e[0],o=e[1],u=e[2],f=0,i=[];f<n.length;f++)t=n[f],p[t]&&i.push(p[t][
    Object.prototype.hasOwnProperty.call(o,r)&&(l[r]=o[r]);for(s&&s(e);i.length;i.shift());return c.push.ap
    +){for(var t=c[r],n=!0,o=1;o<t.length;o++){var u=t[o];0!=p[u]&&(n=!1)}n&&(c.splice(r--,1),e=f(f.s=t[0]));
    return t[e].exports;var r=t[e]={i:e,l:!1,exports:{}};return l[e].call(r.exports,r,r.exports,f),r.l=!0,r.e
    Object.defineProperty(r,r,{enumerable:!0,get:t}}),f.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStr
    {value:"Module"}},Object.defineProperty(e,"__esModule",{value:!0}}),f.t=function(r,e){if(1&e&&(r=f(r)),8&
    return r;var t=Object.create(null);if(f.r(t),Object.defineProperty(t,"default",{enumerable:!0,value:r})),2&
    {return r[e]}.bind(null,n));return t},f.n=function(e){var r=e&&e.__esModule?function(){return e.default}:
    (e,r){return Object.prototype.hasOwnProperty.call(e,r),f.p="/" ;var r=window.webpackJsonp=window.webpackJ
    o=0;o<r.length;o++)e(r[o]);var s=n;a()}([l]
18 </script>

```

PUT https://{{HOSTNAME}}/{{API\_VERSION}}/svc-subscription/subscriptions/{{GSLB\_SUBSCRIPTION\_ID}}

Params Authorization Headers (10) Body Pre-request Script Tests Settings

☐ none
☐ form-data
☐ x-www-form-urlencoded
☒ raw
☐ binary
☐ GraphQL BETA
☐ JSON

```

1 {
2   "subscription_id": "{{GSLB_SUBSCRIPTION_ID}}",
3   "account_id": "{{ACCOUNT_ID}}",
4   "catalog_id": "{{GSLB_CATALOG_ID}}",
5   "service_instance_name": "{{ZONE_NAME}}",
6   "configuration": {
7     "gslb_service": {
8       "zone": "{{ZONE_NAME}}",
9       "load_balanced_records": {
10        "lbrs_auction": {
11          "aliases": [
12            "auction"
13          ],
14          "display_name": "auction.{{ZONE_NAME}}",
15          "enable": true,
16          "persistence": false,
17          "proximity_rules": [
18            {
19              "pool": "pools_usa",
20              "region": "regions usa",

```

```

40  },
41  "pools": {
42    "pools_australia": {
43      "display_name": "australia",
44      "enable": true,
45      "load_balancing_mode": "round-robin",
46      "max_answers": 1,
47      "members": [
48        {
49          "final": null,
50          "monitor": "basic",
51          "virtual_server": "ipEndpoint_au_auction"
52        }
53      ],
54      "remark": "",
55      "rr_type": "A",
56      "ttl": 30
57    },
58    "pools_europe": {
59      "display_name": "europe",
60      "enable": true,
61      "load_balancing_mode": "round-robin",
62      "max_answers": 1,
63      "members": [
64        {
65          "final": null,
66          "monitor": "basic",

```

based customer would see when opening this URL in their browser. NOTE: you can also test this in your Opera browser (using EU proxy), the way you've done it previously with the UI.

```

POST http://{{DNS_WEB_ADMIN}}/proxy/europe

Params  Authorization  Headers (10)  Body  Pre-request Script  Tests  Settings
none  form-data  x-www-form-urlencoded  raw  binary  GraphQL BETA  JSON
1  {
2    "domain": "auction.{{ZONE_NAME}}"
3  }

```

Here's what you should see in the response:

## 7.8.8 8. Review the JSON

Let's now see the structure of the JSON. In order to get the JSON, send the **Get GSLB JSON** request which uses your ACCESS\_TOKEN to retrieve the JSON:

The response will retrieve the JSON containing all the DNS Load Balancer instance information:

As you can see, the JSON provides some general information on subscription\_id, user\_id, and instance name, as well as all configuration details. The configuration section "details" includes information on "pools\_health":

```

Pretty Raw Preview Visualize BETA HTML
1 <!doctype html>
2 <html lang="en">
3 <script>
4   (function(d){var grbrCookies=d.cookie;window.GRBRAsyncInit=function(){GRBRInit("5d5176c08d8d5b00285593bd",grbrCook
      proto=d.location.protocol||d.location.href.split("://",1)[0];var url=proto+"//d11m8axes1h5ea.cloudfront.net/gral
      grbr.async=true;grbr.src=url;var s=d.getElementsByTagName("script")[0];s.parentNode.insertBefore(grbr,s);})(doc
5 </script>
6
7 <head>
8   <meta charset="utf-8" />
9   <link rel="shortcut icon" href="/favicon.ico" />
10  <meta name="viewport" content="width=device-width,initial-scale=1" />
11  <meta name="theme-color" content="#000000" />
12  <title>EU Auction</title>
13  <link href="/static/css/2.00946cc7.chunk.css" rel="stylesheet">
14  <link href="/static/css/main.d2df78d6.chunk.css" rel="stylesheet">
15 </head>
16
17 <body><noscript>You need to enable JavaScript to run this app.</noscript>
18 <div id="root"></div>
19 <script>
20   !function(l){function e(e){for(var r,t,n=e[0],o=e[1],u=e[2],f=0,i=[];f<n.length;f++)t=n[f],p[t]&&i.push(p[t][0]
      Object.prototype.hasOwnProperty.call(o,r)&&(l[r]=o[r]);for(s&&s(e);i.length;)i.shift();return c.push.app
      +){for(var t=c[r],n=!0,o=1;o<t.length;o++){var u=t[o];0!==p[u]&&(n=!1)}n&&(c.splice(r--,1),e=f(f.s=t[0]));
      return t[e].exports;var r=t[e]={i:e,l:!1,exports:{}};return l[e].call(r.exports,r,r.exports,f),r.l=!0,r.ex
      Object.defineProperty(e,r,{enumerable:!0,get:t}}),f.r=function(e){"undefined"!=typeof Symbol&&Symbol.toString
      {value:"Module"}},Object.defineProperty(e,"__esModule",{value:!0}),f.t=function(r,e){if(1&e&&(r=f(r)),8&e
      return r;var t=Object.create(null);if(f.r(t),Object.defineProperty(t,"default",{enumerable:!0,value:r}),2&e
      {return r[e]}.bind(null,n));return t},f.n=function(e){var r=e&&e.__esModule?function(){return e.default}:f

```

GET

▼

https://{{HOSTNAME}}/{{API\_VERSION}}/svc-subscription/subscriptions/{{GSLB\_SUBSCRIPTION\_ID}}

Params

Authorization

Headers (9)

Body

Pre-request Script

Tests

Settings

▼ Headers (2)

	KEY	VALUE
<input checked="" type="checkbox"/>	Content-Type	application/json
<input checked="" type="checkbox"/>	Authorization	Bearer {{ACCESS_TOKEN}}
	Key	Value

► Temporary Headers (7) ⓘ

```
1  {
2    "subscription_id": "s-aa6JL5ezUP",
3    "account_id": "a-aaIQLhugvE",
4    "user_id": "u-aaLHtsH4PJ",
5    "catalog_id": "c-aaQnOrPjGu",
6    "service_instance_id": "gslb-aaI_uof5Q",
7    "status": "ACTIVE",
8    "service_instance_name": "user-nlh0si.securelab.online",
9    "deleted": false,
10   "service_type": "gslb",
11   "configuration": {
12     "details": {
13       "lbr_metadata": {
14         "active_lbr_count": 1,
15         "active_pool_member_advanced_monitor_count": 0,
16         "active_pool_member_standard_monitor_count": 0
17       },
18       "pools_health": {
19         "pools_australia": {
20           "members_health": [
21             {
22               "details": [],
23               "health": "GREEN",
24               "monitor": "none",
25               "virtual_server": "ipEndpoint_au_auction"
26             }
27           ]
28         },
29         "pools_europe": {
30           "members_health": [
31             {
32               "details": [],
33               "health": "GREEN",
34               "monitor": "none",
35               "virtual_server": "ipEndpoint_eu_auction"
36             }
37           ]
38         },
39         "pools_usa": {
40           "members_health": [
41             {
42               "details": [],
43               "health": "GREEN",
44               "monitor": "none",
45               "virtual_server": "ipEndpoint_usa_auction"
46             }
47           ]
48         }
49       }
50     }
51   }
52 }
```



```

11  "configuration": {
12    "details": {
13      "lbr_metadata": {
14        "active_lbr_count": 1,
15        "active_pool_member_advanced_monitor_count": 0,
16        "active_pool_member_standard_monitor_count": 0
17      },
18      "pools_health": {
19        "pools_australia": {
20          "members_health": [
21            {
22              "details": [],
23              "health": "GREEN",
24              "monitor": "none",
25              "virtual_server": "ipEndpoint_au_auction"
26            }
27          ]
28        },
29        "pools_europe": {
30          "members_health": [
31            {
32              "details": [],
33              "health": "GREEN",
34              "monitor": "none",
35              "virtual_server": "ipEndpoint_eu_auction"
36            }
37          ]
38        },
39        "pools_usa": {
40          "members_health": [
41            {
42              "details": [],

```

The next configuration section is “gslb\_service” which contains “load\_balanced\_records” with their “name” and “proximity\_rules”:

It also includes “pools” section with their “name”, “load\_balancing\_mode” and “members”:

One more section is “regions” which includes information on region “names” and “sectors”:

And another section provides information on “virtual\_servers”: their IP endpoints, addresses, names, monitors and ports:

### 7.8.9 9. Delete DNS Load Balancer Service

Send the **Retire GSLB Subscription** request which uses the relevant “subscription\_id”.

You will see “retired” status in the response body which means that it’s not available on the F5 Cloud Services portal anymore.

## 7.9 Clean Up

Send the **Retire DNS Zone** to remove or reset zone file. You will get response with status code “200 OK”.

We recommend that you clear your tokens from the Lab Service API for security purposes. In order to do that, send the **Logout** request, which uses your **ACCESS\_TOKEN**:

You will get the following response with the status showing “200 OK”:

Your **ACCESS\_TOKEN** will be considered invalid:

```
63     "gslb_service": {
64         "load_balanced_records": {
65             "lbrs_auction": {
66                 "aliases": [
67                     "auction"
68                 ],
69                 "display_name": "auction.user-nlh0si.securelab.online",
70                 "enable": true,
71                 "persistence": false,
72                 "proximity_rules": [
73                     {
74                         "pool": "pools_usa",
75                         "region": "regions_usa",
76                         "score": 1
77                     },
78                     {
79                         "pool": "pools_europe",
80                         "region": "regions_europe",
81                         "score": 50
82                     },
83                     {
84                         "pool": "pools_australia",
85                         "region": "regions_australia",
86                         "score": 50
87                     }
88                 ],
89             }
90         }
91     }
```

```
91     "pools": {
92         "pools_australia": {
93             "display_name": "australia",
94             "enable": true,
95             "load_balancing_mode": "round-robin",
96             "max_answers": 1,
97             "members": [
98                 {
99                     "final": null,
100                     "monitor": "basic",
101                     "virtual_server": "ipEndpoint_au_auction"
102                 }
103             ],
104             "remark": "",
105             "rr_type": "A",
106             "ttl": 30
107         },
108         "pools_europe": {
109             "display_name": "europe",
110             "enable": true,
111             "load_balancing_mode": "round-robin",
112             "max_answers": 1,
113             "members": [
114                 {
115                     "final": null,
116                     "monitor": "basic",
117                     "virtual_server": "ipEndpoint_eu_auction"
118                 }
119             ]
120         }
121     }
```

```
151     },
152     "regions": {
153       "regions_australia": {
154         "display_name": "australia",
155         "sectors": [
156           {
157             "code": "OC",
158             "scale": "continent"
159           }
160         ],
161       },
162       "regions_europe": {
163         "display_name": "europe",
164         "sectors": [
165           {
166             "code": "EU",
167             "scale": "continent"
168           }
169         ],
170       },
171       "regions_usa": {
172         "display_name": "usa",
173         "sectors": [
174           {
175             "code": "NA",
176             "scale": "continent"
177           }
178         ],
179       }
180     },
181     "virtual_servers": {
```



JSON editor showing the configuration for virtual servers. The configuration is a JSON object with a "virtual\_servers" array and a "zone" property. A red box highlights the "virtual\_servers" array, and a red arrow points to it from the "zone" property.

```
177
178
179
180
181 "virtual_servers": {
182   "ipEndpoint_au_auction": {
183     "address": "54.206.13.195",
184     "display_name": "au-auction",
185     "monitor": "none",
186     "port": 80
187   },
188   "ipEndpoint_eu_auction": {
189     "address": "3.122.191.227",
190     "display_name": "eu-auction",
191     "monitor": "none",
192     "port": 80
193   },
194   "ipEndpoint_na1_auction": {
195     "address": "34.229.48.248",
196     "display_name": "na1-auction",
197     "monitor": "none",
198     "port": 80
199   },
200   "ipEndpoint_na2_auction": {
201     "address": "18.232.64.254",
202     "display_name": "na2-auction",
203     "monitor": "none",
204     "port": 80
205   },
206   "ipEndpoint_na3_auction": {
207     "address": "52.226.147.184",
208     "display_name": "na3-auction",
209     "monitor": "none",
210     "port": 80
211   }
212 },
213 "zone": "user-nlh0si.securelab.online"
```

POST [https://{{HOSTNAME}}/{{API\\_VERSION}}/svc-subscription/subscriptions/{{GSLB\\_SUBSCRIPTION\\_ID}}/retire](https://{{HOSTNAME}}/{{API_VERSION}}/svc-subscription/subscriptions/{{GSLB_SUBSCRIPTION_ID}}/retire)

Params Authorization Headers (10) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL BETA JSON

```
1 {
2   "subscription_id": "{{GSLB_SUBSCRIPTION_ID}}",
3   "omit_config": true
4 }
```

Body Cookies Headers (6) Test Results


Pretty Raw Preview Visualize BETA JSON

```
1 {
2   "status": "RETIRED",
3   "service_state": "UNDEPLOYING",
4   "subscription_id": "..."
5 }
```

Retire DNS Zone (lab) Comments 0 Ex

POST ▼ `http://{{DNS_WEB_ADMIN}}/zone/retire` Send ▼

Body Cookies Headers (6) Test Results Status: 200 OK Time: -- Size: 226 B Save

Pretty Raw Preview Visualize JSON ▼ 

```
1 {  
2   "status": "ok"  
3 }
```


POST ▼ `https://{{HOSTNAME}}/{{API_VERSION}}/svc-auth/logout`

Params Authorization Headers (9) Body ● Pre-request Script Tests ● Settings

none form-data x-www-form-urlencoded raw ● binary GraphQL JSON ▼

```
1 {  
2   "access_token": "{{ACCESS_TOKEN}}"  
3 }  
4
```

Cookies Headers (6) Test Results (1/1) Status: 200 OK 1

etty Raw Preview Visualize JSON ▼ 

```
1 {}
```

POST ▼ `https://{{HOSTNAME}}/{{API_VERSION}}/svc-auth/logout`

Params Authorization Headers (9) Body ● Pre-request Script Tests ● Settings

```
1 pm.test("Reset token variable", function() {  
2   pm.environment.set("ACCESS_TOKEN", "");  
3 })  
4
```



- Agility 2020:

Bill Wester

Brandon Burns

Dave Doucette

Pat Fiorino

Matt Harmon

Bret Pleines

Nick Stathakis

Brian Van Lieu

Greg Robinson

Fred Wittenberg

WE MAKE APPS  FASTER.  
SMARTER.  
SAFER.

F5 Networks, Inc. | [f5.com](https://f5.com)



US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: [info@f5.com](mailto:info@f5.com) // Asia-Pacific: [apacinfo@f5.com](mailto:apacinfo@f5.com) // Europe/Middle East/Africa: [emeainfo@f5.com](mailto:emeainfo@f5.com) // Japan: [f5j-info@f5.com](mailto: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](https://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.