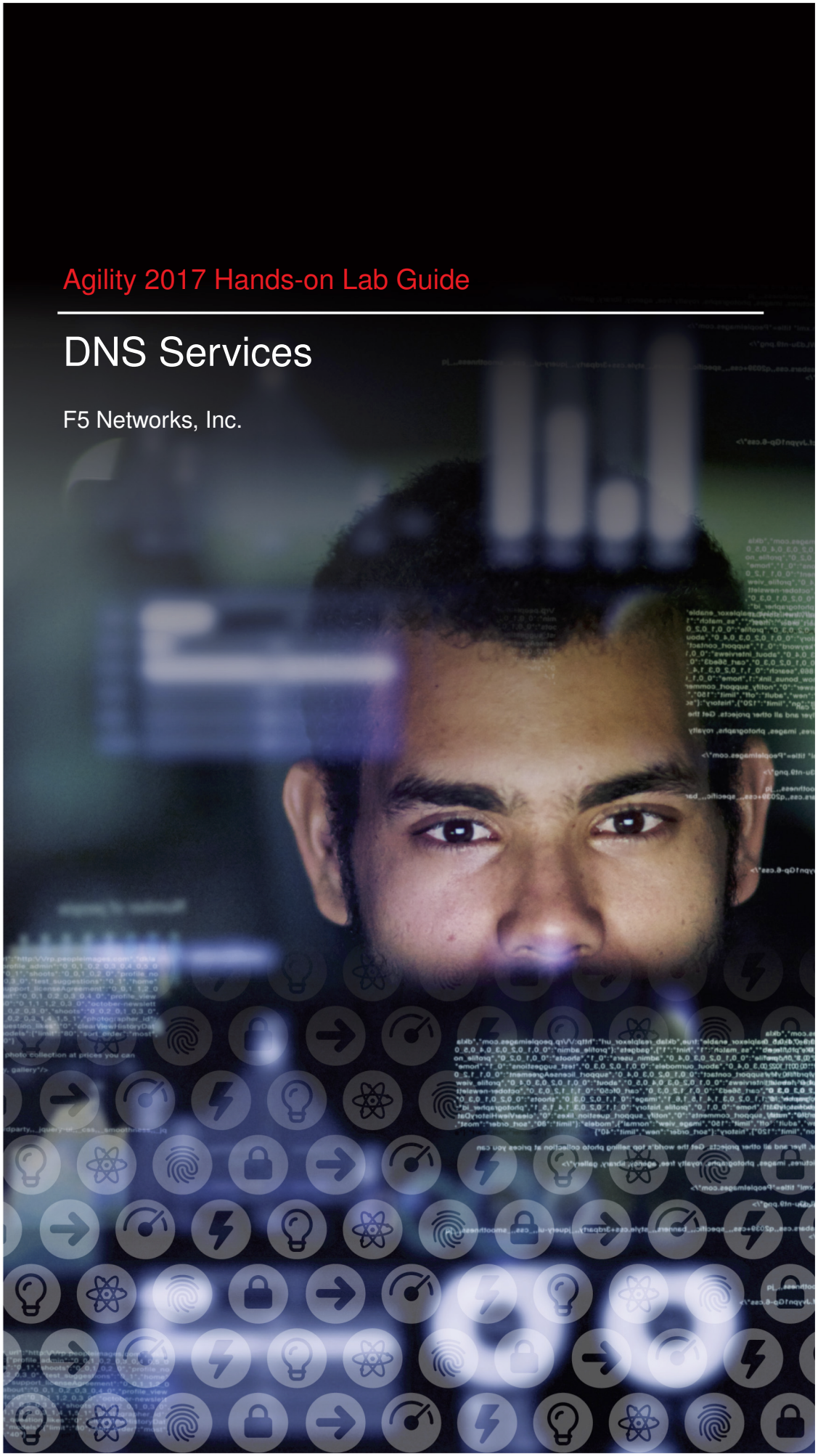


Agility 2017 Hands-on Lab Guide

# DNS Services

F5 Networks, Inc.

# Contents:


**1 Lab Environment** **5**

**2 Class 1 - Availability** **11**
2.1 Settings . . . 12
2.2 Listeners . . . 13
2.2.1 Logging . . . 13
2.2.2 DNS Profile . . . 17
2.2.3 UDP Profile . . . 20
2.2.4 TCP Profile . . . 21
2.2.5 UDP IP Address . . . 23
2.2.6 TCP IP Address . . . 26
2.3 Datacenters . . . 28
2.3.1 Servers . . . 29
2.3.1.1 gtm1.site1 . . . 30
2.3.1.2 gtm1.site2 . . . 35
2.3.1.3 site1_ha-pair . . . 39
2.3.1.4 site2_ha-pair . . . 44
2.3.2 Device Trust . . . 50
2.3.3 Sync Group . . . 53
2.4 Pools . . . 54
2.5 FQDN . . . 57
2.6 Delegation . . . 59
2.6.1 A Records . . . 59
2.6.2 Sub Domain . . . 60
2.6.3 CNAME . . . 66
2.7 Results . . . 69
2.8 Persistence . . . 74
2.9 LB Methods . . . 77

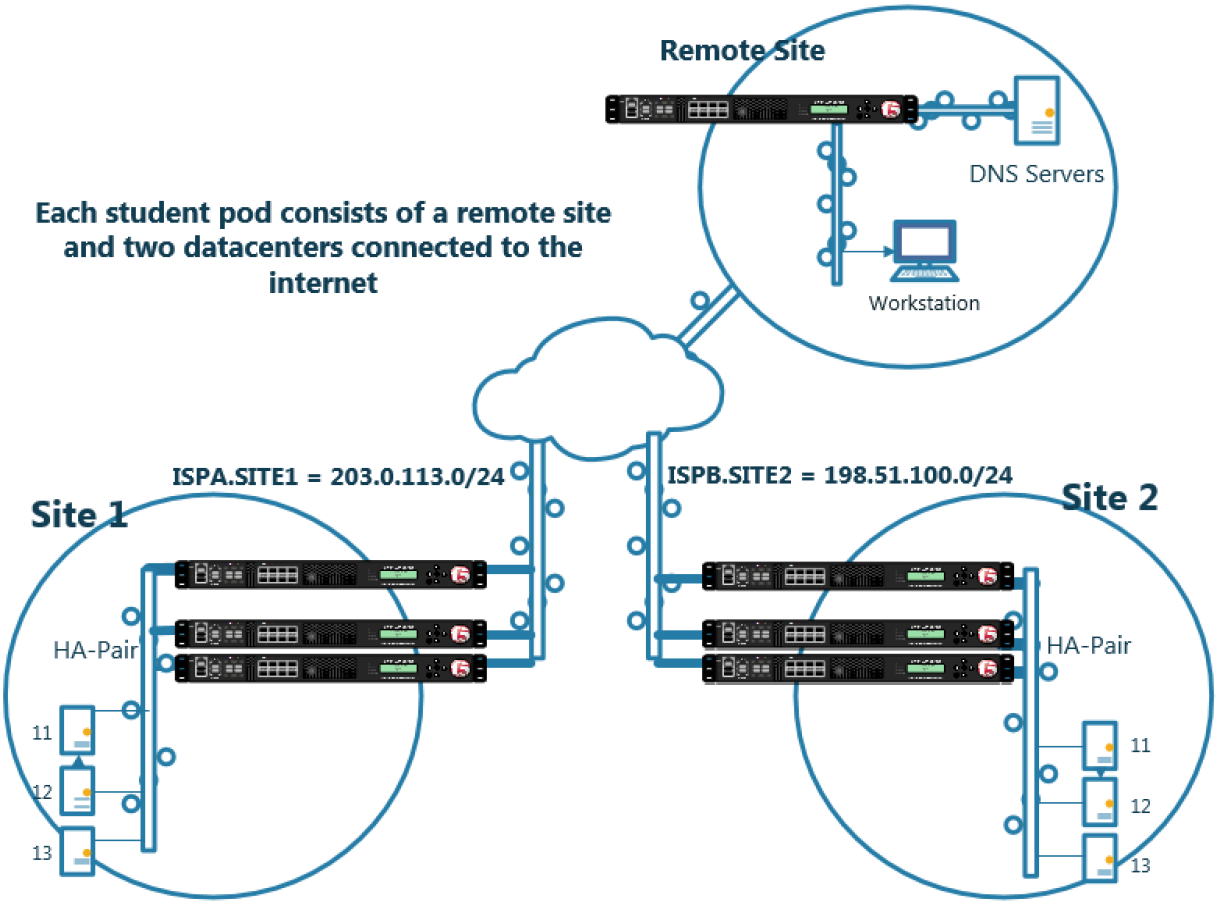
**3 Class 2 - Security** **83**
3.1 Transparent Cache . . . 84
3.1.1 Monitors . . . 84
3.1.2 Load Balancing . . . 86
3.1.3 Results . . . 89
3.2 Listeners . . . 95

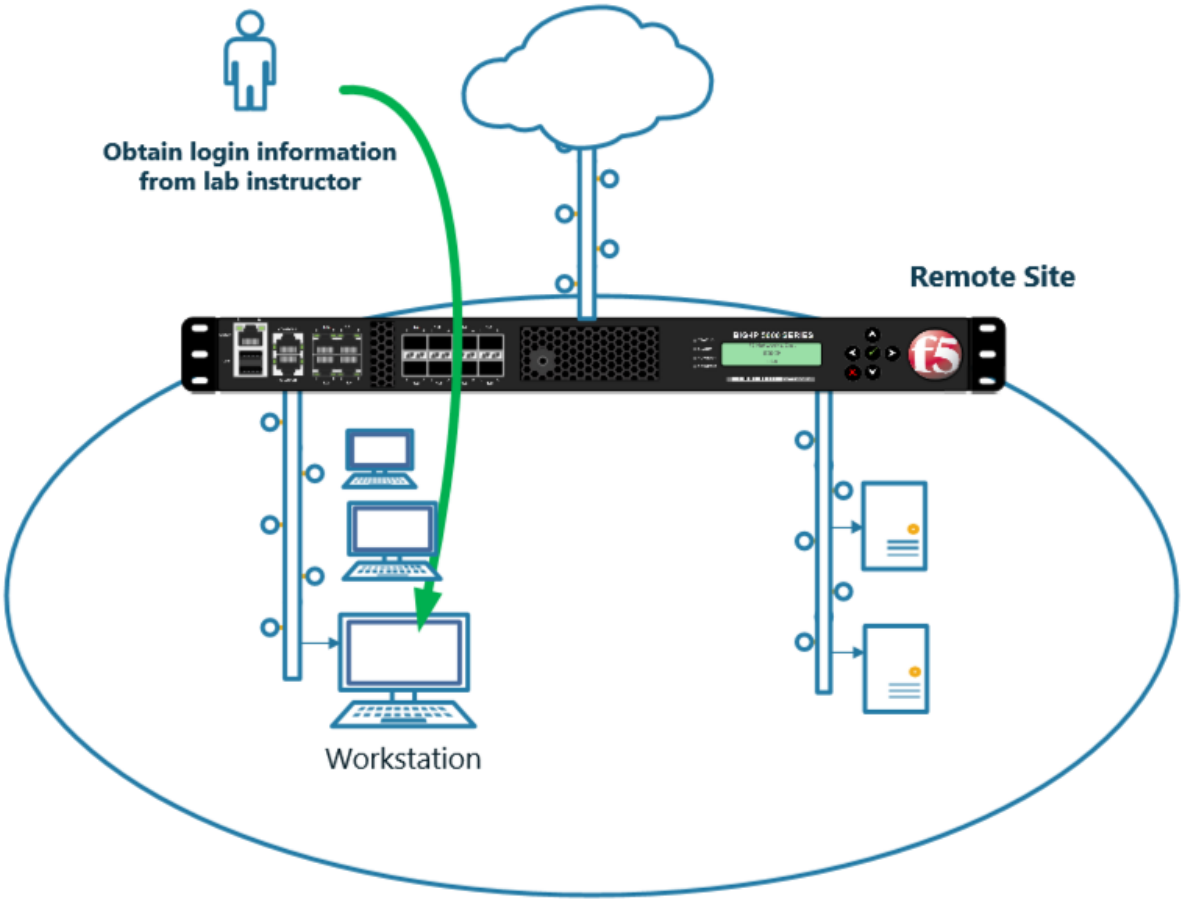
3.2.1 Log Profile . . . 96
3.2.2 DNS Profile . . . 100
3.2.3 UDP Profile . . . 103
3.2.4 TCP Profile . . . 104
3.2.5 UDP Listener . . . 106
3.2.6 TCP Listeners . . . 109
3.2.7 Results . . . 112
3.3 Hidden Master . . . 115
3.3.1 Name Server . . . 115
3.3.2 DNS Express . . . 117
3.4 DNSSec . . . 120
3.4.1 Zone Signing Key . . . 120
3.4.2 Key Signing Key . . . 122
3.4.3 Signed Zone . . . 124
3.4.4 Results . . . 126
3.5 Validating Resolver . . . 127
3.5.1 Trust Anchors . . . 127
3.5.2 DLV Anchors . . . 131
3.5.3 Modify DNS Profile . . . 132
3.5.4 Results . . . 135
3.6 RPZ . . . 143
3.6.1 Zone Runner . . . 143
3.6.2 Name Server . . . 147
3.6.3 DNS Express . . . 149
3.6.4 Local Zone . . . 151
3.6.5 Walled Garden . . . 154
3.6.6 Results . . . 156
3.7 URL Categorization . . . 156
3.7.1 Create an iRule . . . 157
3.7.2 iRule assignment . . . 159
3.7.3 Results . . . 162
3.8 IP Intelligence . . . 168
3.8.1 Create an iRule . . . 168
3.8.2 iRule assignment . . . 170
3.8.3 Results . . . 172

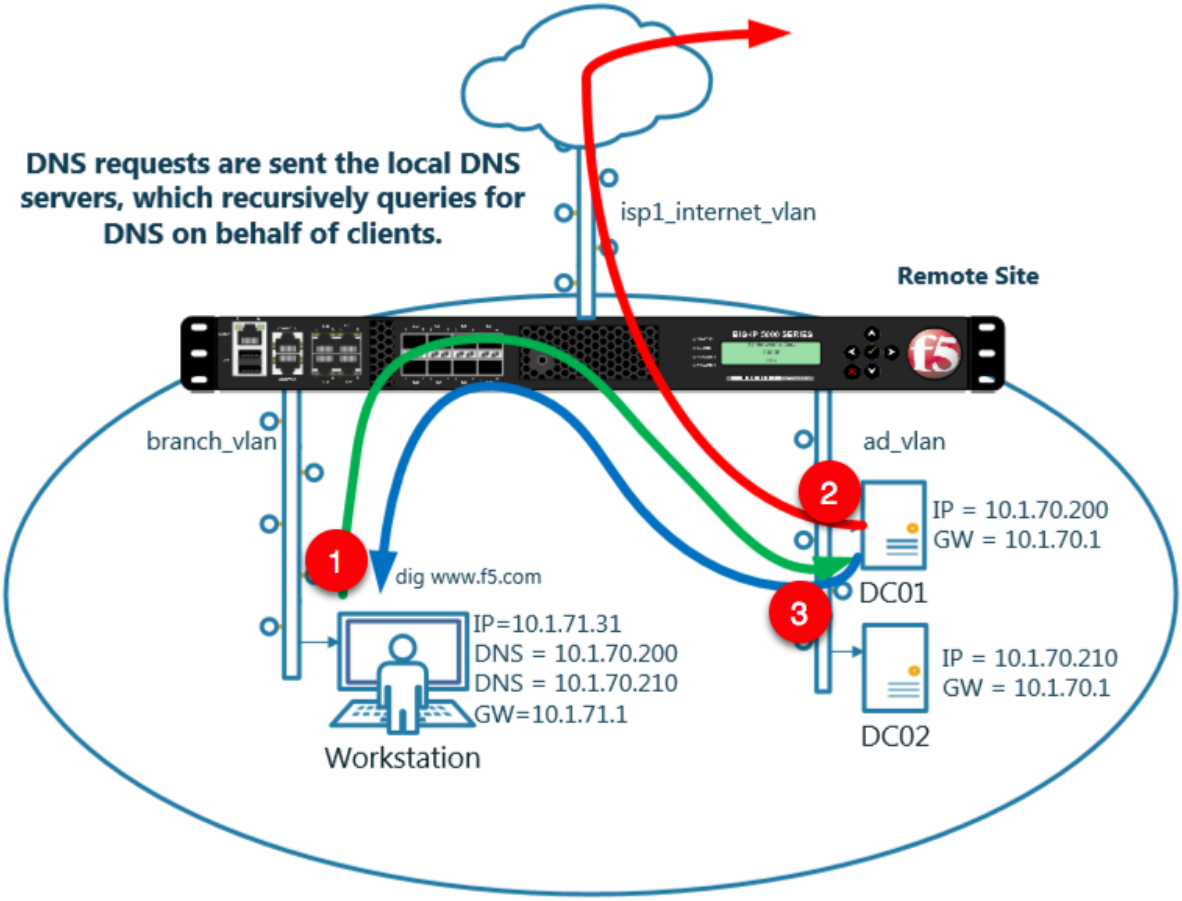
**4 Credits 173**

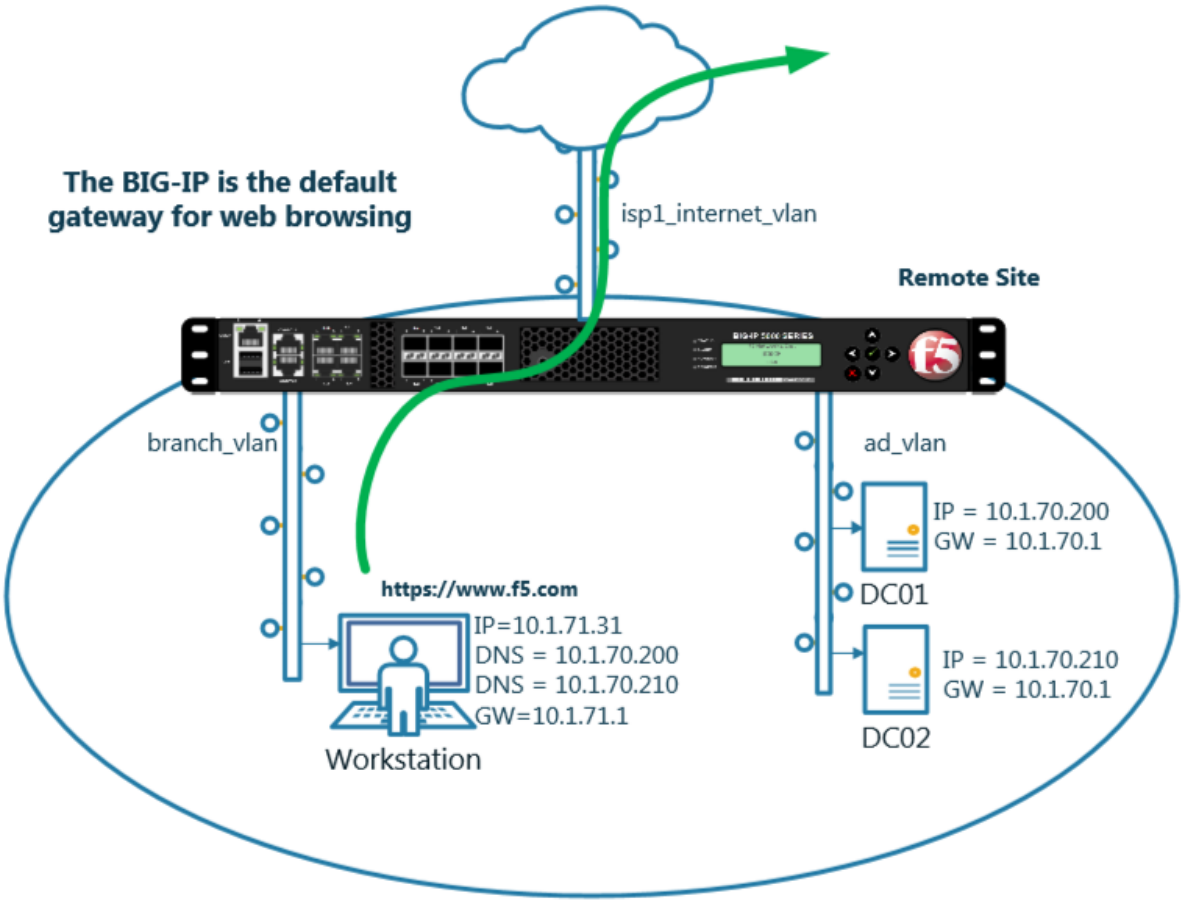
# 1

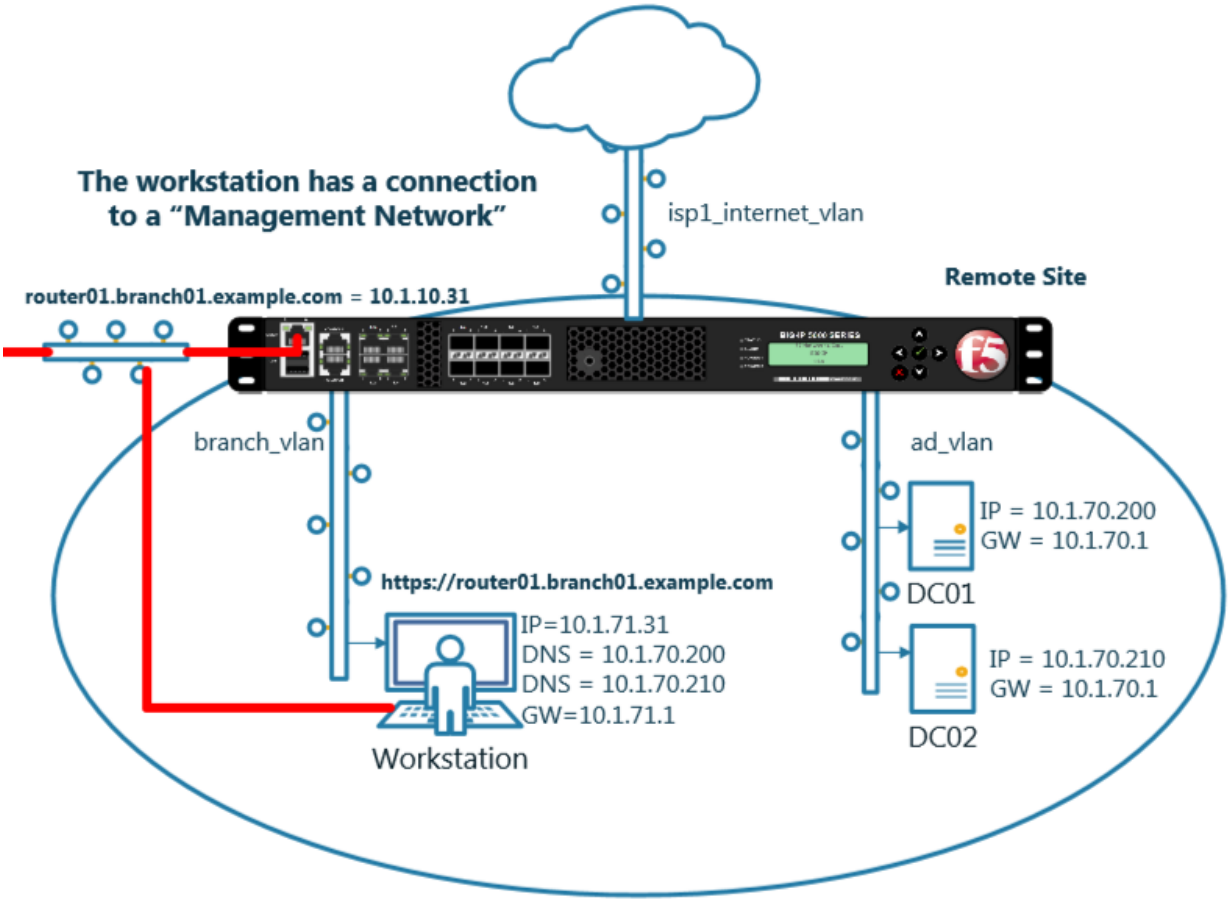
# Lab Environment

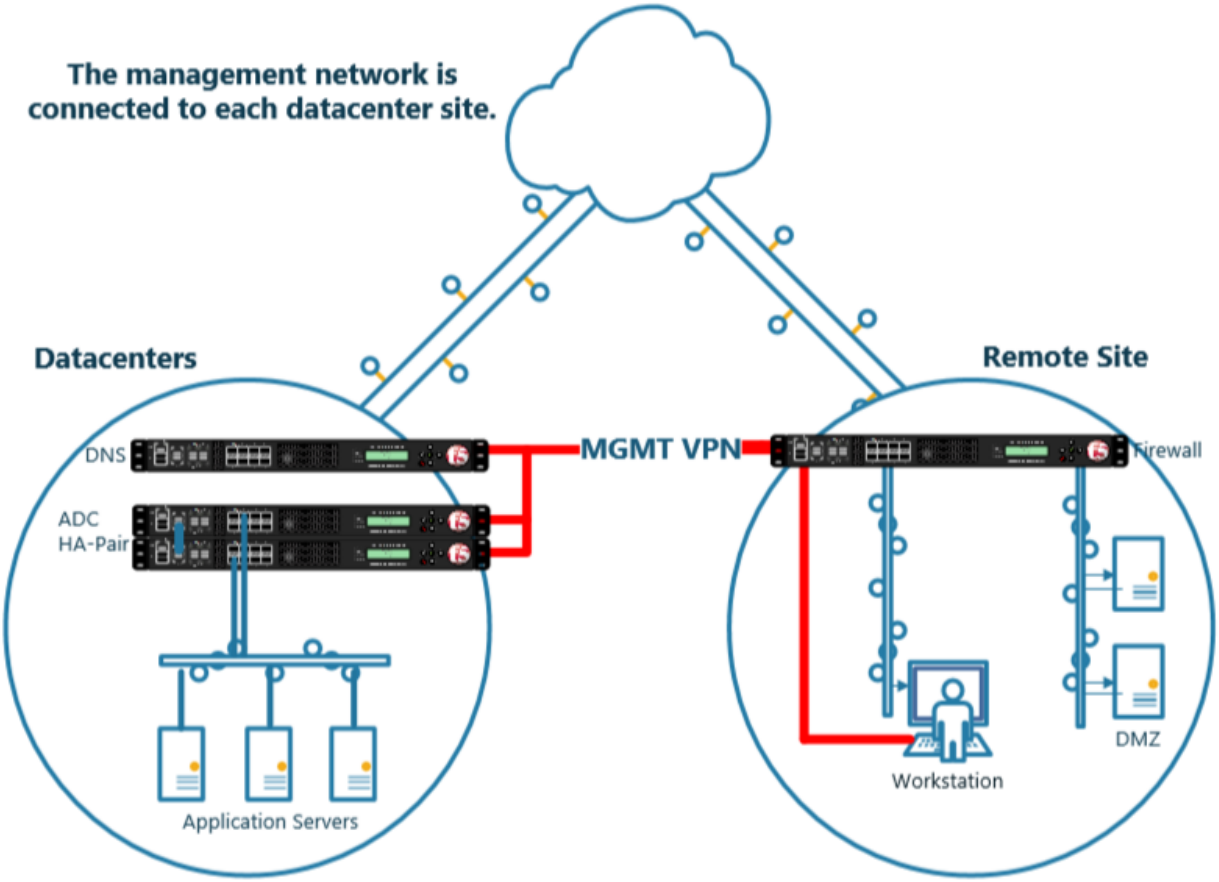



Obtain login information
from lab instructor
Remote Site
Workstation


DNS requests are sent the local DNS servers, which recursively queries for DNS on behalf of clients.
isp1_internet_vlan
Remote Site
branch_vlan
ad_vlan
1
dig www.f5.com
2
IP = 10.1.70.200
GW = 10.1.70.1
DC01
3
IP=10.1.71.31
DNS = 10.1.70.200
DNS = 10.1.70.210
GW=10.1.71.1
Workstation
IP = 10.1.70.210
GW = 10.1.70.1
DC02

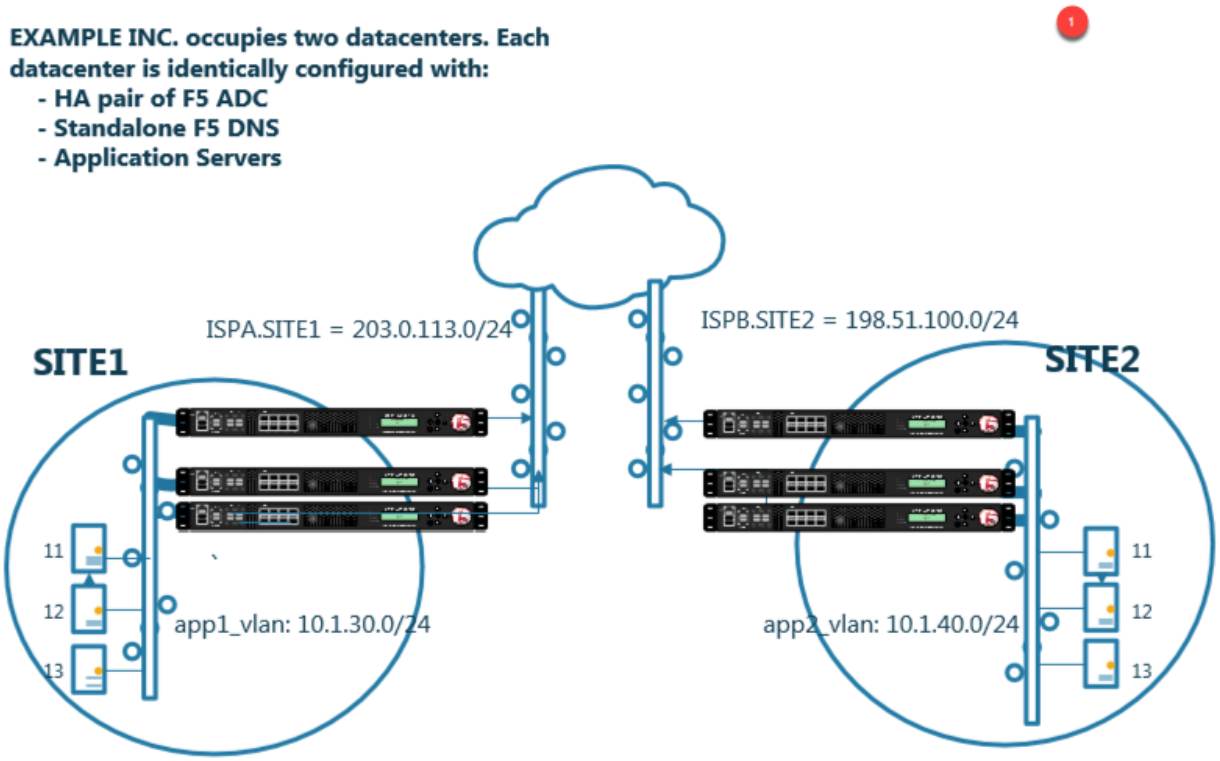

The BIG-IP is the default gateway for web browsing
isp1_internet_vlan
Remote Site
branch_vlan
ad_vlan
IP = 10.1.70.200
GW = 10.1.70.1
DC01
https://www.f5.com
IP=10.1.71.31
DNS = 10.1.70.200
DNS = 10.1.70.210
GW=10.1.71.1
Workstation
IP = 10.1.70.210
GW = 10.1.70.1
DC02


The workstation has a connection
to a "Management Network"
isp1_internet_vlan
Remote Site
router01.branch01.example.com = 10.1.10.31
branch_vlan
ad_vlan
IP = 10.1.70.200
GW = 10.1.70.1
DC01
https://router01.branch01.example.com
IP=10.1.71.31
DNS = 10.1.70.200
DNS = 10.1.70.210
GW=10.1.71.1
Workstation
IP = 10.1.70.210
GW = 10.1.70.1
DC02


The management network is connected to each datacenter site.
Datacenters
Remote Site
DNS
ADC HA-Pair
MGMT VPN
Firewall
Application Servers
Workstation
DMZ

# 2

# Class 1 - Availability




- 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.

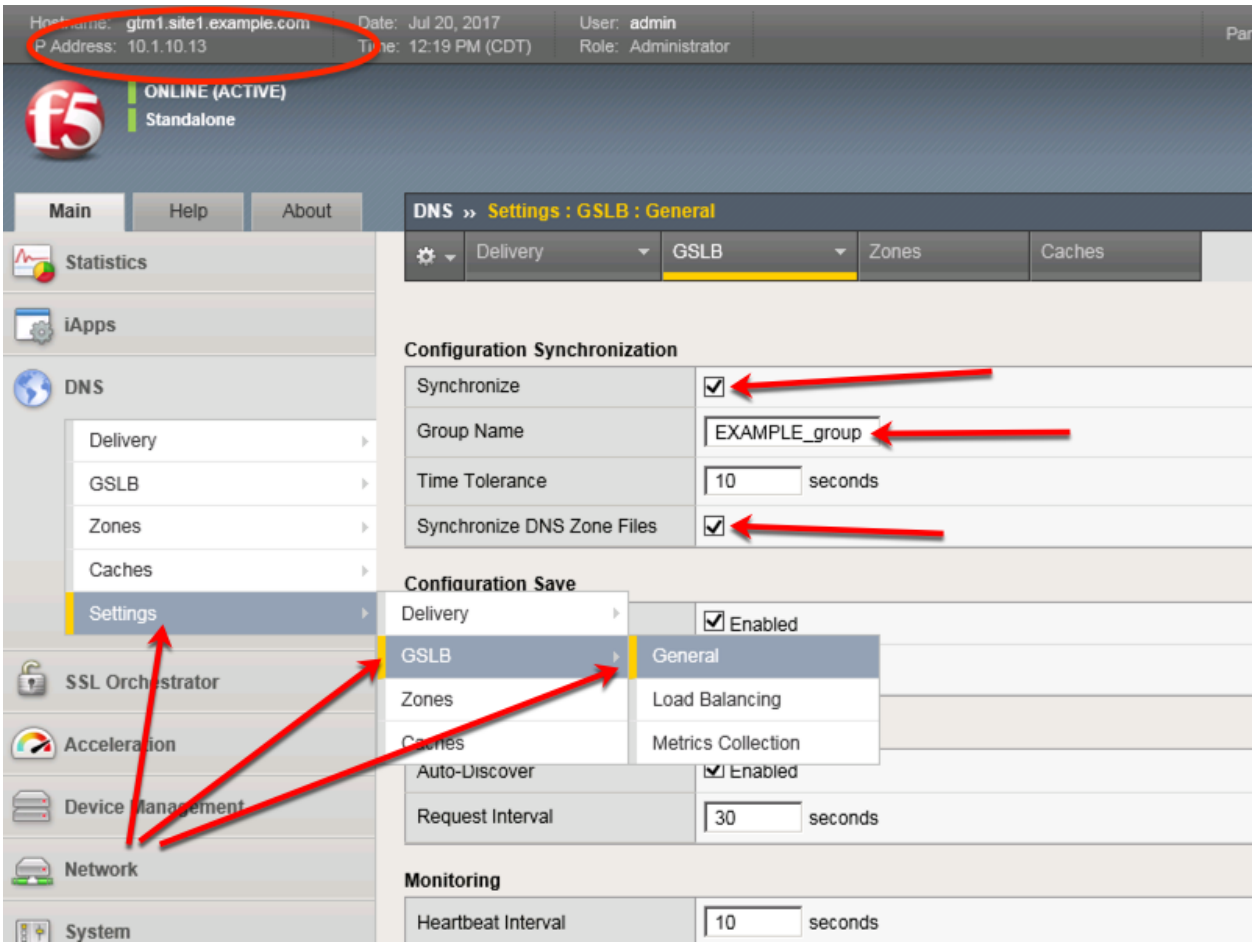
## 2.1 Settings

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 |




https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/settings/gslb/properties_general.jsp

**TMSH**

tmsh modify gtm global-settings general synchronization yes synchronization-group-name EXAMPLE_group synchronize-zone-files yes

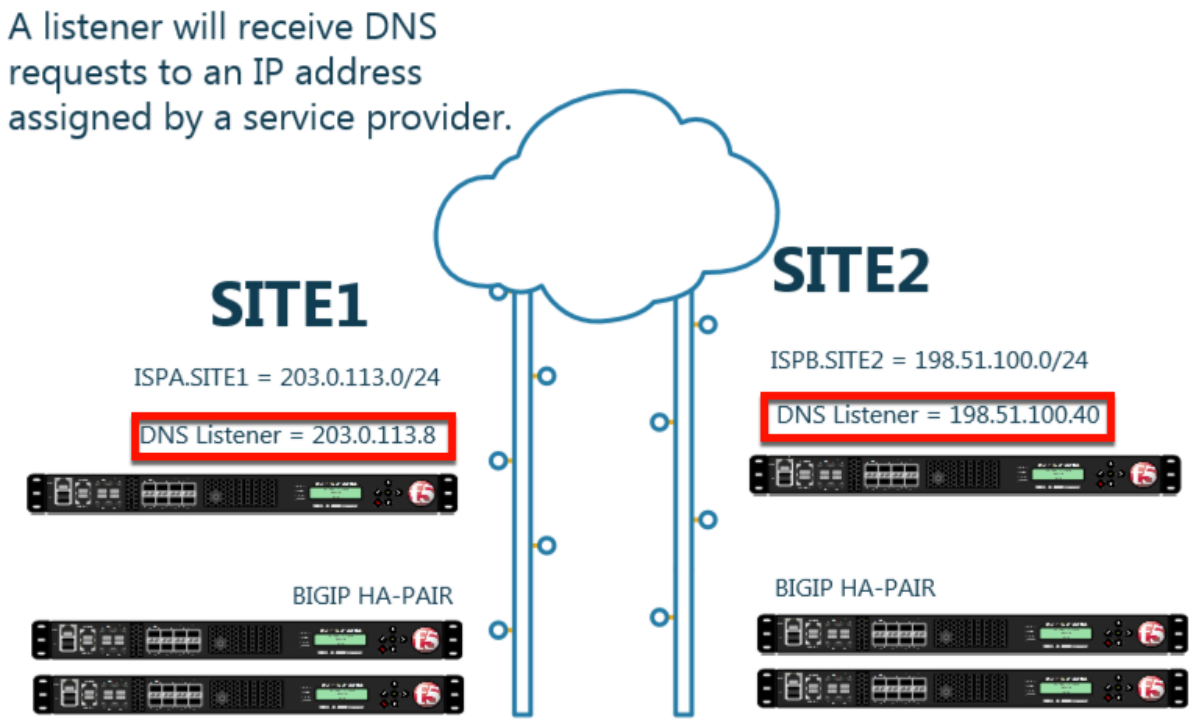
https://support.f5.com/csp/article/K13734

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

We will be creating both TCP and UDP based listeners.

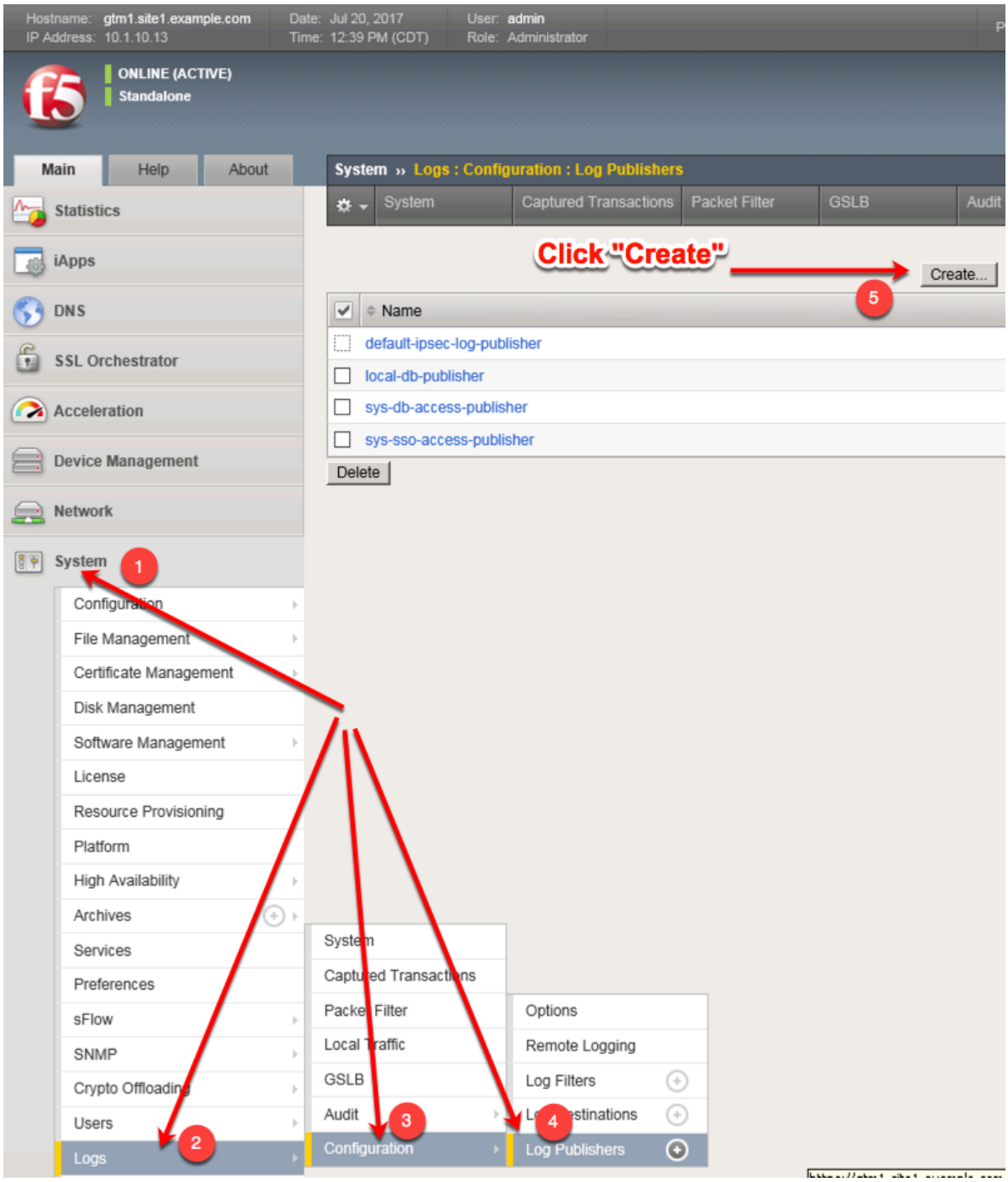



### 2.2.1 Logging

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

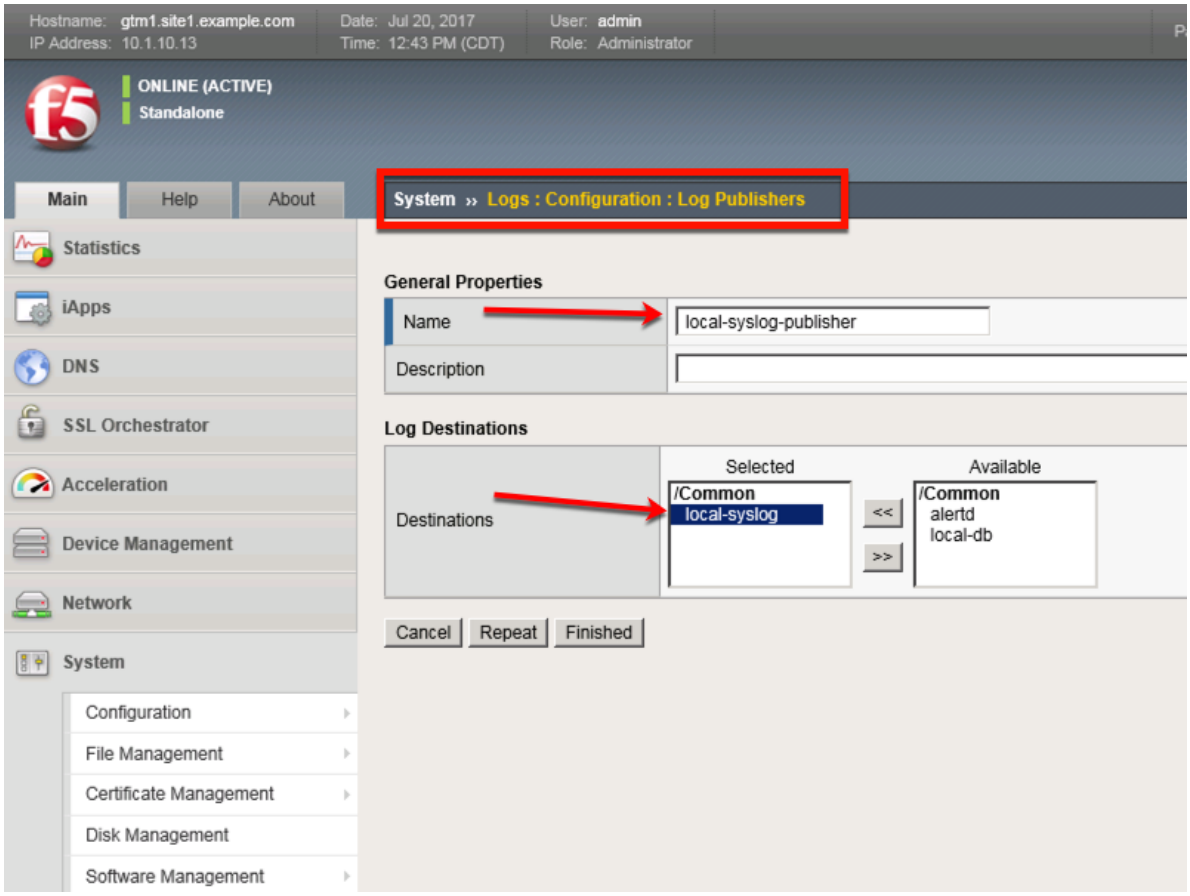
**Note: It is required to complete the following task on both gtm1.site1 and gtm1.site2**

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

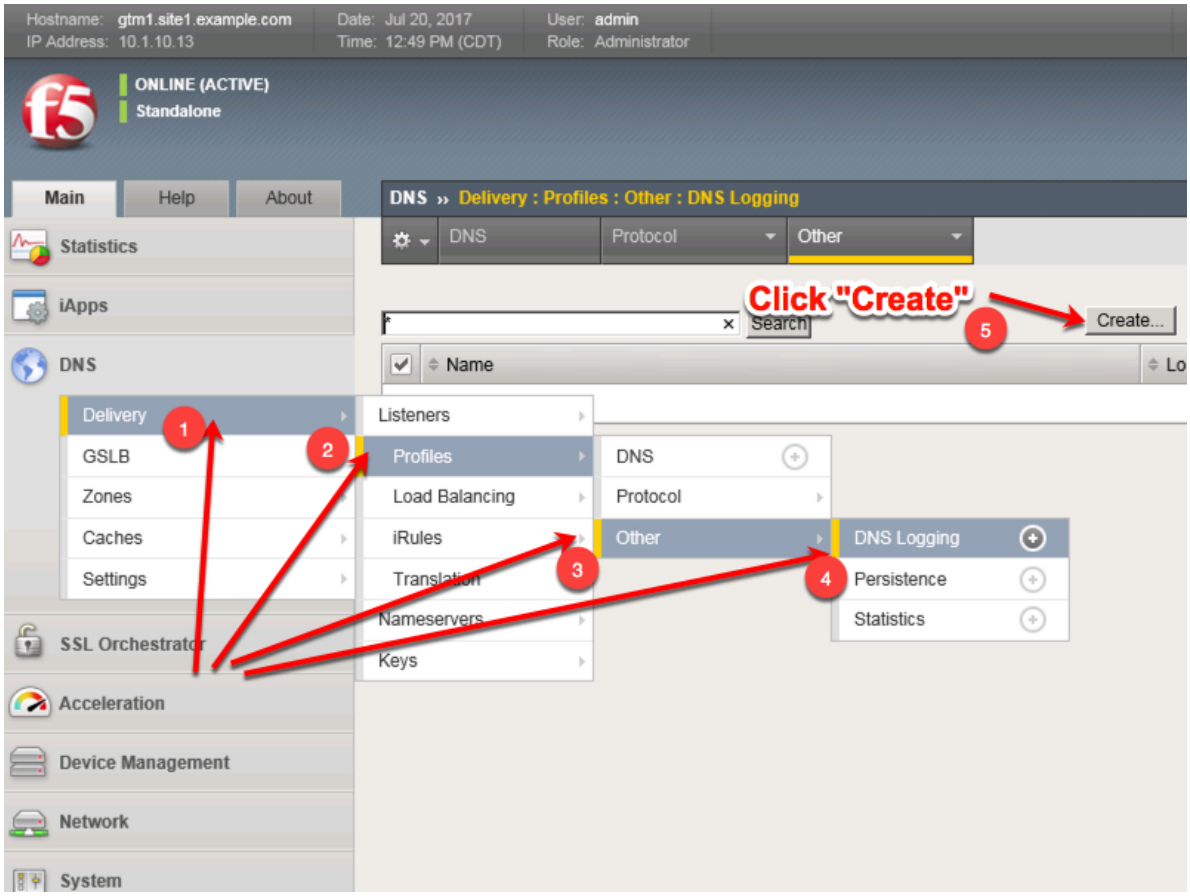
https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/system/log/create_publisher.jsp

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

**TMSH**

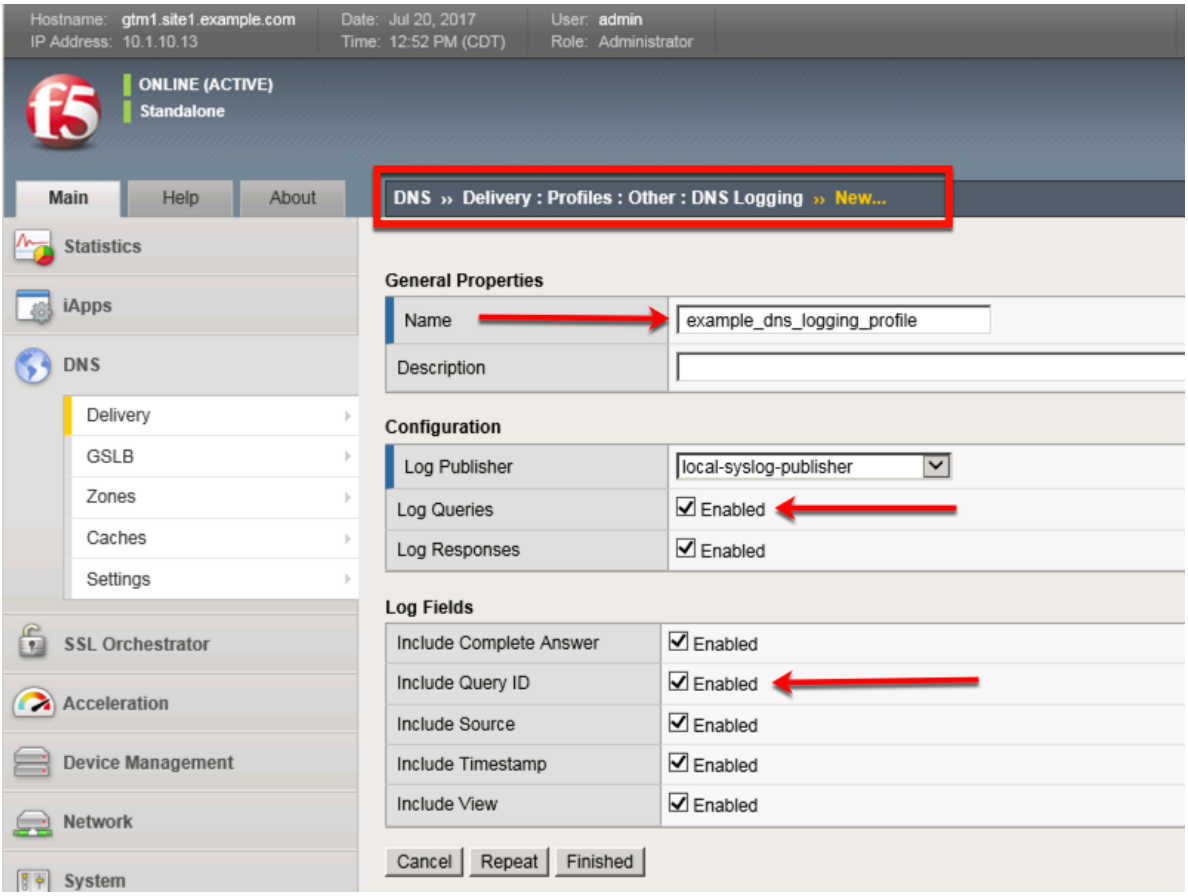
```
tmsh create sys log-config publisher local-syslog-publisher { destinations { local-syslog { } } }
```

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 |




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

**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

### 2.2.2 DNS Profile

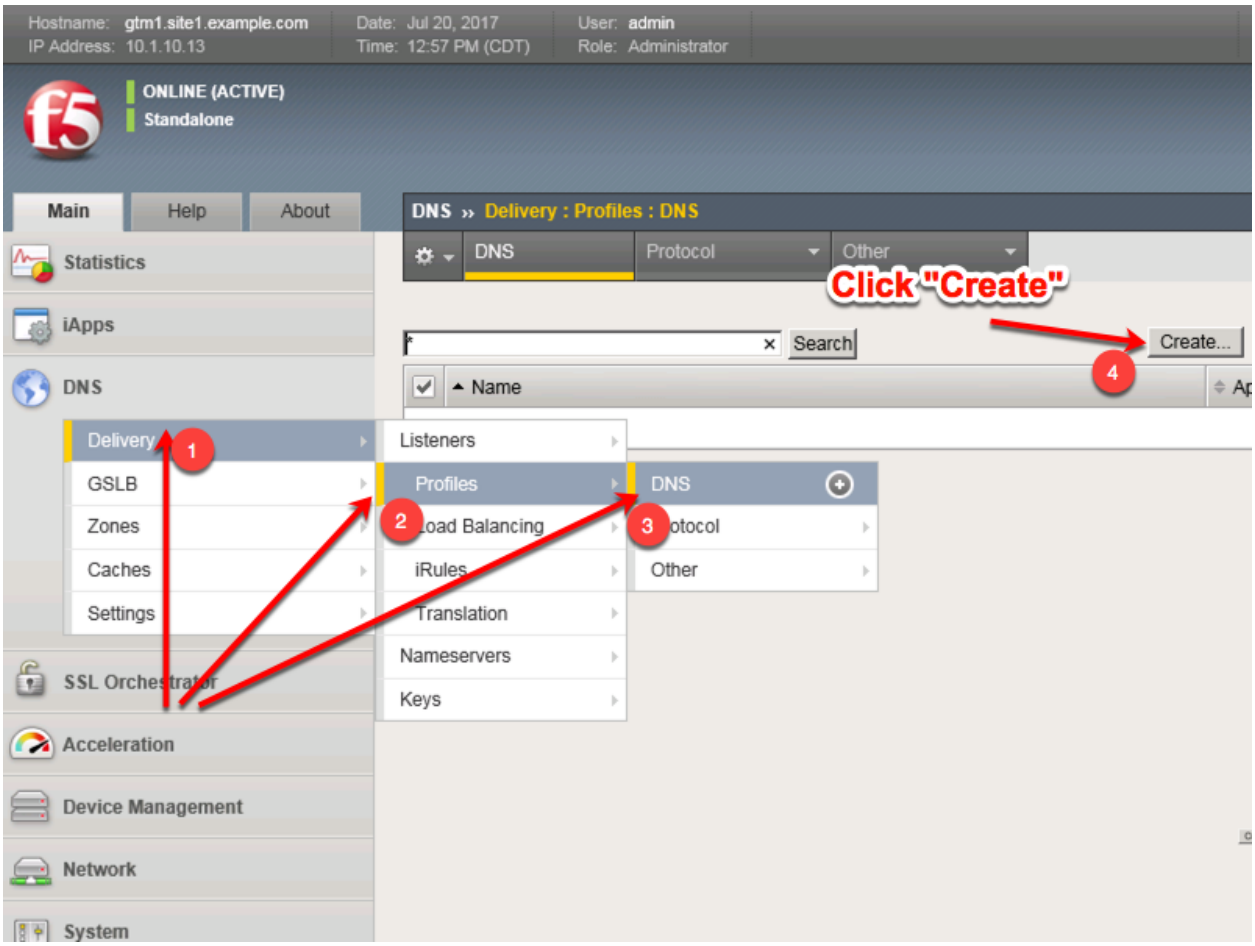
A DNS profile controls the way a listener processes a query.

---

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

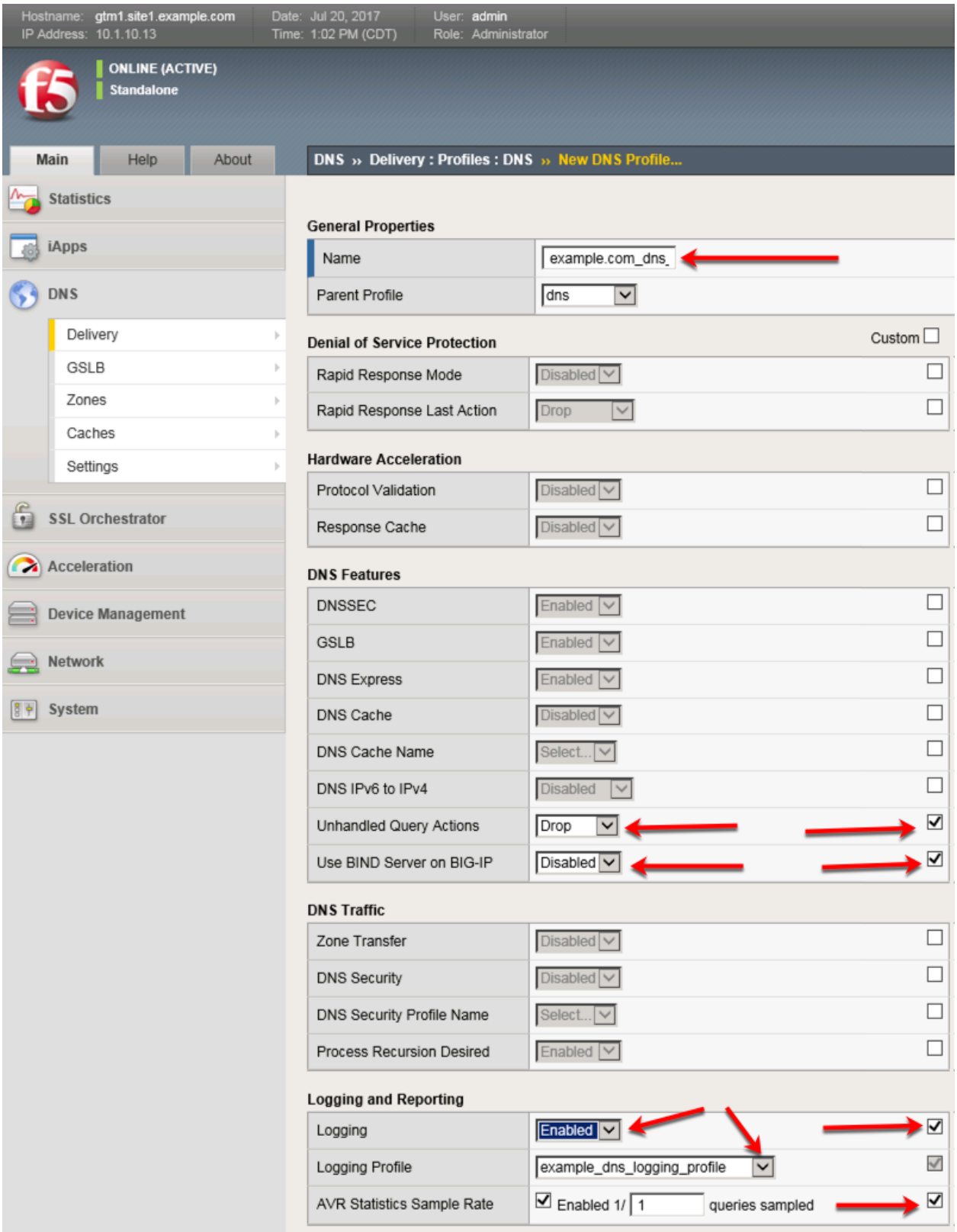
---

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 |




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**

tmsh 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

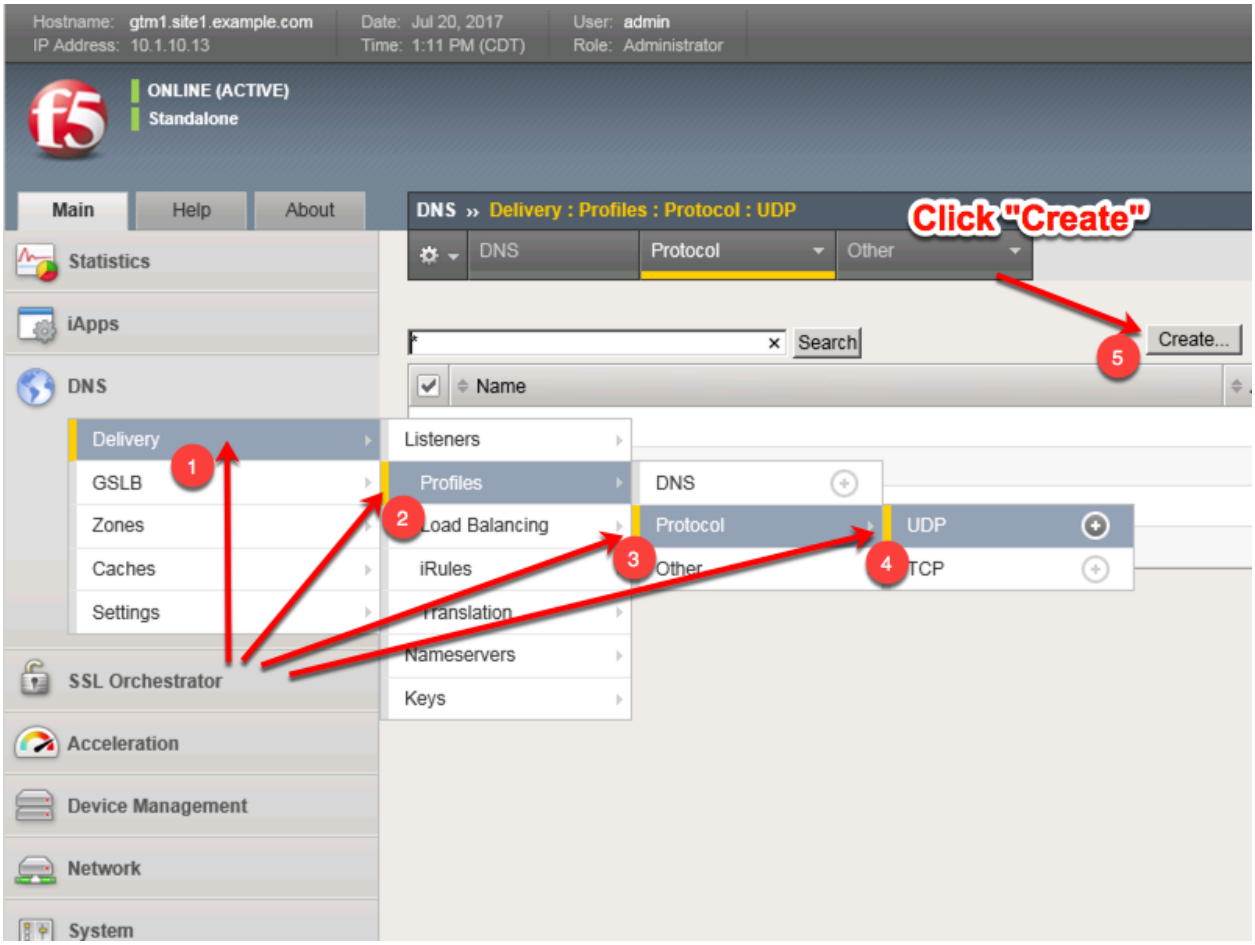
https://support.f5.com/csp/article/K14510

### 2.2.3 UDP Profile

A UDP profile is associated with a listener.

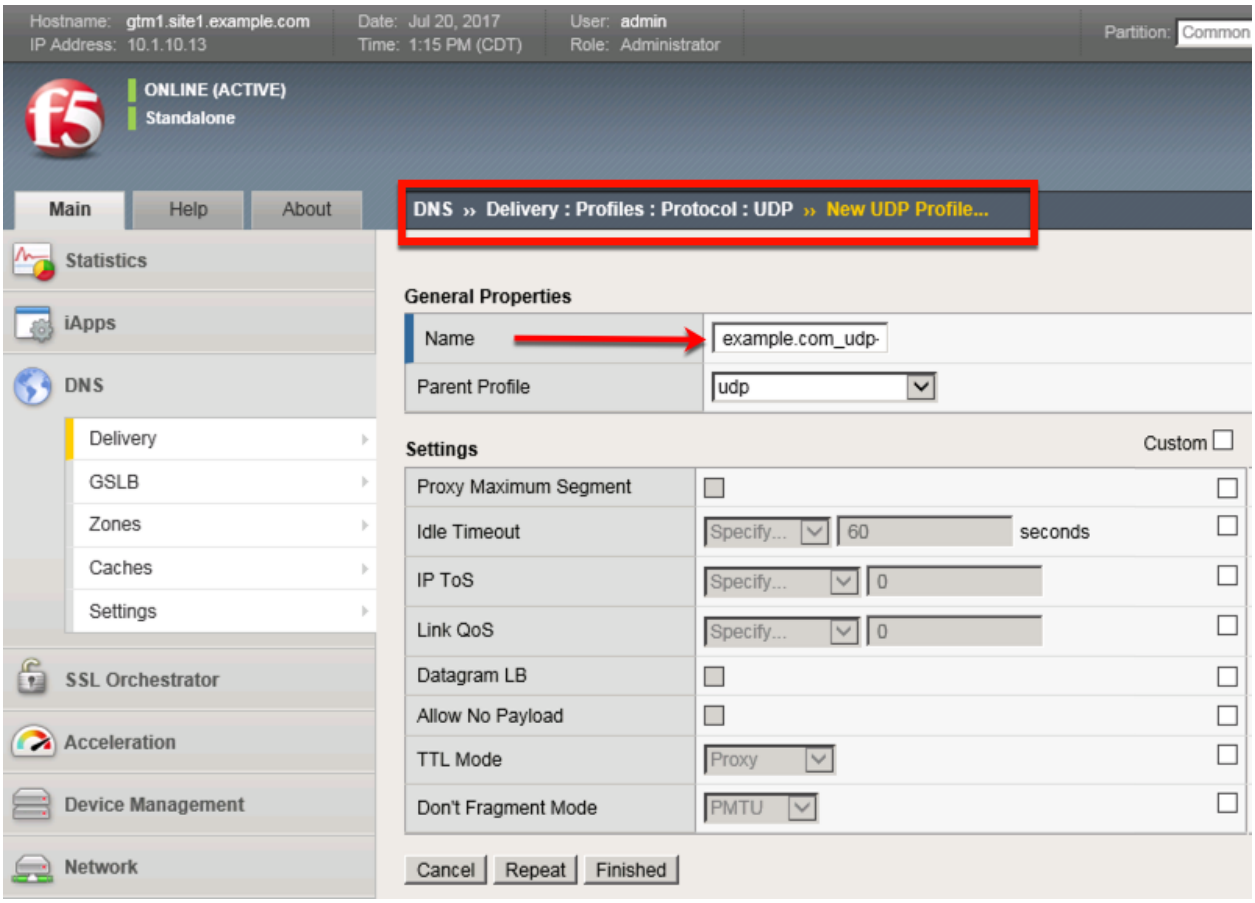
**Note: It is required to complete the following task on both gtm1.site1 and gtm1.site2**

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 |




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**

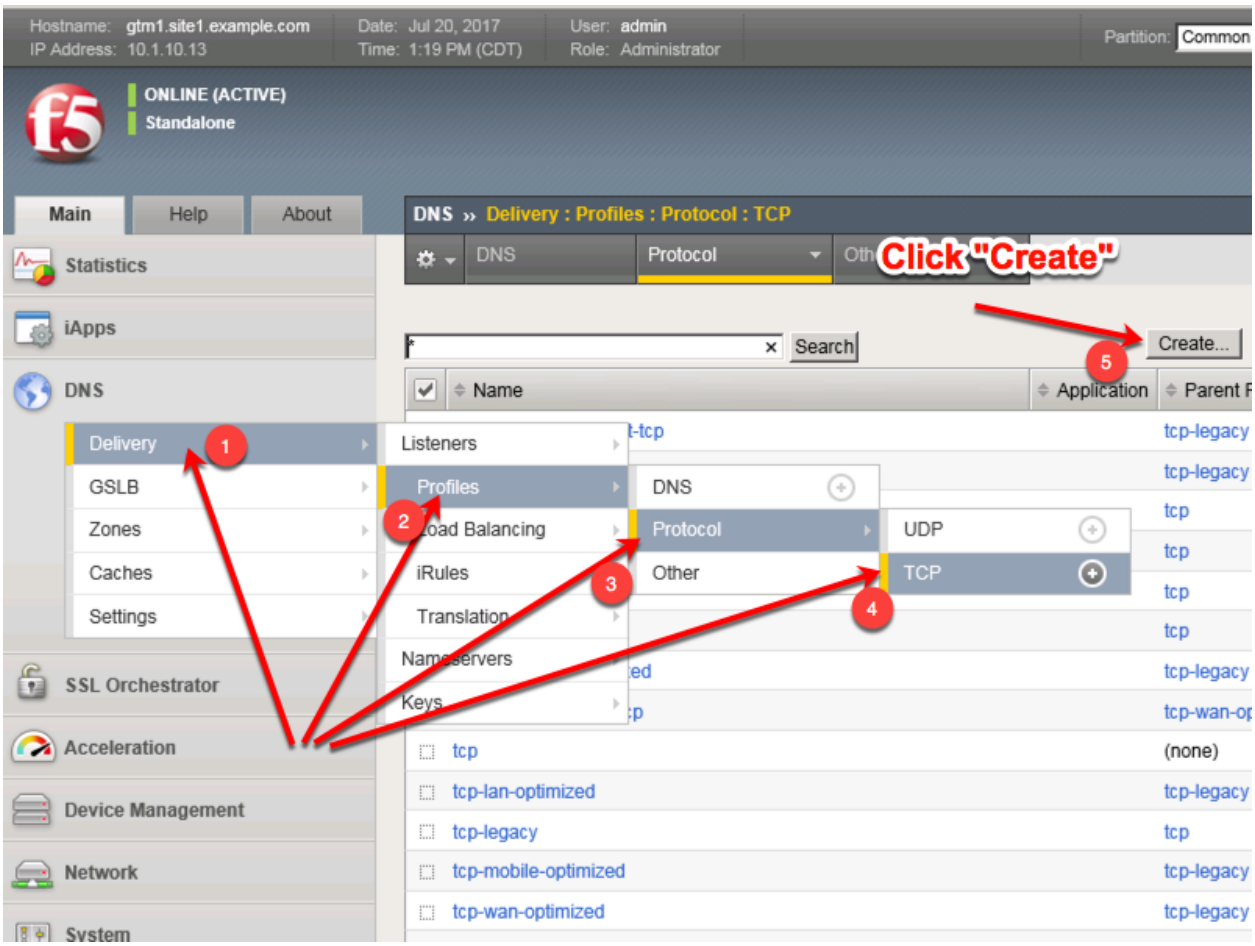
tmsh create ltm profile udp example.com_udp-dns_profile defaults-from udp_gtm_dns

### 2.2.4 TCP Profile

A TCP profile is associated with a listener.

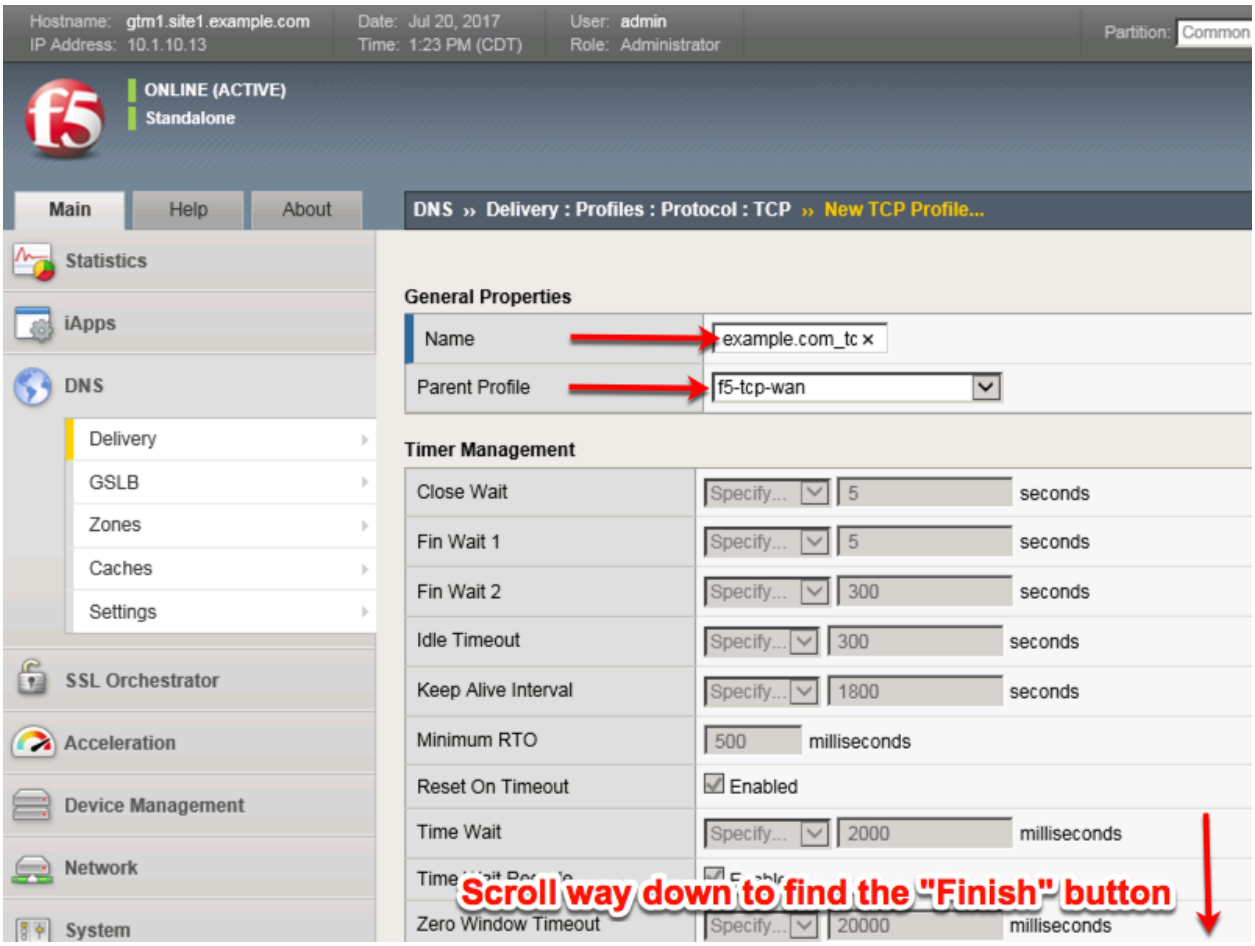
**Note: It is required to complete the following task on both gtm1.site1 and gtm1.site2**

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 |




https://gtm1.site2.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**

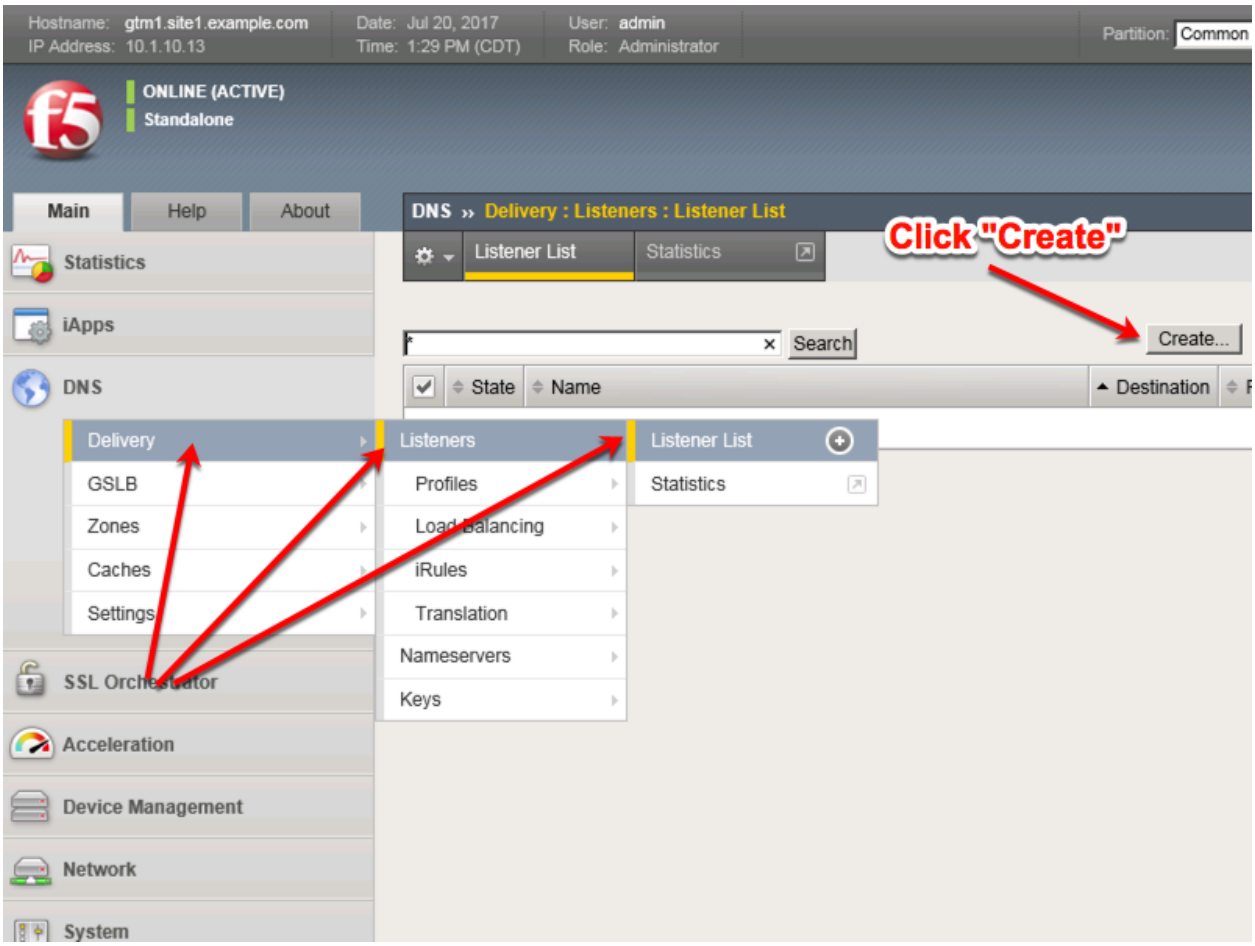
tmsh create ltm profile tcp example.com_tcp-dns_profile defaults-from tcp-wan-optimized

### 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**

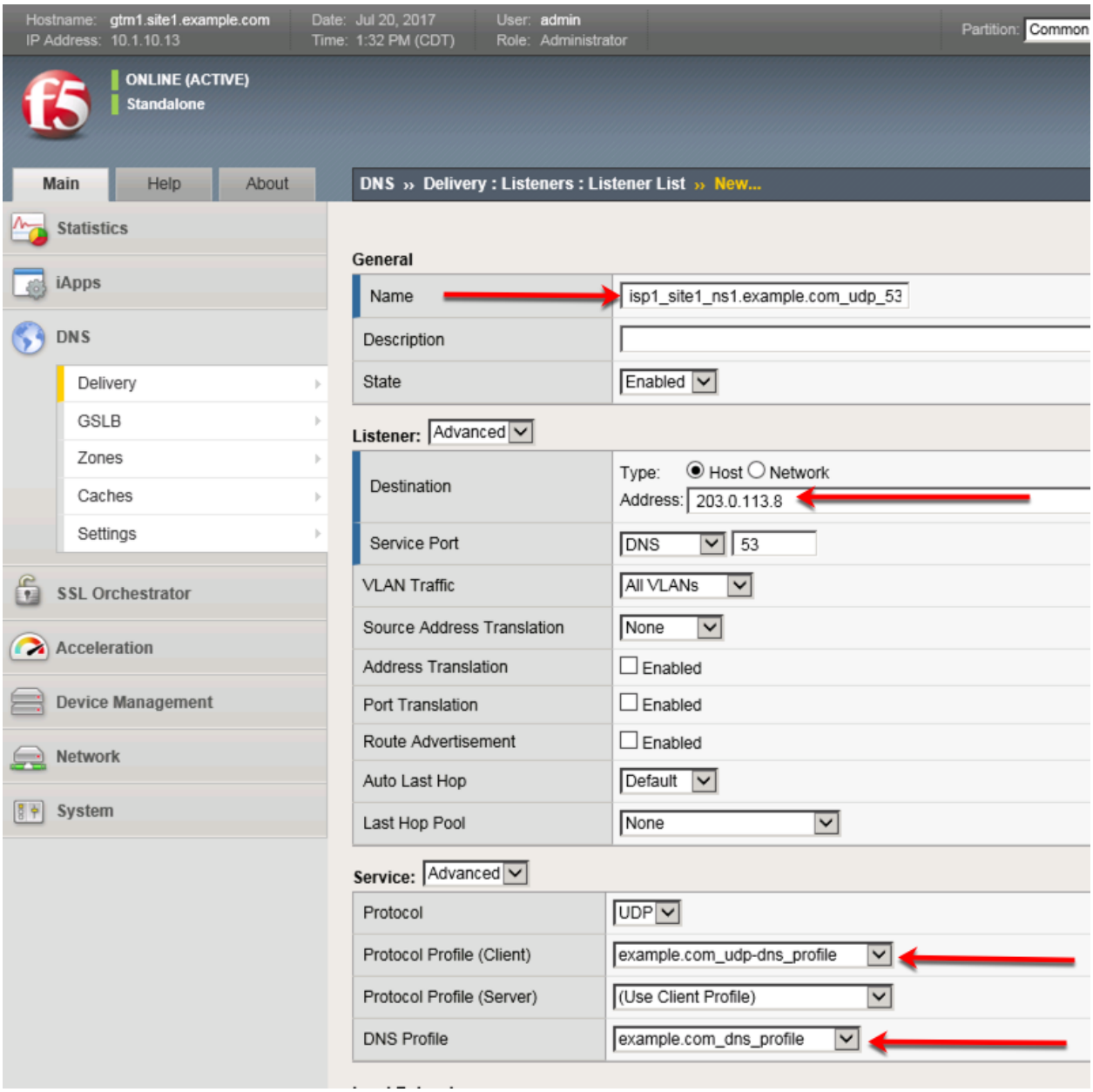



Create a UDP listener according to the following table:

| 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 Profile (Client) | 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




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 isp2_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
```

}

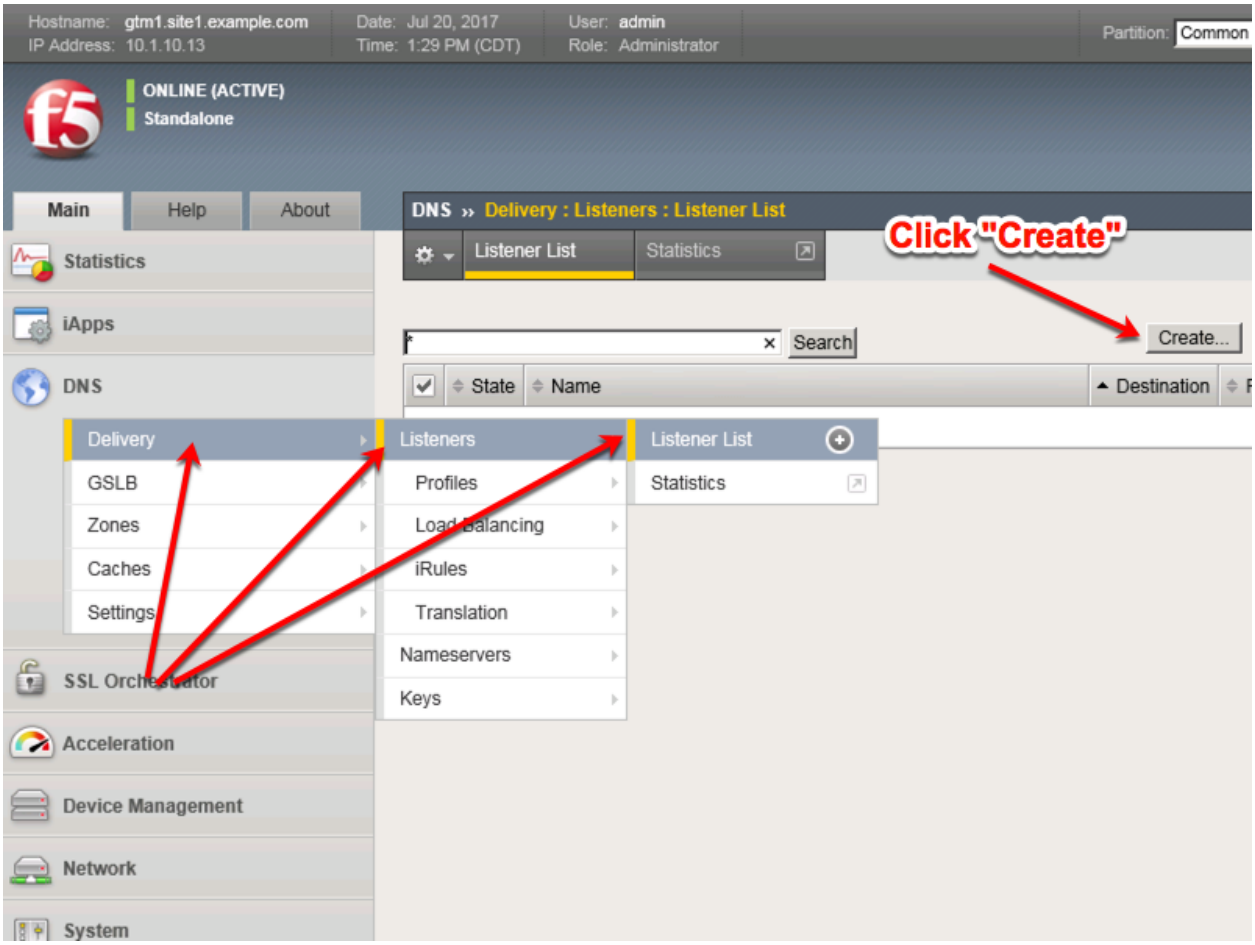
https://support.f5.com/csp/article/K14923

### 2.2.6 TCP IP Address

A TCP listener will receive and process DNS queries.

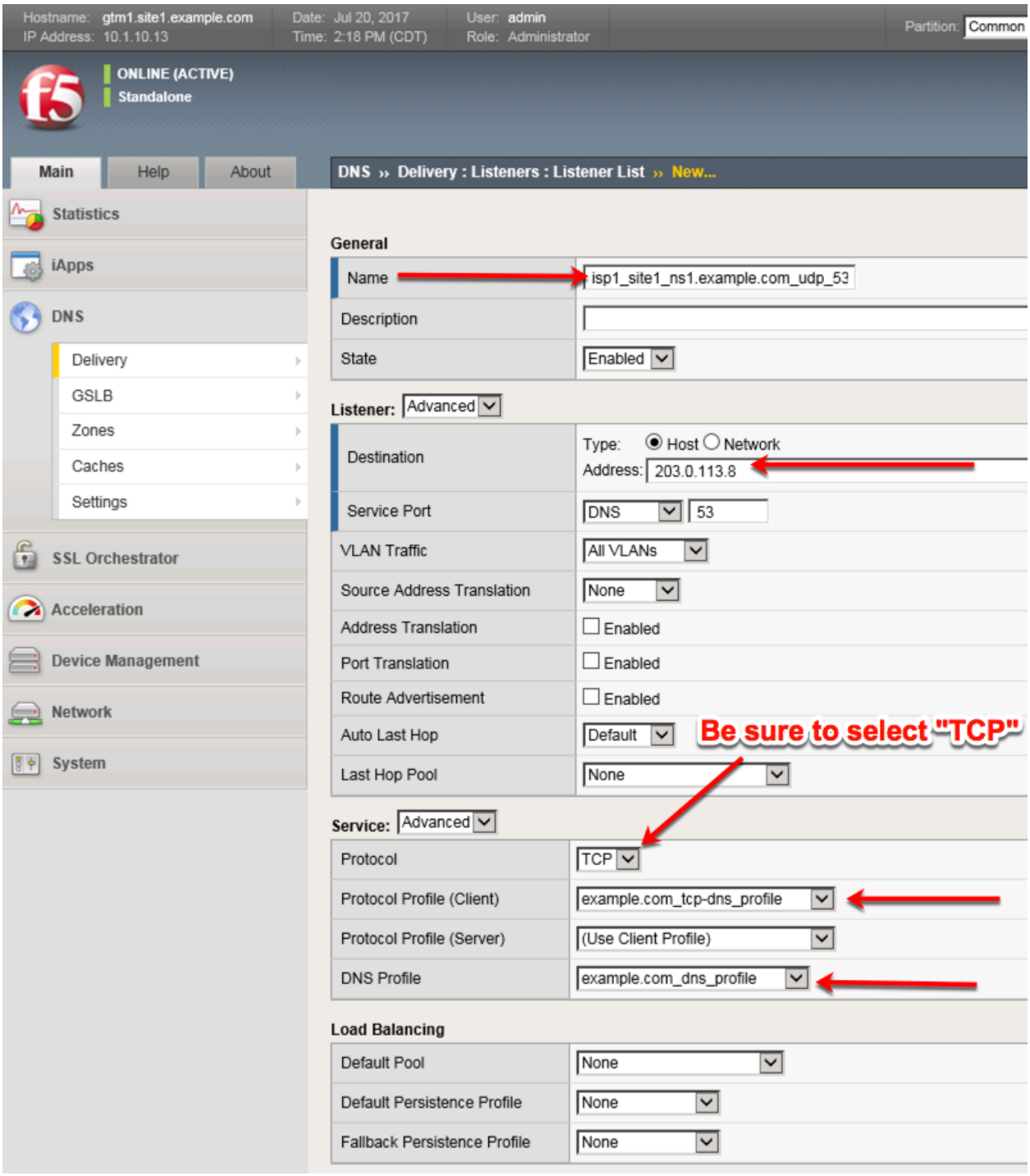
**Note: It is required to complete the following task on both gtm1.site and gtm1.site2**

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 | isp2_site2_ns2.example.com_tcp_53_virtual |
| Destination | 203.0.113.8 | 198.51.100.40 |
| Protocol Profile (Client) | example.com_tcp-dns_profile | example.com_tcp-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

gtm1.site1 TMSH command:

---

**TMSH**

tmsh create gtm listener isp1_site1_ns1.example.com_tcp_53_virtual address 203.0.113.8 ip-protocol tcp

---

mask 255.255.255.255 port 53 profiles add { example.com_dns_profile example.com_tcp-dns_profile }

gtm1.site2 TMSH command:

**TMSH**

tmsh create gtm listener isp1_site2_ns2.example.com_tcp_53_virtual address 198.51.100.40 ip-protocol tcp mask 255.255.255.255 port 53 profiles add { example.com_dns_profile example.com_tcp-dns_profile }

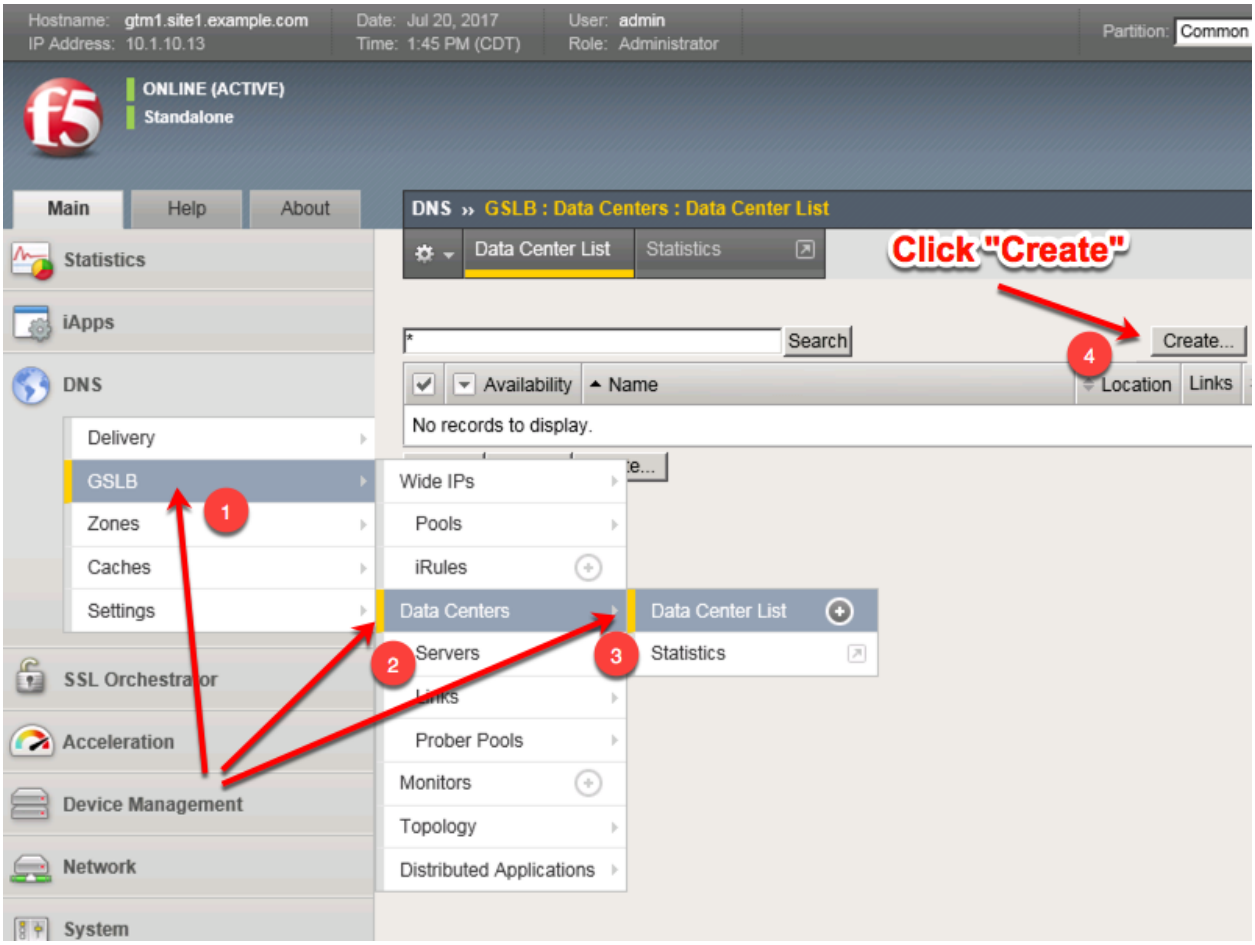
https://support.f5.com/csp/article/K14923

## 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

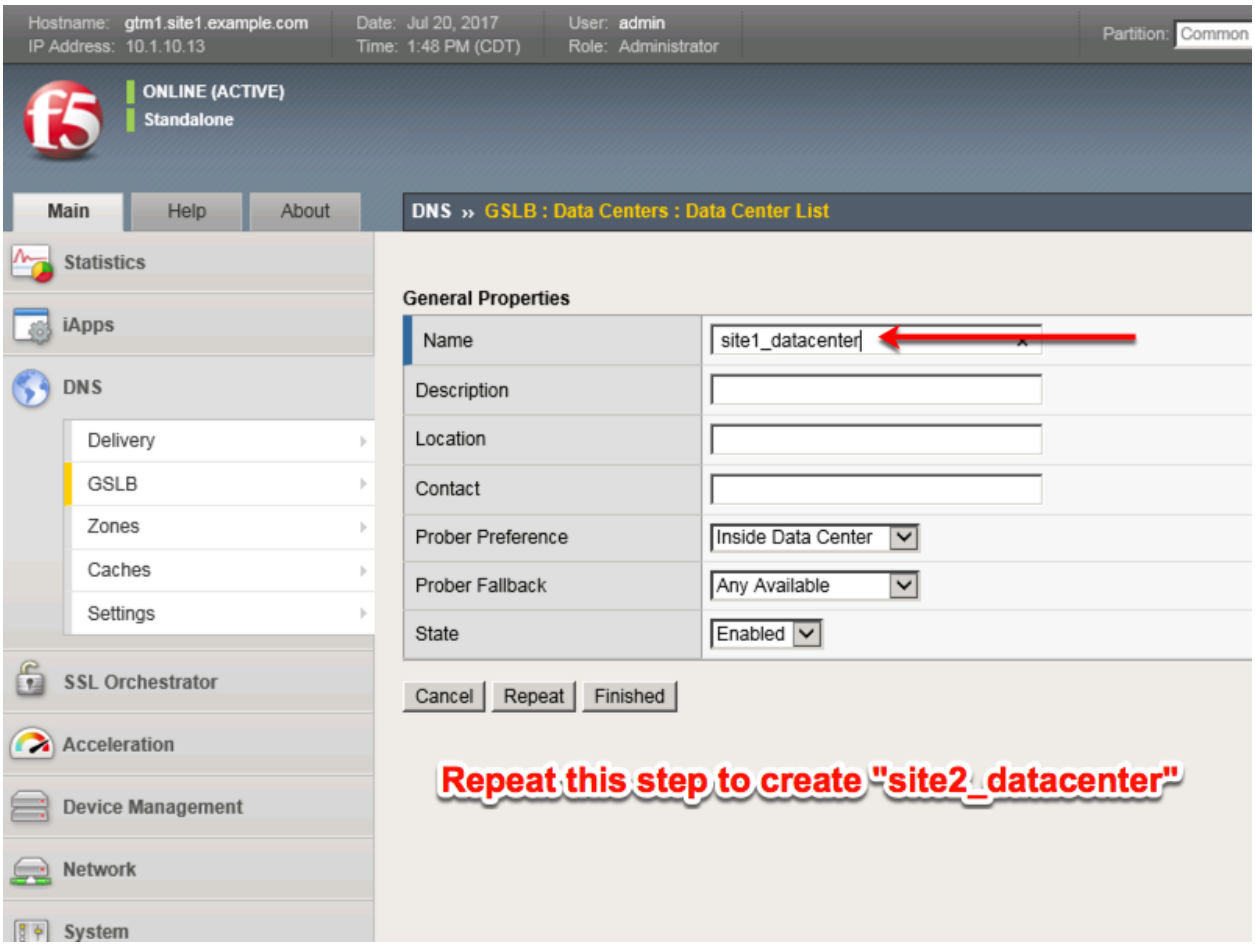
Navigate to: **DNS > GSLB > Data Centers > Data Center List: Create**




https://gtm1.site1.example.com/tmui/Control/jspmap/xsl/gtm_dc/list

Create two data centers according to the table below:

| Setting | Value |
|---|---|
| Name | site1_datacenter |
| Name | site2_datacenter |




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
```

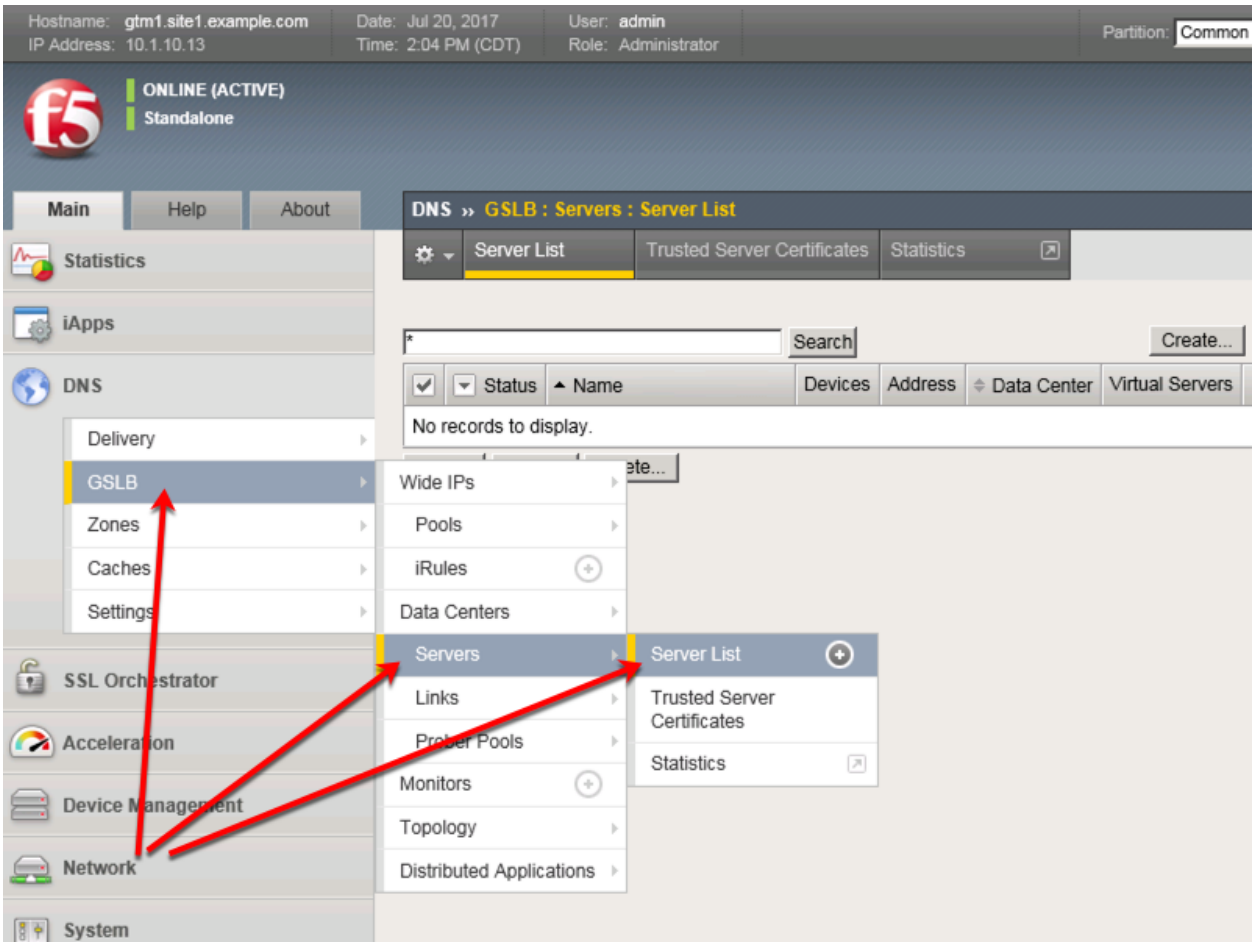
**TMSH**

```
tmsh create gtm datacenter site2_datacenter
```

### 2.3.1 Servers

Server objects need to be defined and grouped into a Datacenter

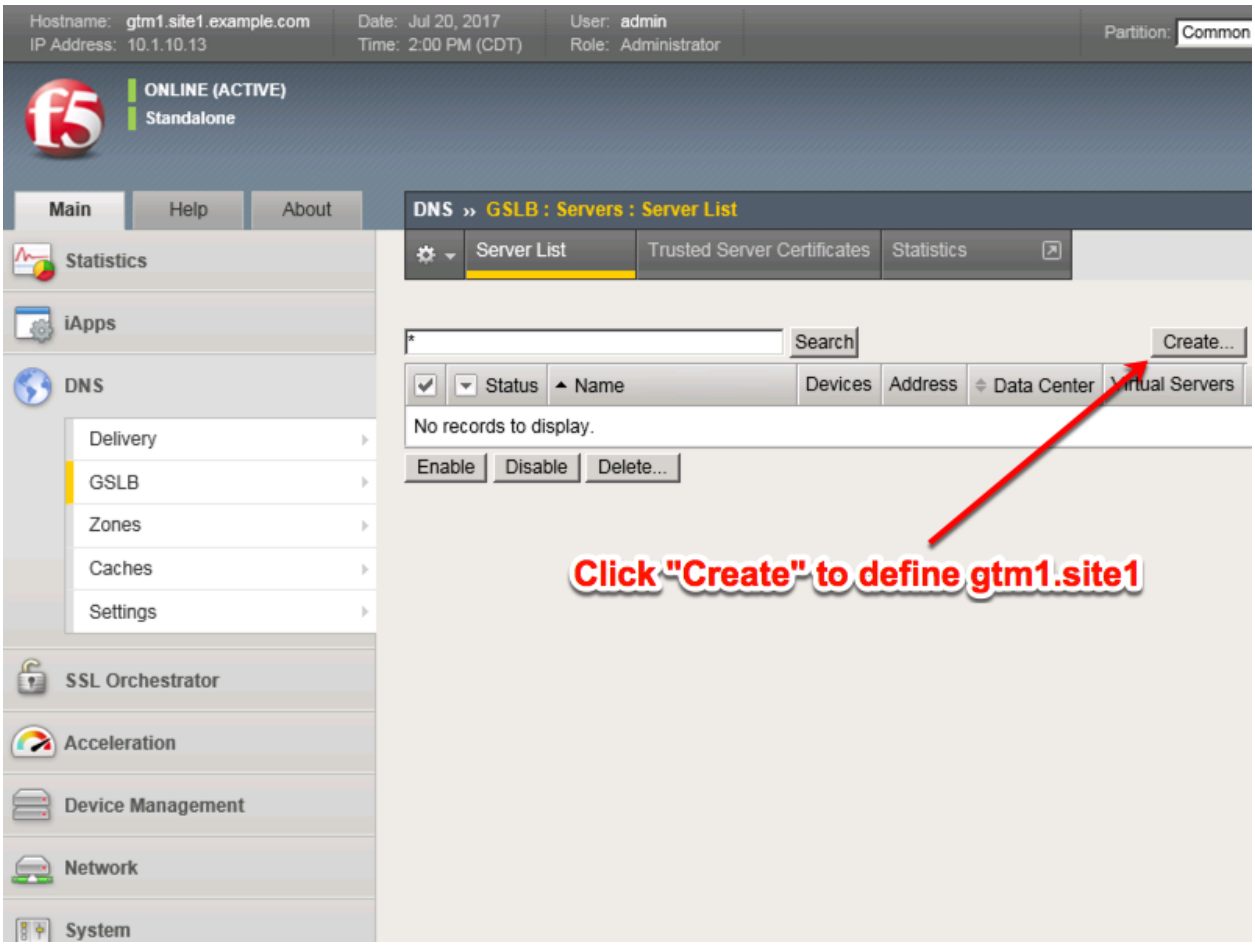
Navigate to: **DNS ›› GSLB : Servers : Server List**




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

#### 2.3.1.1 gtm1.site1

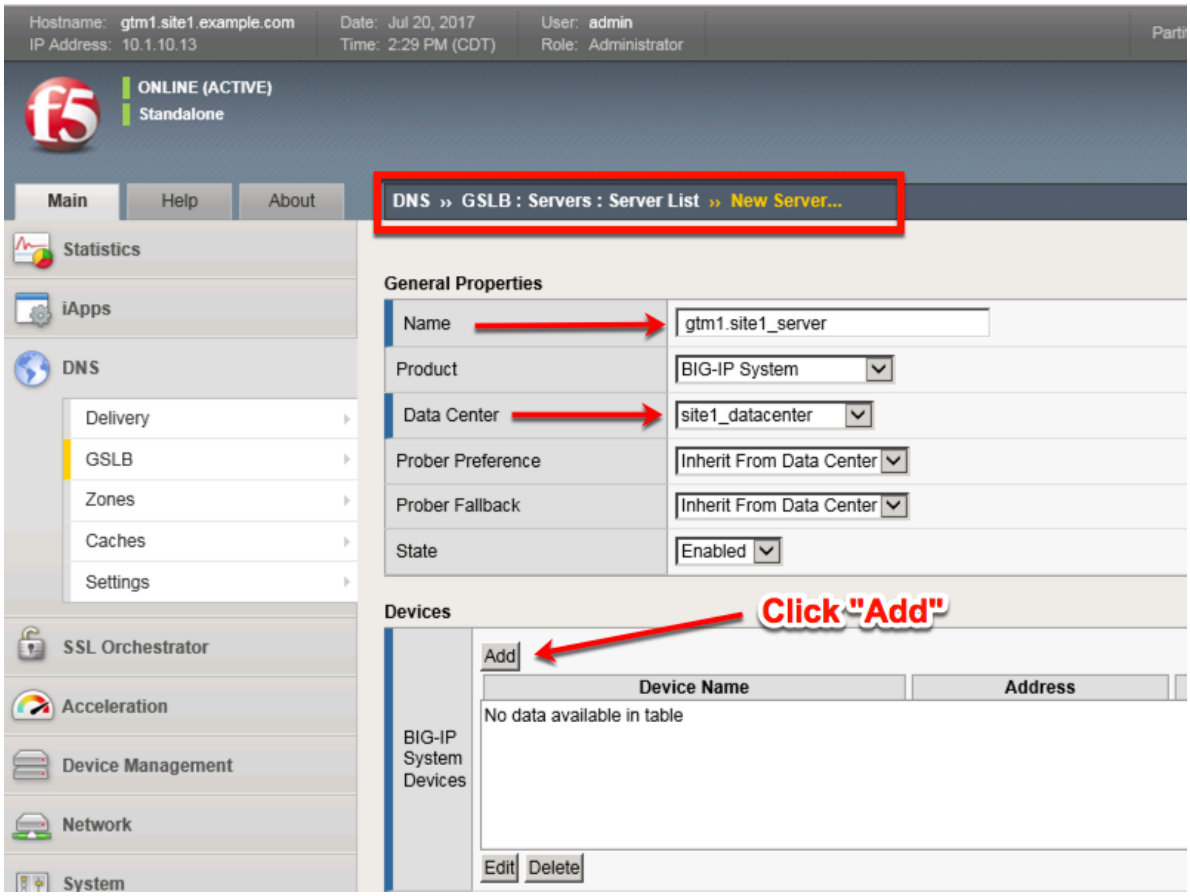
All GTM devices need to be defined. Create a server object for gtm1.site1



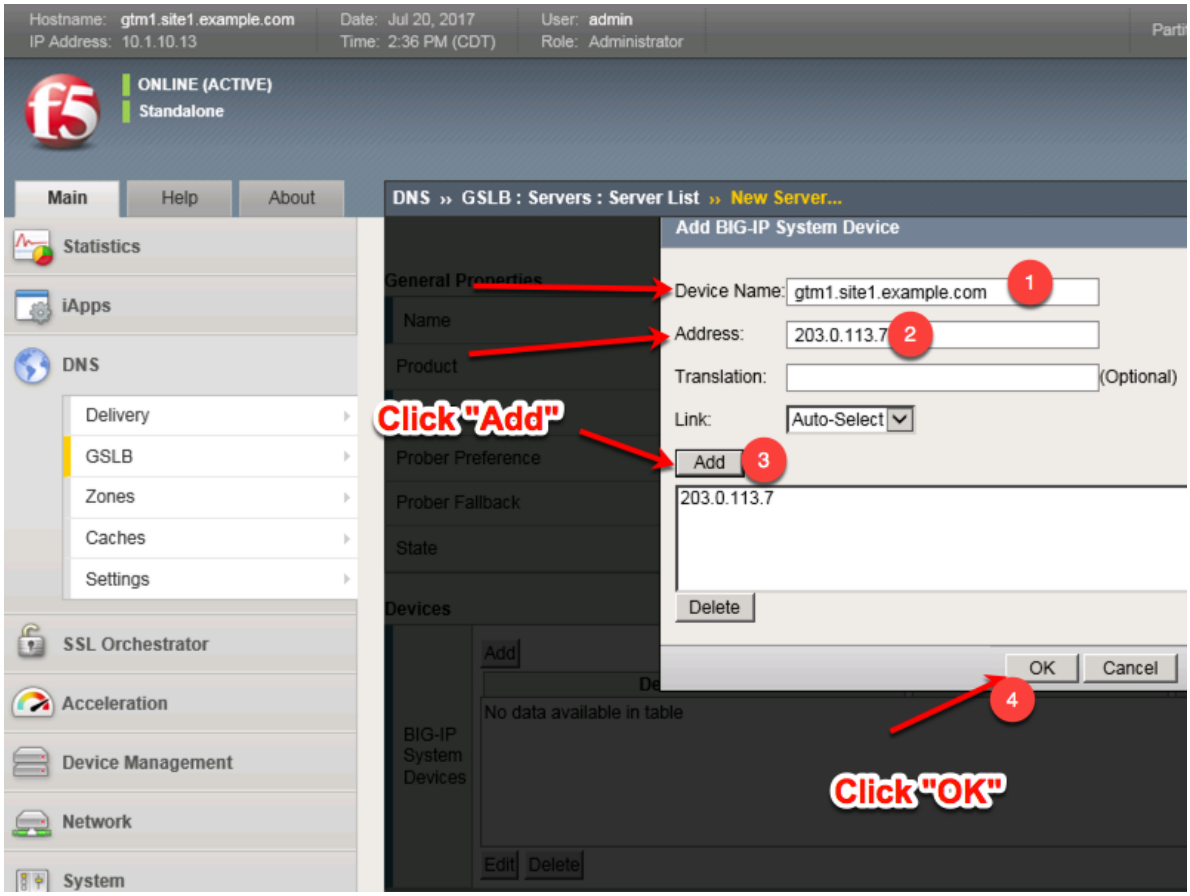

Click “Create” to define gtm1.site1 as defined in the table below:

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

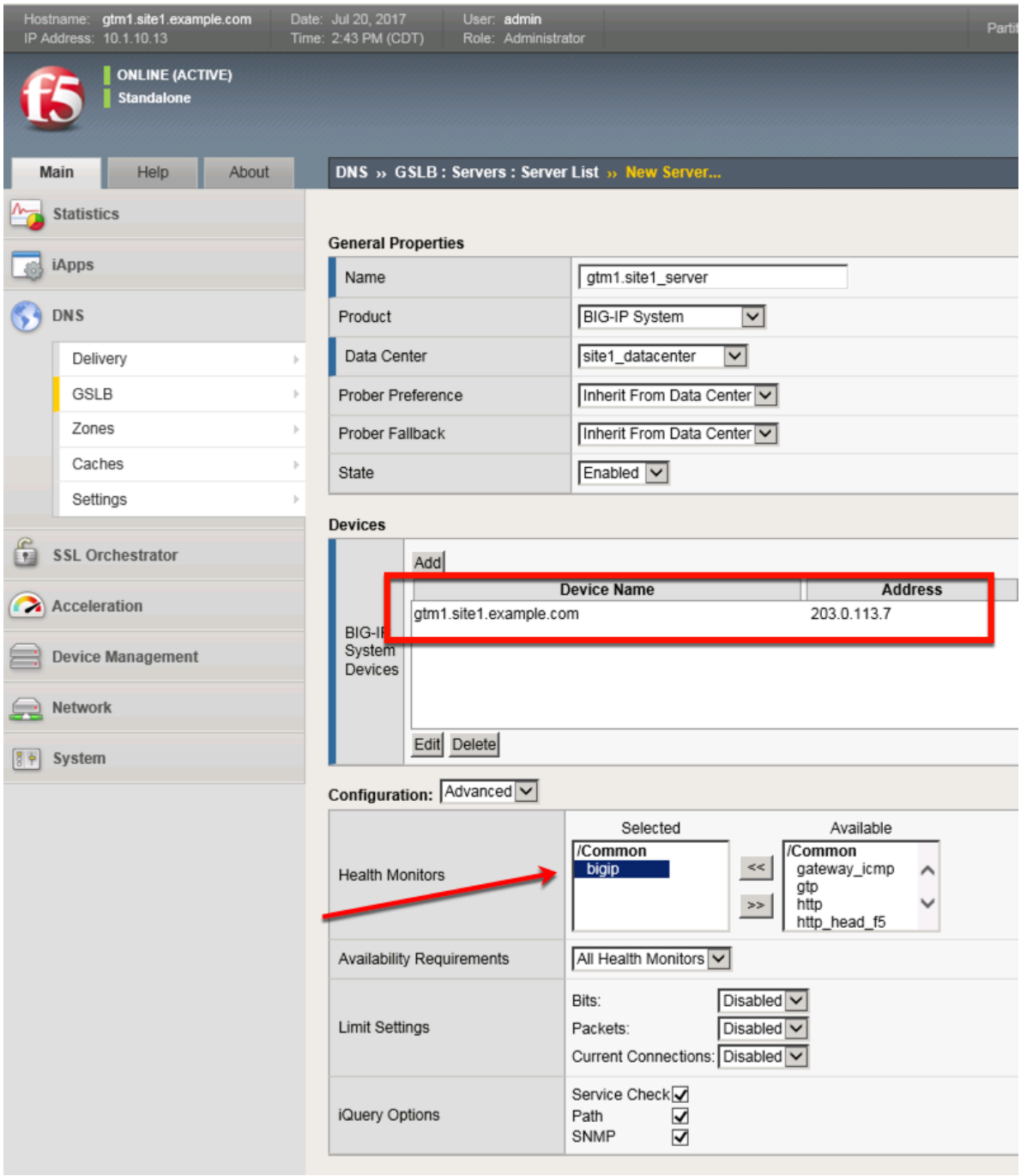
1. Fill in the Name and Datacenter




2. Click the “Add” button to define IP addresses




3. Complete the form and associate the “bigip” “Health Monitor”



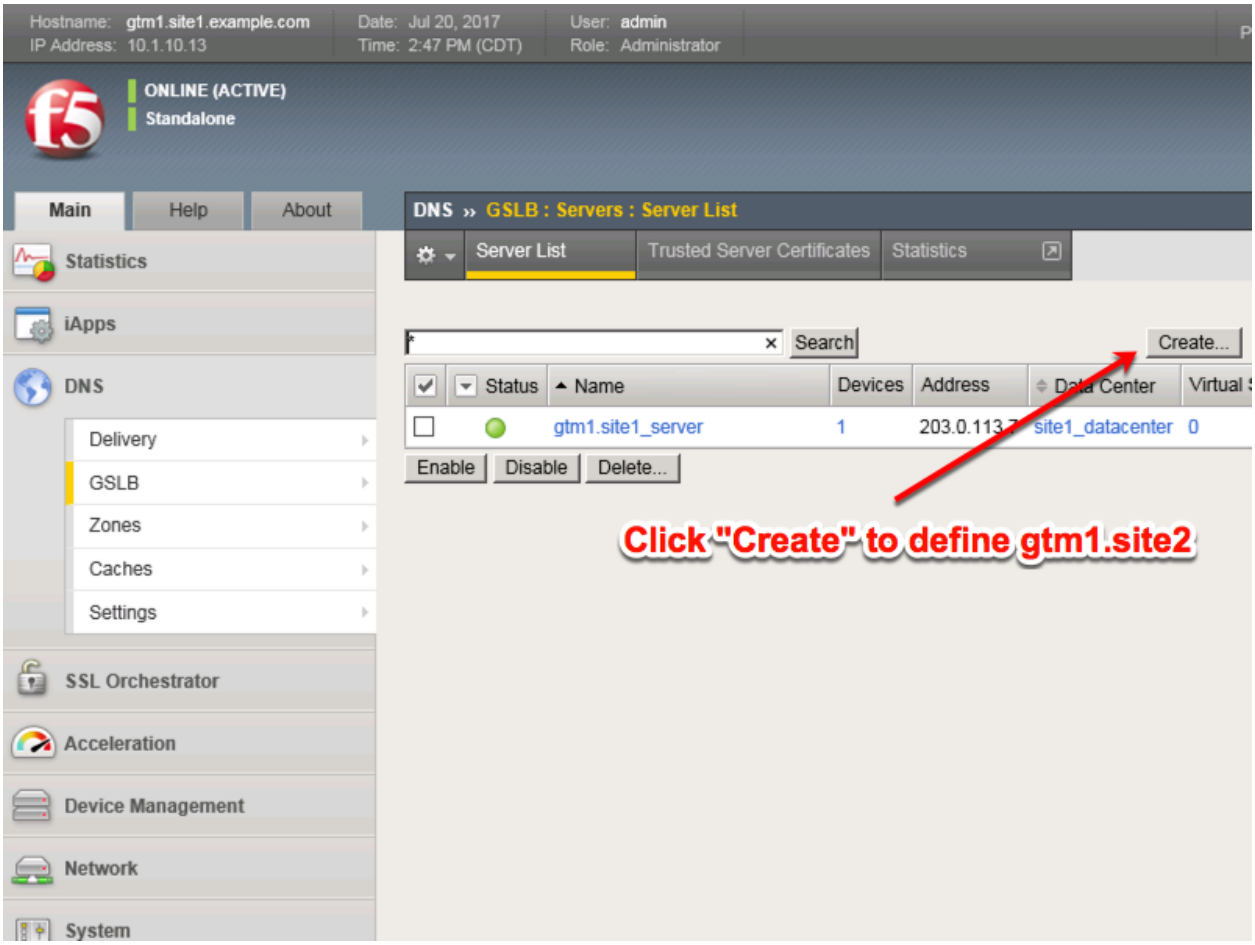

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/server/create.jsp

**TMSH**

tmsh create gtm server gtm1.site1_server datacenter site1_datacenter devices add { gtm1.site1.example.com { addresses add { 203.0.113.7 } } } monitor bigip product bigip

#### 2.3.1.2 gtm1.site2

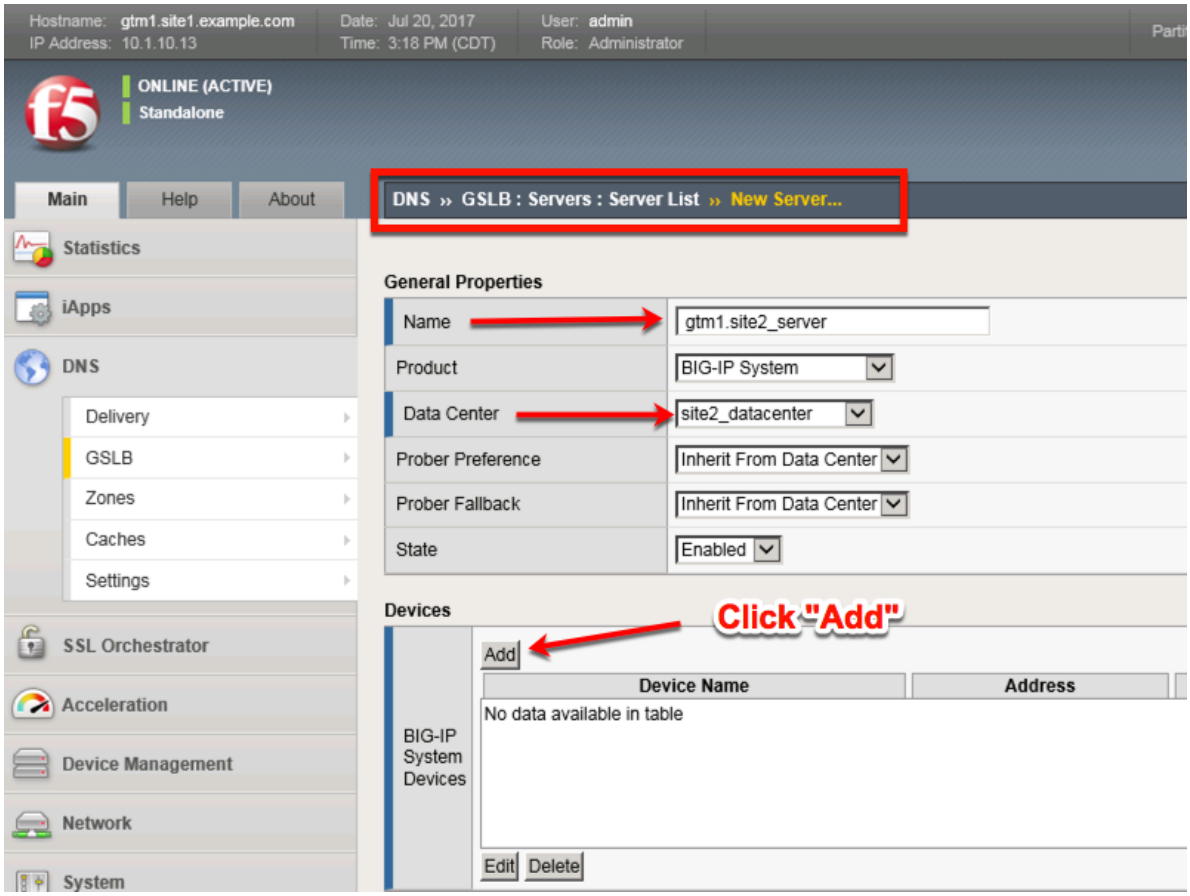
All GTM devices need to be defined. Create a server object for gtm1.site1



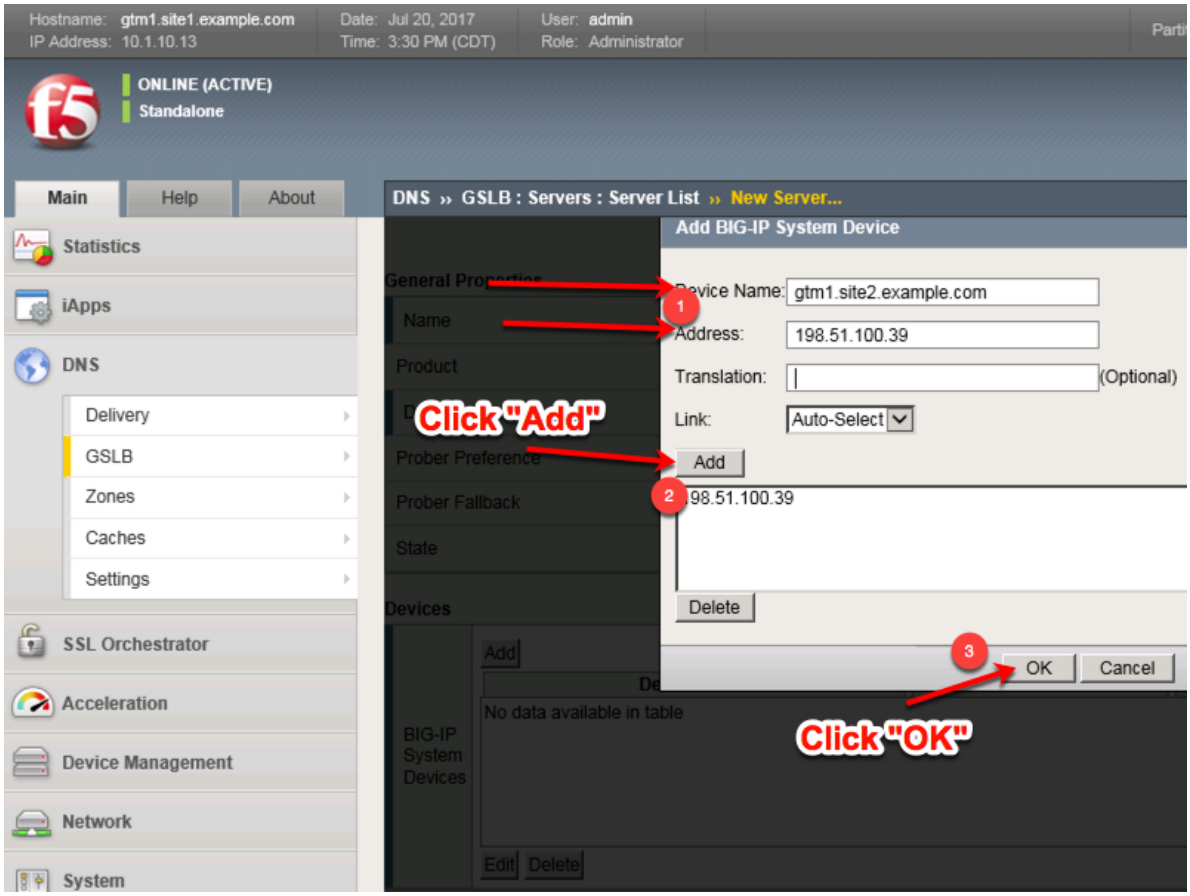

Click “Create” to define gtm1.site1 as defined in the table below:

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

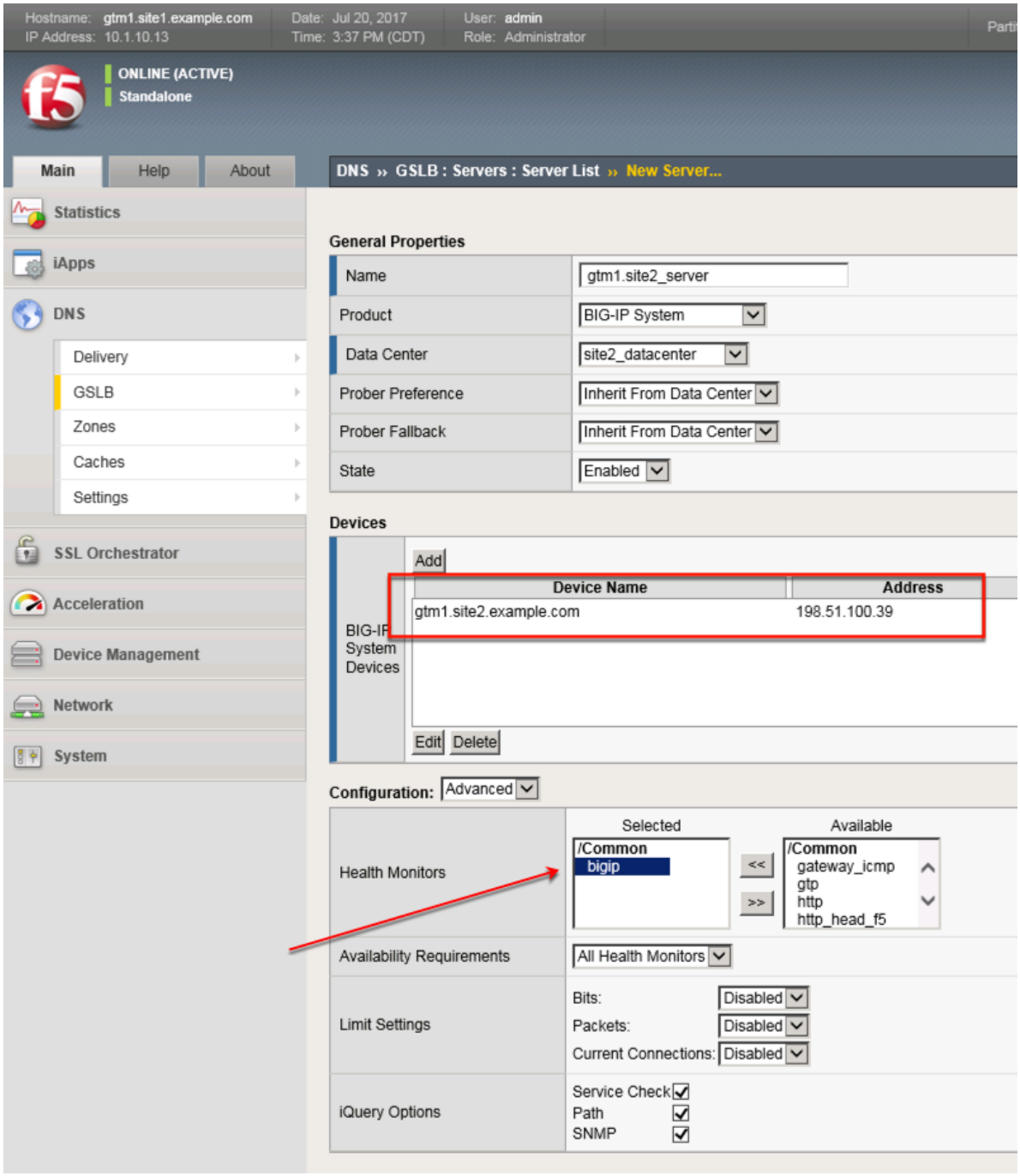
1. Fill in the Name and Datacenter




2. Click the “Add” button to define IP addresses




3. Complete the form and associate the “bigip” “Health Monitor”



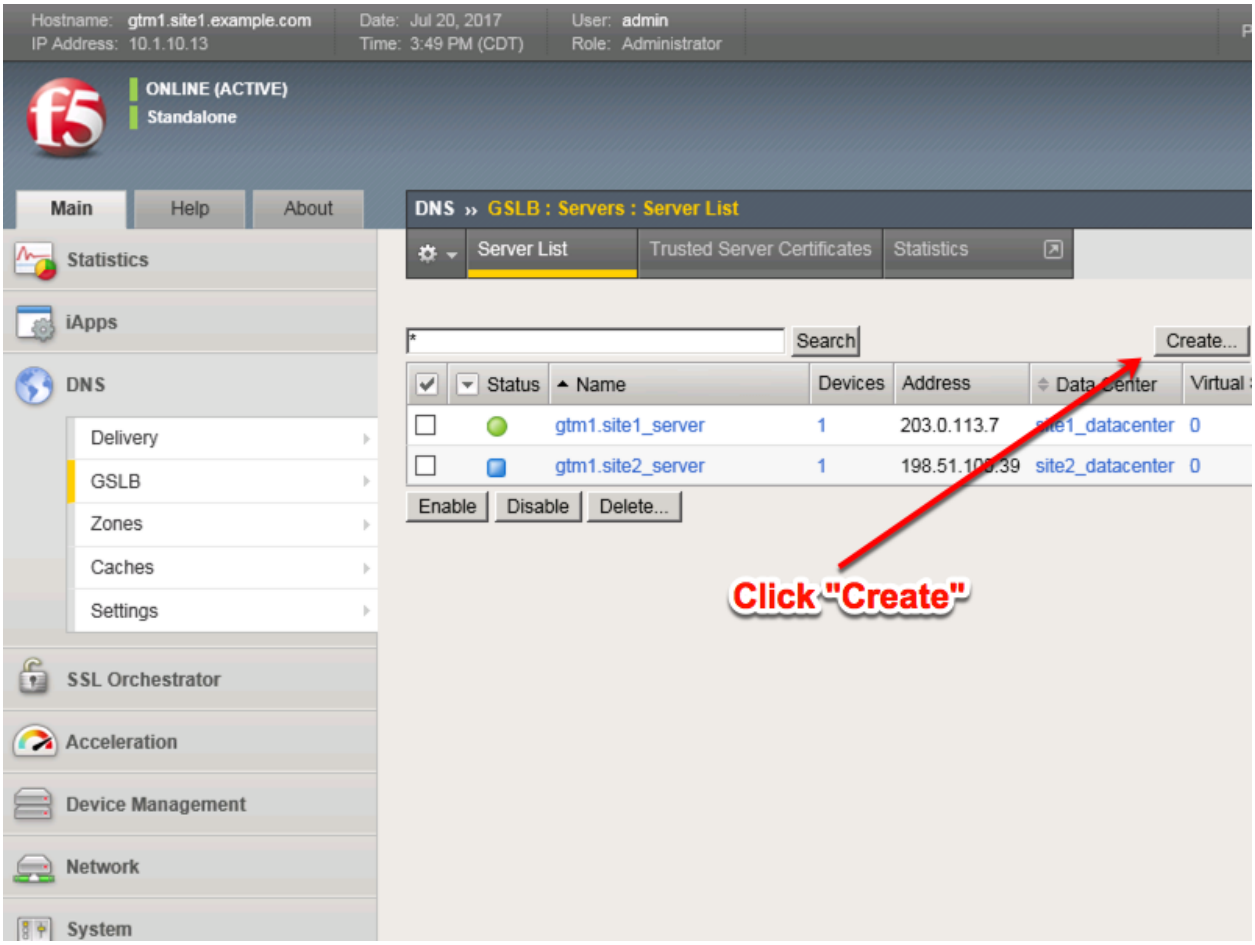

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/server/create.jsp

**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

#### 2.3.1.3 site1_ha-pair

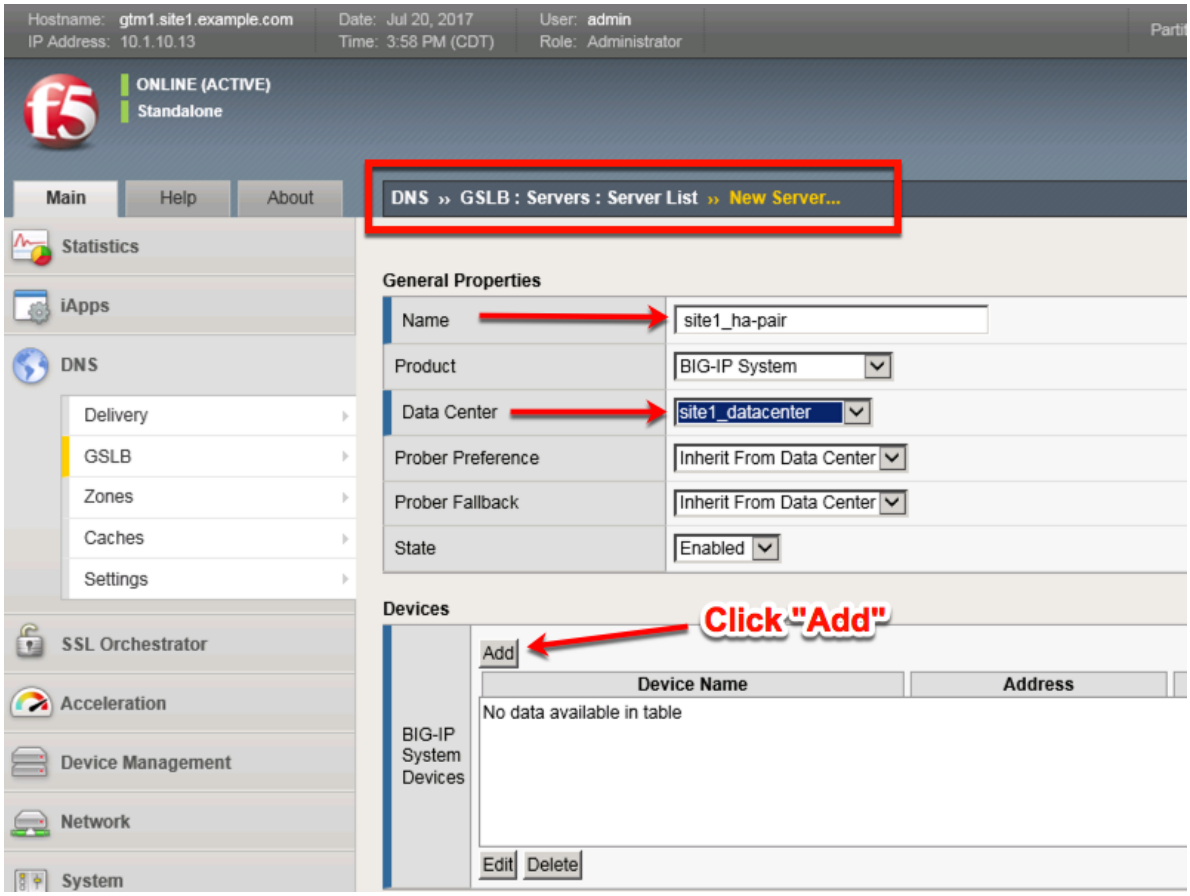
LTM devices need to be defined. Create a server object for the bigip1.site1 and bigip2.site1 HA pair



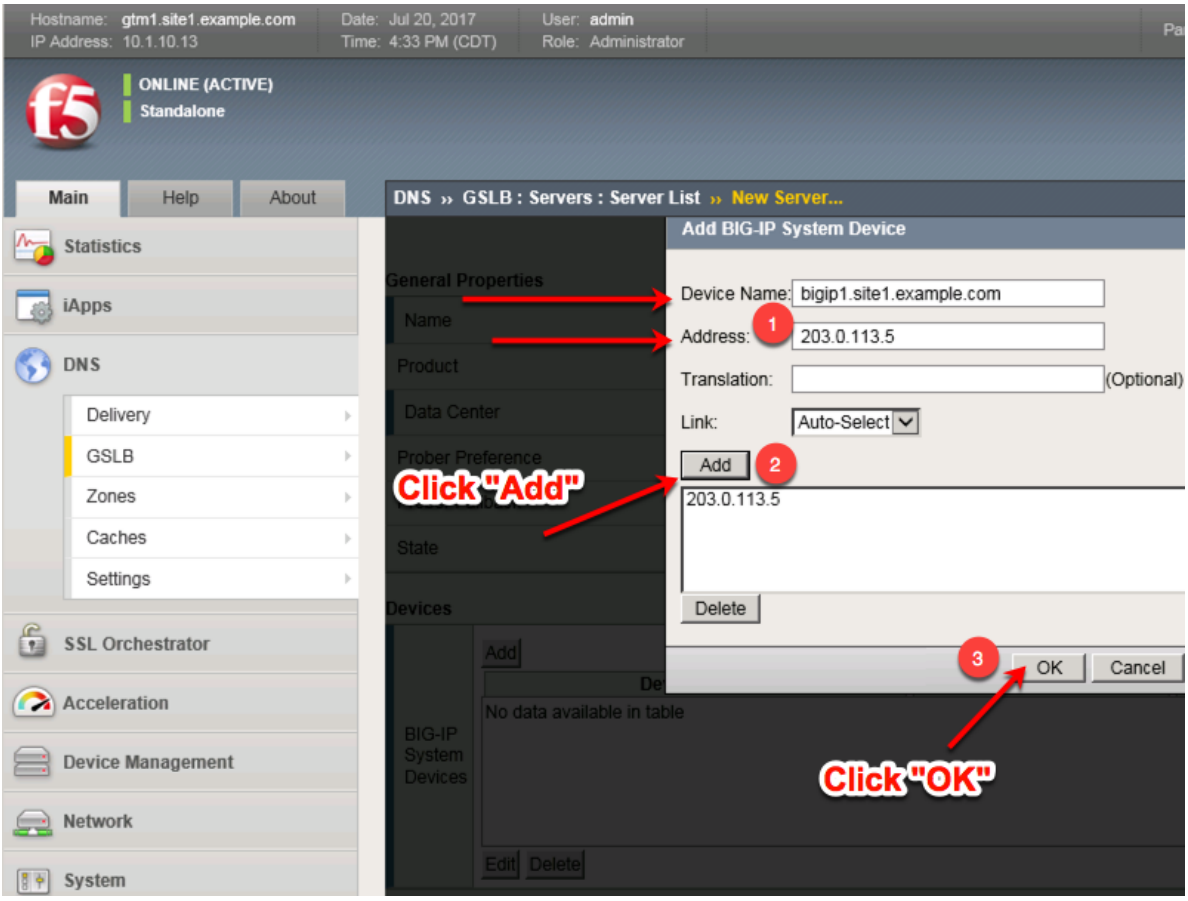

Create a Server Object as defined in the table below:

| 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 |

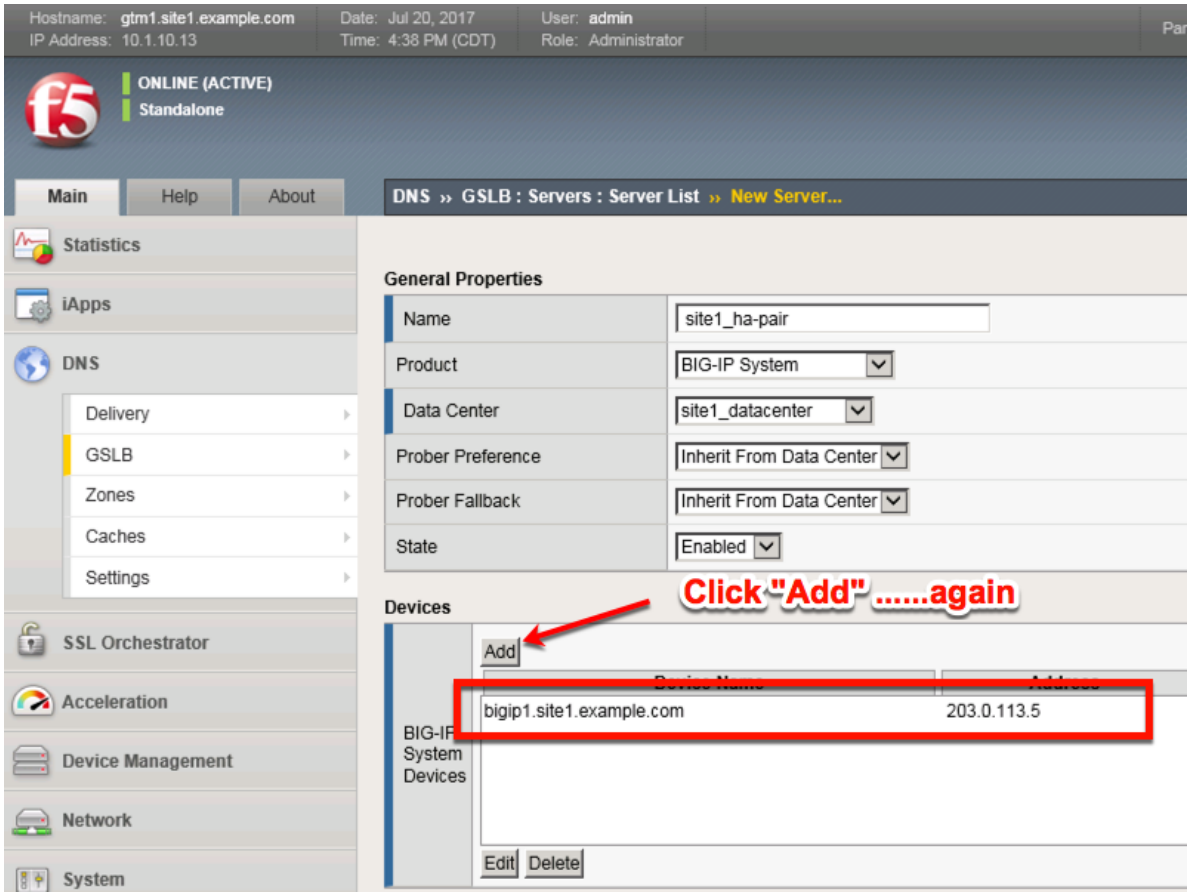
1. Fill in the Name and Datacenter



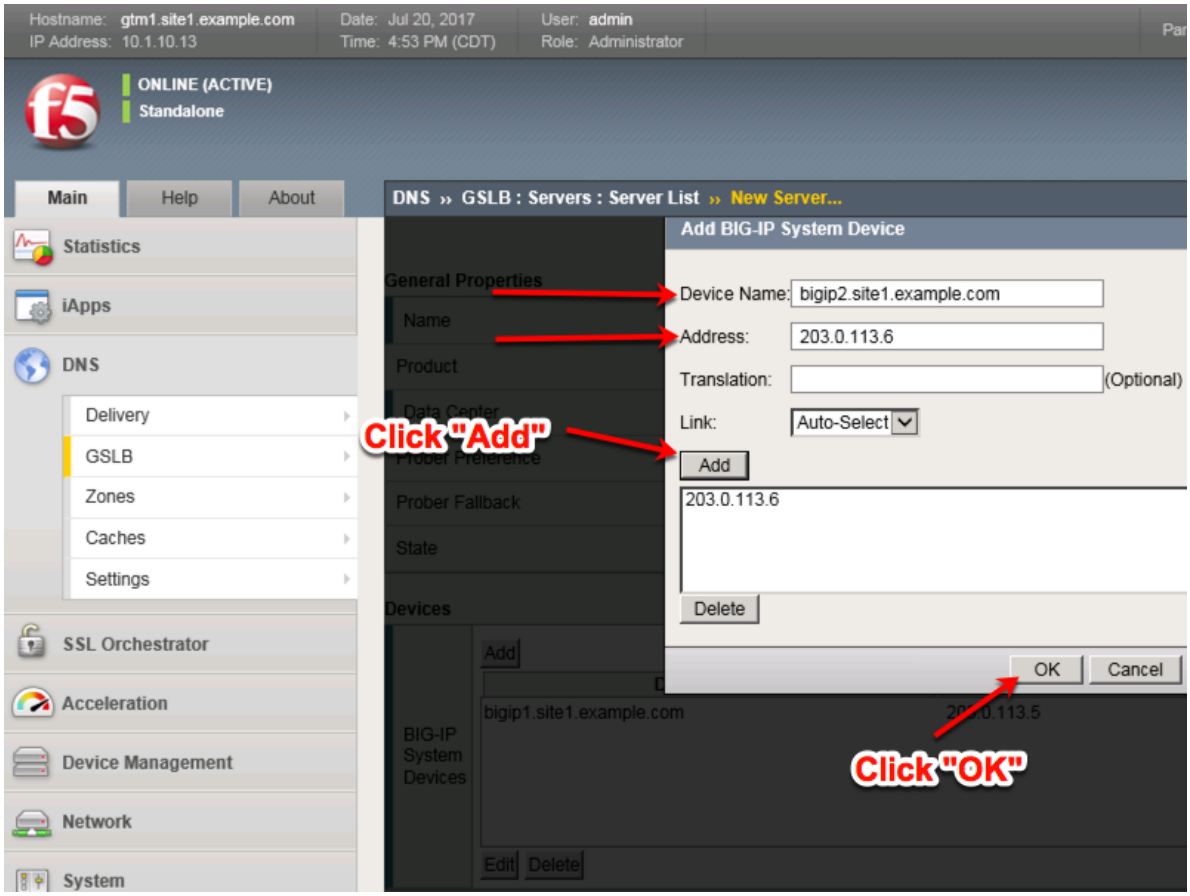

2. Click the “Add” button to define IP addresses



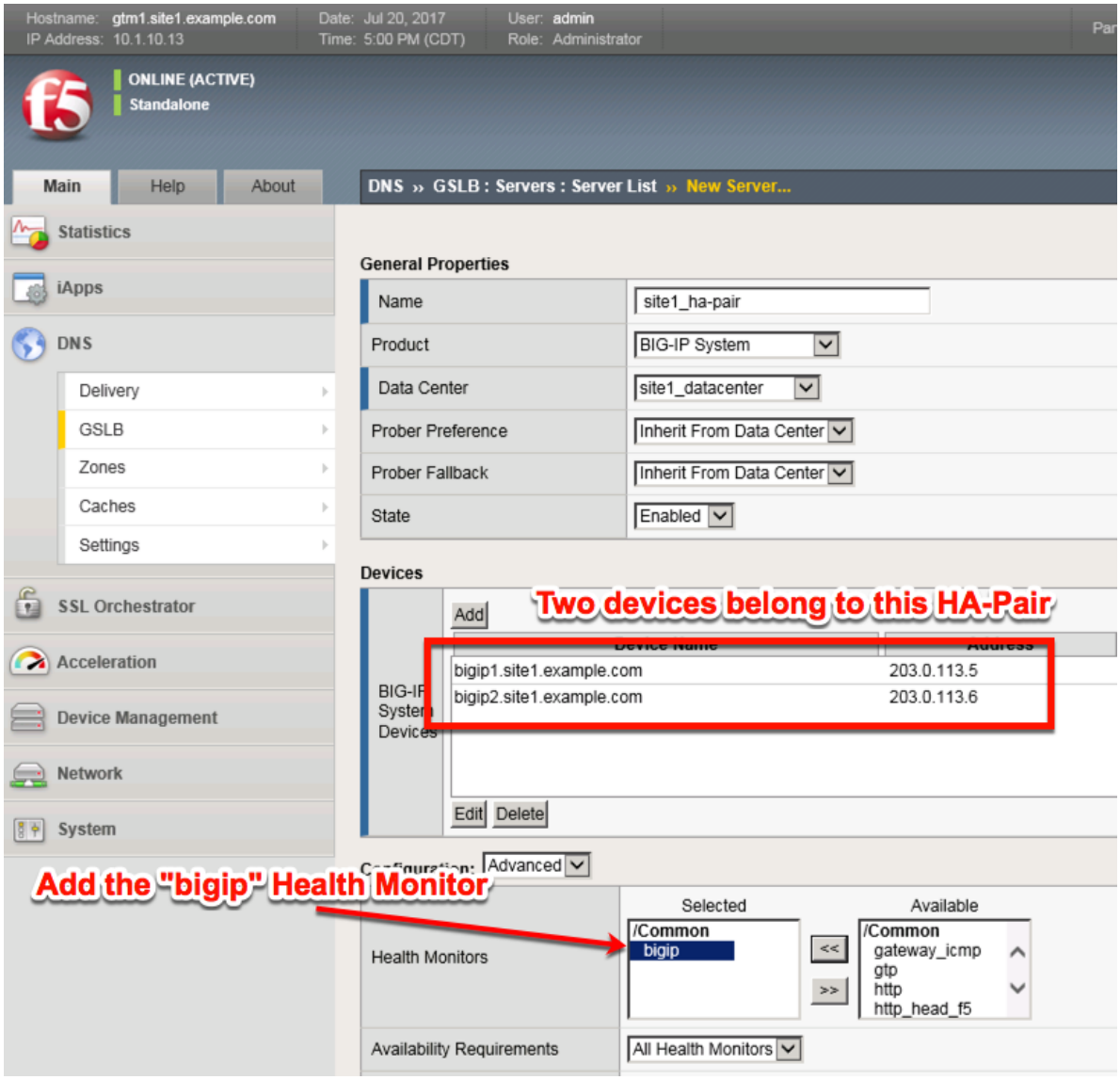

3. Click “Add” again to define the other BIG-IP in the HA pair.




4. Click the “Add” button to define IP addresses




5. Complete the form and associate the “bigip” “Health Monitor”



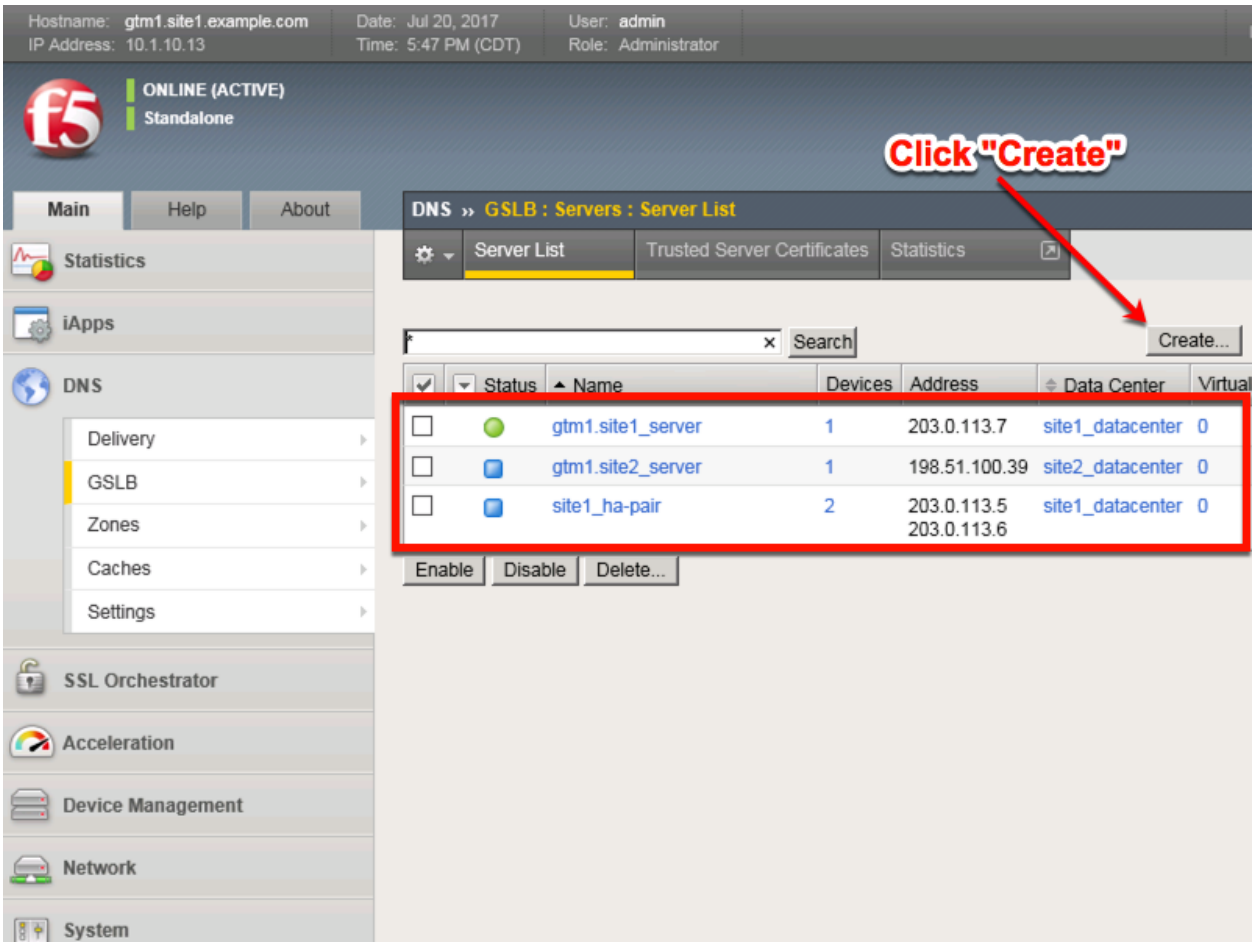

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/server/create.jsp

**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

#### 2.3.1.4 site2_ha-pair

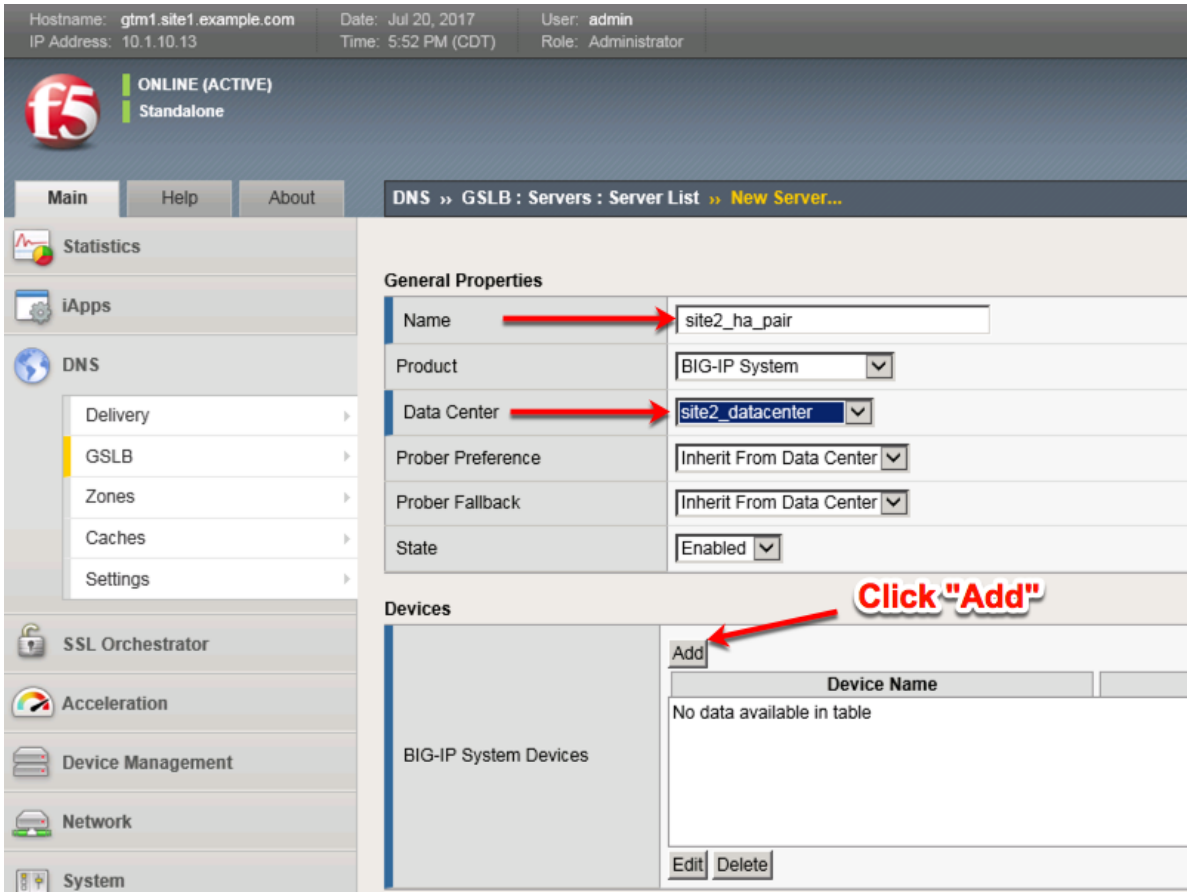
LTM devices need to be defined. Create a server object for the bigip1.site1 and bigip2.site1 HA pair



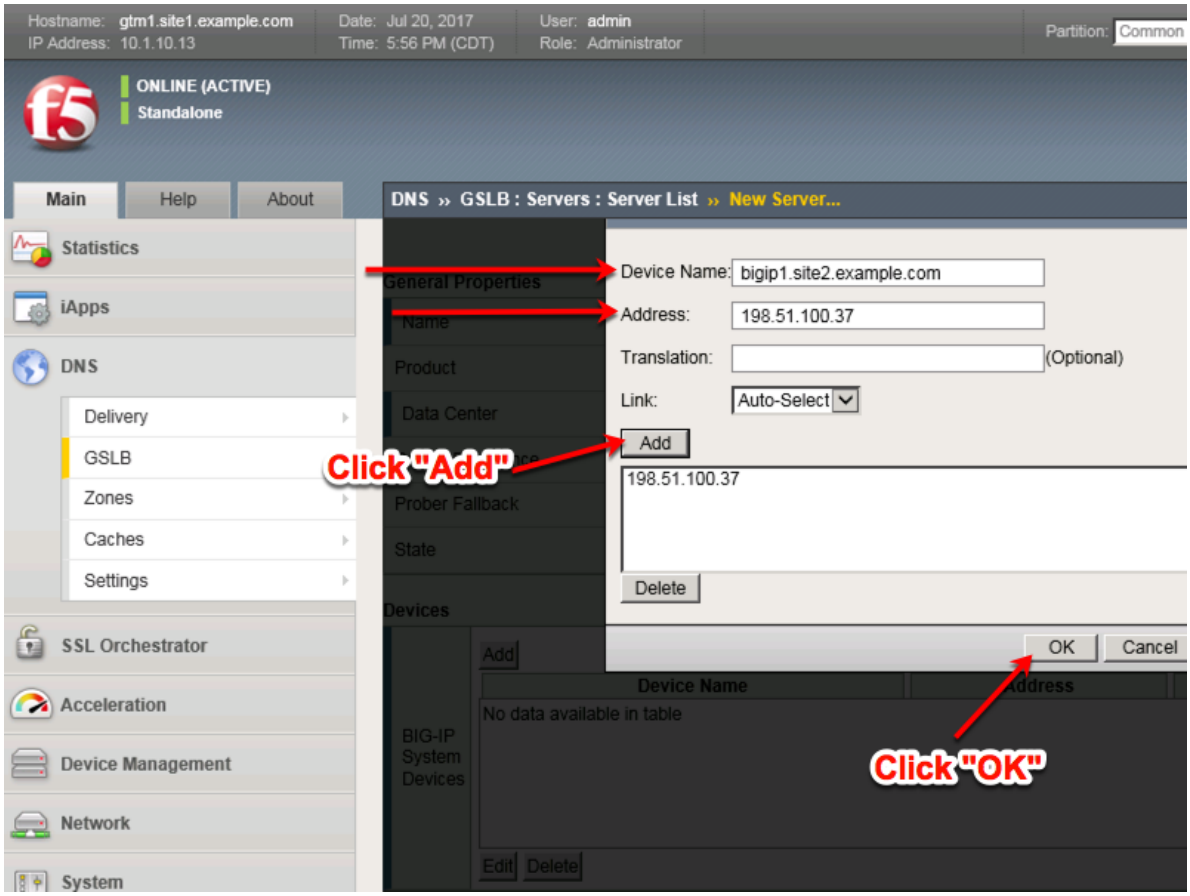

Create a Server Object as defined in the table below:

| Setting | Value |
|---|---|
| Name | 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 |

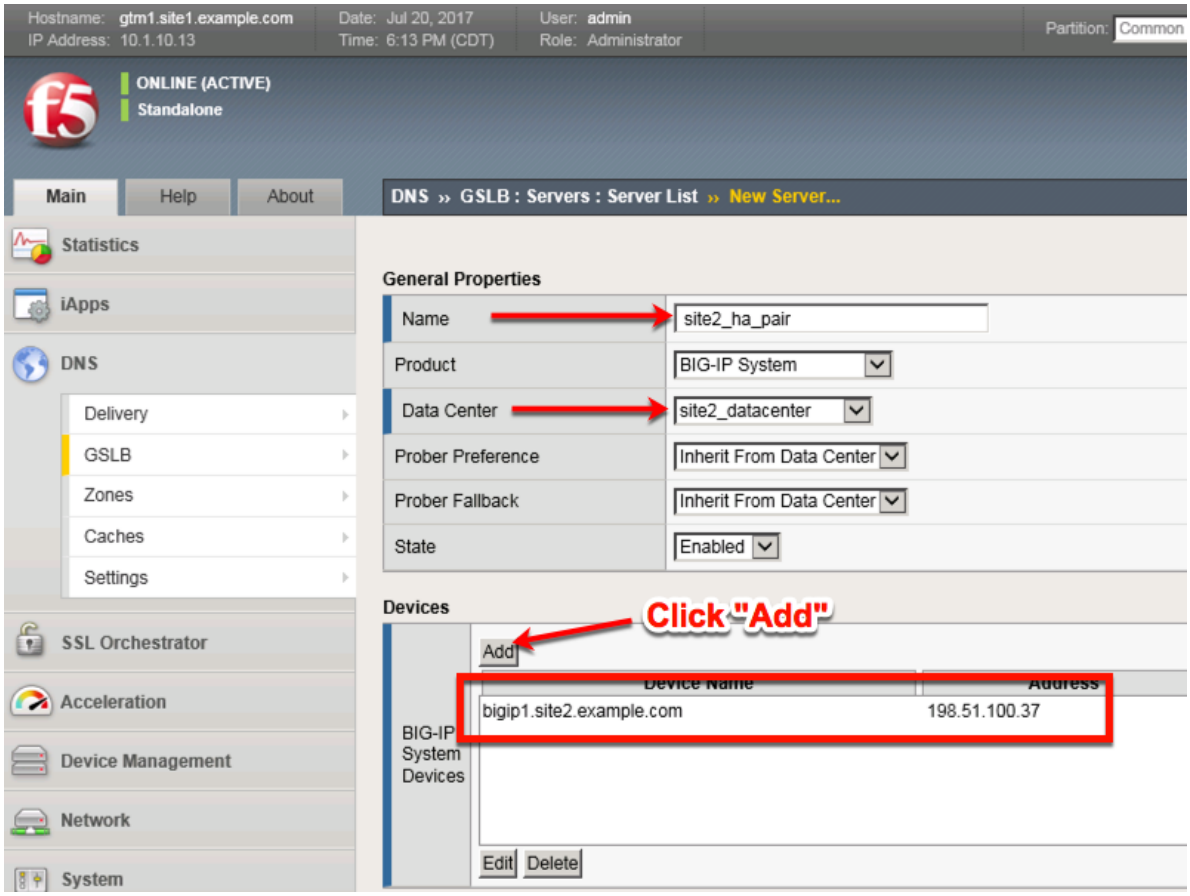
1. Fill in the Name and Datacenter



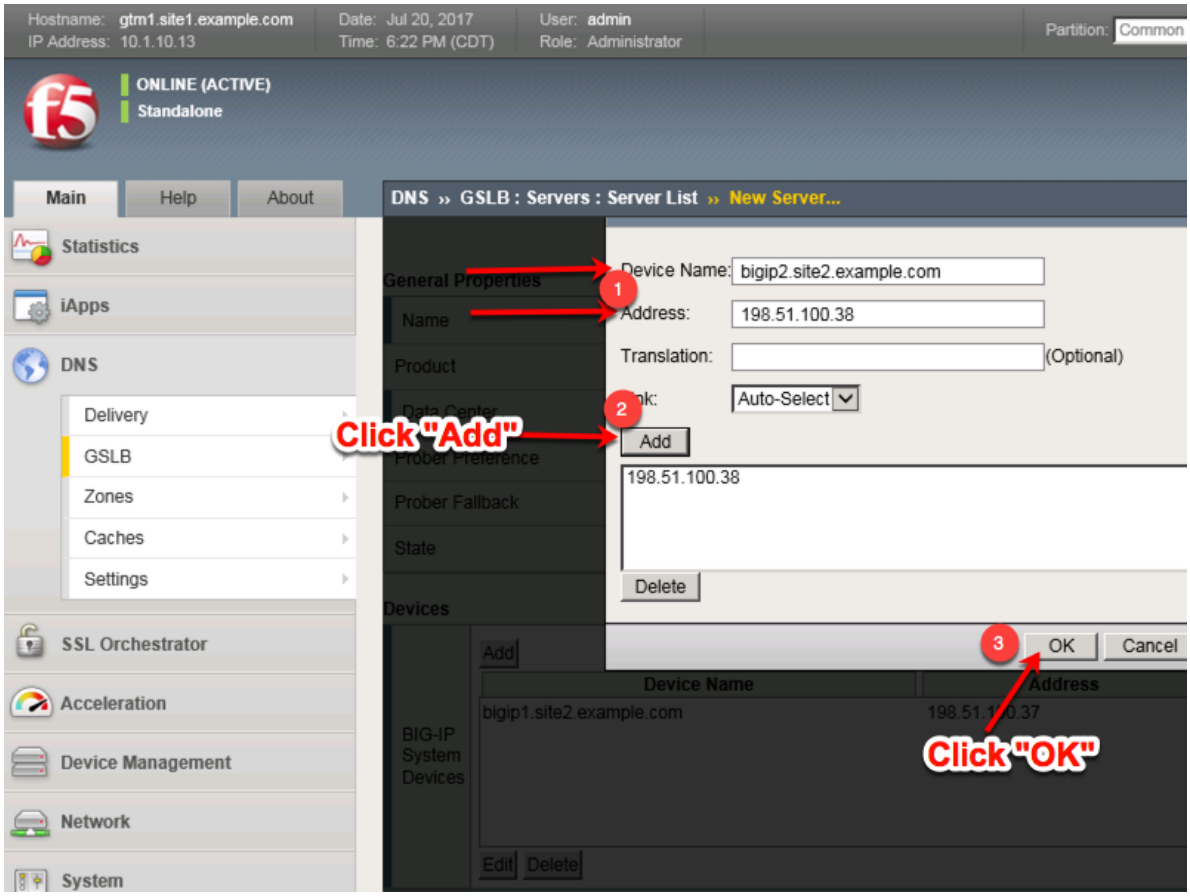

2. Click the “Add” button to define IP addresses



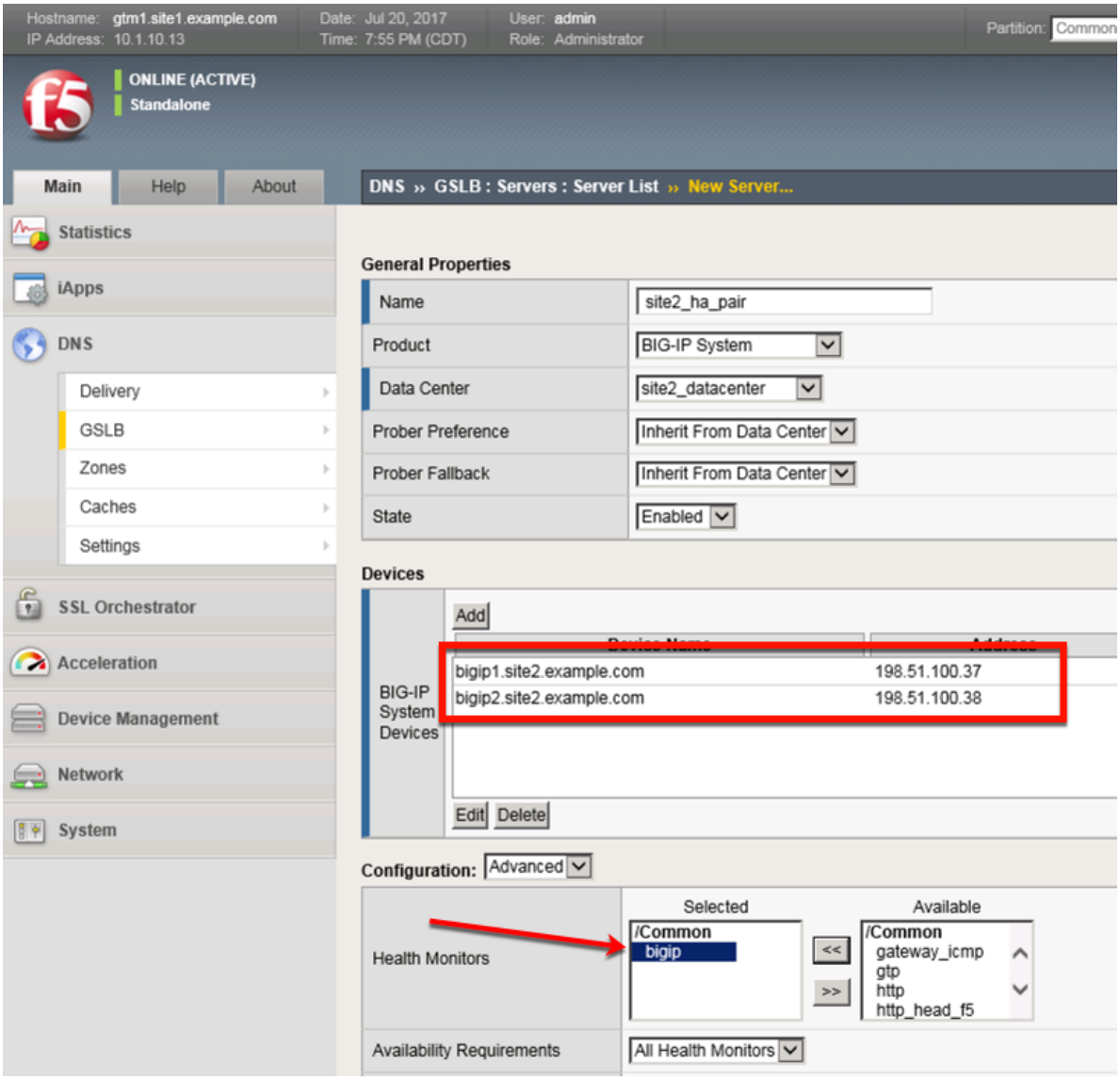

3. Click “Add” again to define the other BIG-IP in the HA pair.




4. Click the “Add” button to define IP addresses




5. Complete the form and associate the “bigip” “Health Monitor”



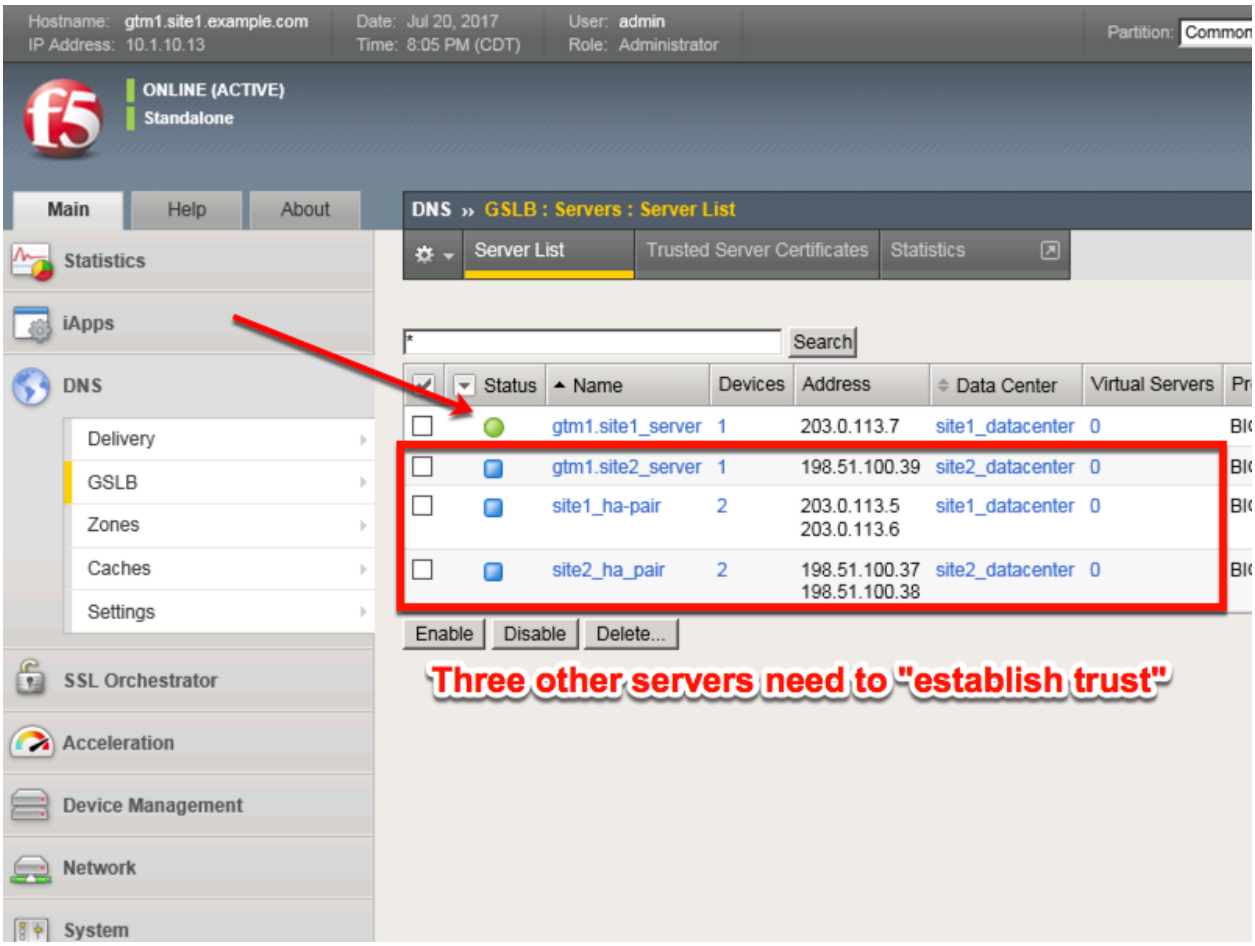

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/server/create.jsp

**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.




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

Run the following command:

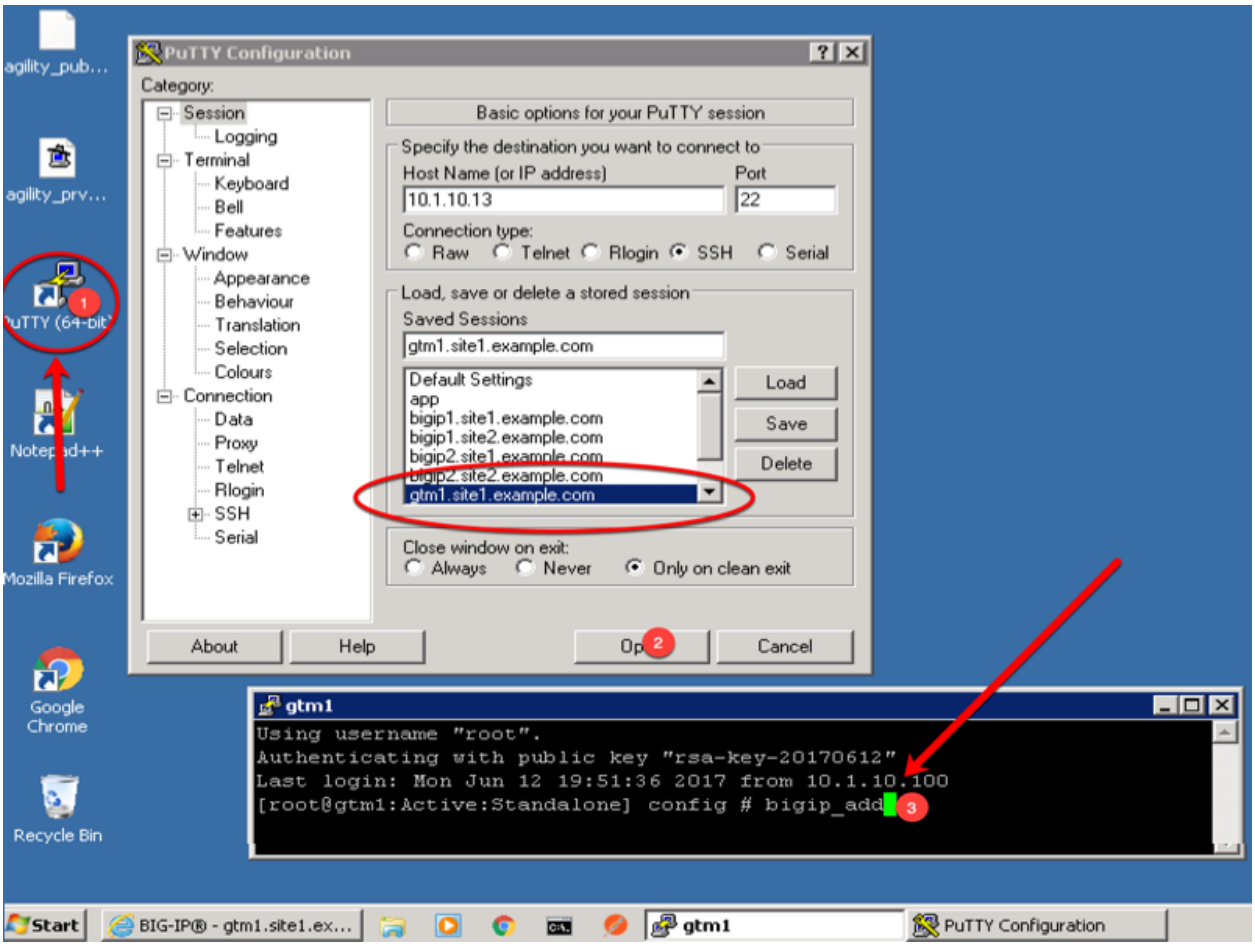
When prompted for a password use “default”.

---

**TMSH**

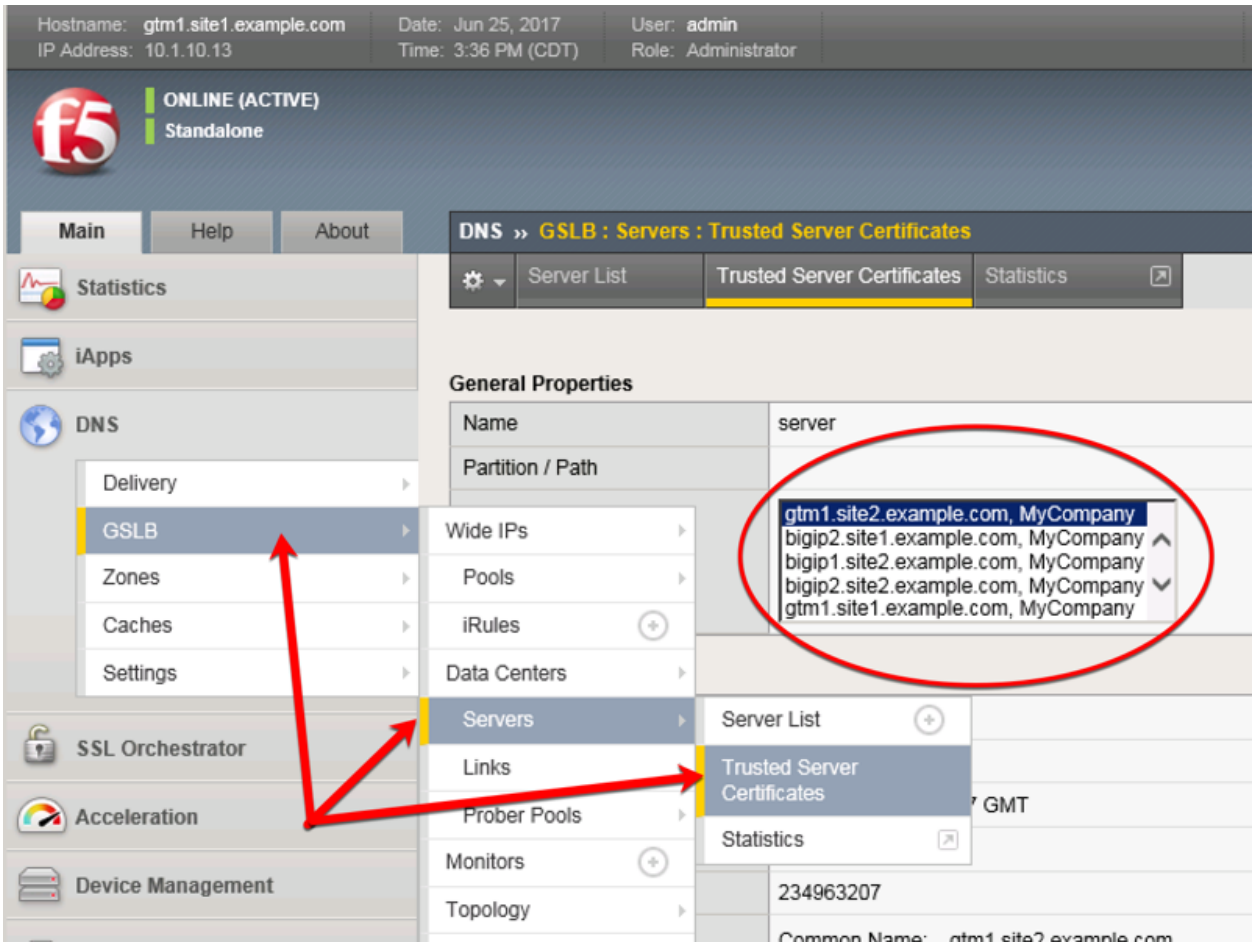
bigip_add

---




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

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/locallb/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.

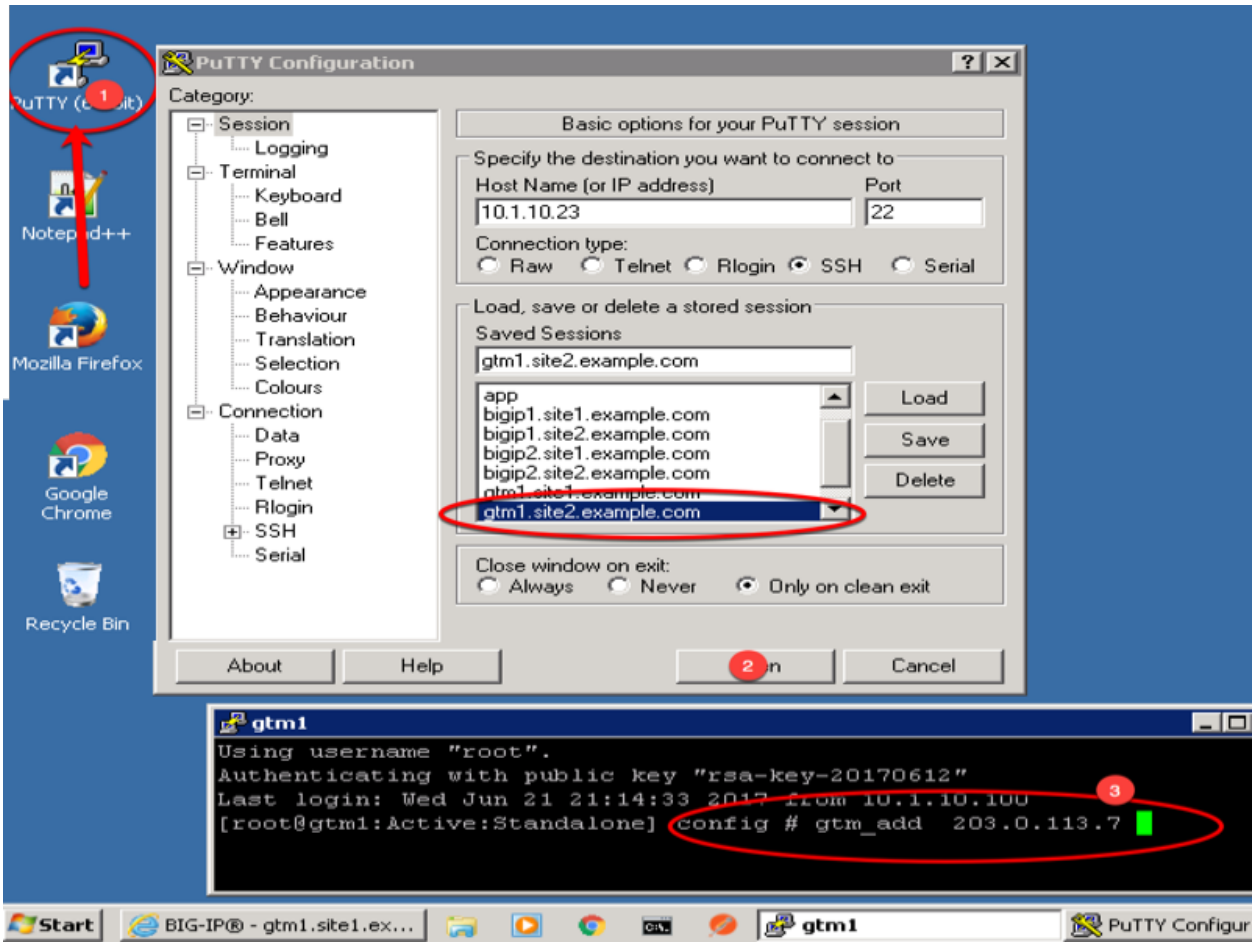
Launch Putty and log in to gtm1.site2

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

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

**TMSH**

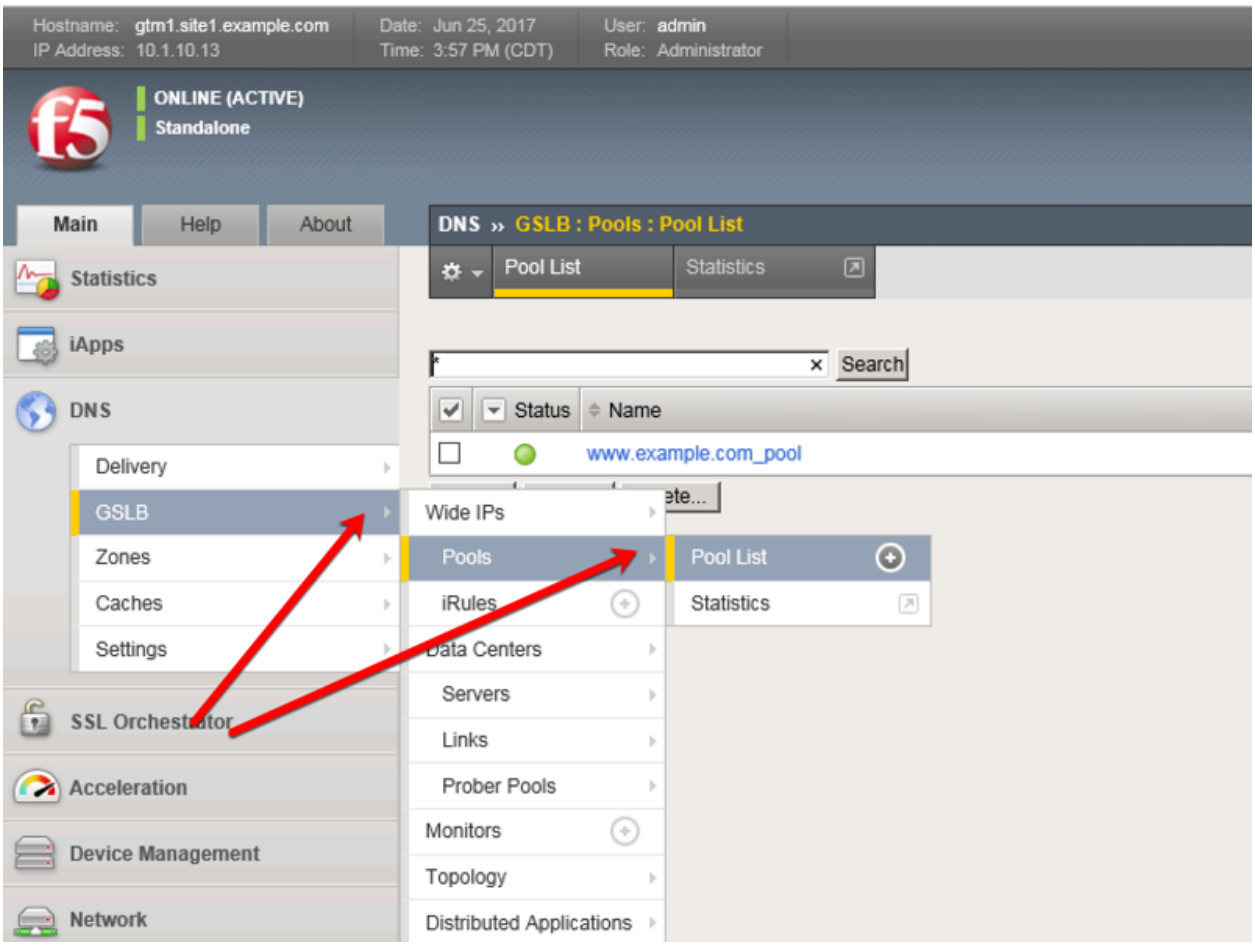
gtm_add 203.0.113.7




## 2.4 Pools

LTM virtual server objects are grouped together into GTM pools.

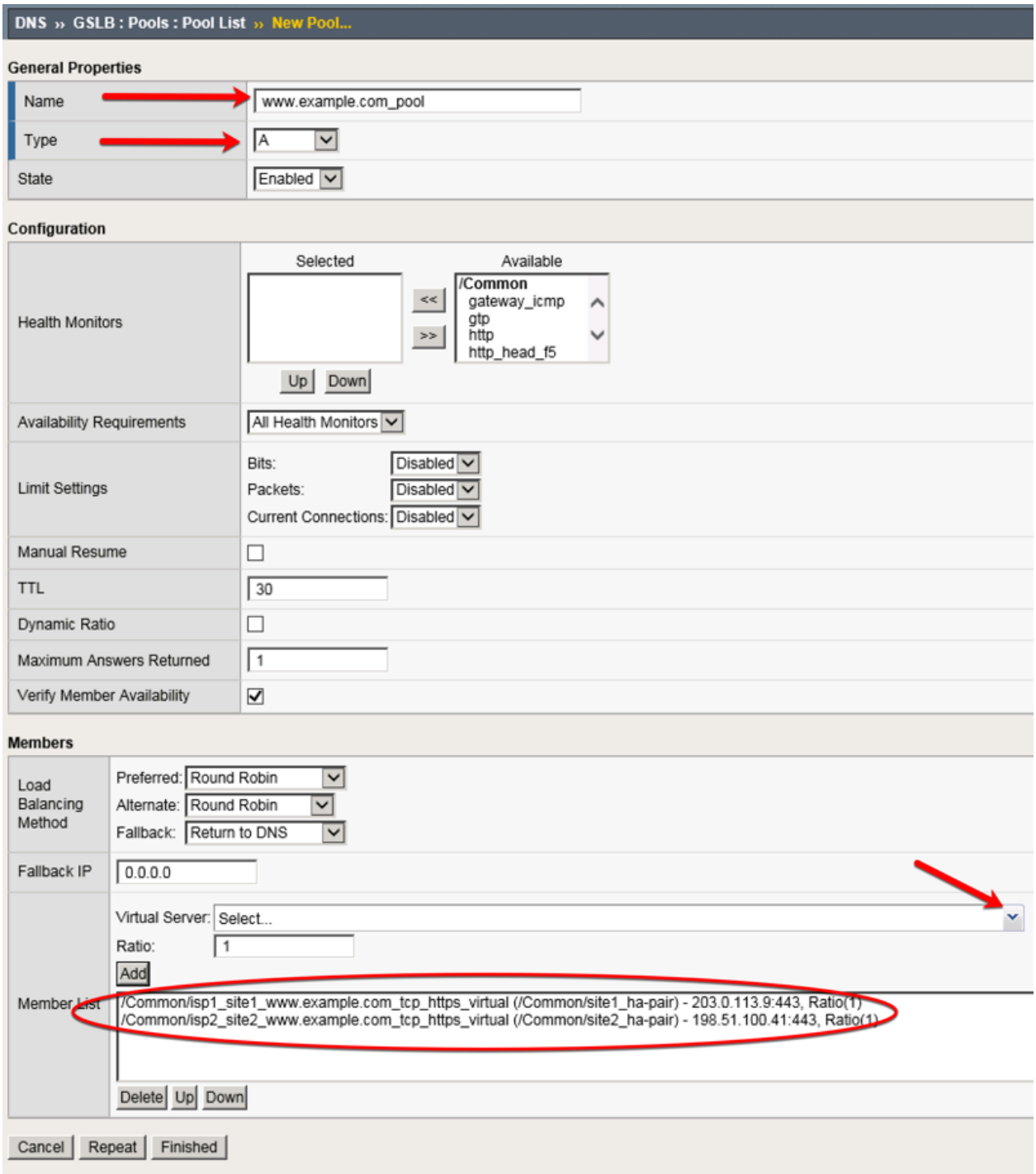
Navigate to: **DNS ›› GSLB : Pools : Pool List**




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




TMSH command to run on only gtm1.site1:

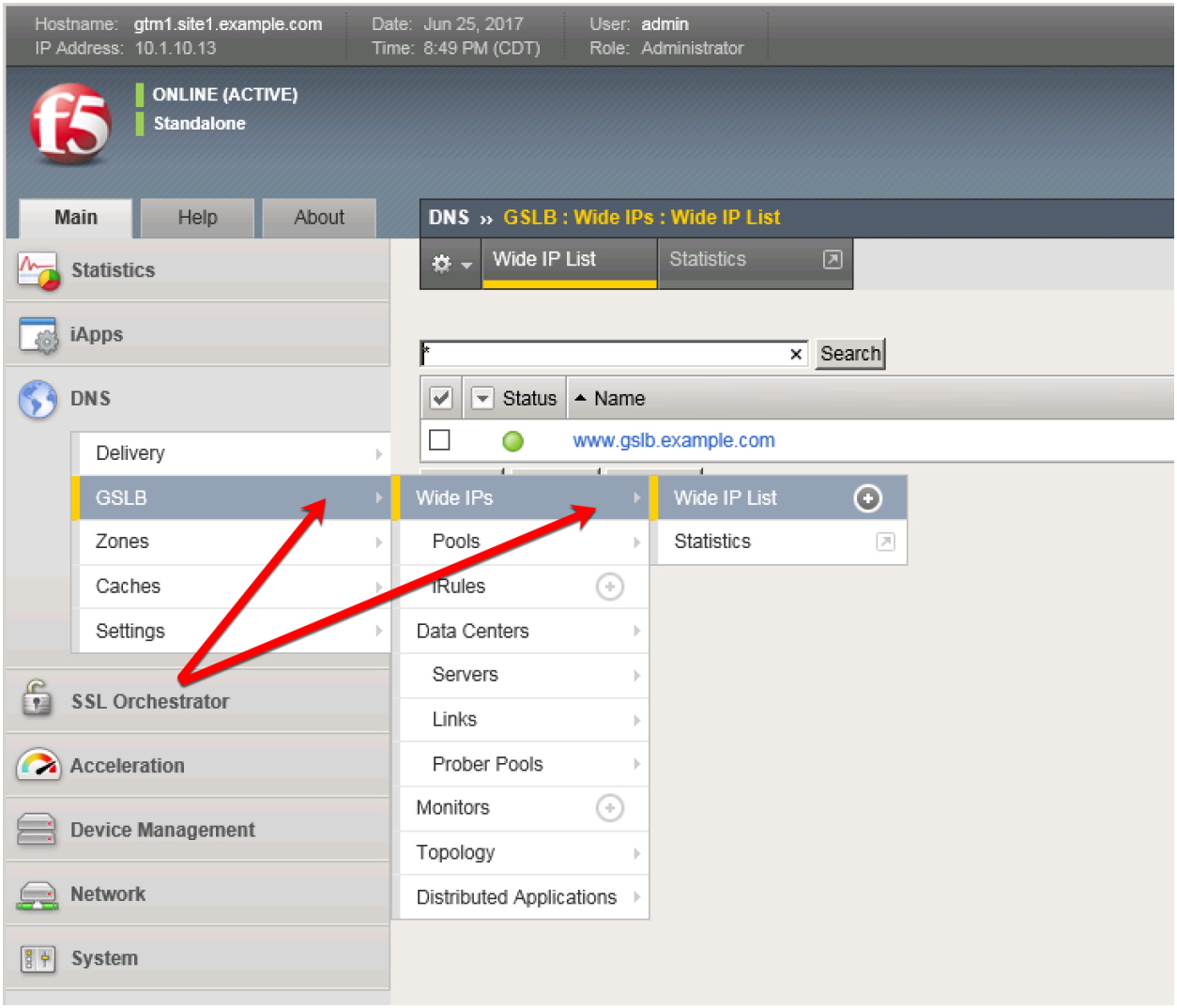
**TMSH**

```
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 |

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

**General Properties:** Advanced

| | |
|---|---|
| Name | www.example.com |
| Type | A |
| Description | |
| Alias List | Alias: <br> Add <br> Delete |
| State | Enabled |
| Minimal Response | Enabled |
| Return Code On Failure | Disabled |
| Load-Balancing Decision Log | ☐ Pool Selection <br> ☐ Pool Traversal <br> ☐ Pool Member Selection <br> ☐ Pool Member Traversal |

**iRules**

| | |
|---|---|
| iRule List | Selected / Available <br> << <br> >> <br> Up Down |

**Pools**

| | |
|---|---|
| Load Balancing Method | Round Robin |
| Persistence | Disabled |
| | Pool Select... |

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

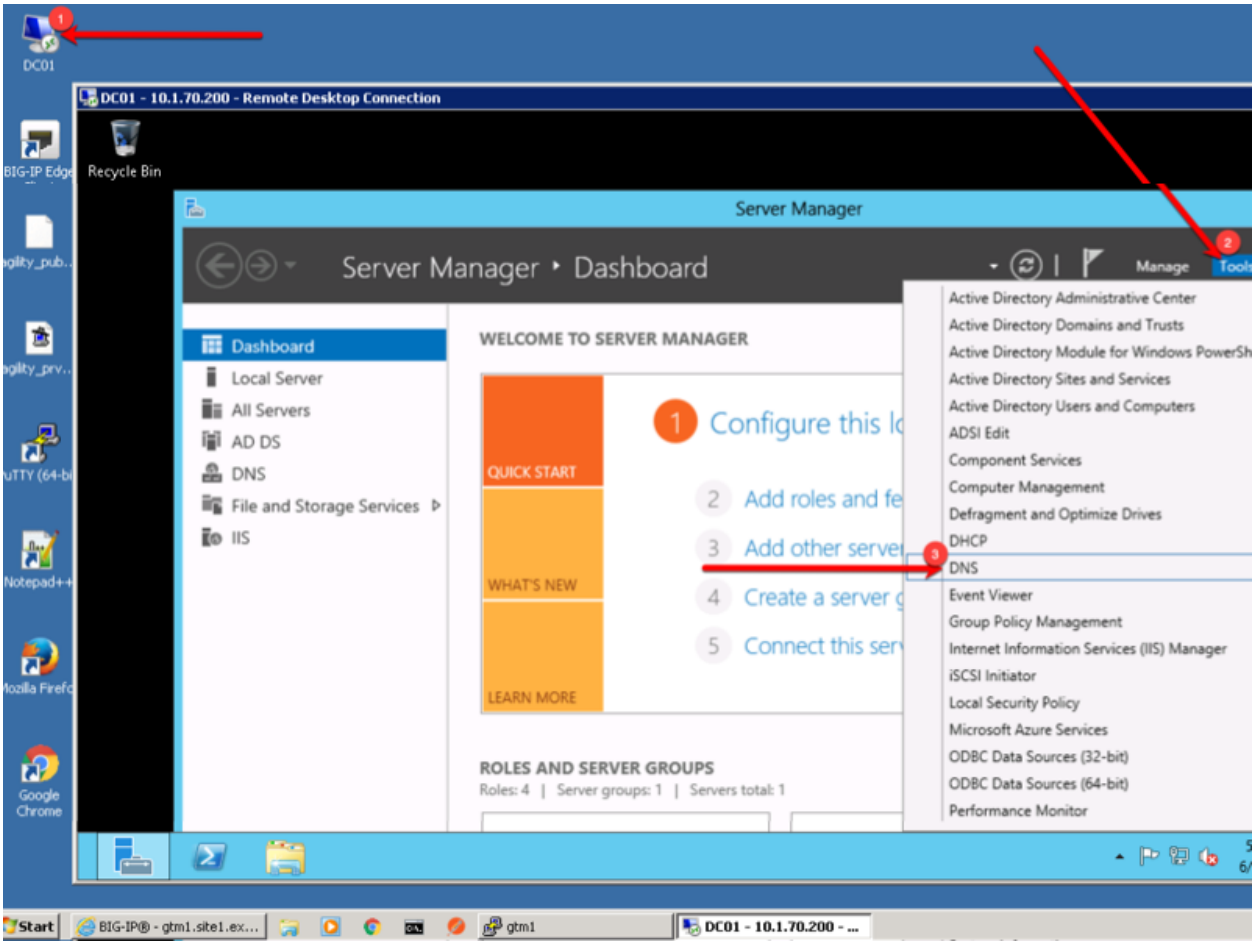
TMSH command to run on only gtm1.site1:

**TMSH**

```
tmsh 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, and open the DNS management UI:

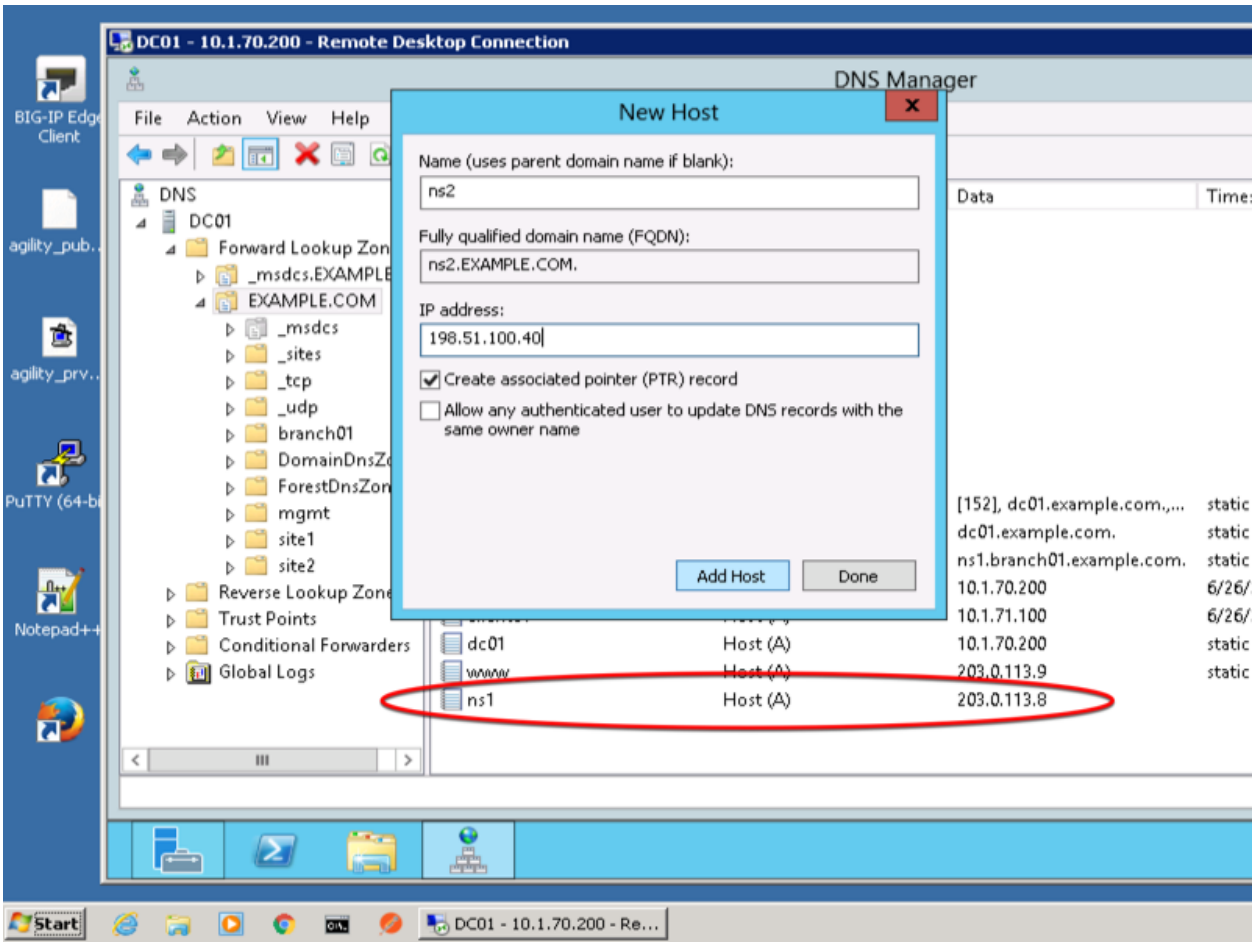



### 2.6.1 A Records

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

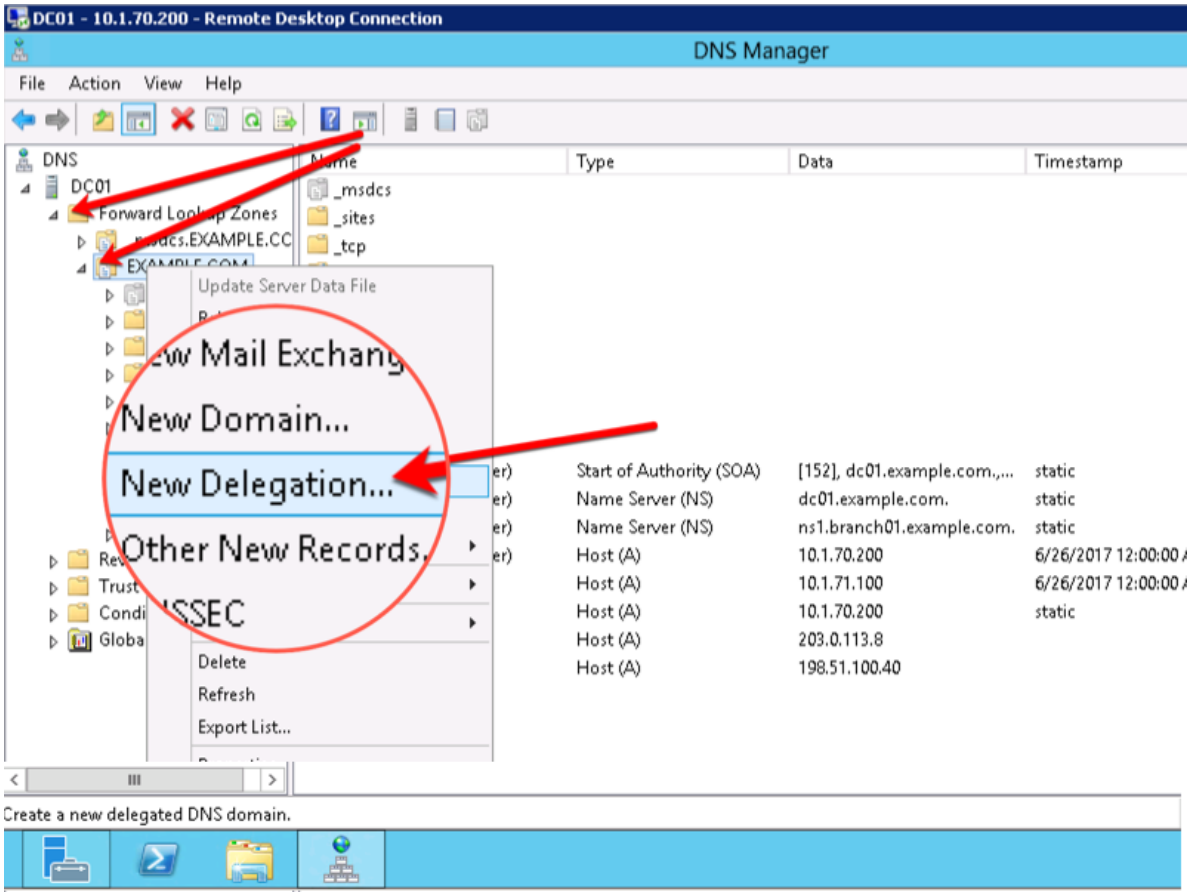
| Setting | Value |
|---|---|
| ns1.example.com. | 203.0.113.8 |
| ns2.example.com. | 198.51.100.40 |

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

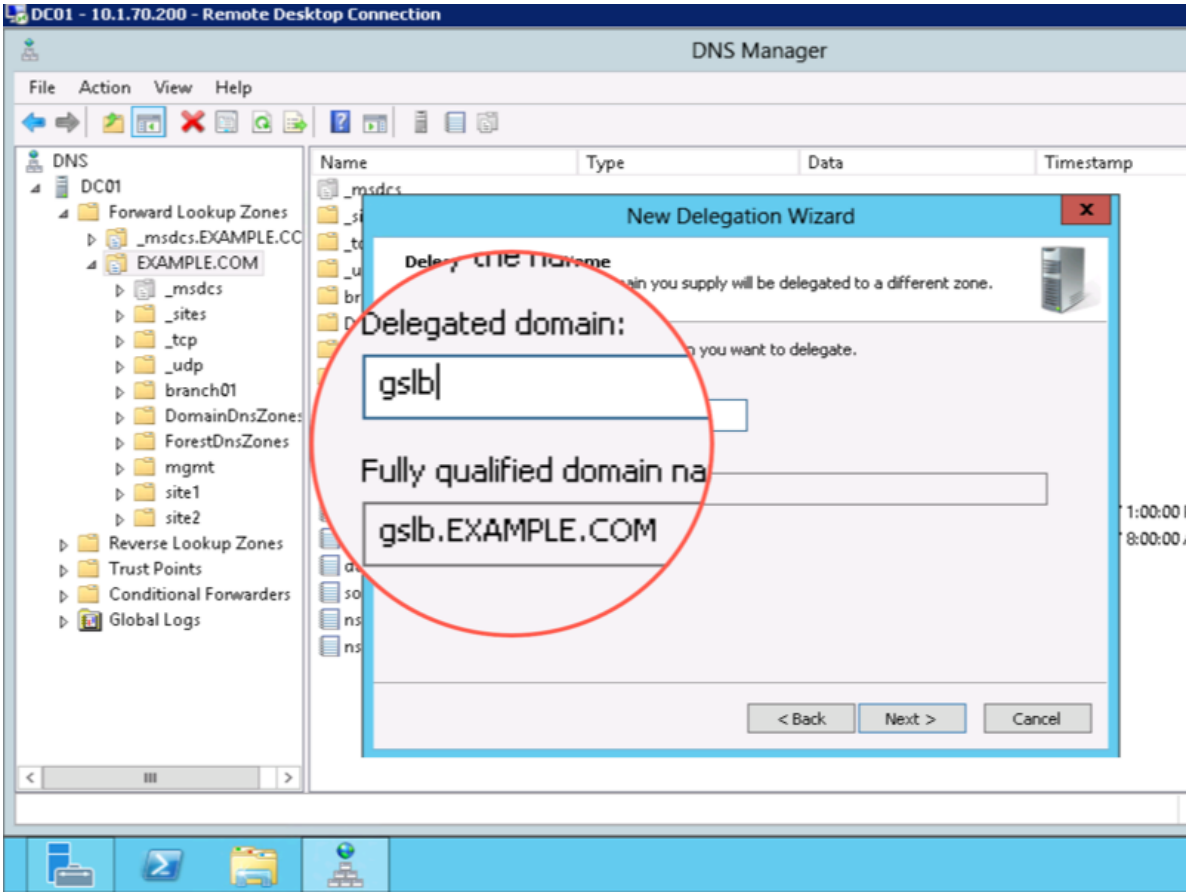



## 2.6.2 Sub Domain

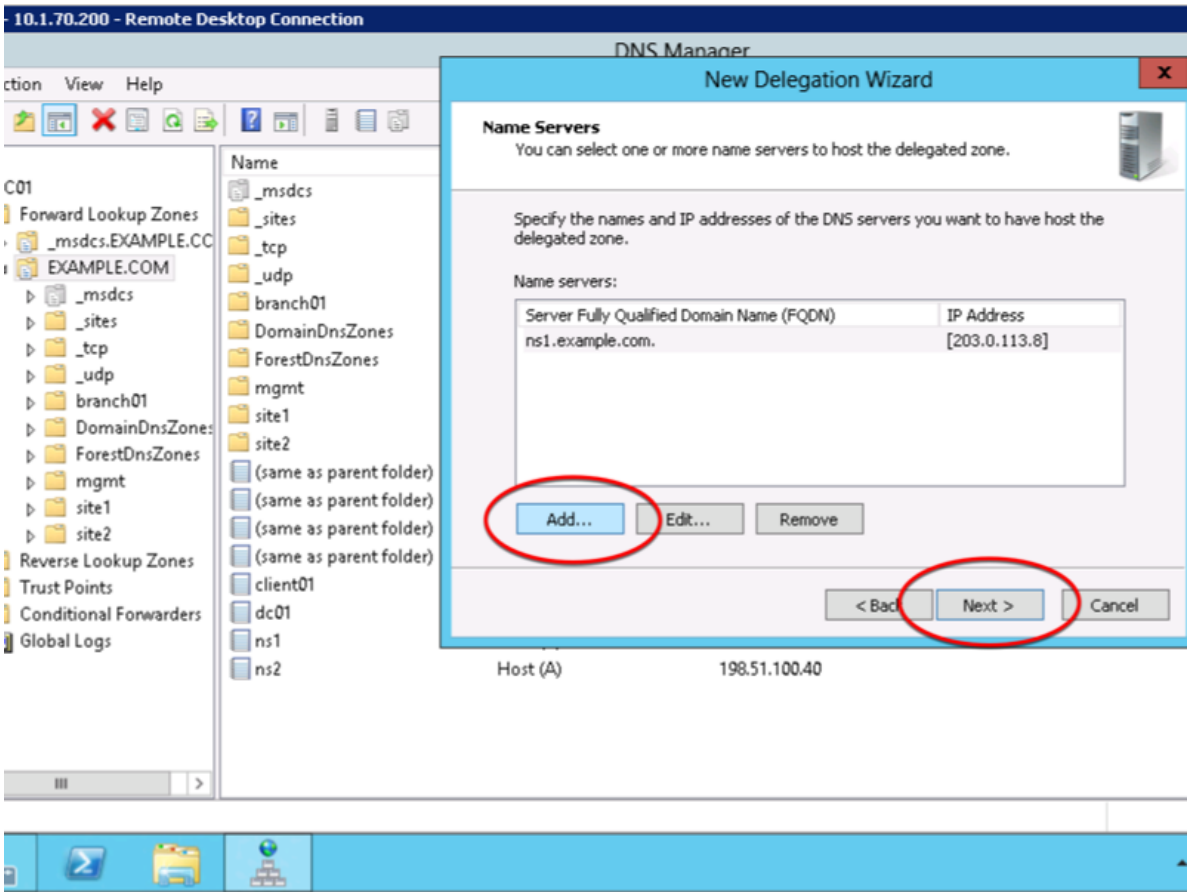
1. Expand “Forward Lookup Zones”, and right click on “EXAMPLE.com



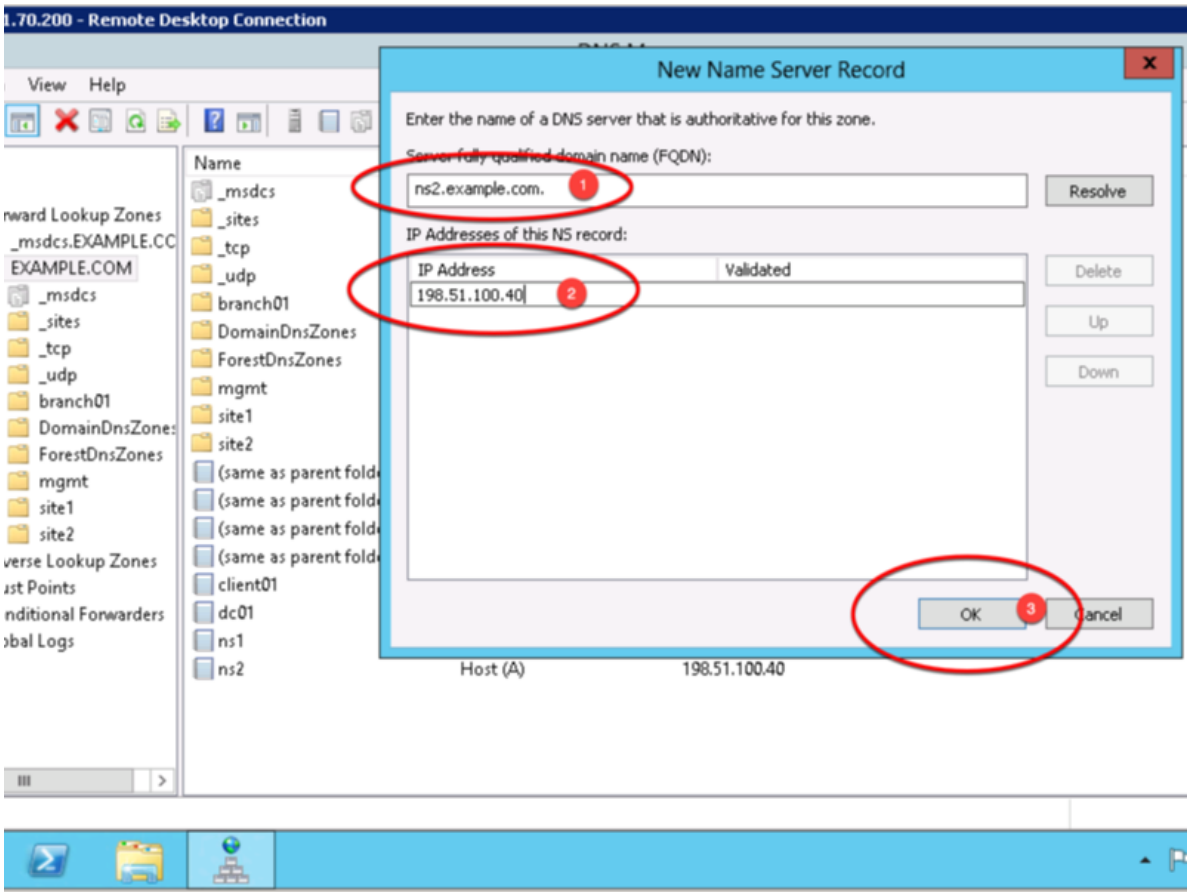

2. Create the “gslb” subdomain.



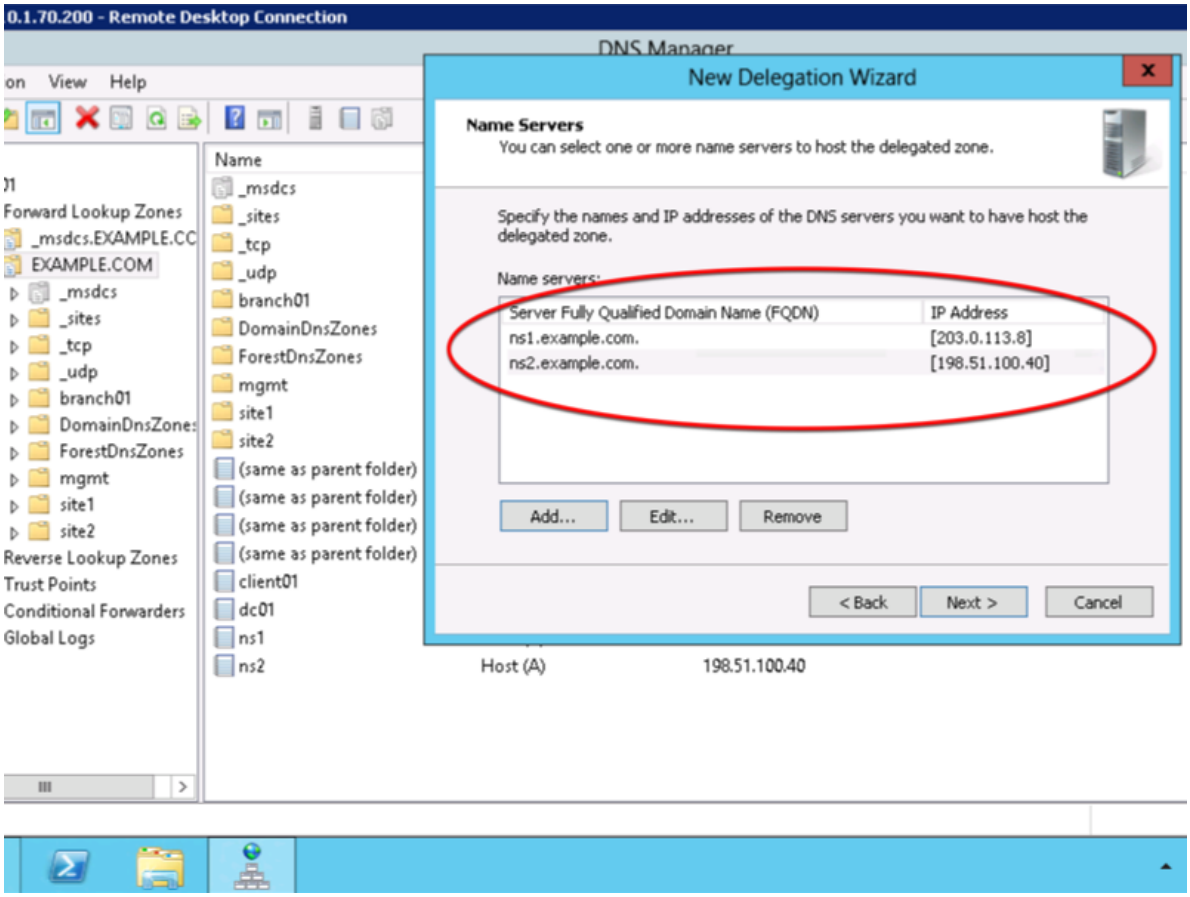

3. Step through the Delegation Wizard. Add “ns1.example.com - 203.0.113.8”



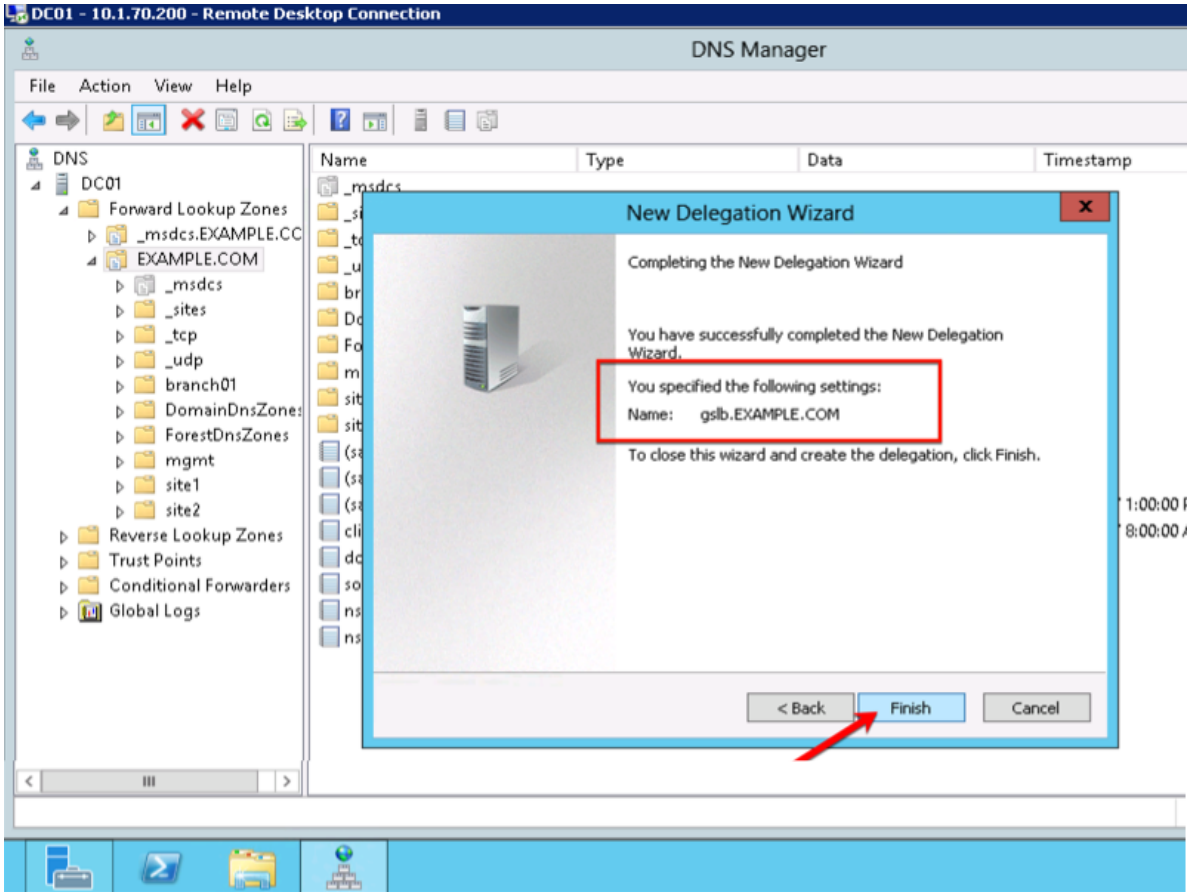

4. Also add “ns2.example.com - 198.51.100.40”




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

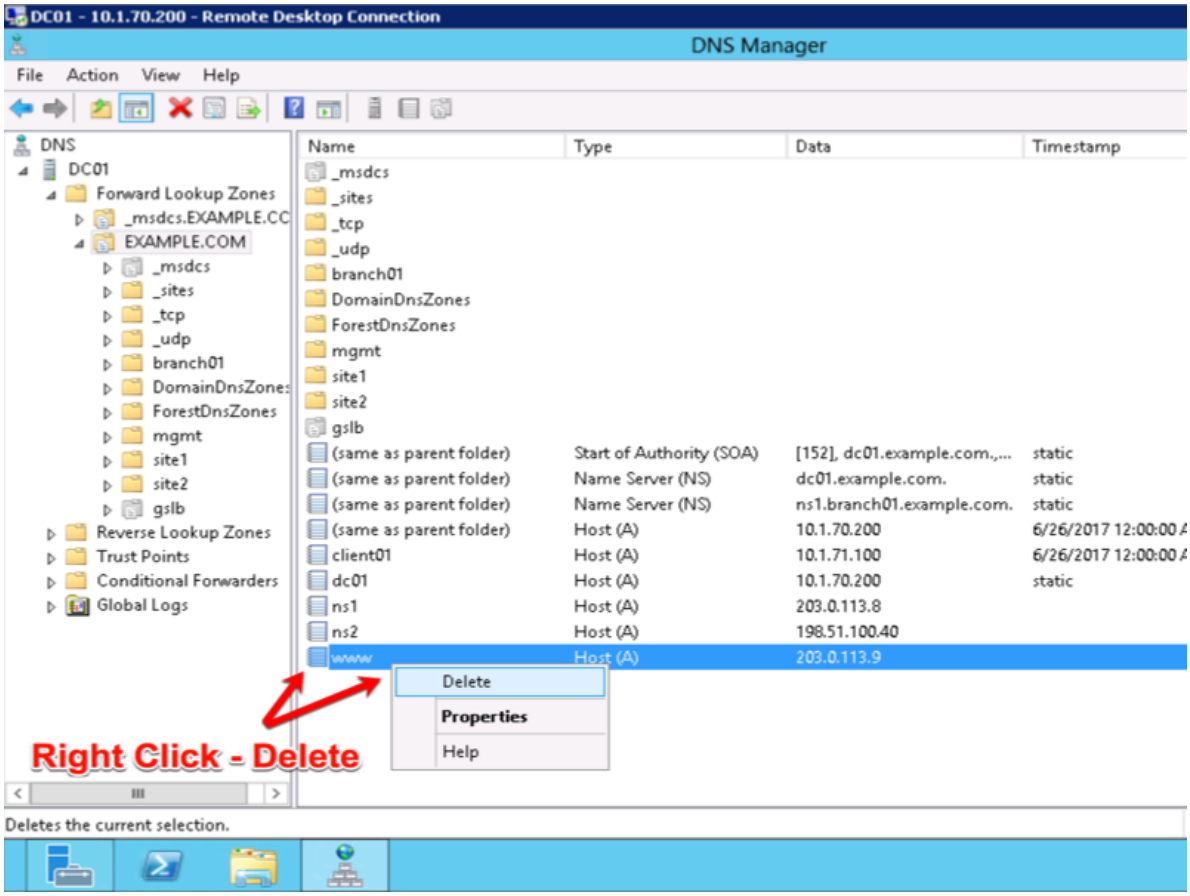



6. Click “Finish”

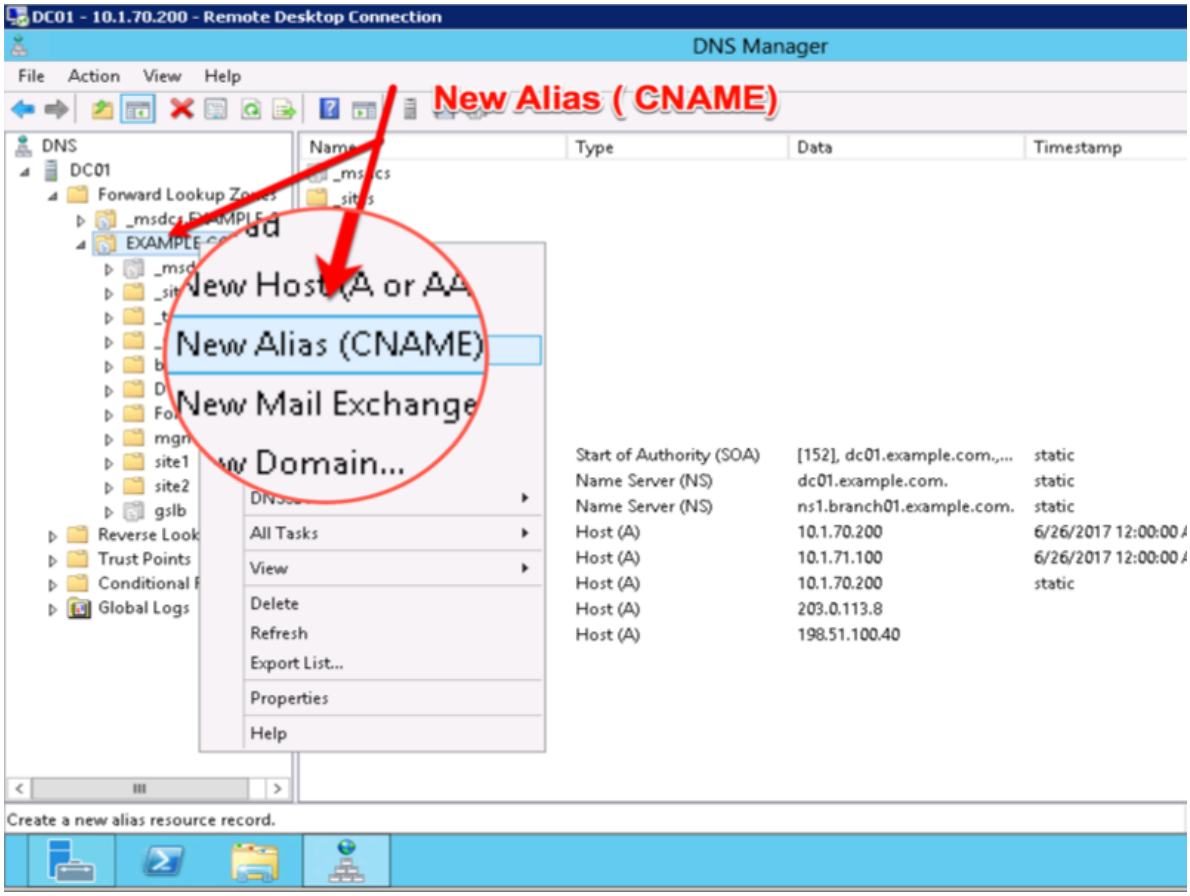



### 2.6.3 CNAME

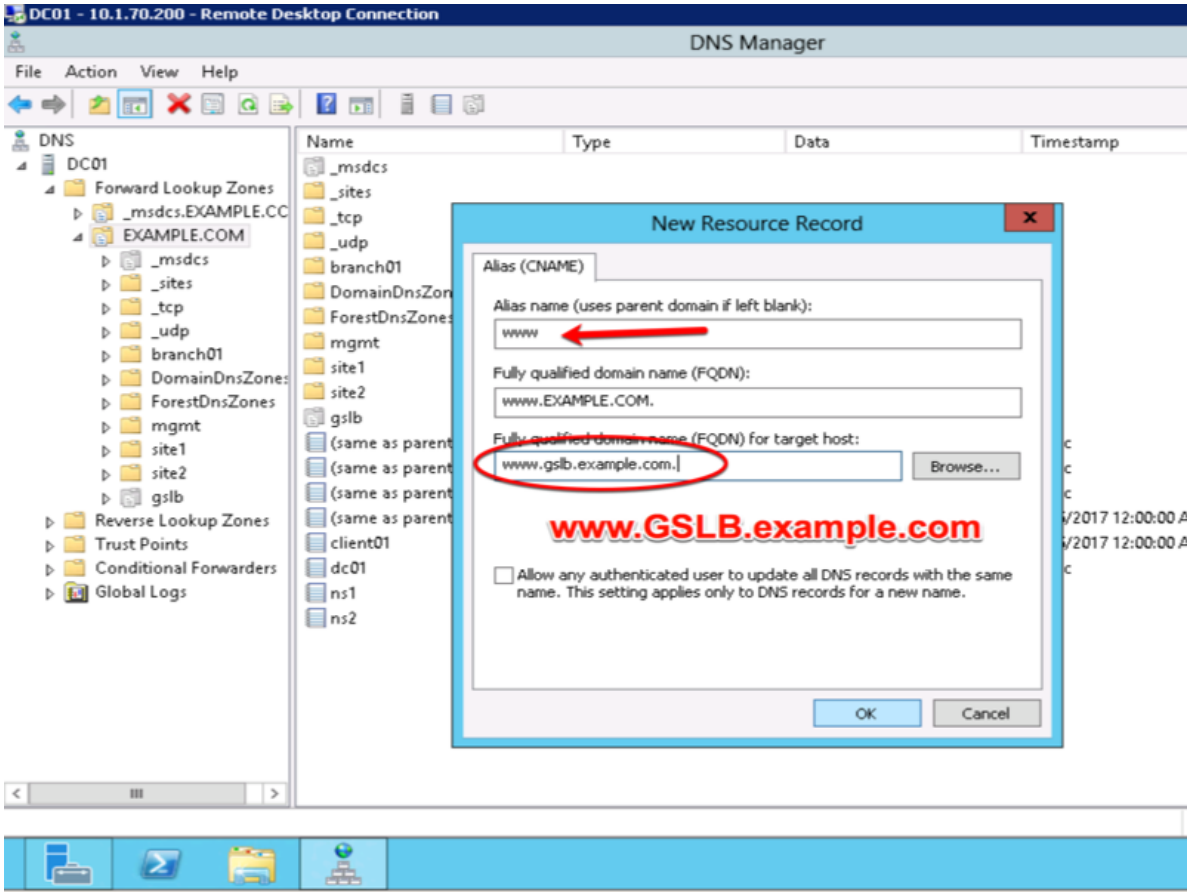
1. Make sure “Forward Lookup Zones” and “EXAMPLE.COM” is expanded. Right click on “www”, and select delete.




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

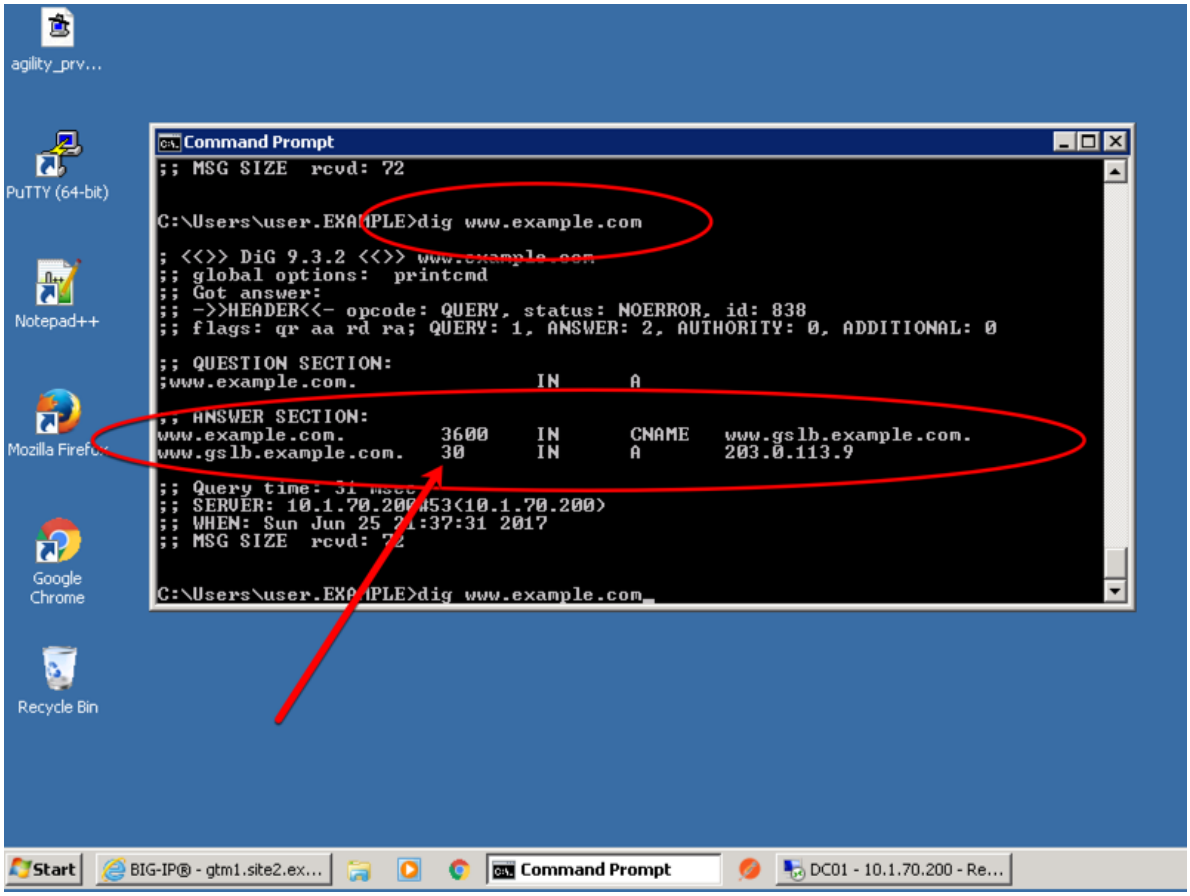



3. Add “www - www.gslb.example.com”



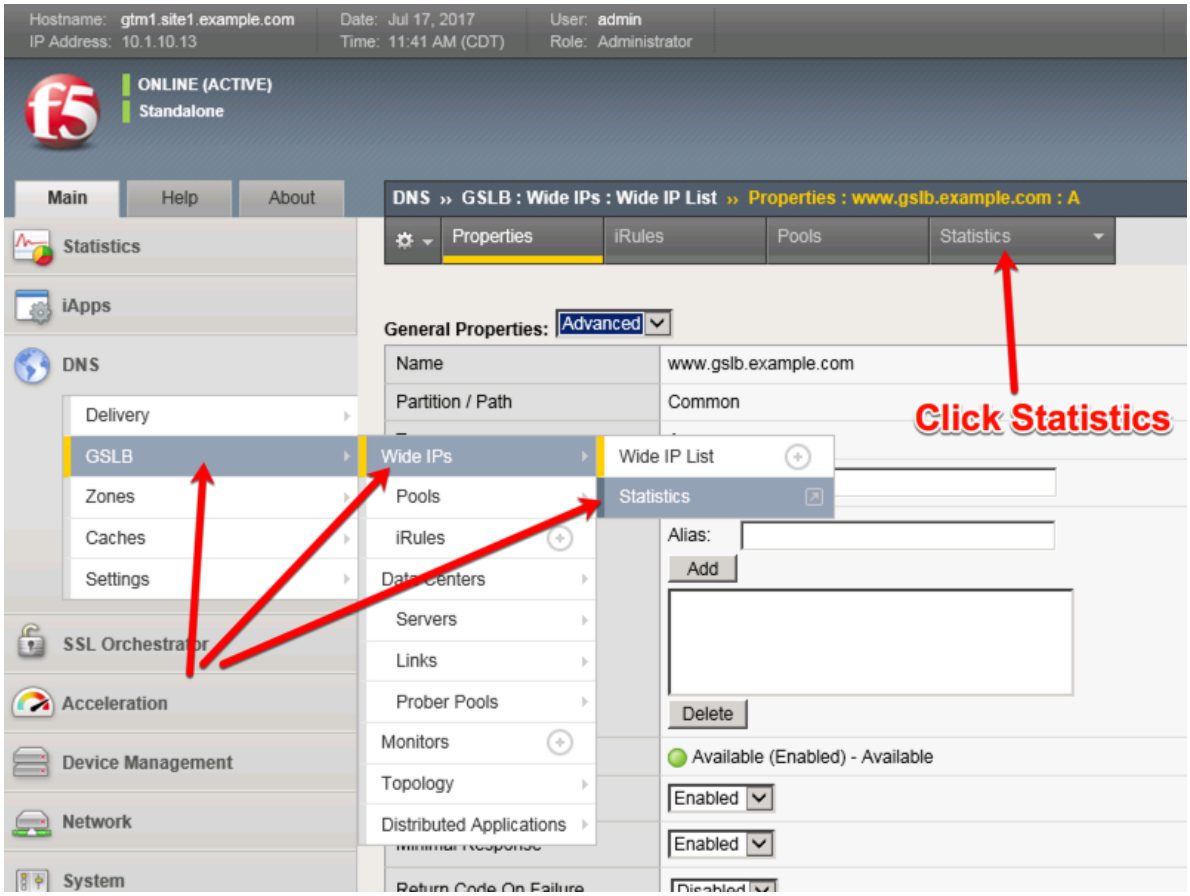

## 2.7 Results

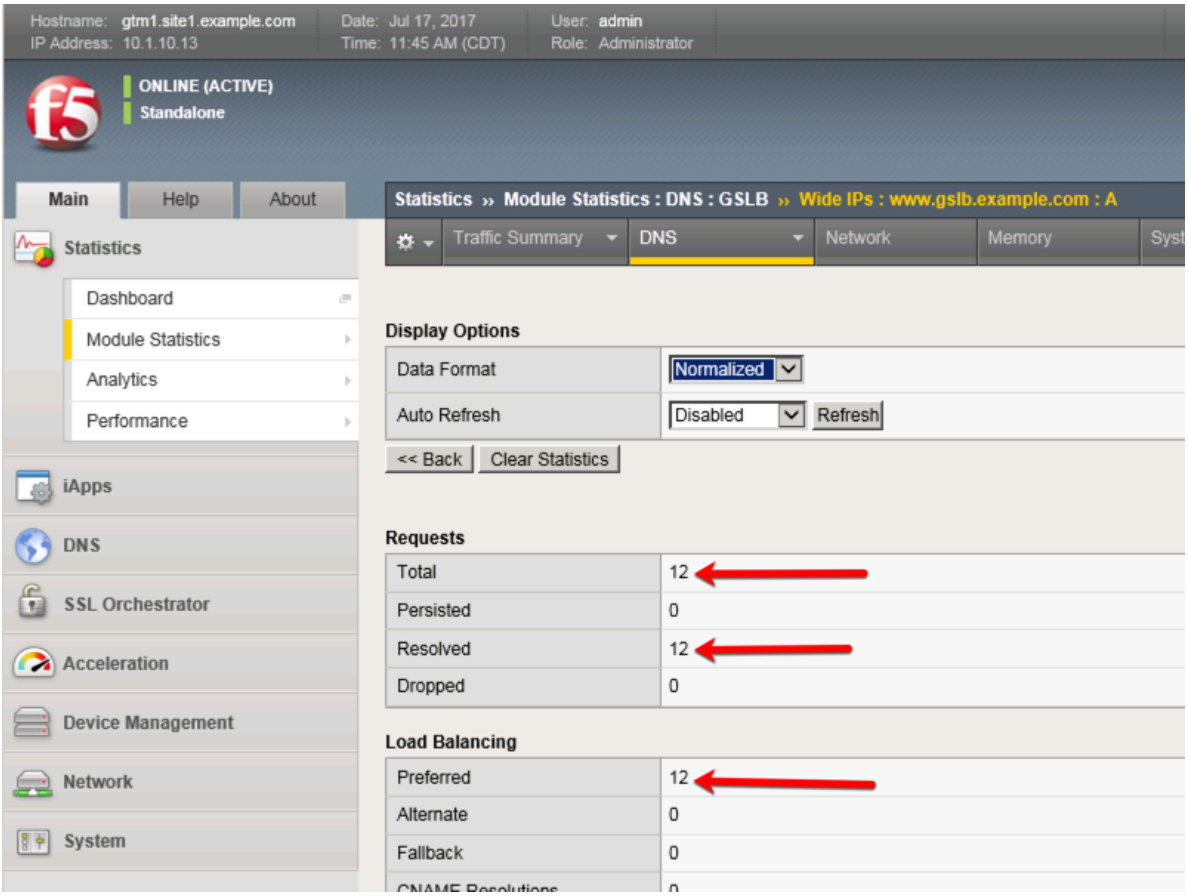
1. From the Workstation command prompt type “dig www.example.com”




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/globallb/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
IP Address: 10.1.10.13
Date: Jul 17, 2017
Time: 11:41 AM (CDT)
User: admin
Role: Administrator
ONLINE (ACTIVE)
Standalone
Main
Help
About
DNS » GSLB : Wide IPs : Wide IP List » Properties : www.gslb.example.com : A
Properties
iRules
Pools
Statistics
Statistics
iApps
DNS
Delivery
GSLB
Zones
Caches
Settings
SSL Orchestrator
Acceleration
Device Management
Network
System
Wide IPs
Pools
iRules
Data Centers
Servers
Links
Prober Pools
Monitors
Topology
Distributed Applications
Wide IP List
Statistics
General Properties:
Advanced
Name
www.gslb.example.com
Partition / Path
Common
Alias:
Add
Delete
Available (Enabled) - Available
Enabled
Enabled
Click Statistics




**TMSH**

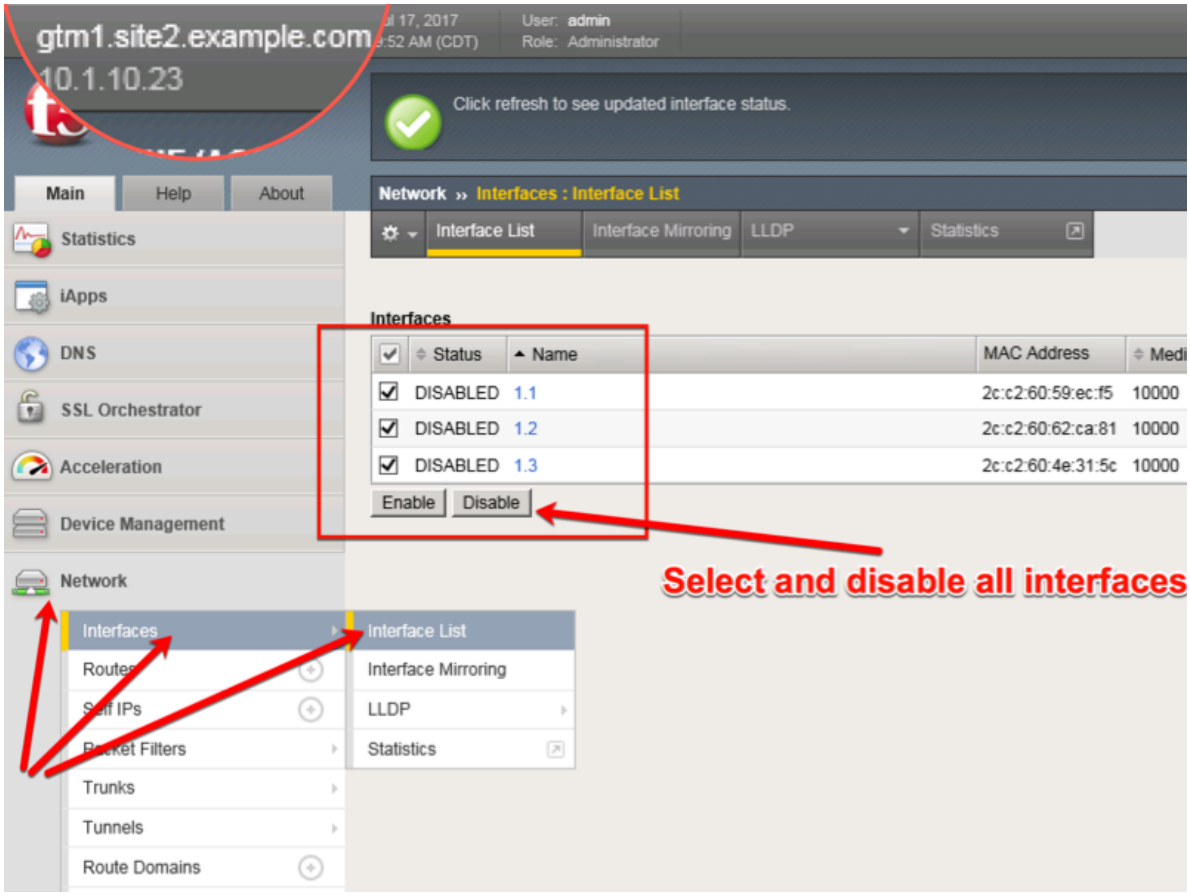
tmsh show gtm wideip a www.gslb.example.com

3. 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/globallb/stats/wideip/stats_detail.jsp?name=%2FCommon%2Fwww.gslb.example.com&type=1&identity=www.gslb.example.com+%3A+A

4. 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




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/globallb/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.

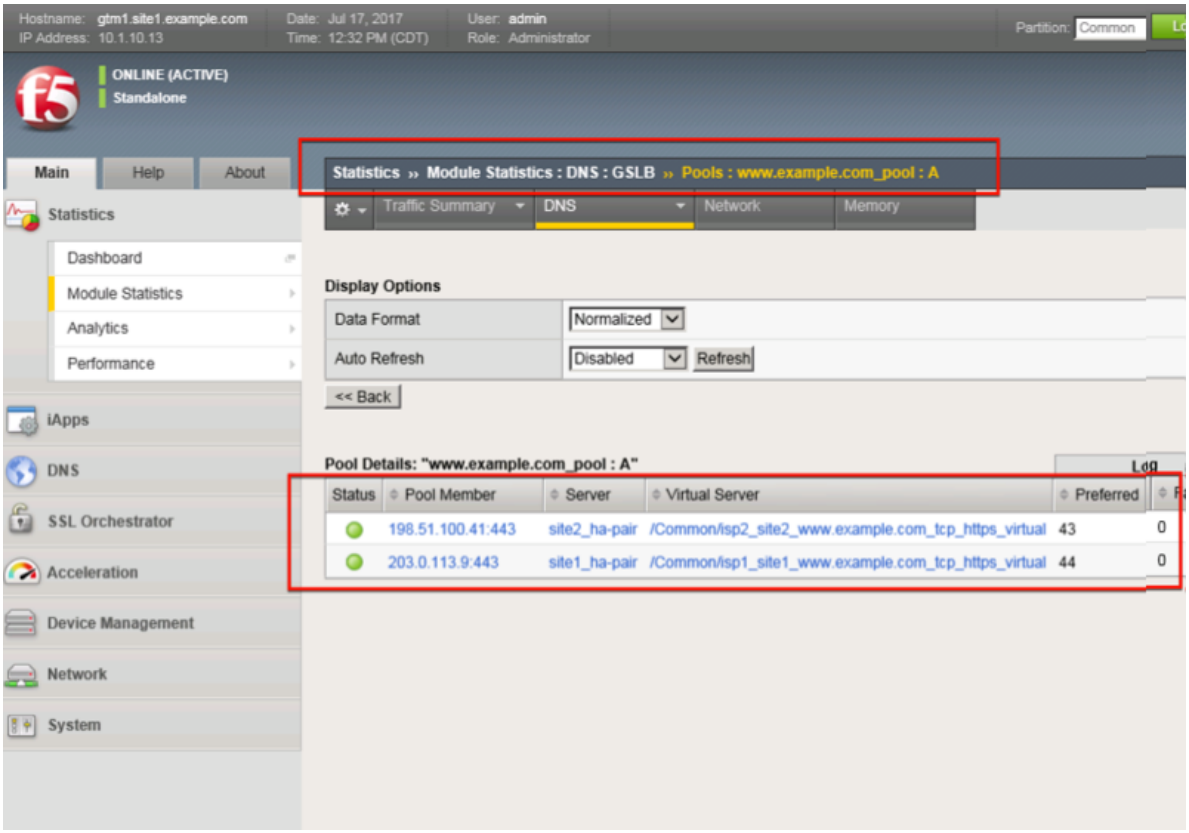
   TMSH command to run on only gtm1.site2:

   **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/globallb/stats/pool/stats_detail.jsp?name=%2FCommon%2Fwww.example.com_pool&pool_type=1&identity=www.example.com_pool+%3A+A




**TMSH**

show gtm pool a www.example.com_pool

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

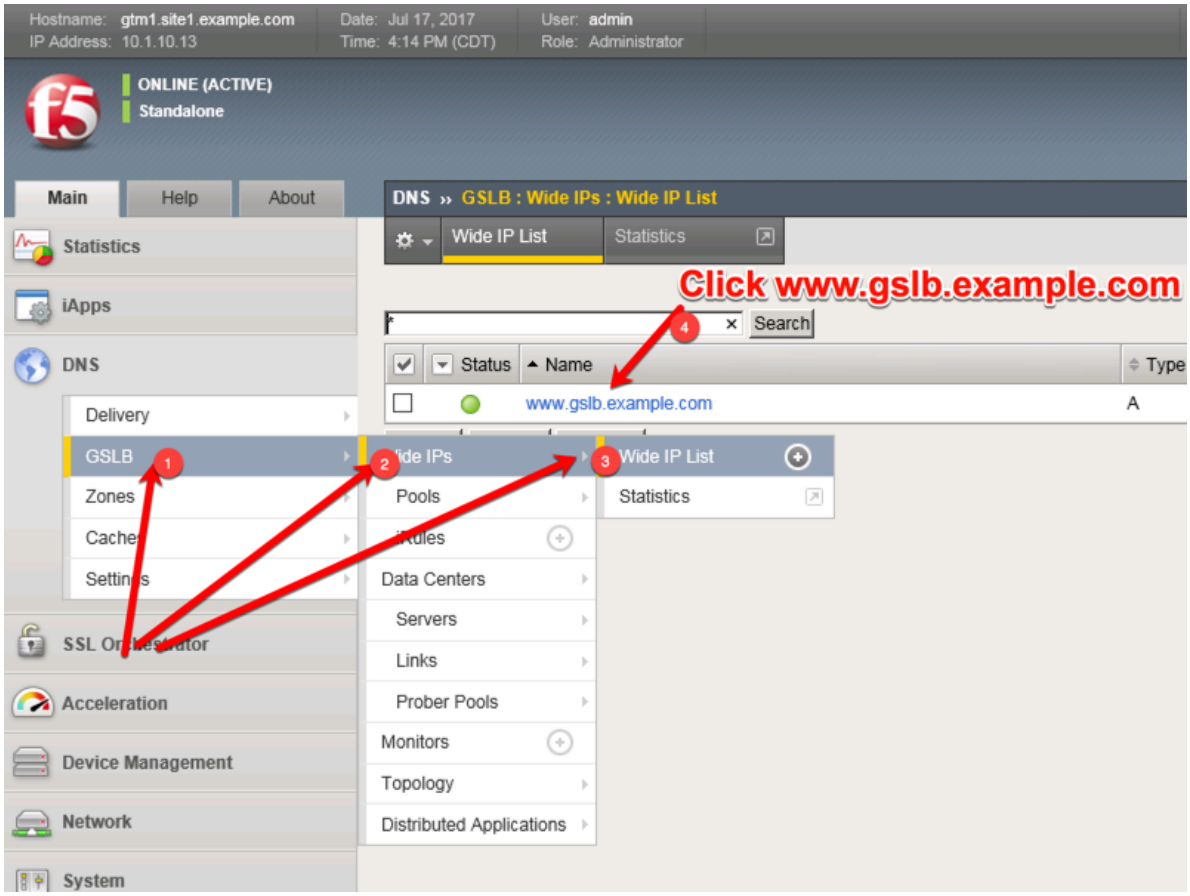
**TMSH**

tail -f /var/log/ltm

## 2.8 Persistence

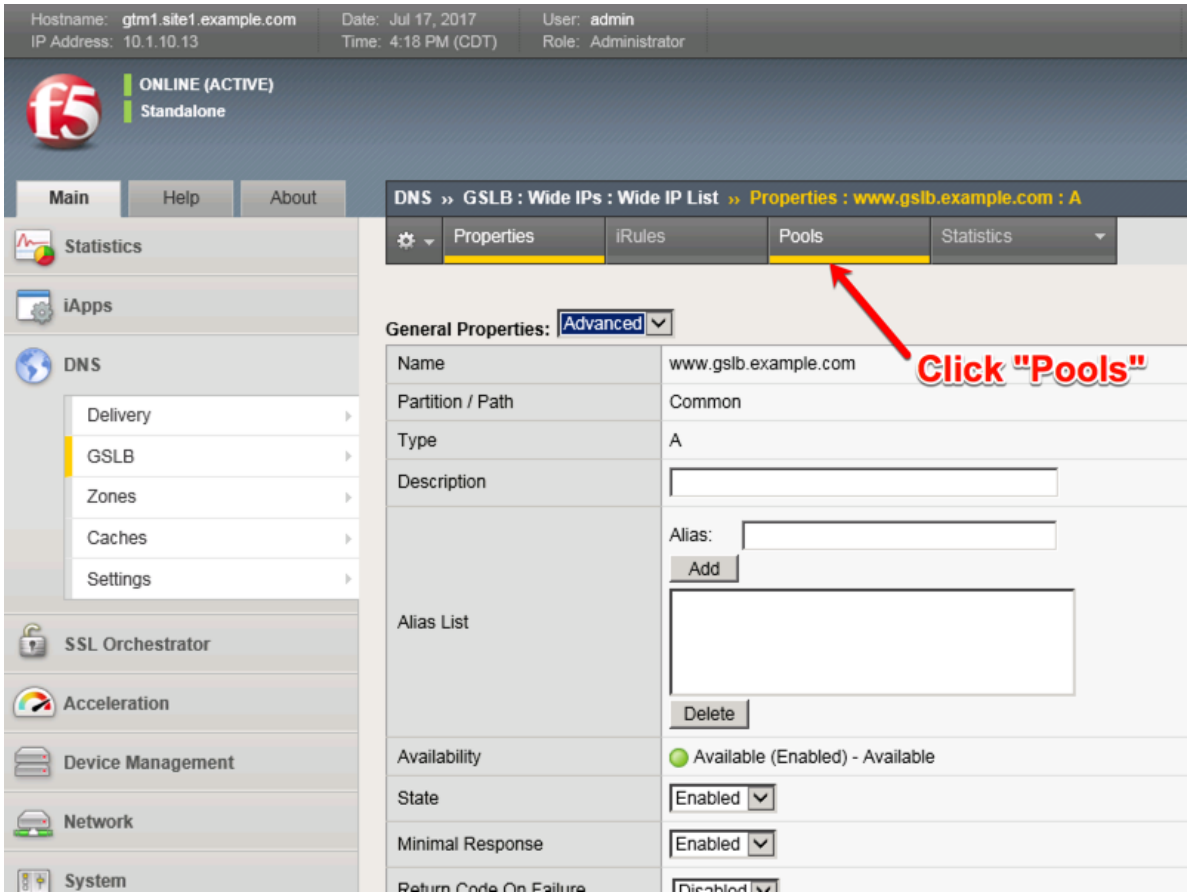
Modify the GSLB configuration so that LDNS servers continually receive the same DNS answer.

1. On gtm1.site1 navigate to: **DNS ›› GSLB : Pools : Pool List ›› Members : www.example.com_pool**



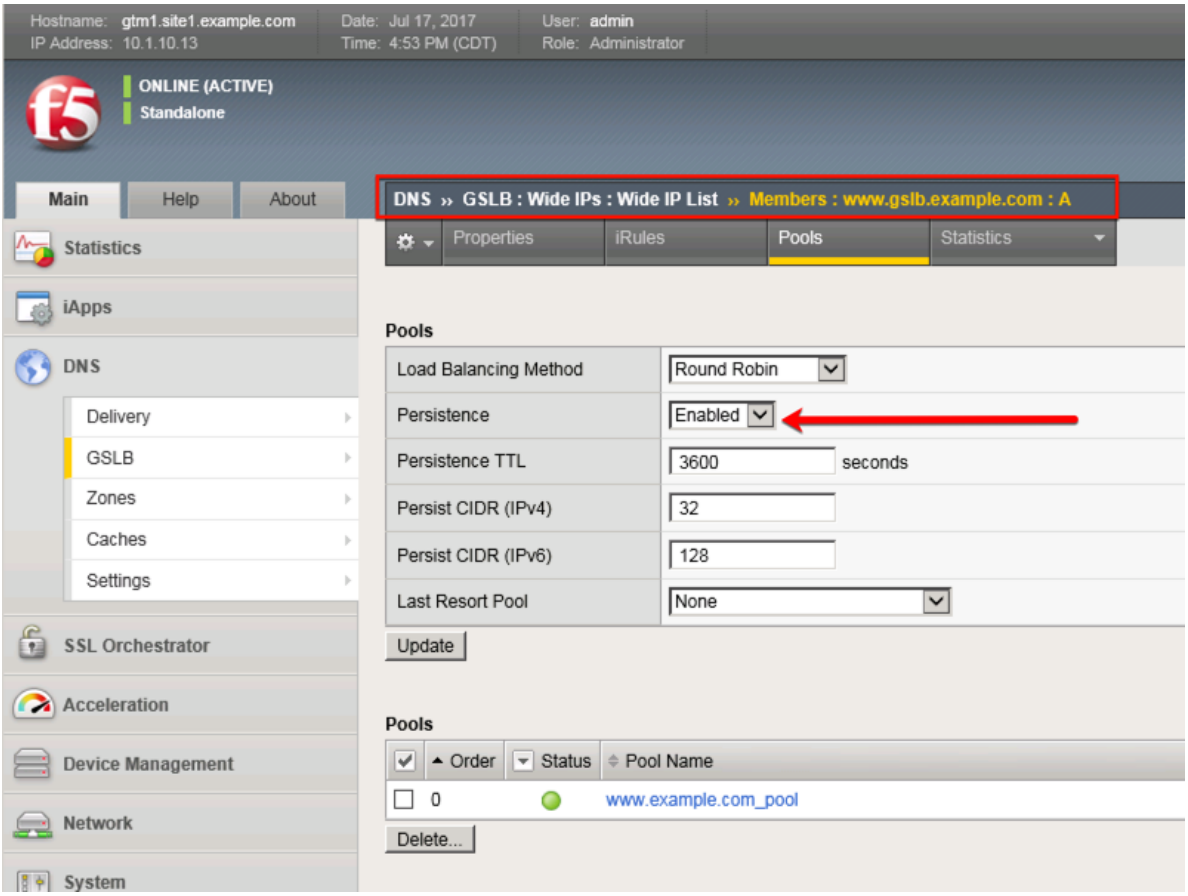

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/wideip/list.jsp

2. Click into the “Pools” tab:




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

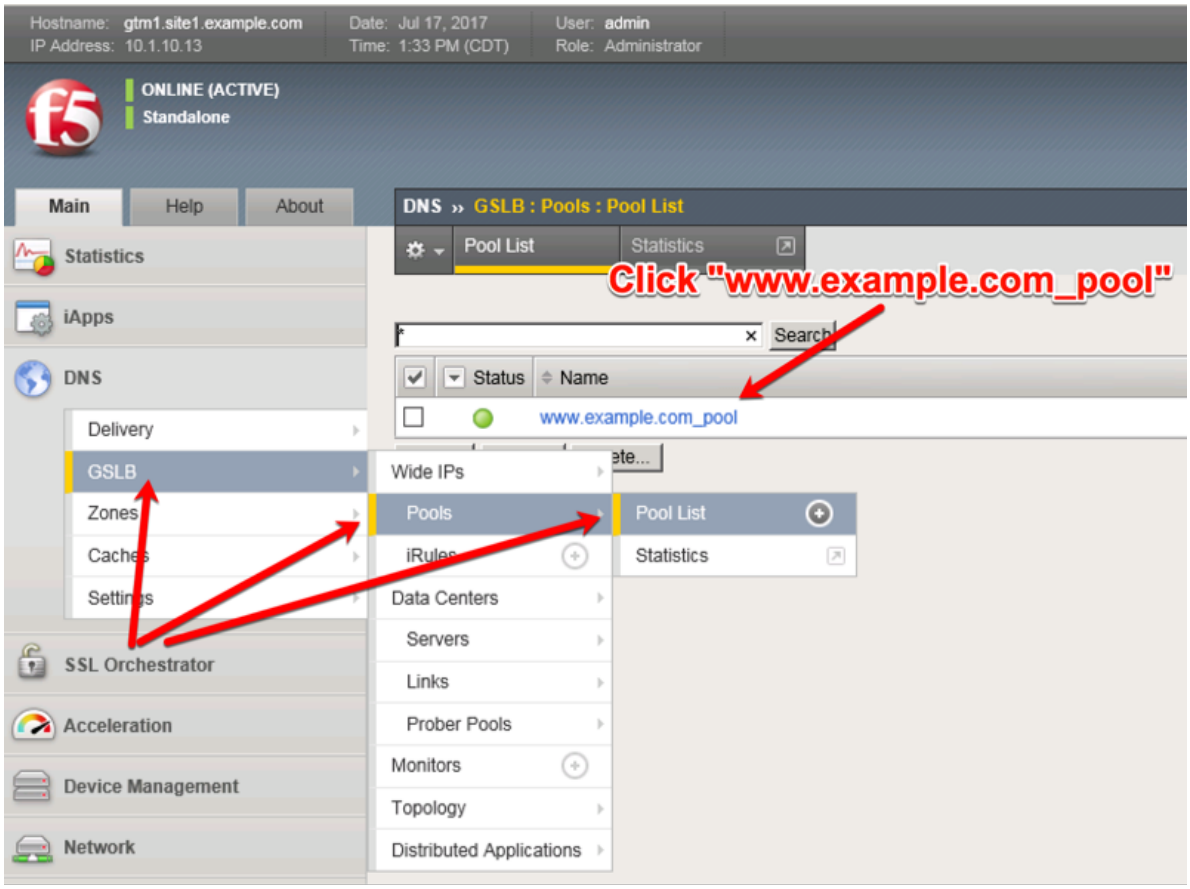
Modify the GSLB configuration so that site2 is a standby DR site.

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

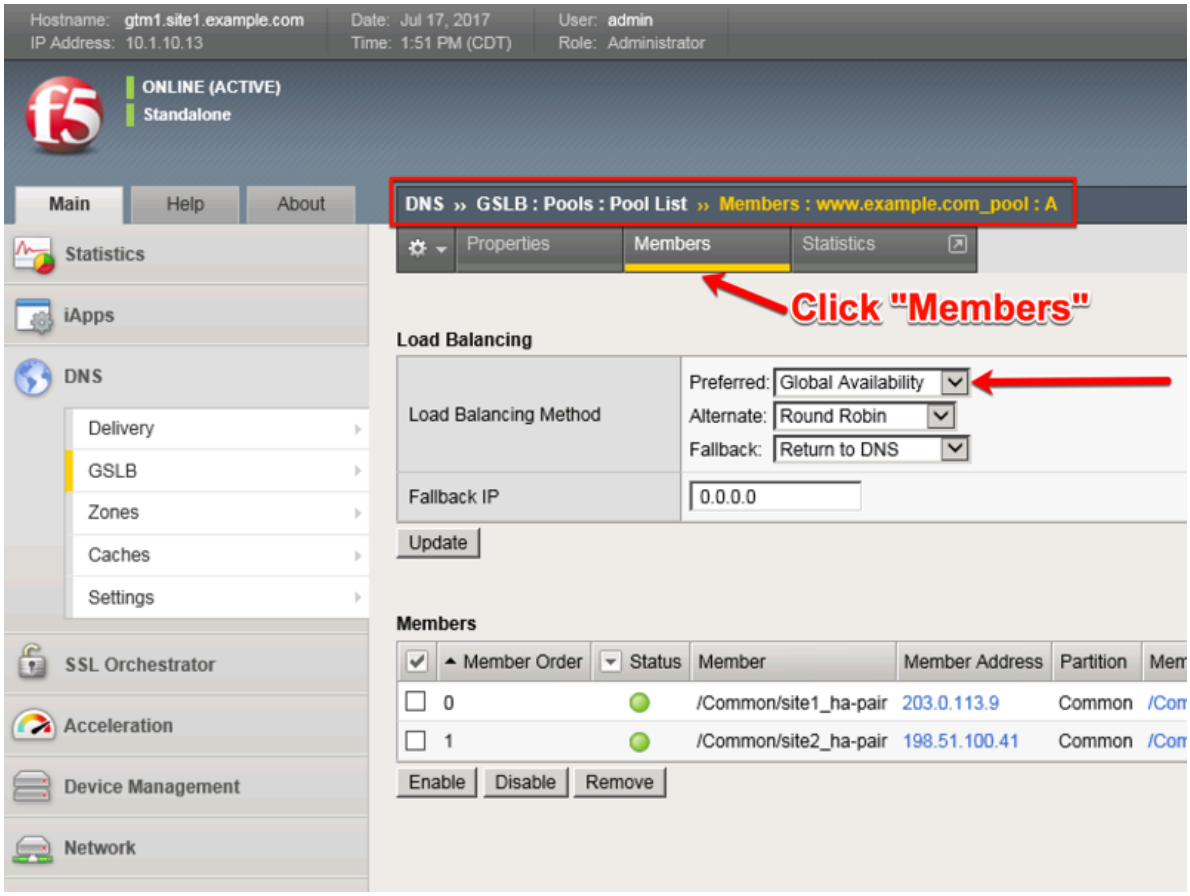
An ISP network outage can automatically cause DR activation.

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/globallb/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”



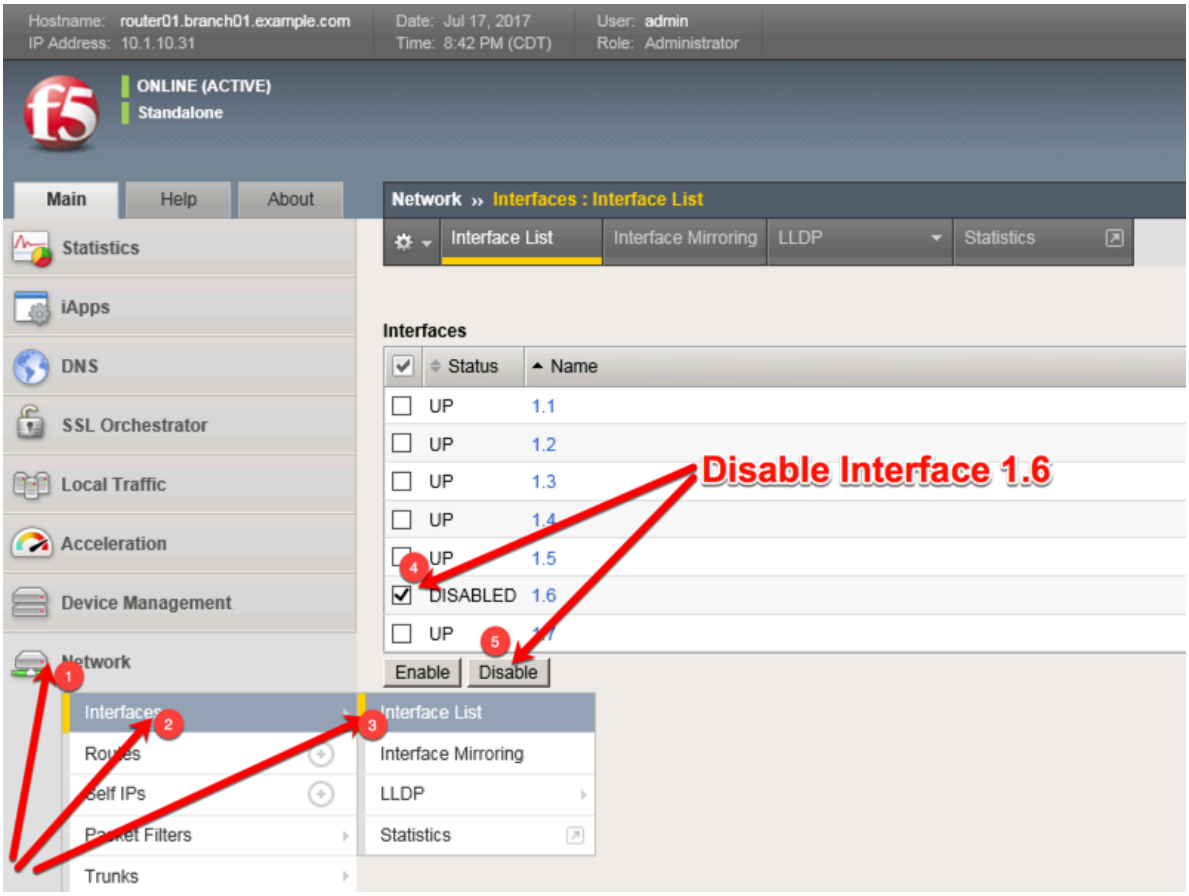

**TMSH**

tmsh modify gtm pool a www.example.com_pool load-balancing-mode global-availability

3. 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/locallb/network/interface/list.jsp



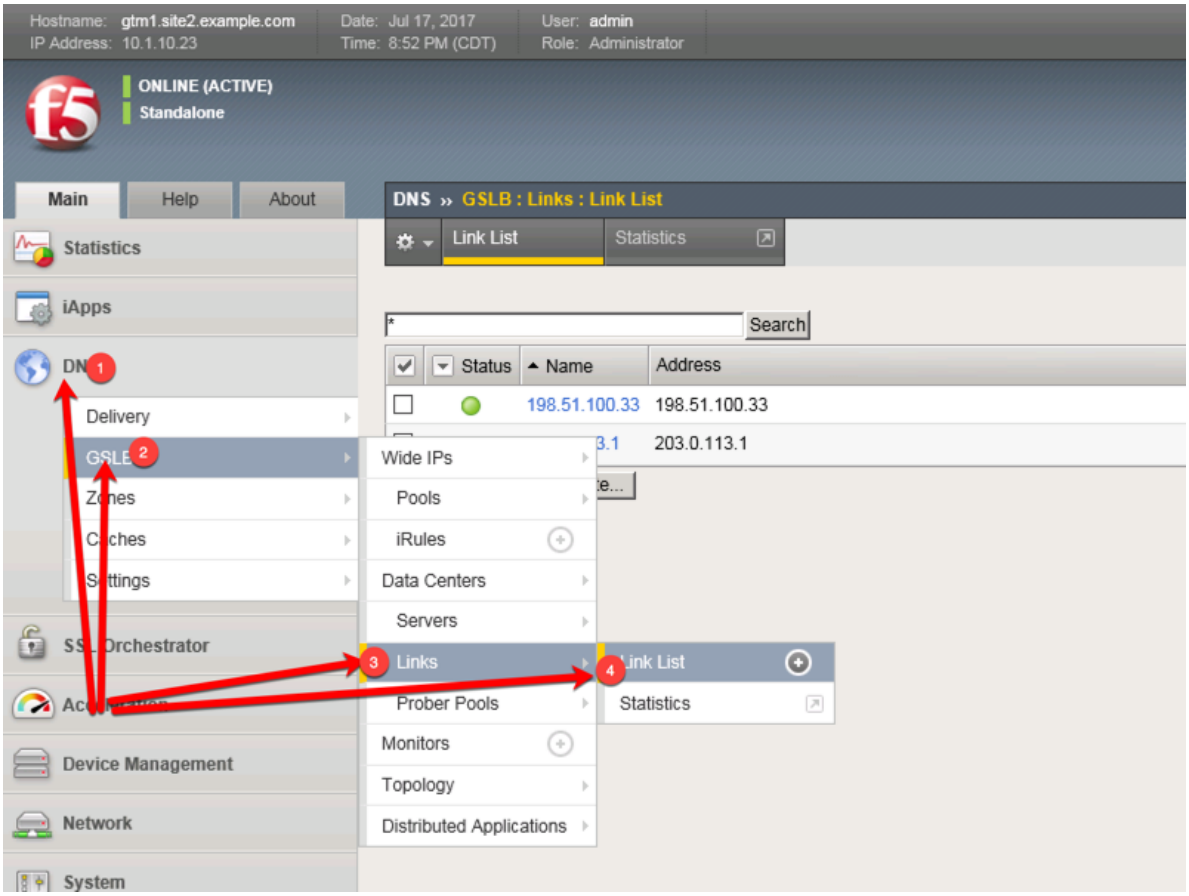

TMSH command to run on the router01 to simulate an ISP failure

**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

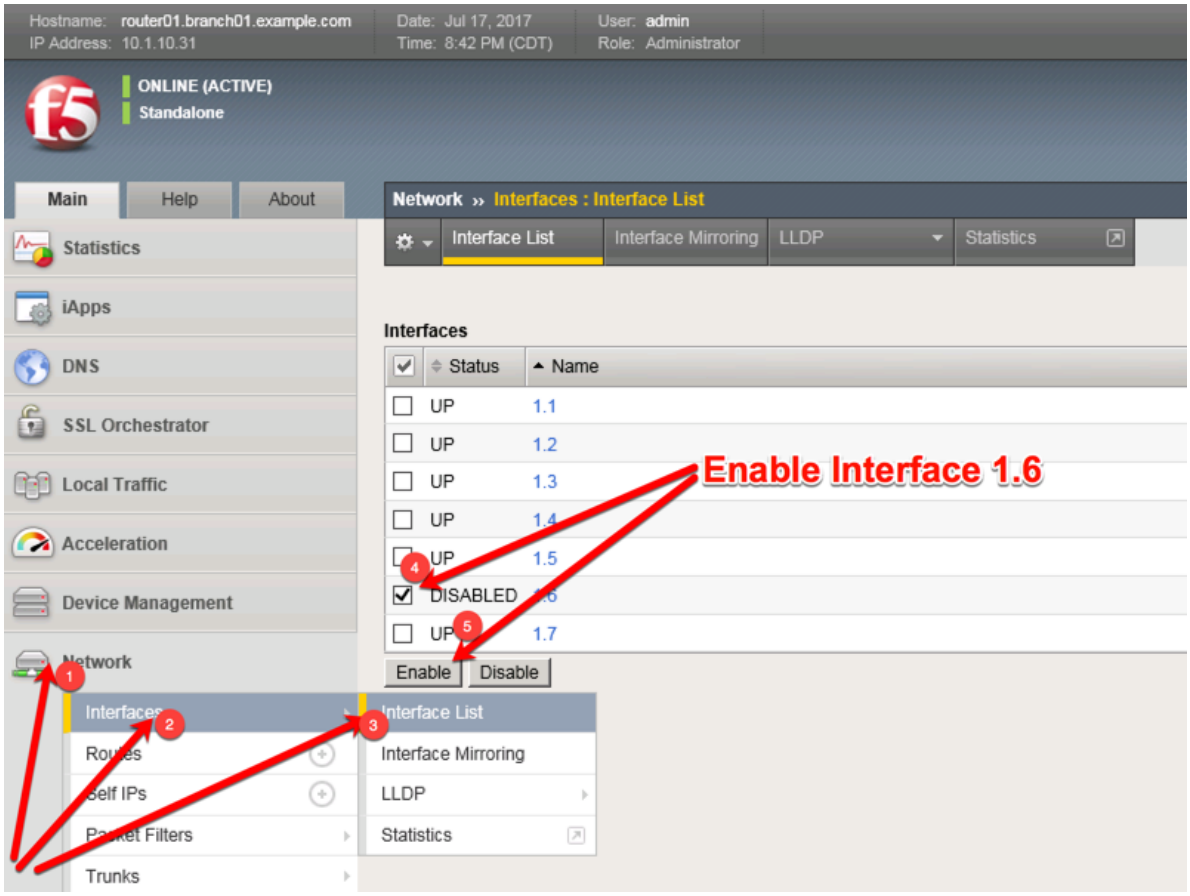
**TMSH**

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

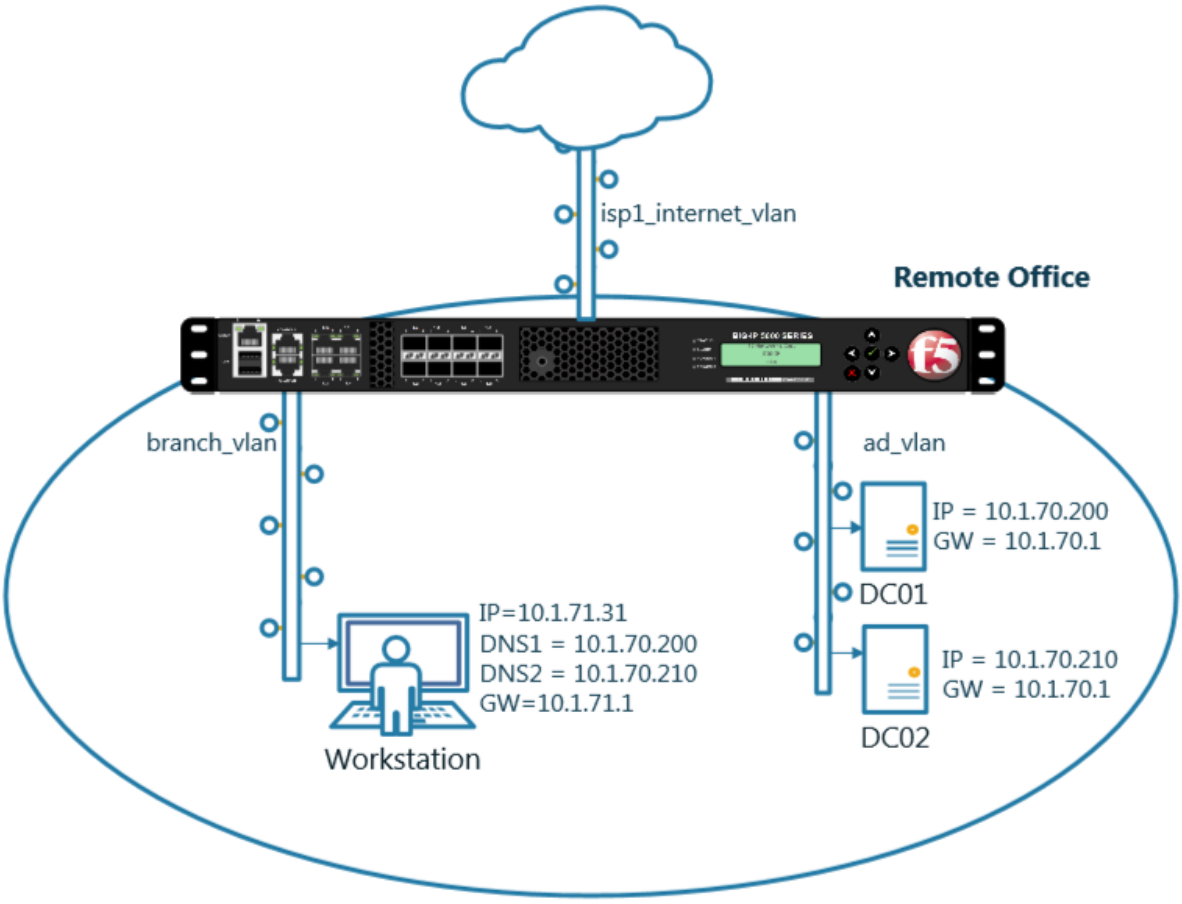
Note: Even though you re-enabled the primary site1, a persistence record from the previous lab is still in place.

# 3

# Class 2 - Security

The lab environment consists of a Lan of workstations in a remote location with internal DNS servers behind an F5 firewall.

The F5 device is directly connected to the internet.




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

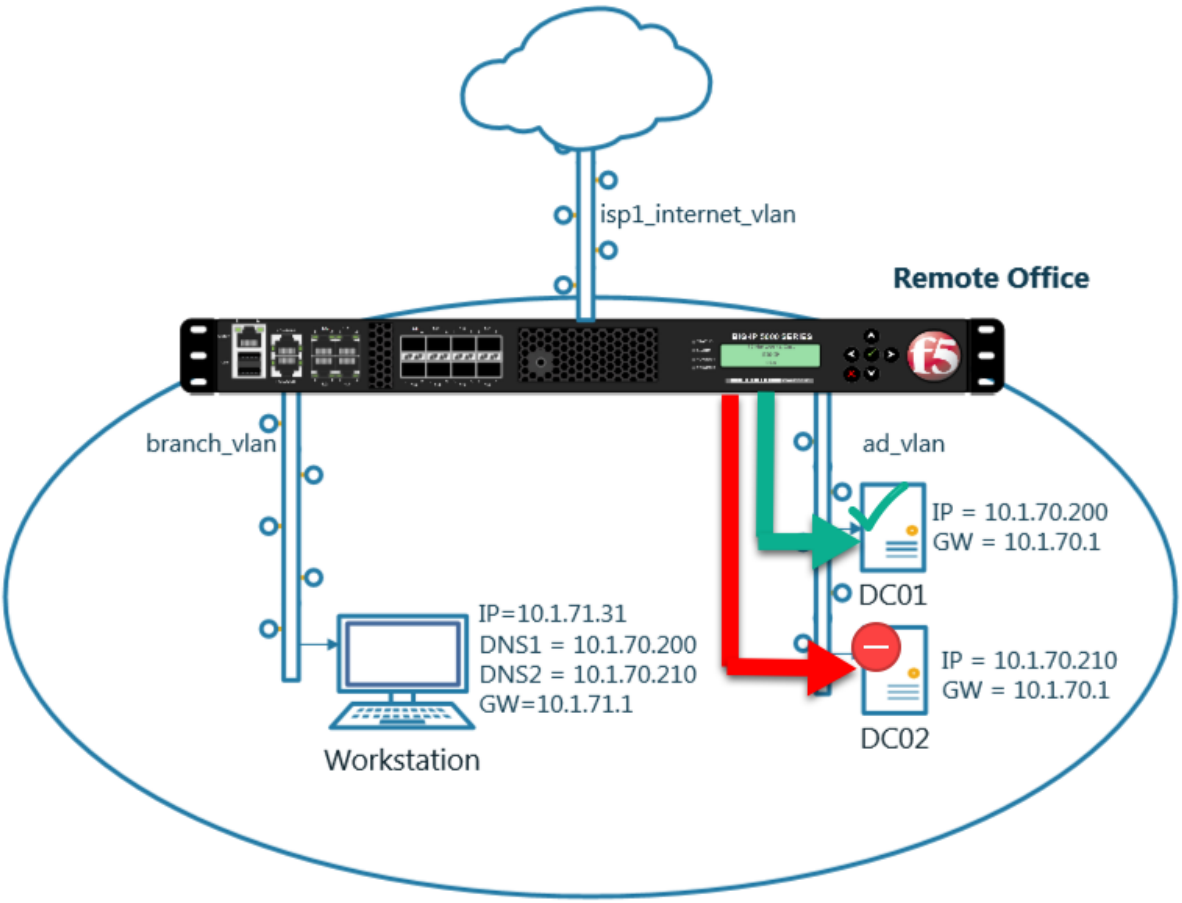
1. Transparent Cache

2. Hidden Master
3. DNSSec
4. Validating Resolver
5. RPZ
6. URL Categorization

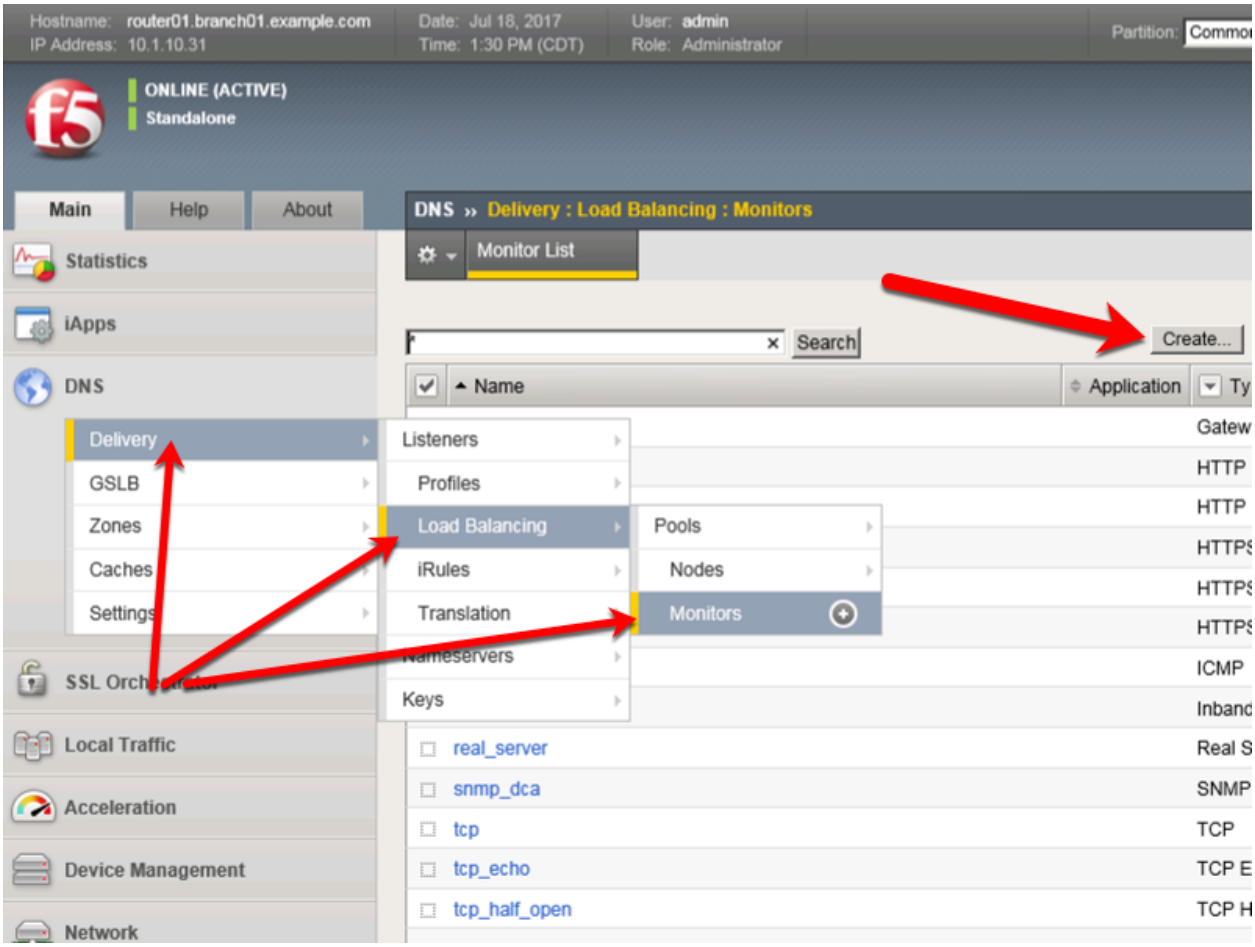
## 3.1 Transparent Cache

### 3.1.1 Monitors

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



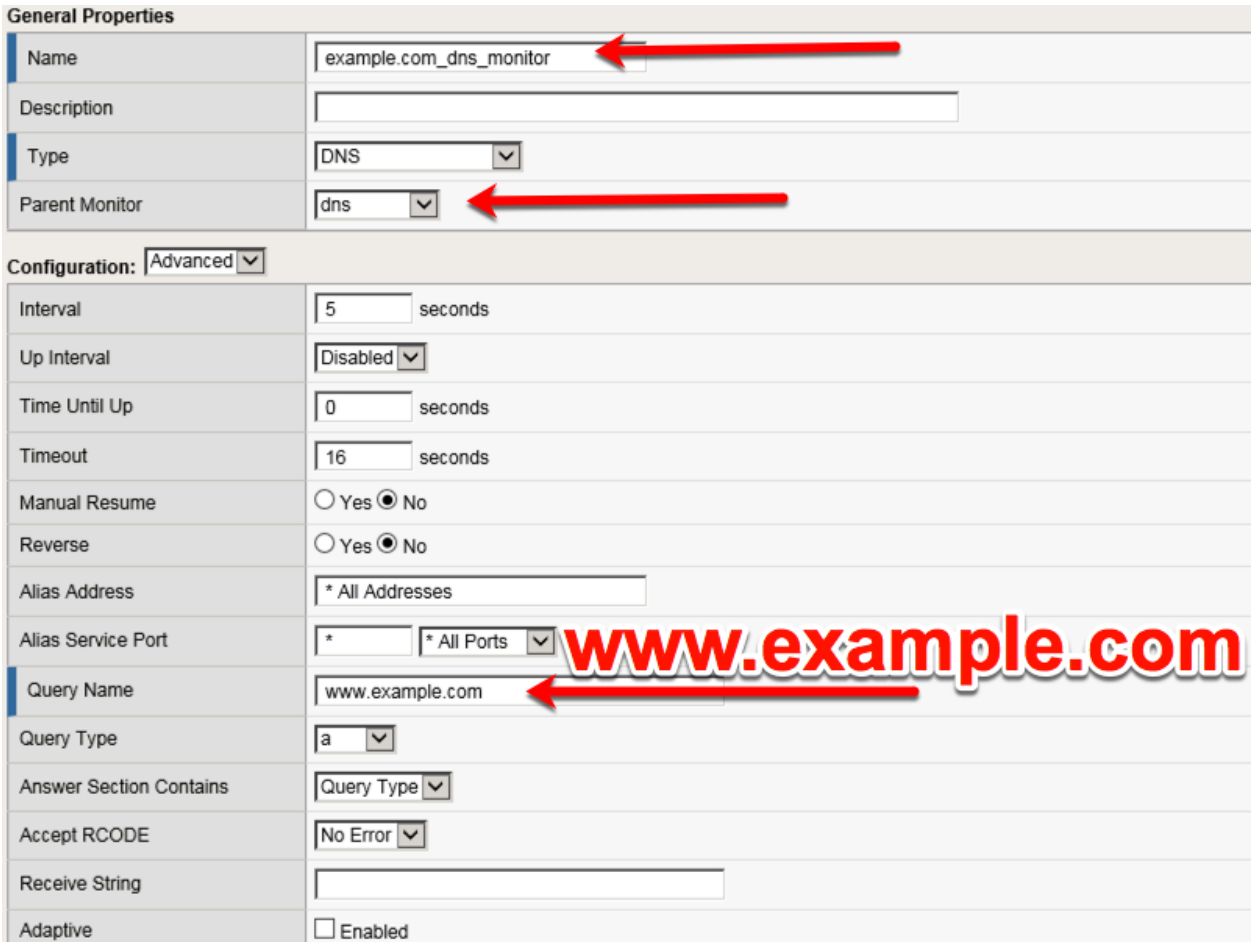

Navigate to: **Delivery : Load Balancing : Monitors**




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

Create a monitor according to the following table:

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




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

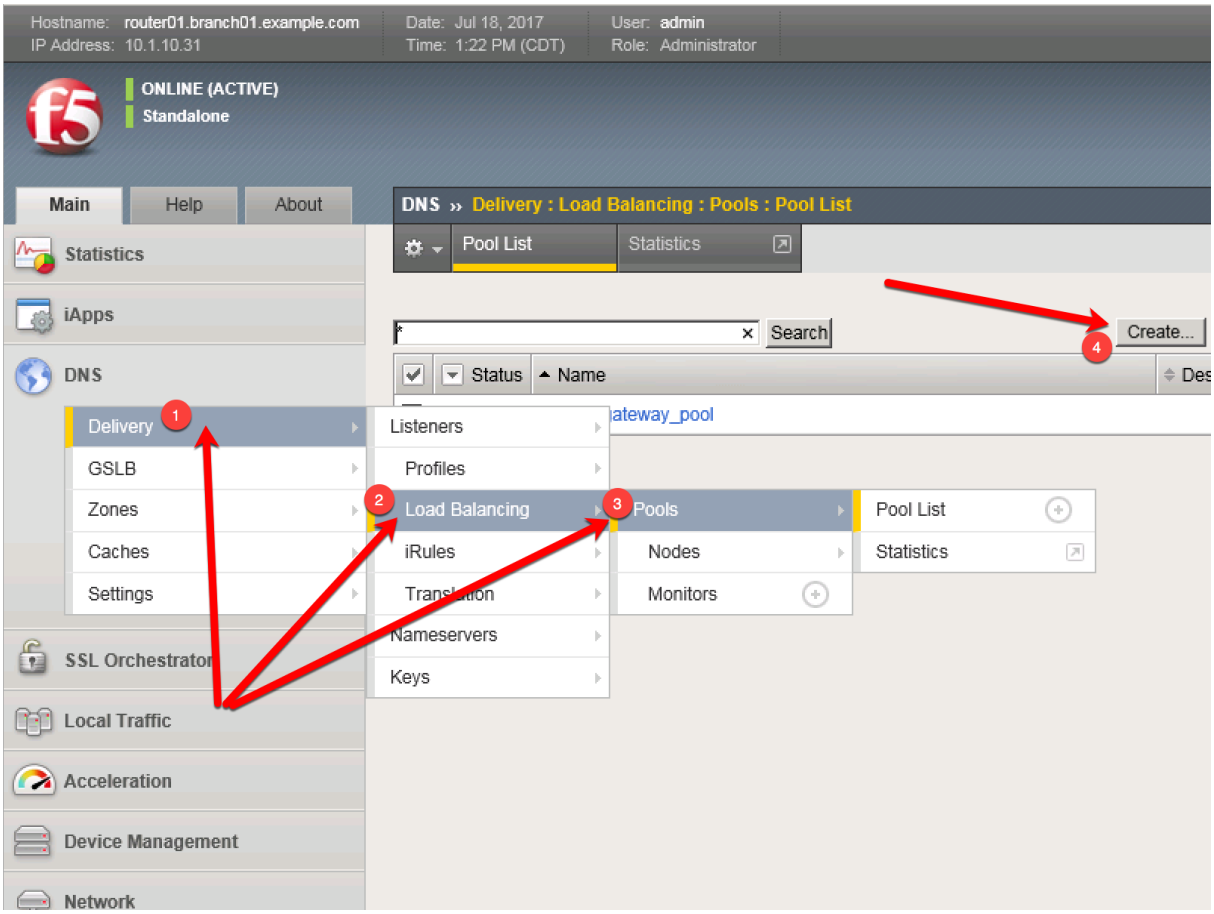
**TMSH**

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

### 3.1.2 Load Balancing

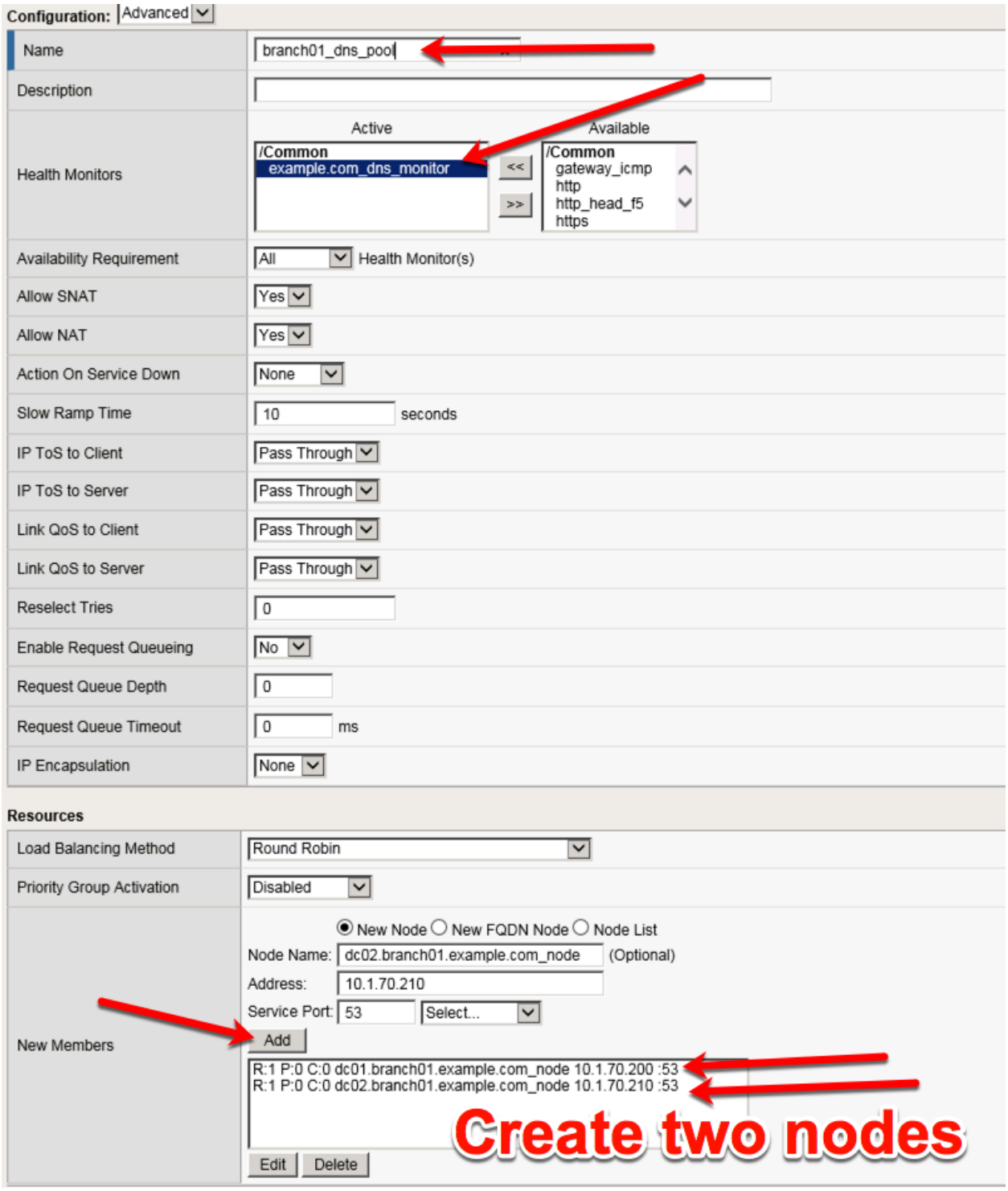
Augment and scale an existing DNS infrastructure by Load Balancing DNS queries across a pool of DNS servers.

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




Create a pool according to the following table:

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




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

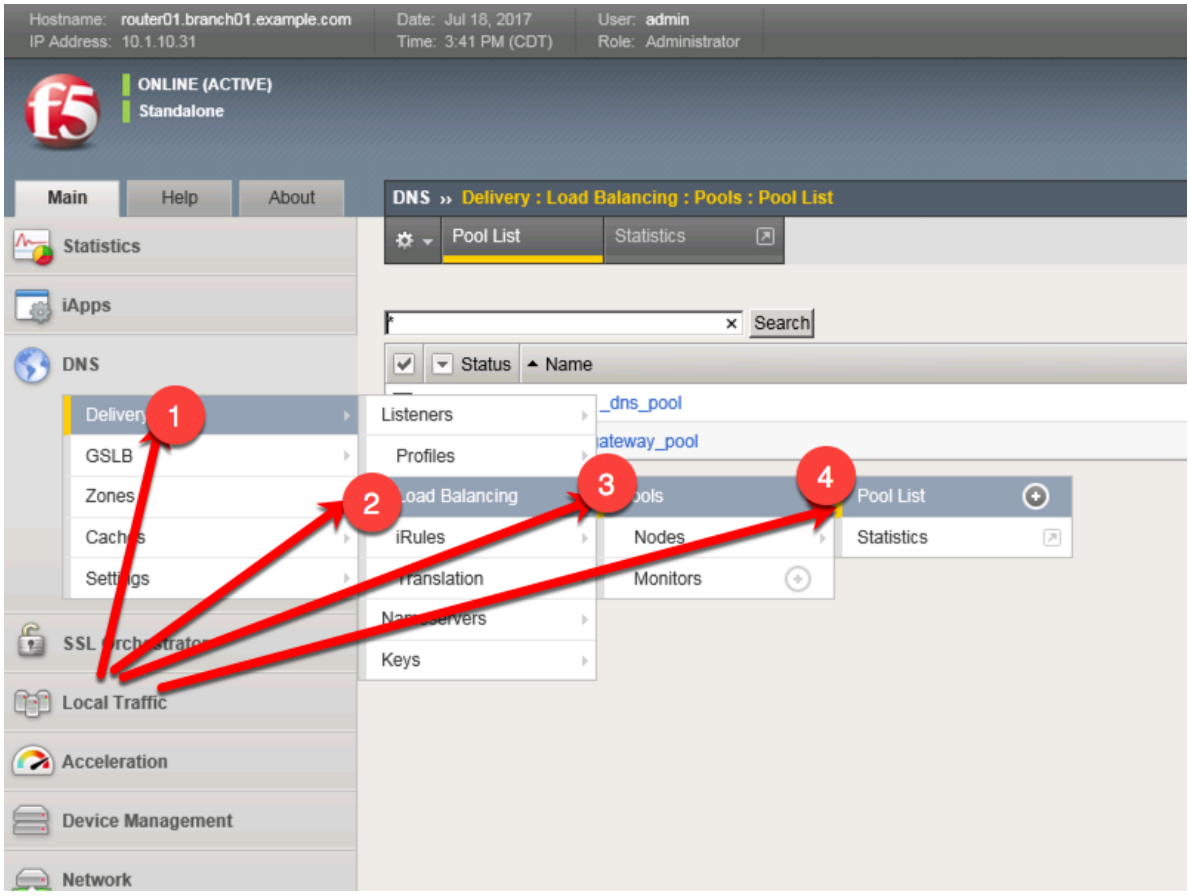
**TMSH**

tmsh create ltm pool branch01_dns_pool members add { dc01.branch01.example.com_node:53 { address 10.1.70.200 } dc02.branch01.example.com_node:53 { address 10.1.70.210 } } monitor exam-

### 3.1.3 Results

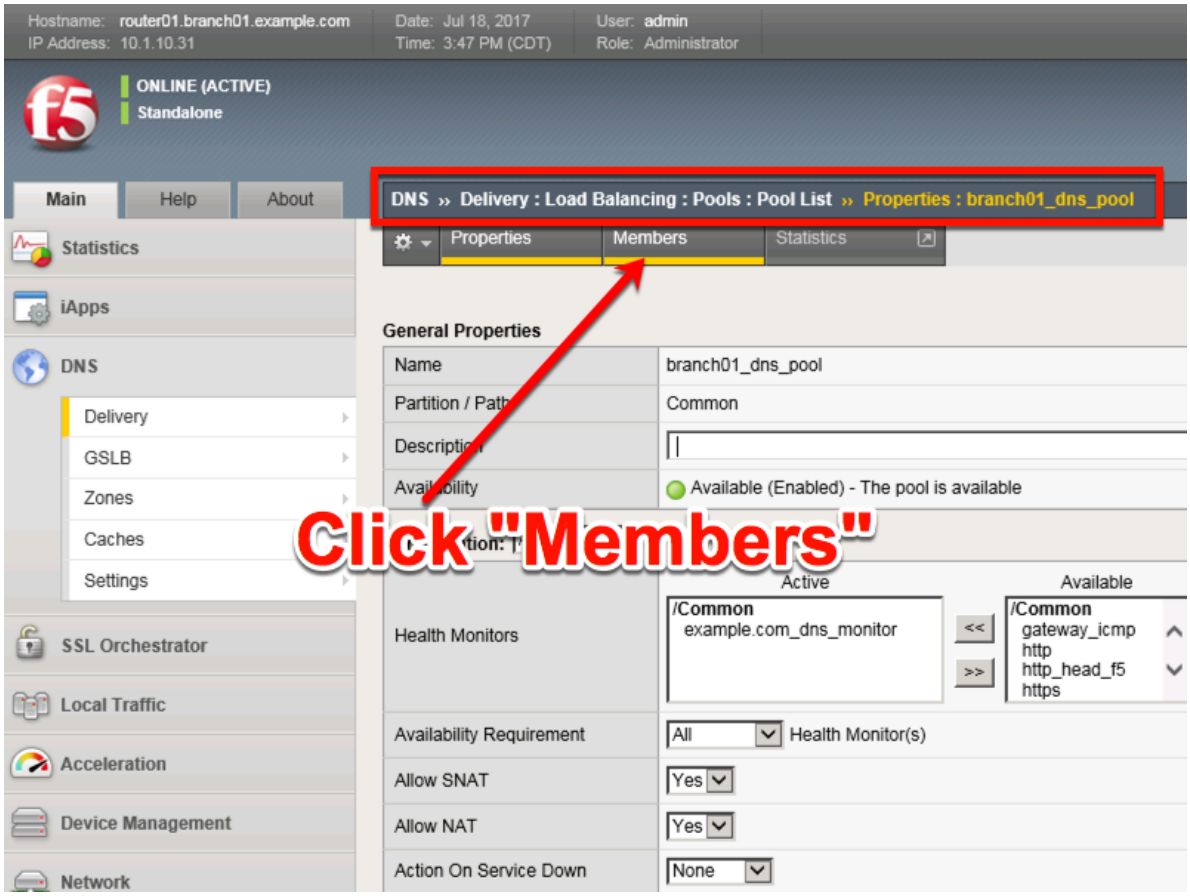
1. Navigate to: **DNS ›› Delivery : Load Balancing : Pools : Pool List**

   Click to select the branch01_dns_pool, and then click “Members”



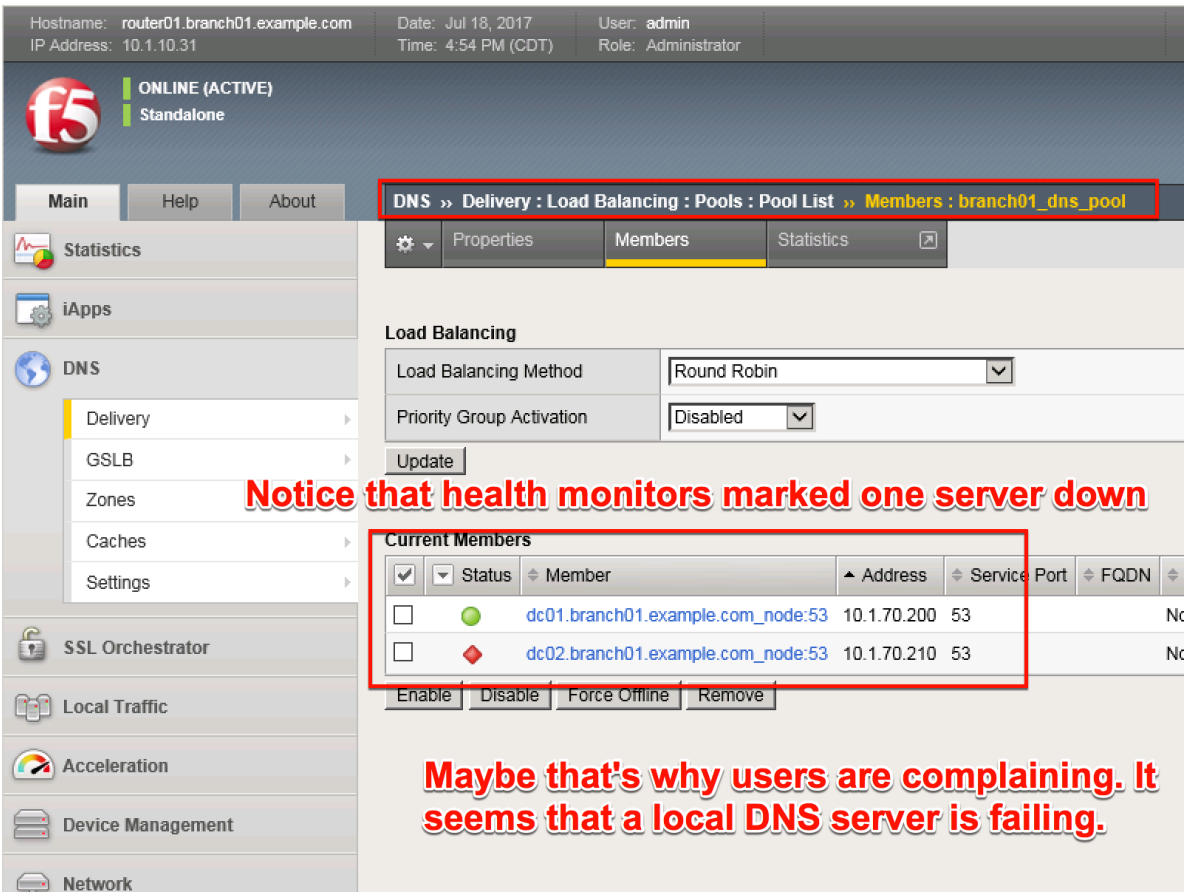

   https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/pool/list.jsp

2. Click to select “branch01_dns_pool”, and then select “Members”



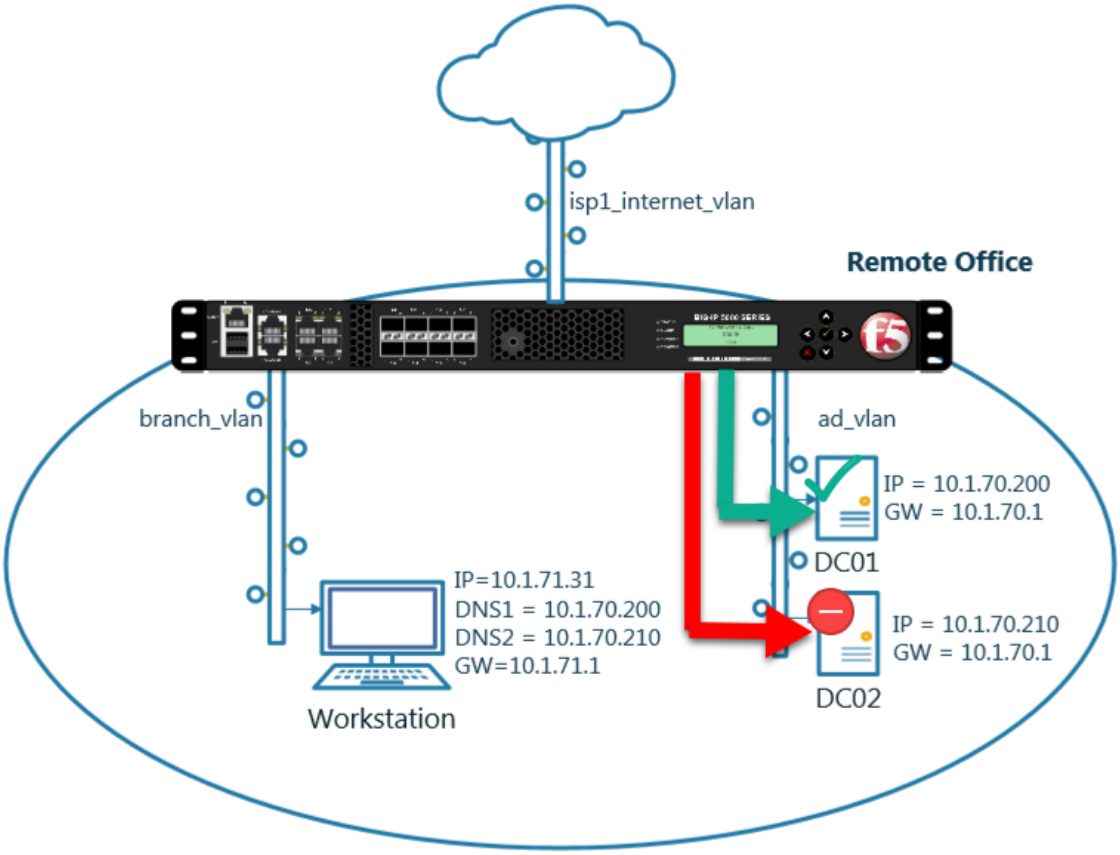

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/pool/resources.jsp?name=/Common/branch01_dns_pool

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



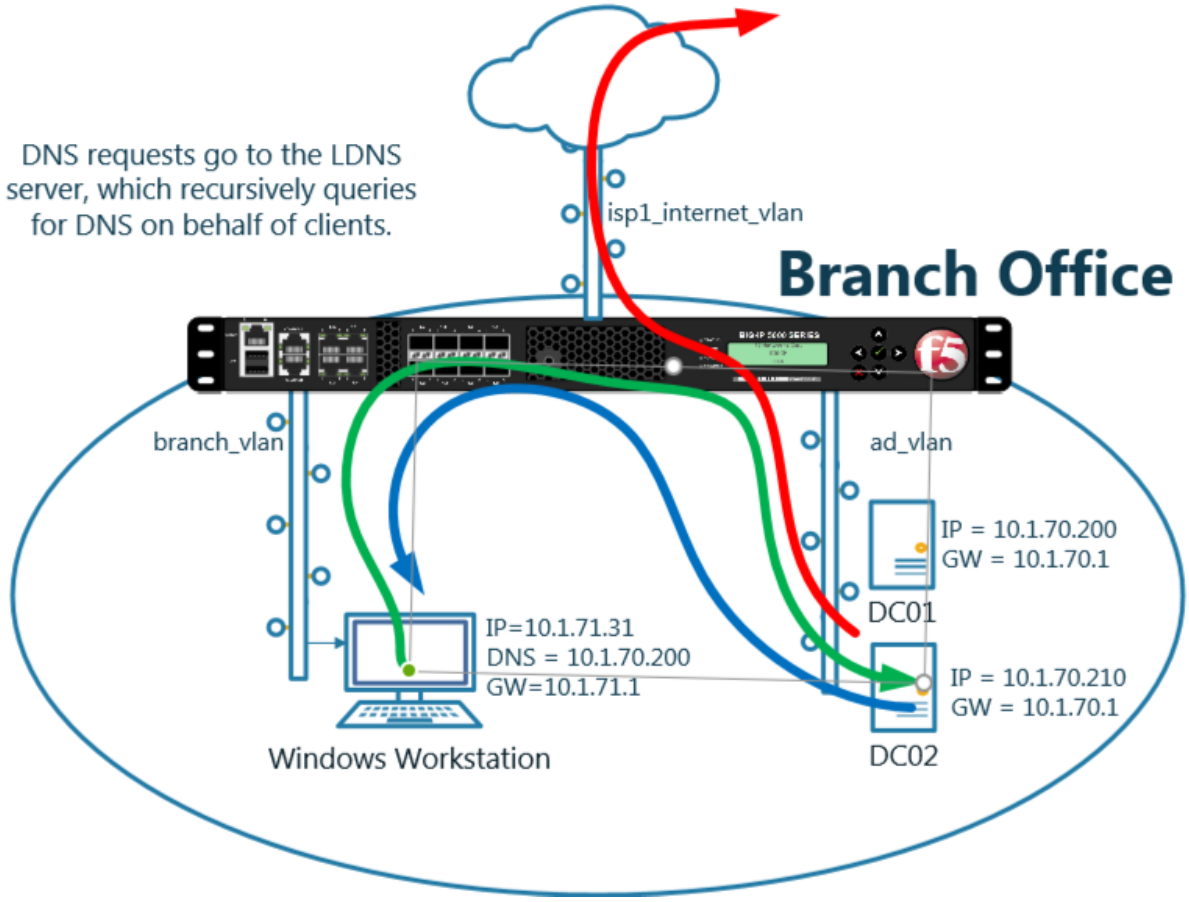

**TMSH**

tmsh show ltm pool branch01_dns_pool detail

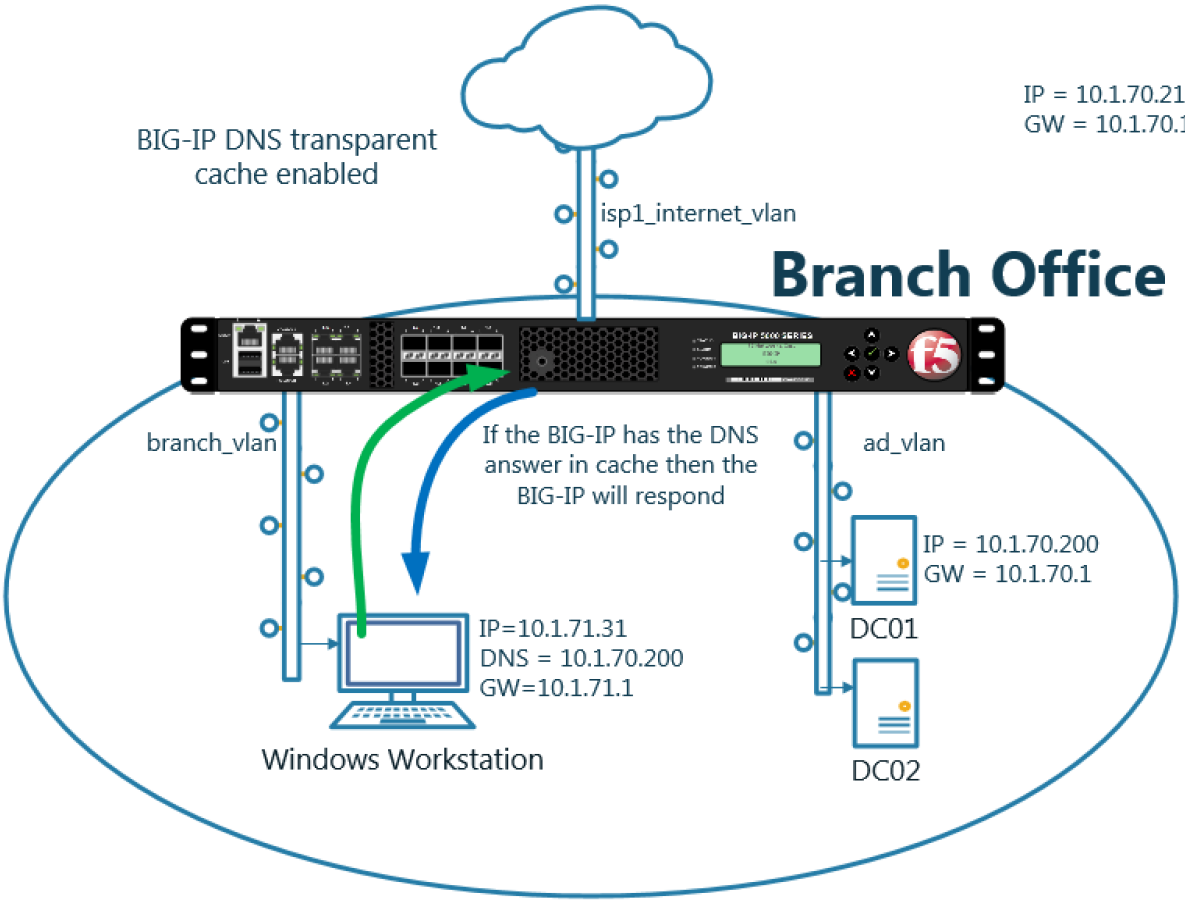



In this module we will prepare the objects required to build a transparent cache.

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




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

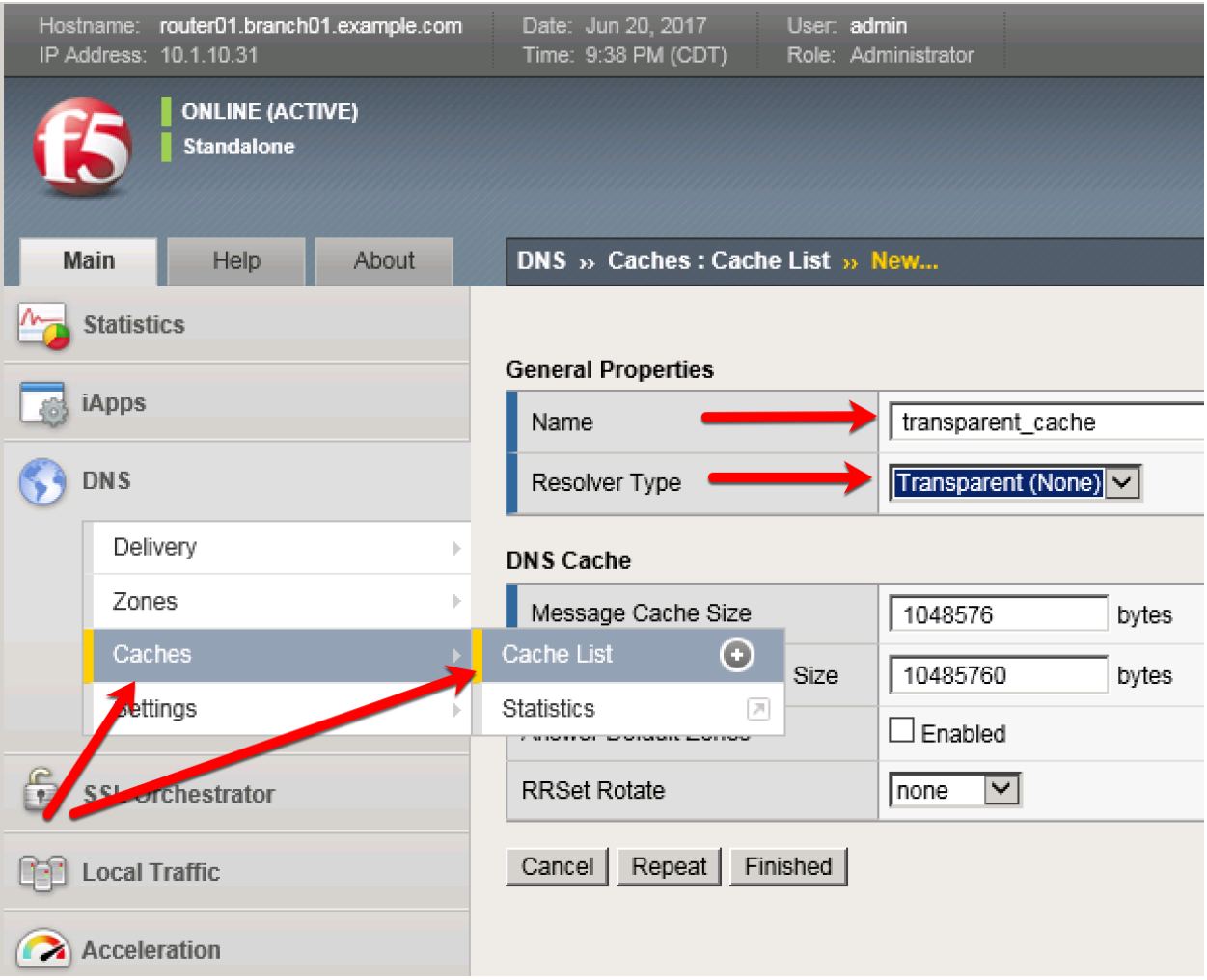



Log into the gateway device router01.brancho1 in the **branch office**

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

Create a transparent cache

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




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

TMSH command for router01.branch01:

**TMSH**

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

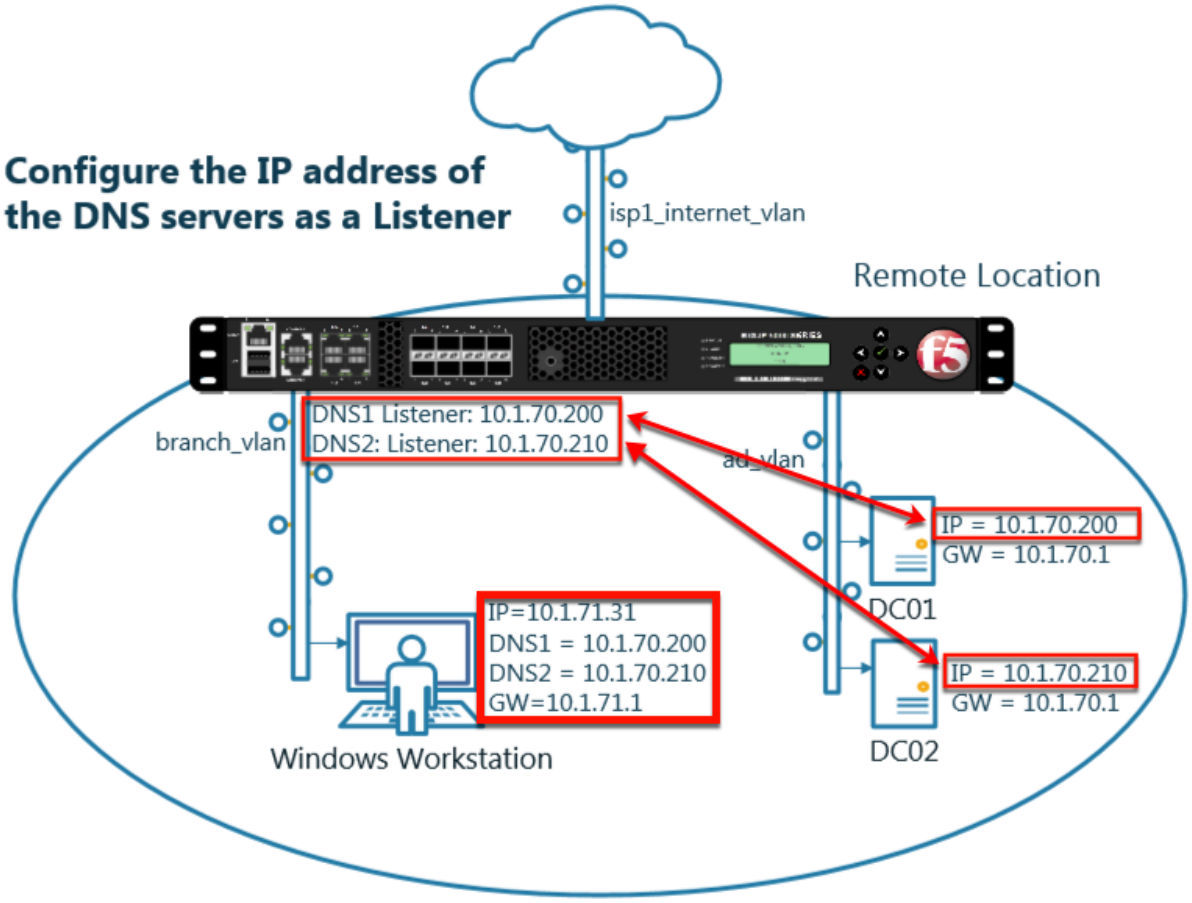
## 3.2 Listeners

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

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

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

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

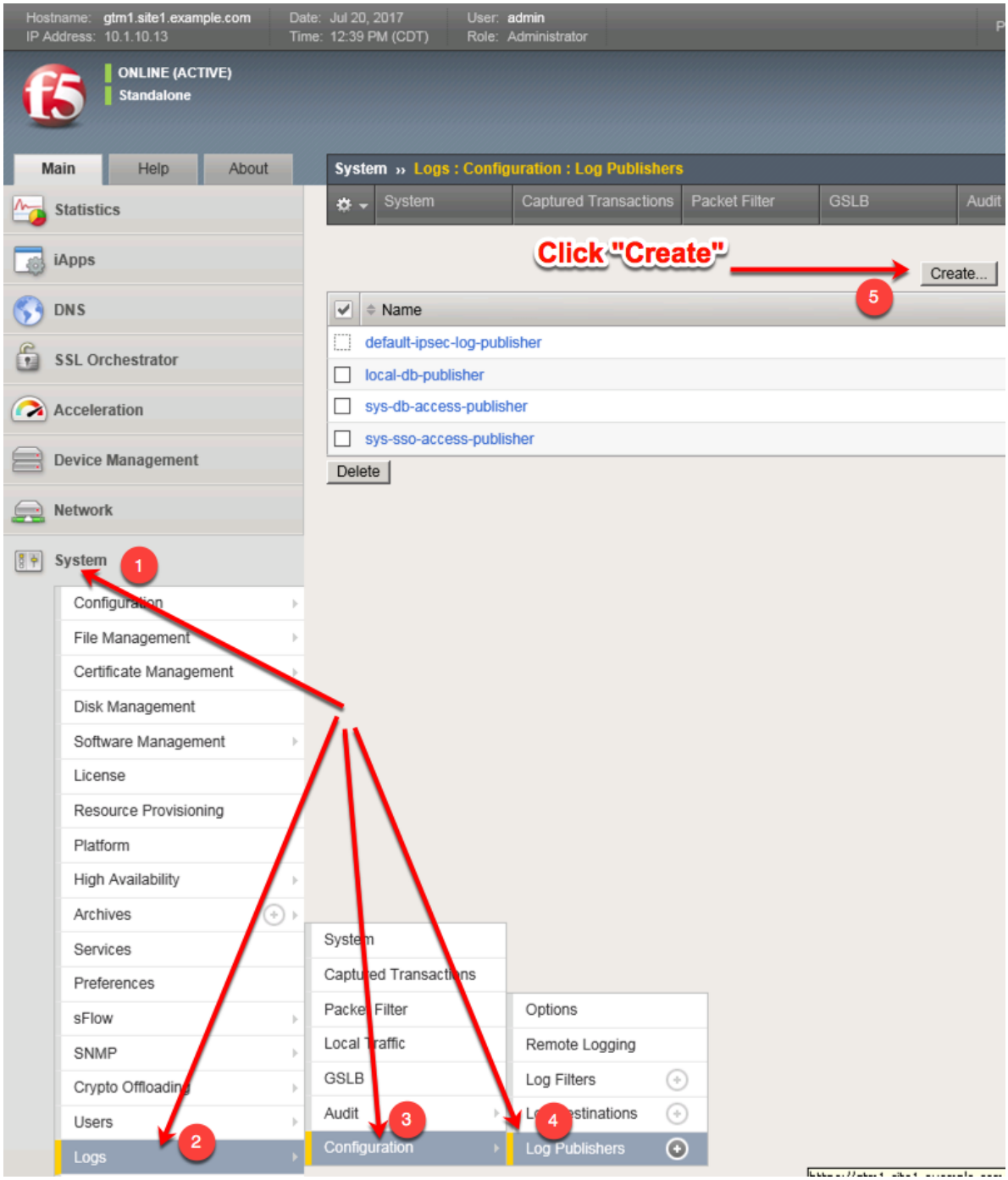



### 3.2.1 Log Profile

Configure DNS query and response logging.

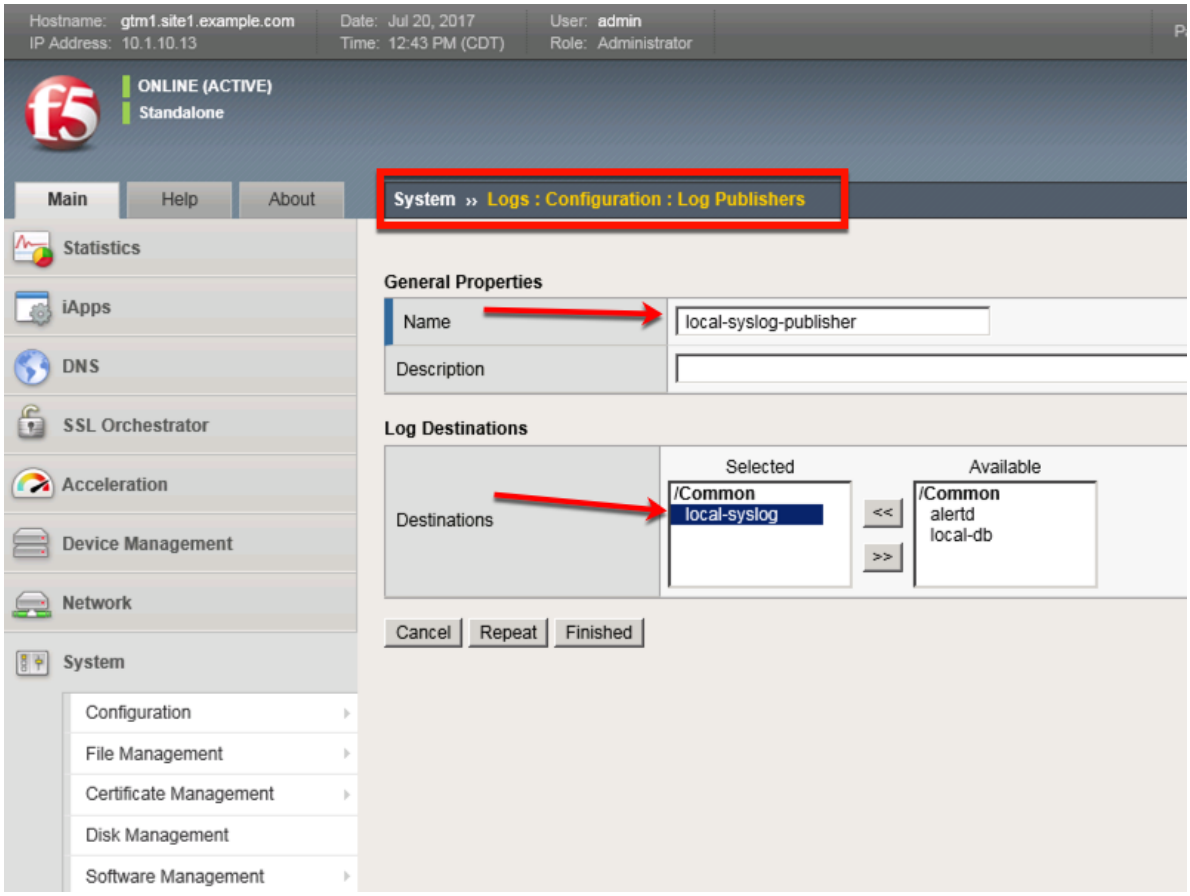
1. Create a “Log Publisher” for local syslog.

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




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

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



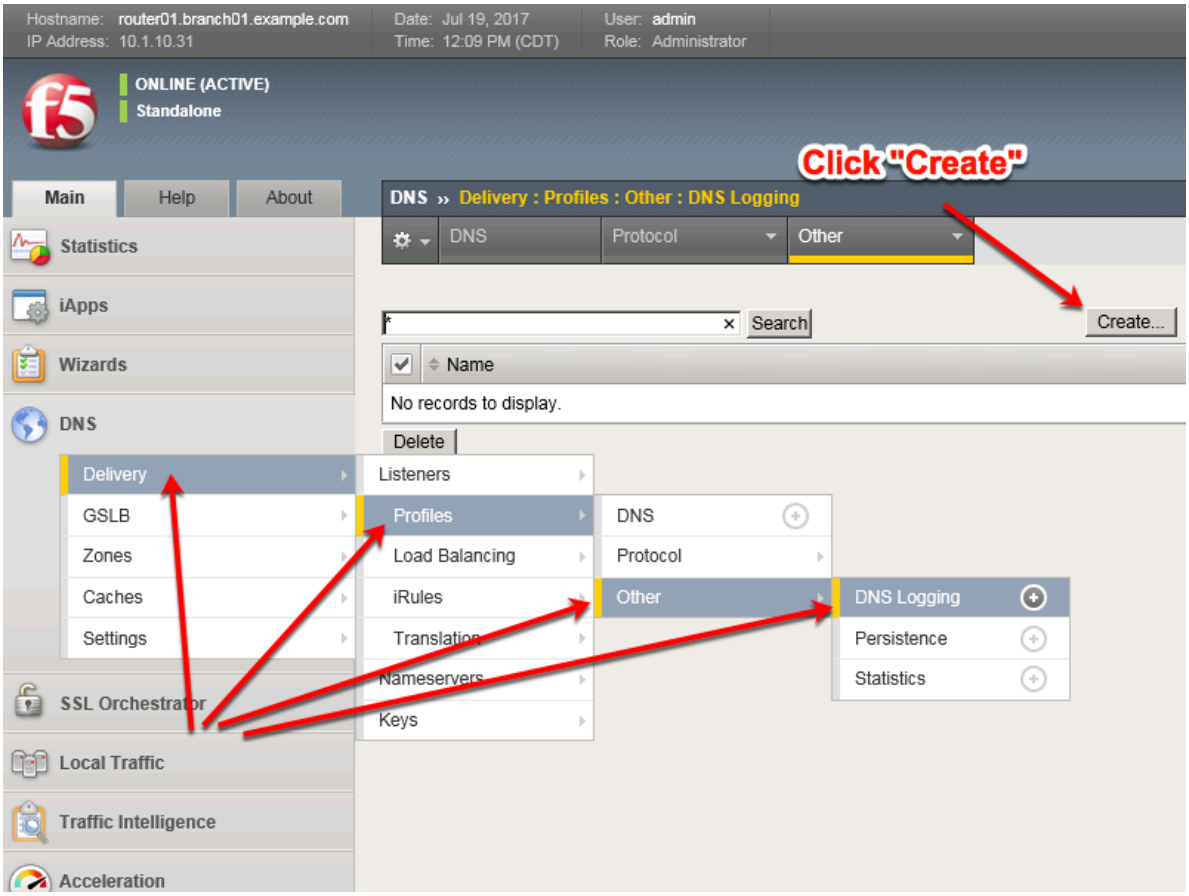

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/system/log/create_publisher.jsp

**TMSH**

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

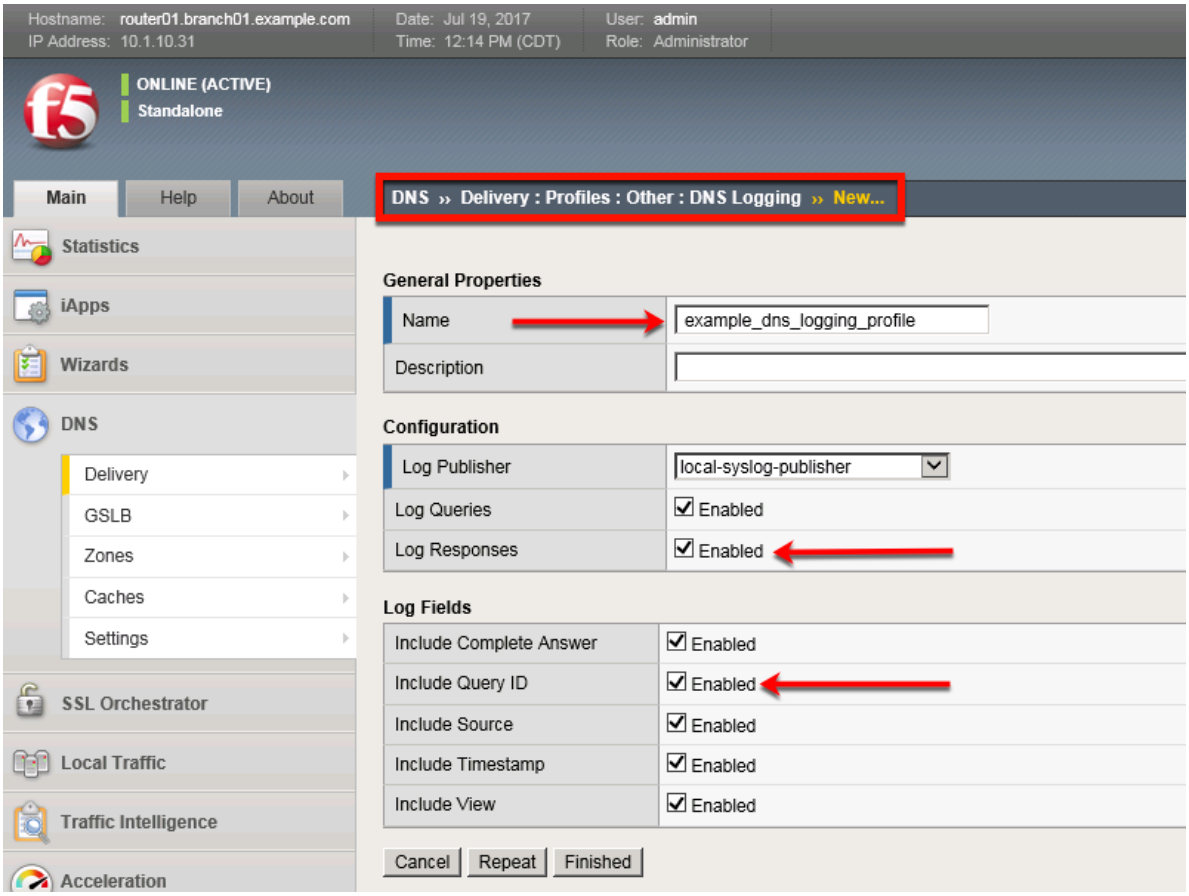
2. Create a “Logging Profile”

   Navigate to **DNS ›› Delivery : Profiles : Other : DNS Logging**




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 |




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

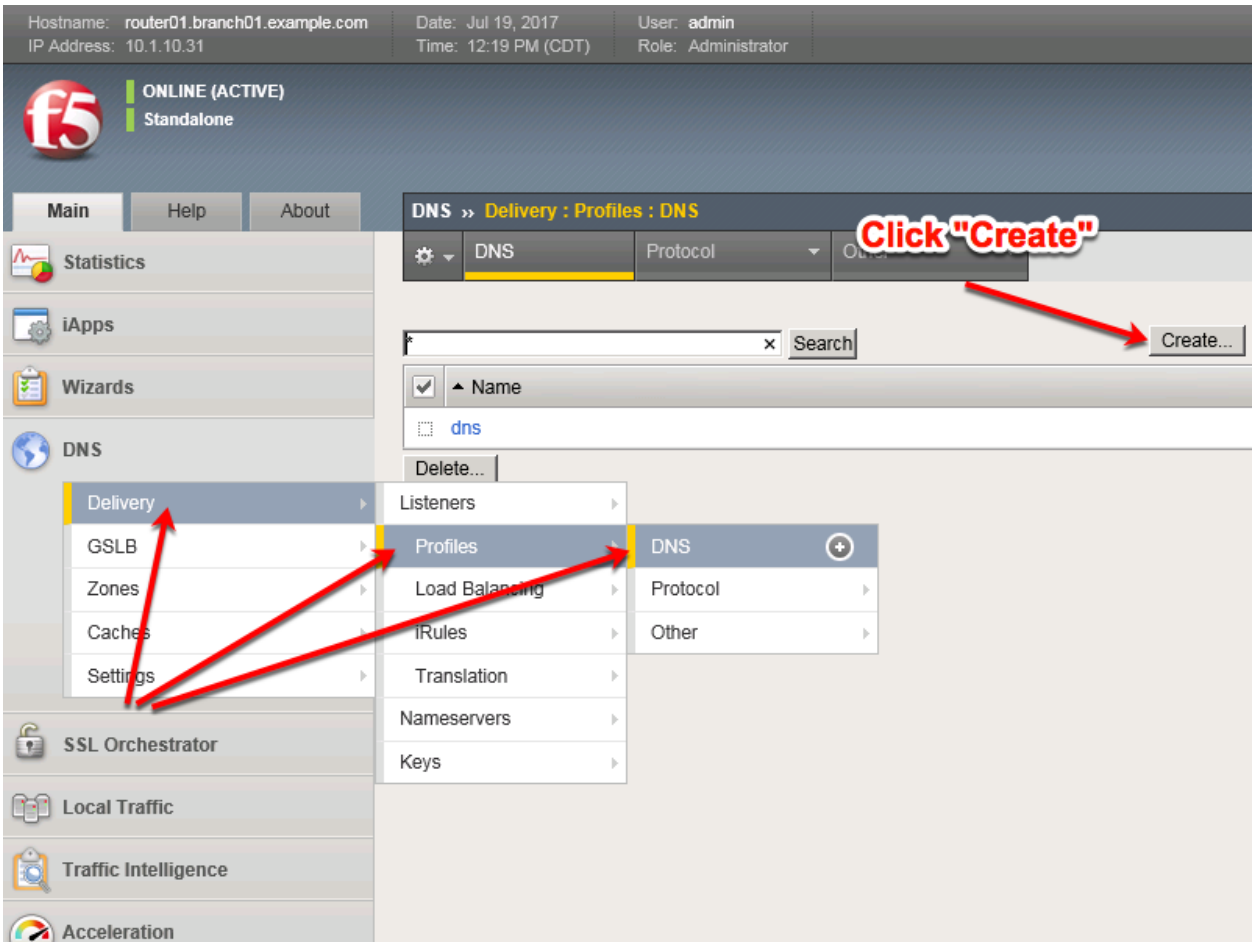
**TMSH**

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

### 3.2.2 DNS Profile

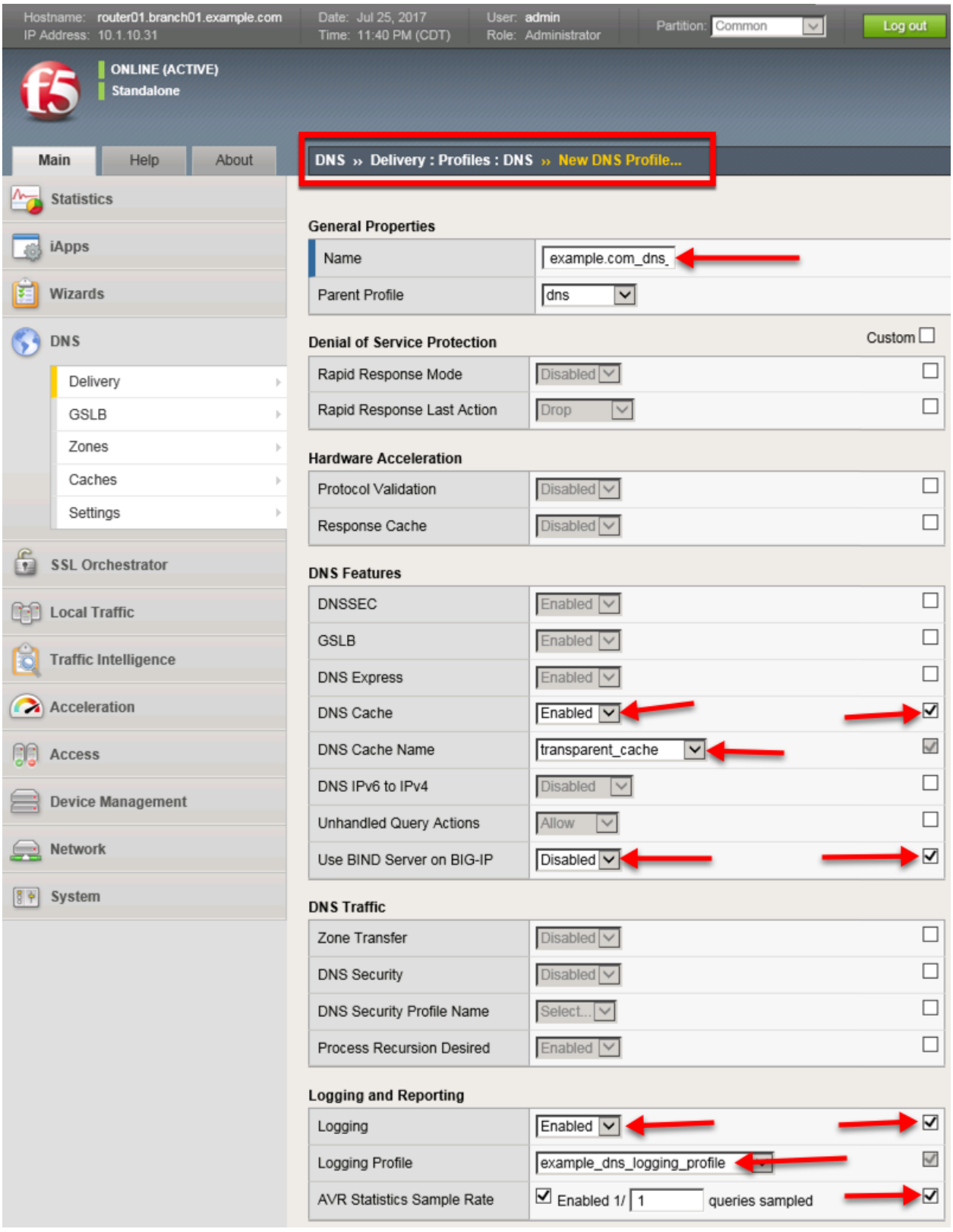
A DNS profile will control which features are enabled as part of processing a query.

Navigate to: **DNS ›› Delivery : Profiles : DNS**




Create a DNS profile as shown in the table below.

| 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 |




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

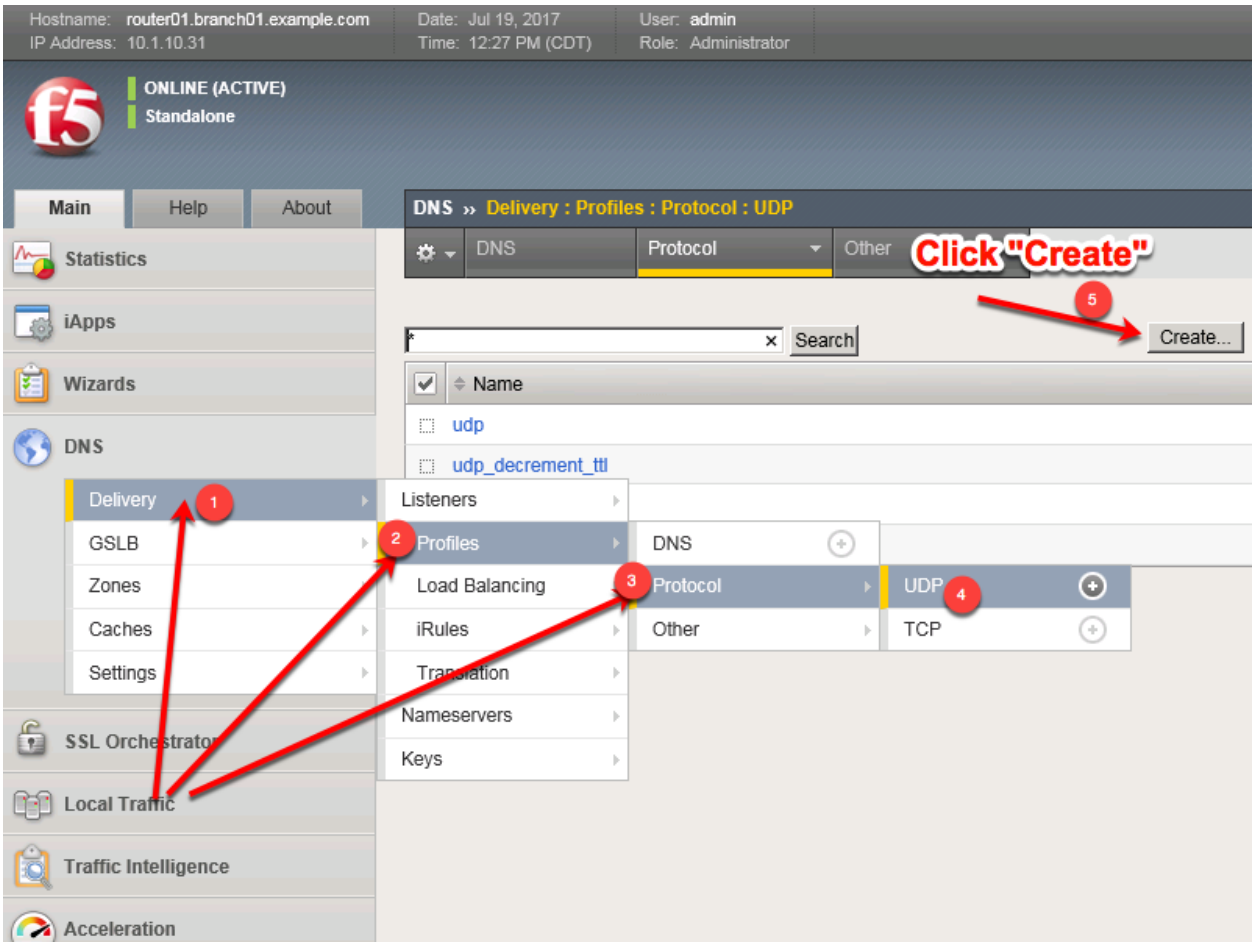
**TMSH**

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

### 3.2.3 UDP Profile

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

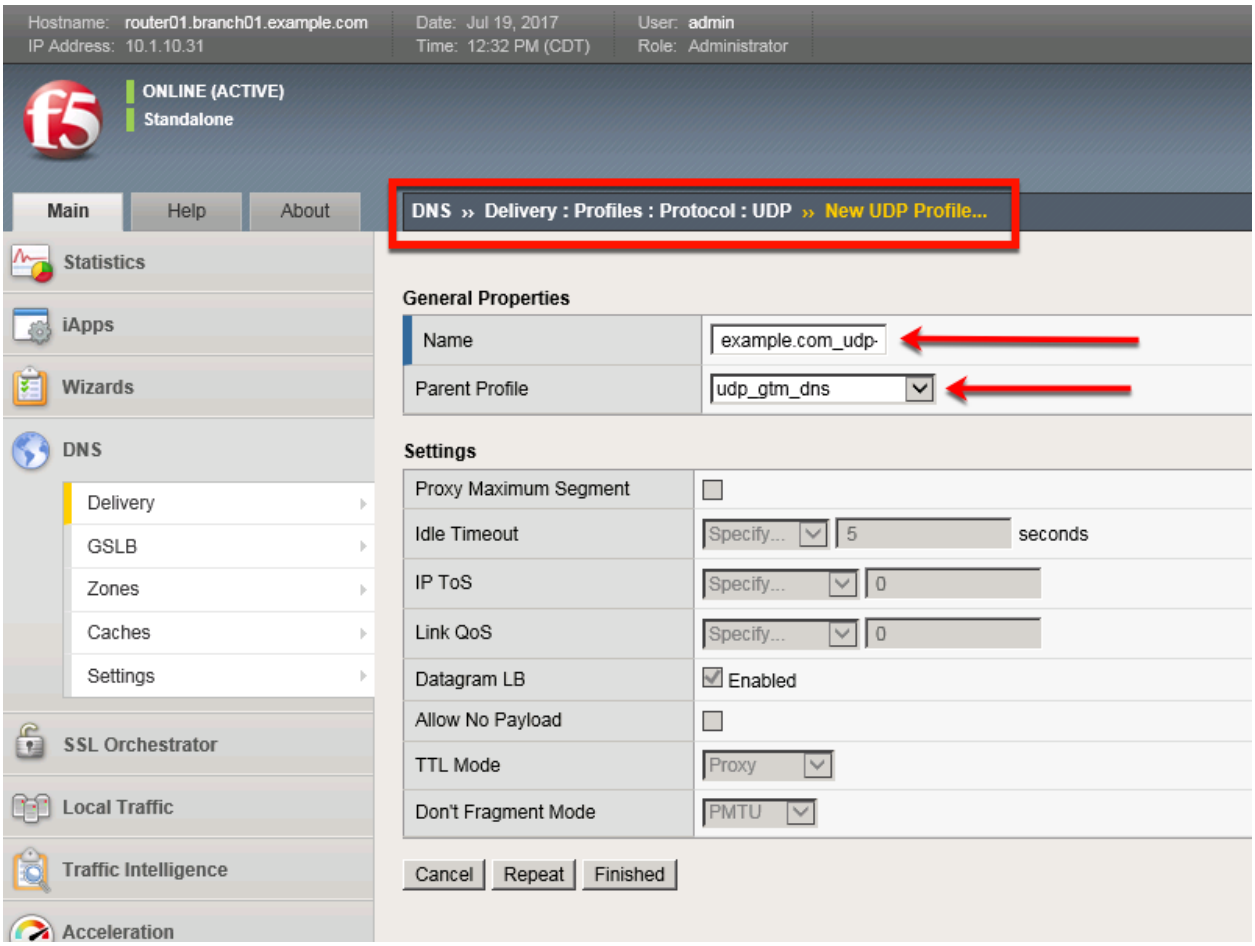
Navigate to: **DNS ›› Delivery : Profiles : Protocol : UDP**




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

Create a UDP profile as shown in the following table.

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




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

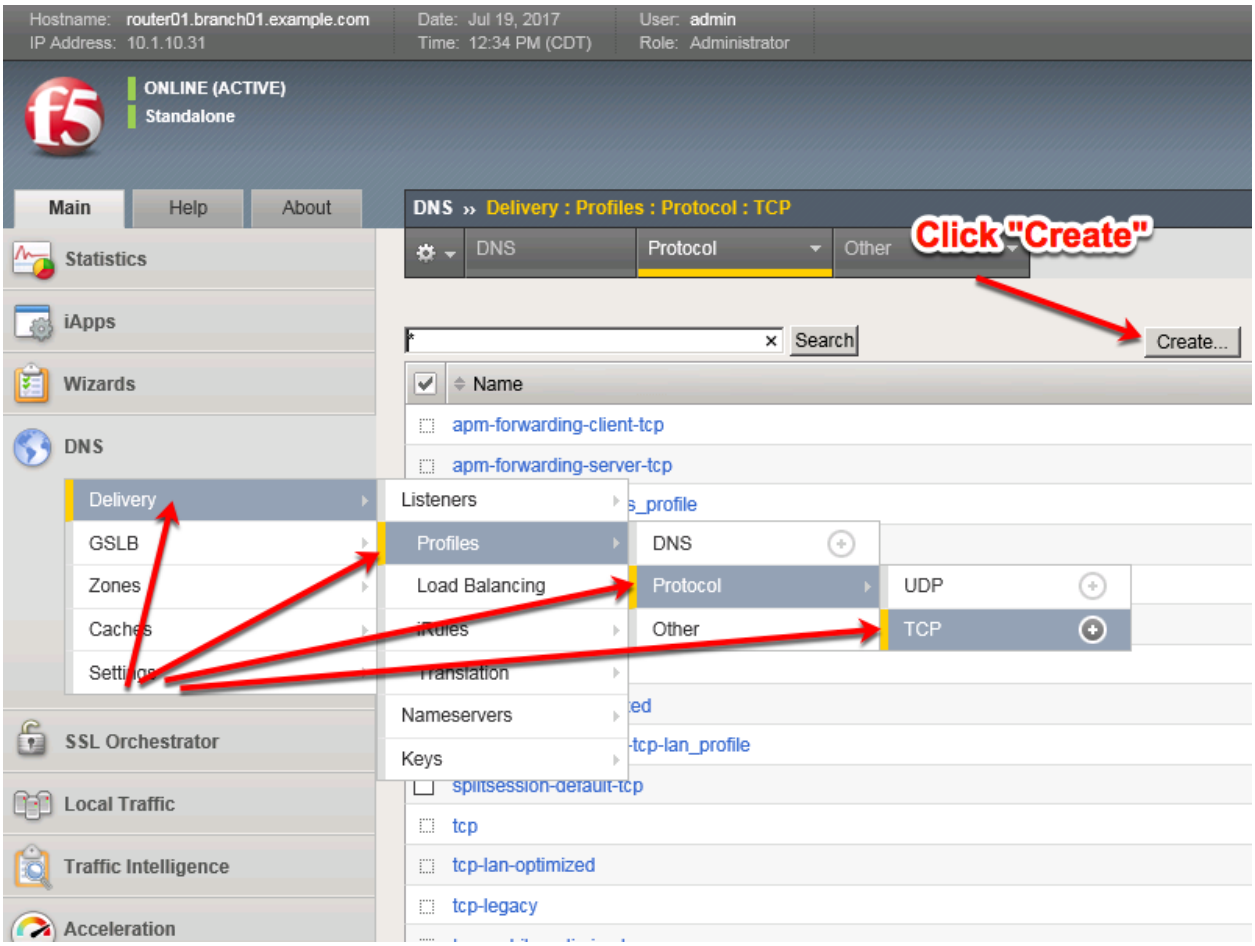
**TMSH**

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

### 3.2.4 TCP Profile

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

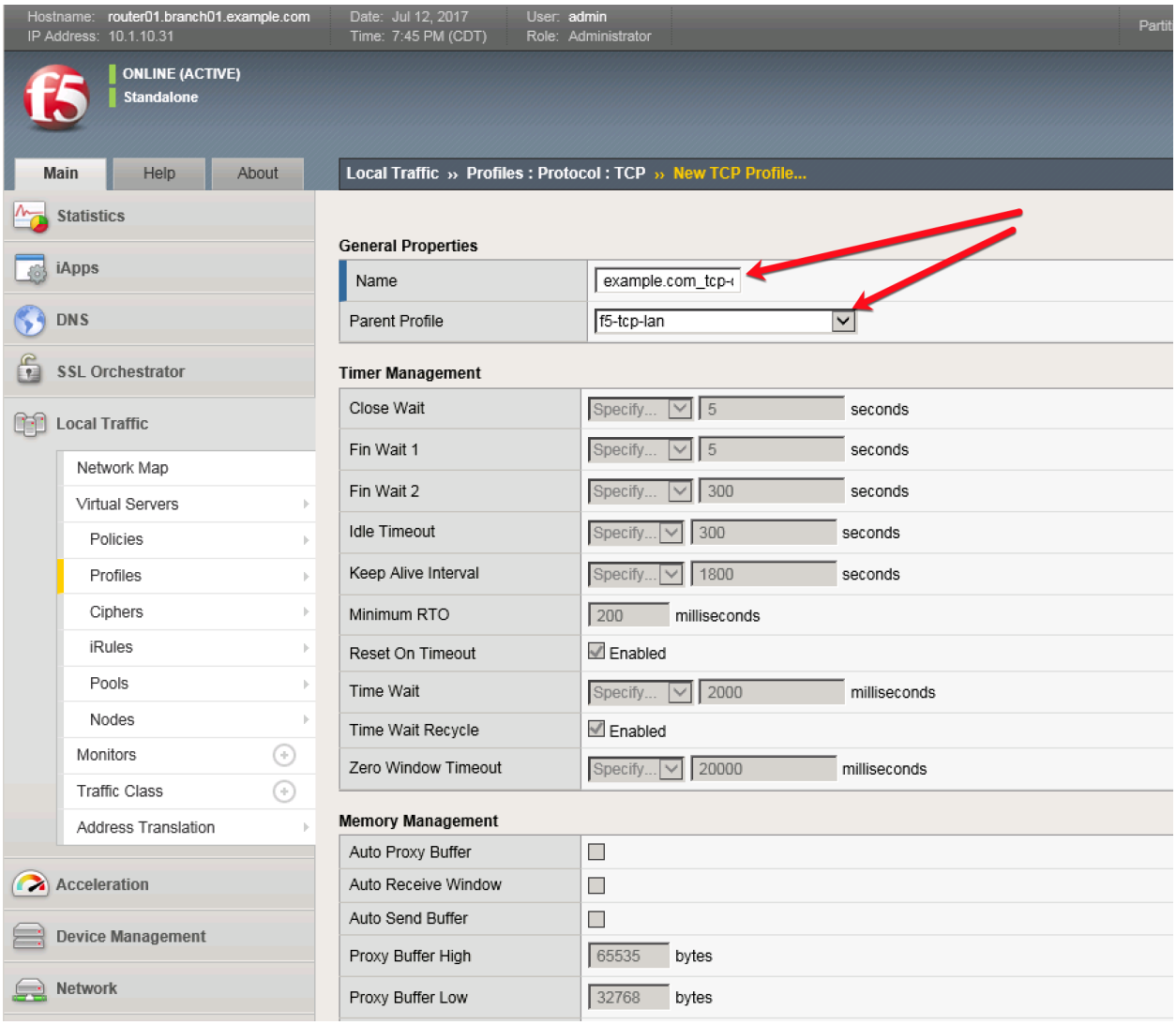
Navigate to: **DNS ›› Delivery : Profiles : Protocol : TCP**




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

Create a TCP profile as shown in the following table.

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




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

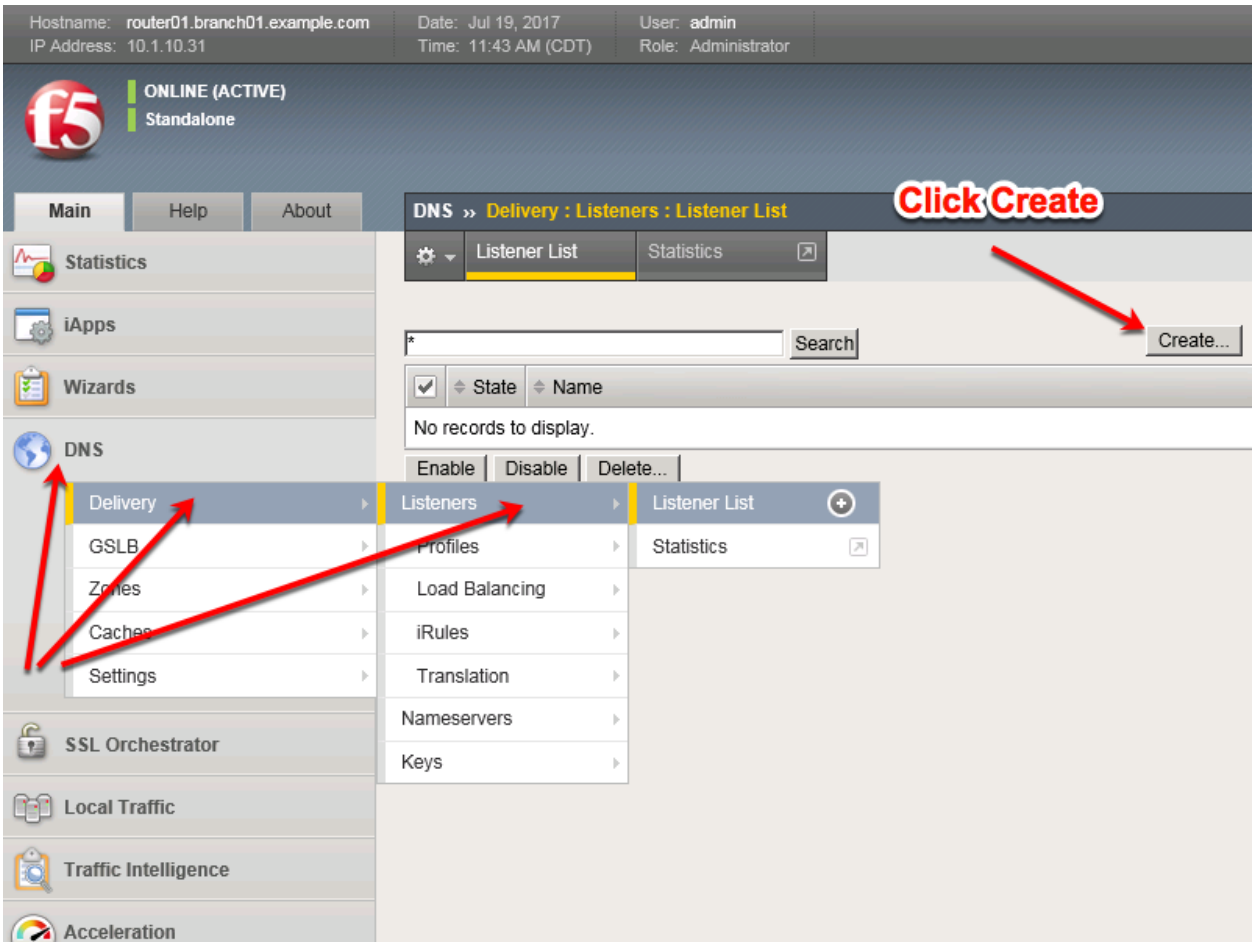
**TMSH**

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

### 3.2.5 UDP Listener

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

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

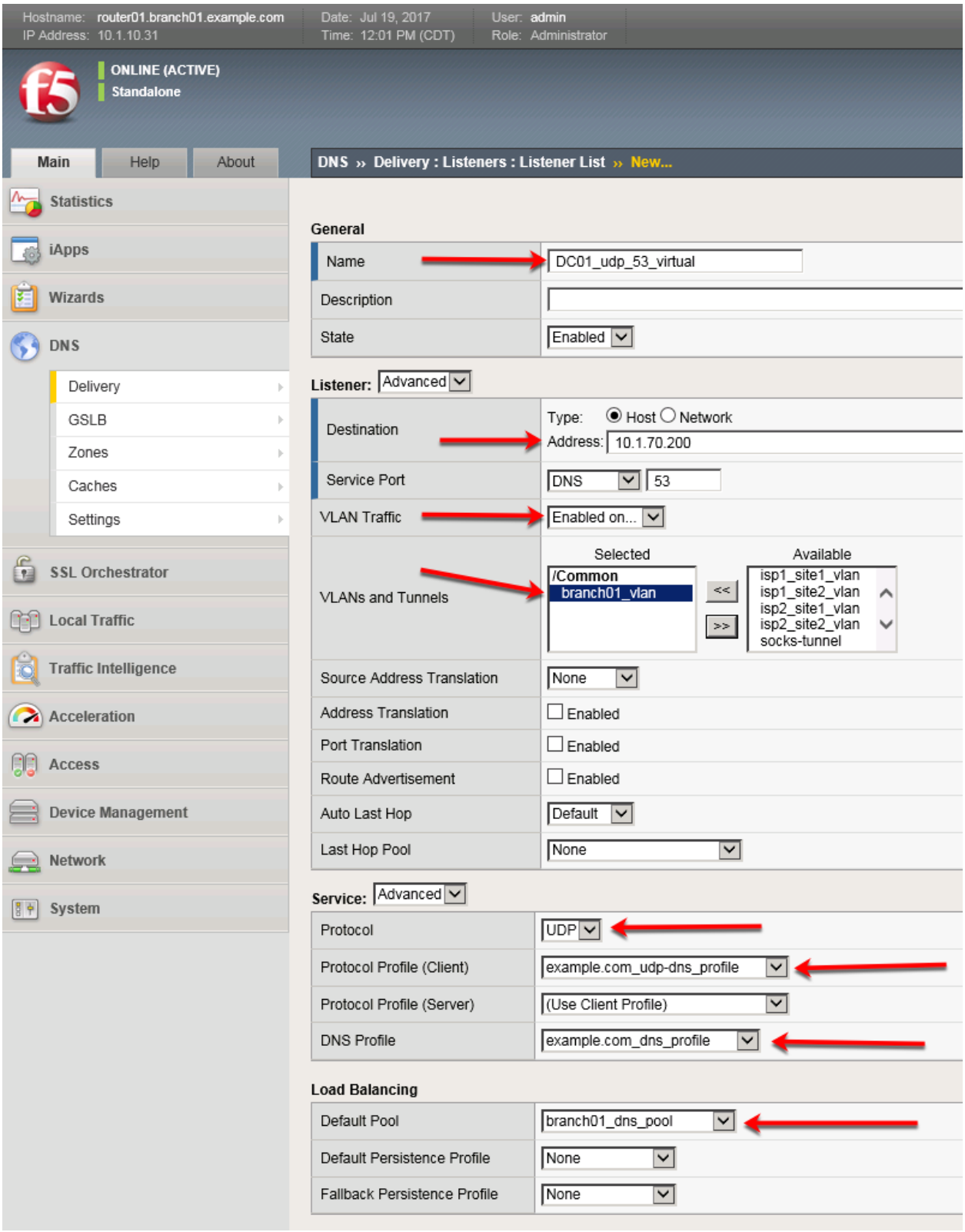



https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/listener/list.jsp

Create two UDP listeners according to the tables below:

| Setting | Value |
|---|---|
| Name | DC01_udp_53_virtual |
| Destination Address | 10.1.70.200 |
| Service Port | DNS 53 |
| VLAN and Tunnel Traffic -> Enabled on.. | branch01_vlan |
| Protocol | UDP |
| Protocol Profile (Client) | example.com_udp-dns_profile |
| DNS Profile | example.com_dns_profile |
| Default Pool | branch01_dns_pool |

| Setting | Value |
|---|---|
| Name | DC02_udp_53_virtual |
| Destination Address | 10.1.70.210 |
| Service Port | DNS 53 |
| VLAN and Tunnel Traffic -> Enabled on.. | branch01_vlan |
| Protocol | UDP |
| Protocol Profile (Client) | example.com_udp-dns_profile |
| DNS Profile | example.com_dns_profile |
| Default Pool | branch01_dns_pool |




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

**TMSH**

tmsh create gtm listener DC01_udp_virtual address 10.1.70.200 port 53 ip-protocol udp pool branch01_dns_pool profiles add { example.com_dns_profile example.com_udp-dns_profile } vlans add { branch01_vlan } vlans-enabled

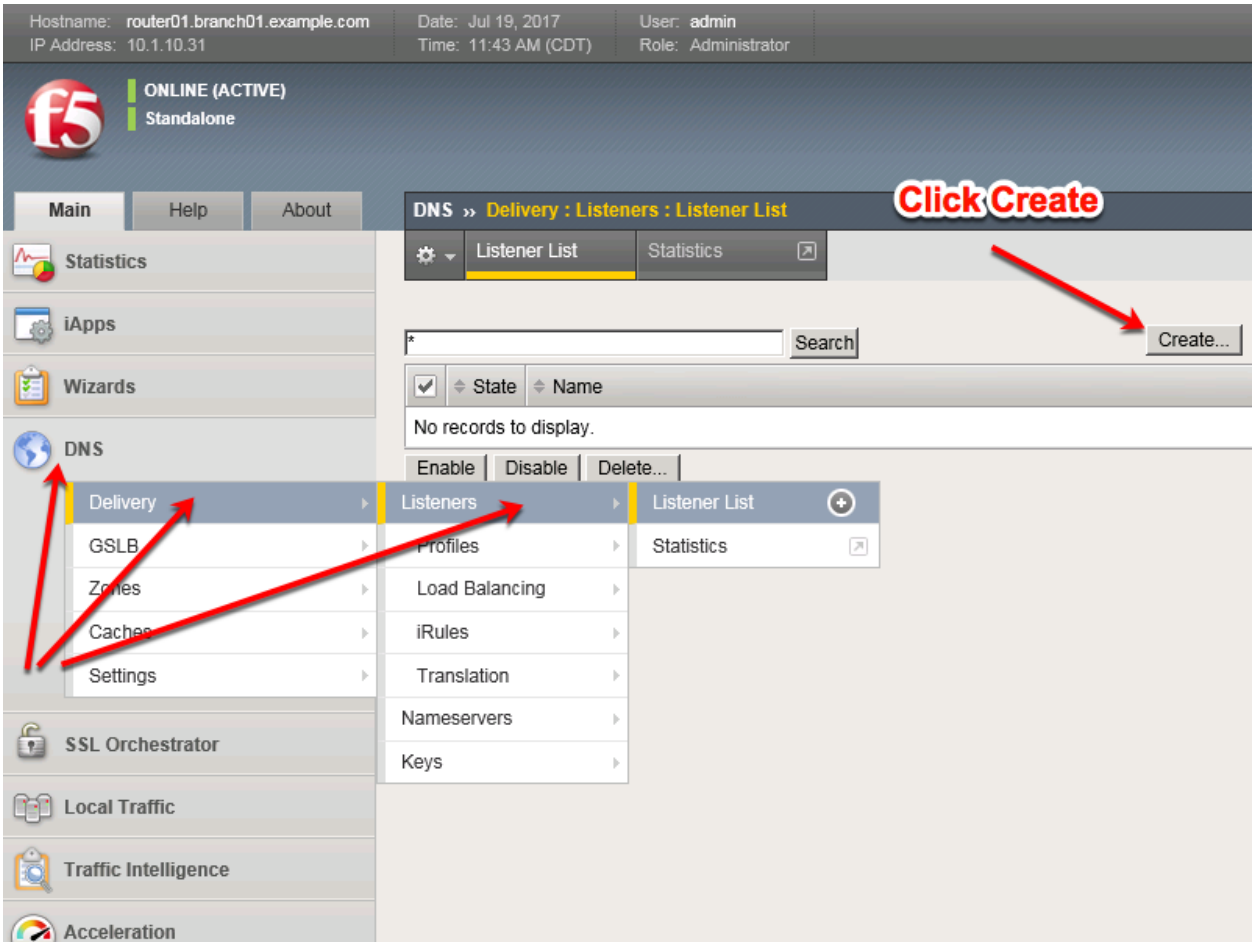
**TMSH**

tmsh create gtm listener DC02_udp_virtual address 10.1.70.210 port 53 ip-protocol udp pool branch01_dns_pool profiles add { example.com_dns_profile example.com_udp-dns_profile } vlans add { branch01_vlan } vlans-enabled

### 3.2.6 TCP Listeners

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

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

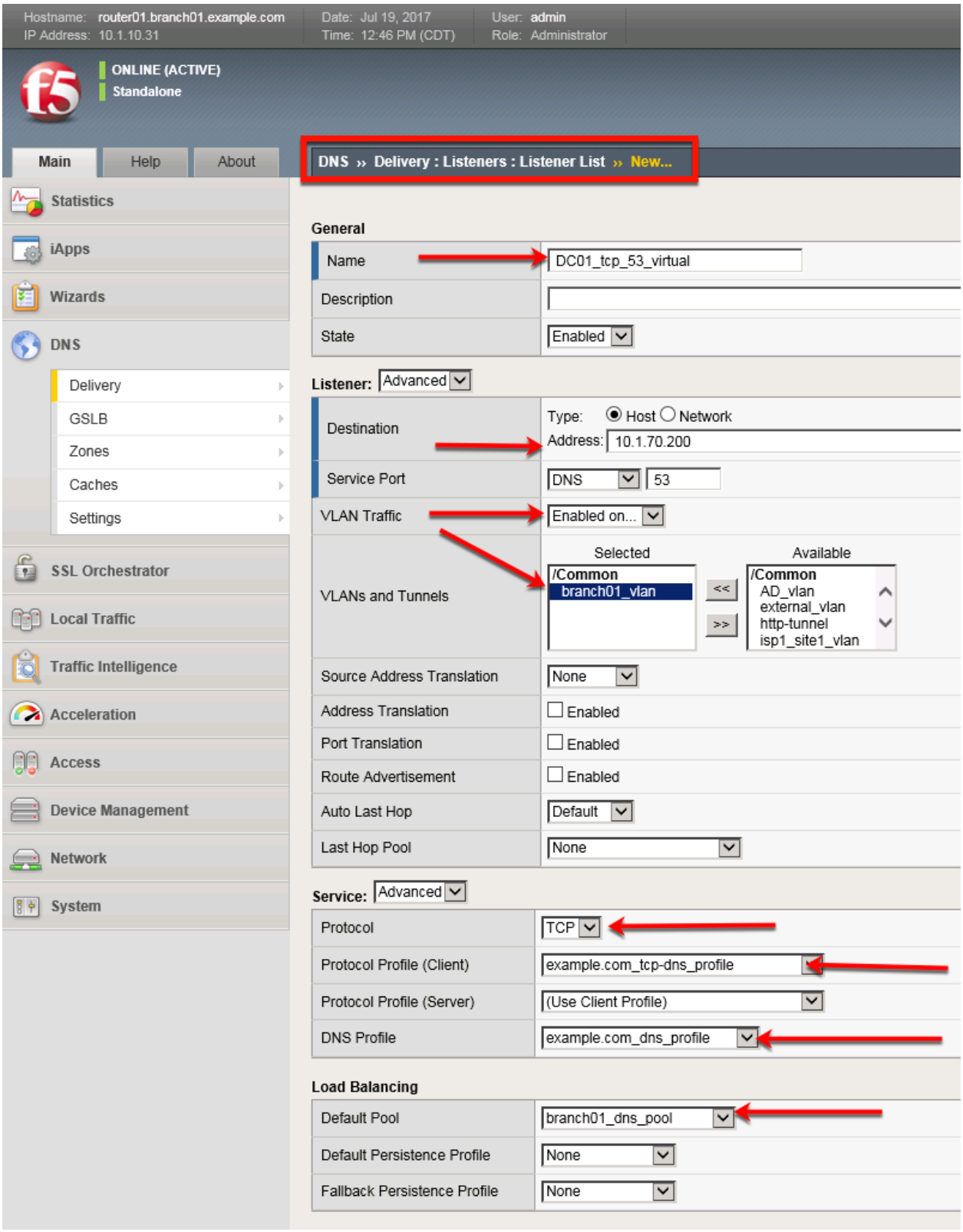



https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/listener/list.jsp

Create two TCP listeners according to the table below:

| Setting | Value |
|---|---|
| Name | DC01_tcp_53_virtual |
| Destination | 10.1.70.200 |
| Service Port | DNS 53 |
| VLAN and Tunnel Traffic -> Enabled on.. | branch01_vlan |
| Protocol | TCP |
| Protocol Profile (Client) | example.com_tcp-dns_profile |
| DNS Profile | example.com_dns_profile |
| Pool | branch01_dns_pool |

| Setting | Value |
|---|---|
| Name | DC02_tcp_53_virtual |
| Destination | 10.1.70.210 |
| Service Port | DNS 53 |
| VLAN and Tunnel Traffic -> Enabled on.. | branch01_vlan |
| Protocol | TCP |
| Protocol Profile (Client) | example.com_tcp-dns_profile |
| DNS Profile | example.com_dns_profile |
| Pool | branch01_dns_pool |




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

**TMSH**

tmsh create gtm listener DC01_tcp_virtual address 10.1.70.200 port 53 ip-protocol tcp pool branch01_dns_pool profiles add { example.com_dns_profile example.com_tcp-dns_profile } vlans add { branch01_vlan } vlans-enabled

---

**TMSH**

tmsh create gtm listener DC02_tcp_virtual address 10.1.70.210 port 53 ip-protocol tcp pool branch01_dns_pool profiles add { example.com_dns_profile example.com_tcp-dns_profile } vlans add { branch01_vlan } vlans-enabled

---

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

### 3.2.7 Results

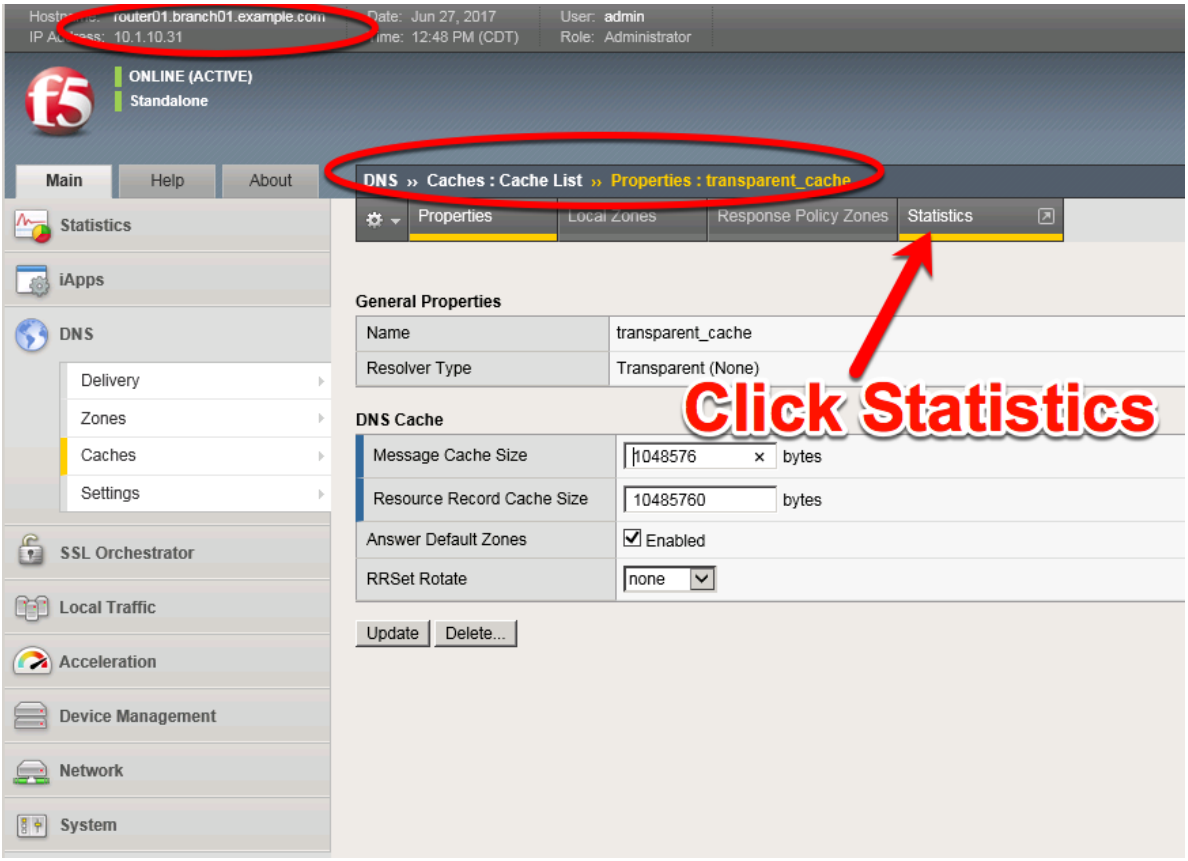
1. From the jumpbox open a command prompt, perform several recursive queries to your new listener to test.

   Repeat some of the same queries multiple times

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

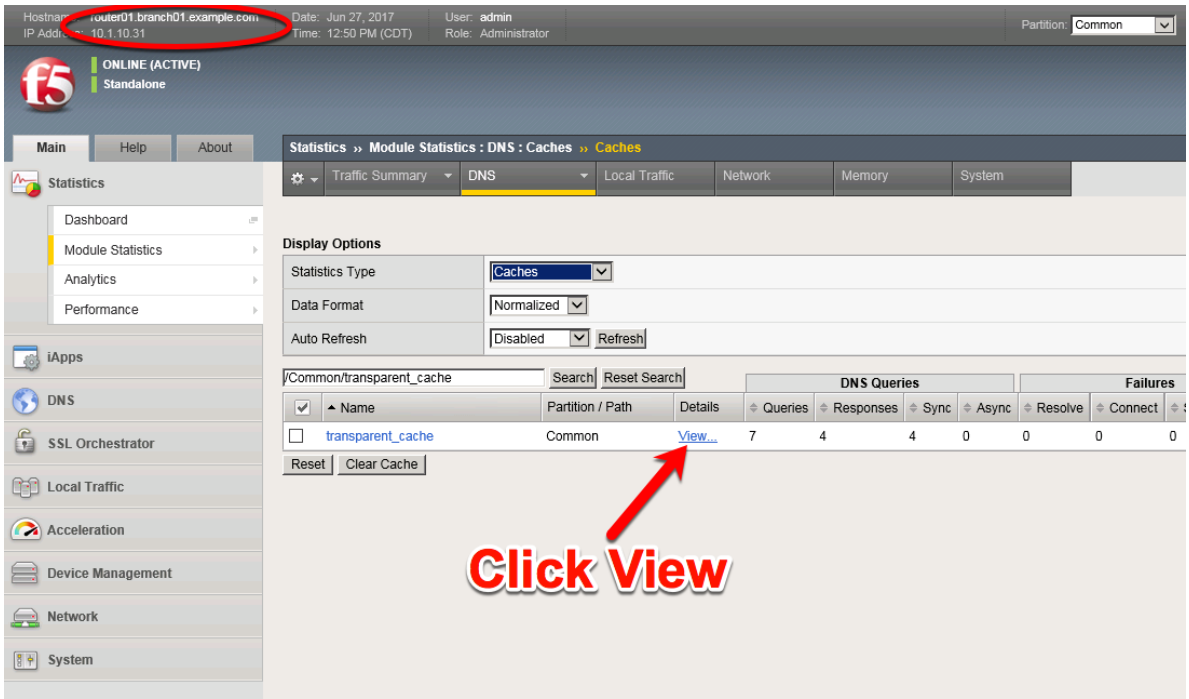
2. Viewing Cache Entries

   Navigate to: **DNS ›› Caches : Cache List ›› Properties : transparent_cache**

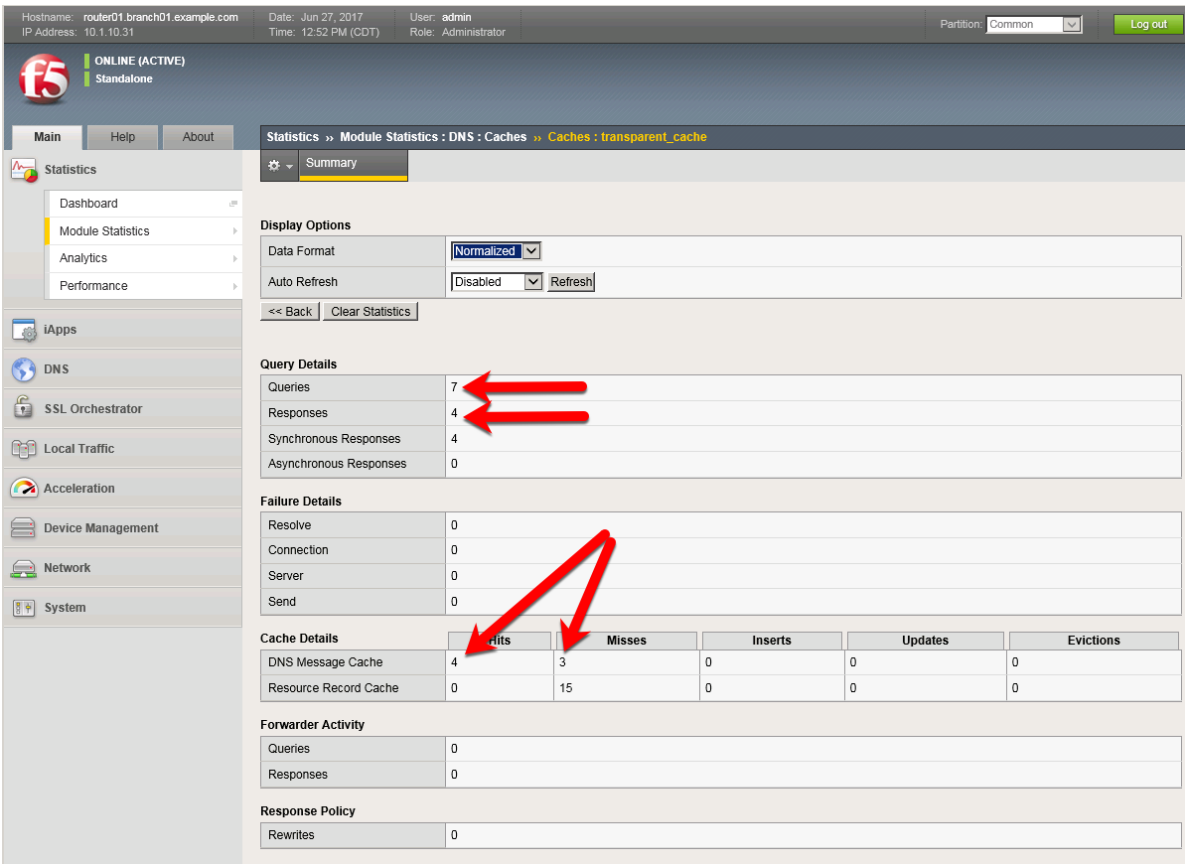



https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/properties.jsp?name=%2FCommon%2Ftransparent_cache

Navigate to: **Statistics ›› Module Statistics : DNS : Caches ›› Caches**



Navigate to: **Statistics ›› Module Statistics : DNS : Caches ›› Caches : transparent_cache**




https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/stats_detail.jsp?name=/Common/transparent_cache

---

**TMSH**

tmsh show ltm dns cache records rrset cache transparent_cache

---

```
[root@router01:Active:Standalone] config # tmsh show ltm dns cache records rrset cache transparent_cache
----------------------------------
Ltm::DNS-Cache/Resolver RR Records
----------------------------------
Owner                TTL   Type   Class  rdata
www.gslb.example.com  25    A      IN     203.0.113.9
www.example.com       3595  CNAME  IN     www.gslb.example.com
www.ncsu.edu          3588  A      IN     152.1.227.242
www.ncsu.edu          3588  A      IN     152.1.227.243
www.ncsu.edu          3588  A      IN     152.1.227.241
www.ncsu.edu          3588  A      IN     152.1.227.240
Owner              TTL  Type  Class  rdata
www.wikipedia.org  578  A     IN     198.35.26.96
Total records returned (tmm0): 7
[root@router01:Active:Standalone] config #
```

show ltm dns cache transparent transparent_cache

3. Clearing Entire Cache

   Navigate to **Statistics > Module Statistics > DNS > Caches**

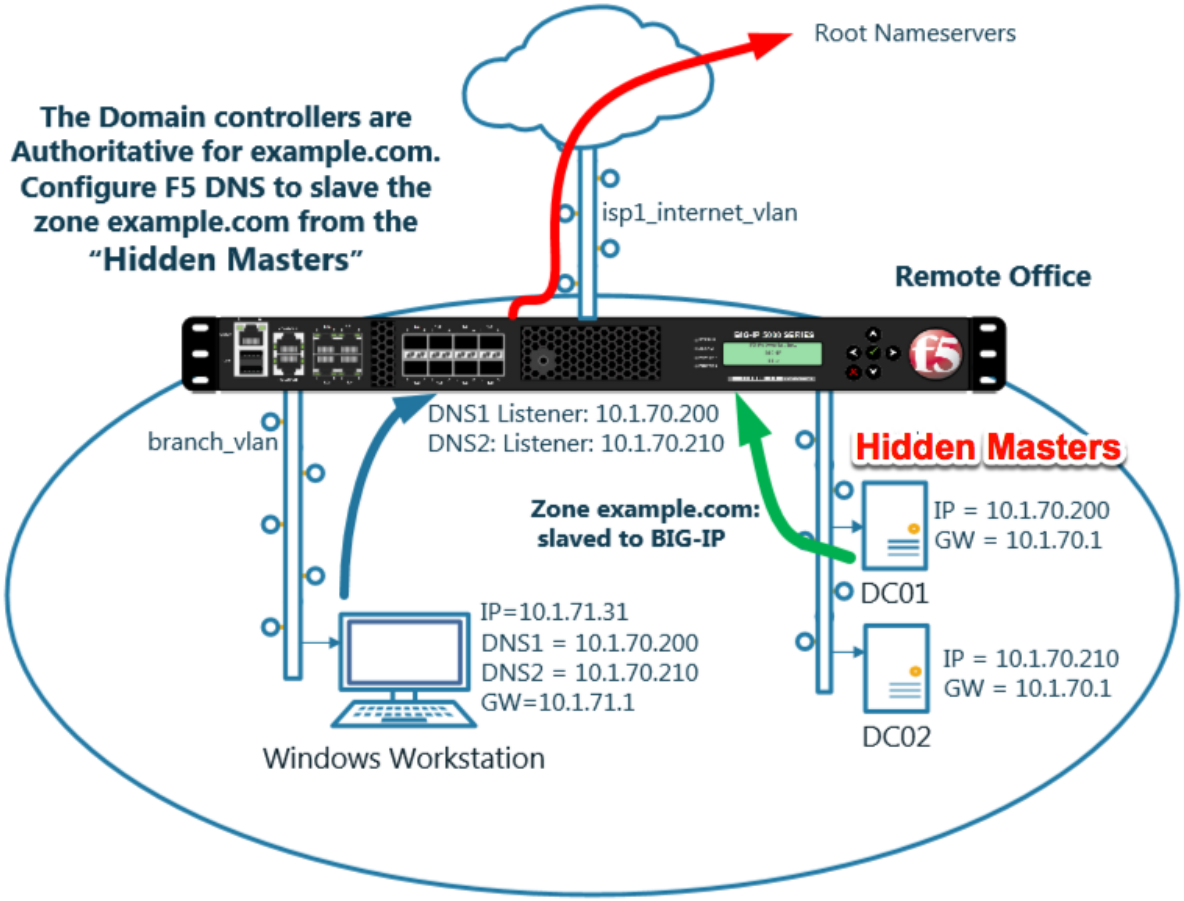
   Set “Statistics Type” to “Caches”.

   Select the cache and click “Clear Cache” to empty the cache.

## 3.3 Hidden Master

The internal DNS servers are authoritative for example.com so we need to slave the zone to the BIG-IP.

After this module is complete the BIG-IP will become an authoritative slave.

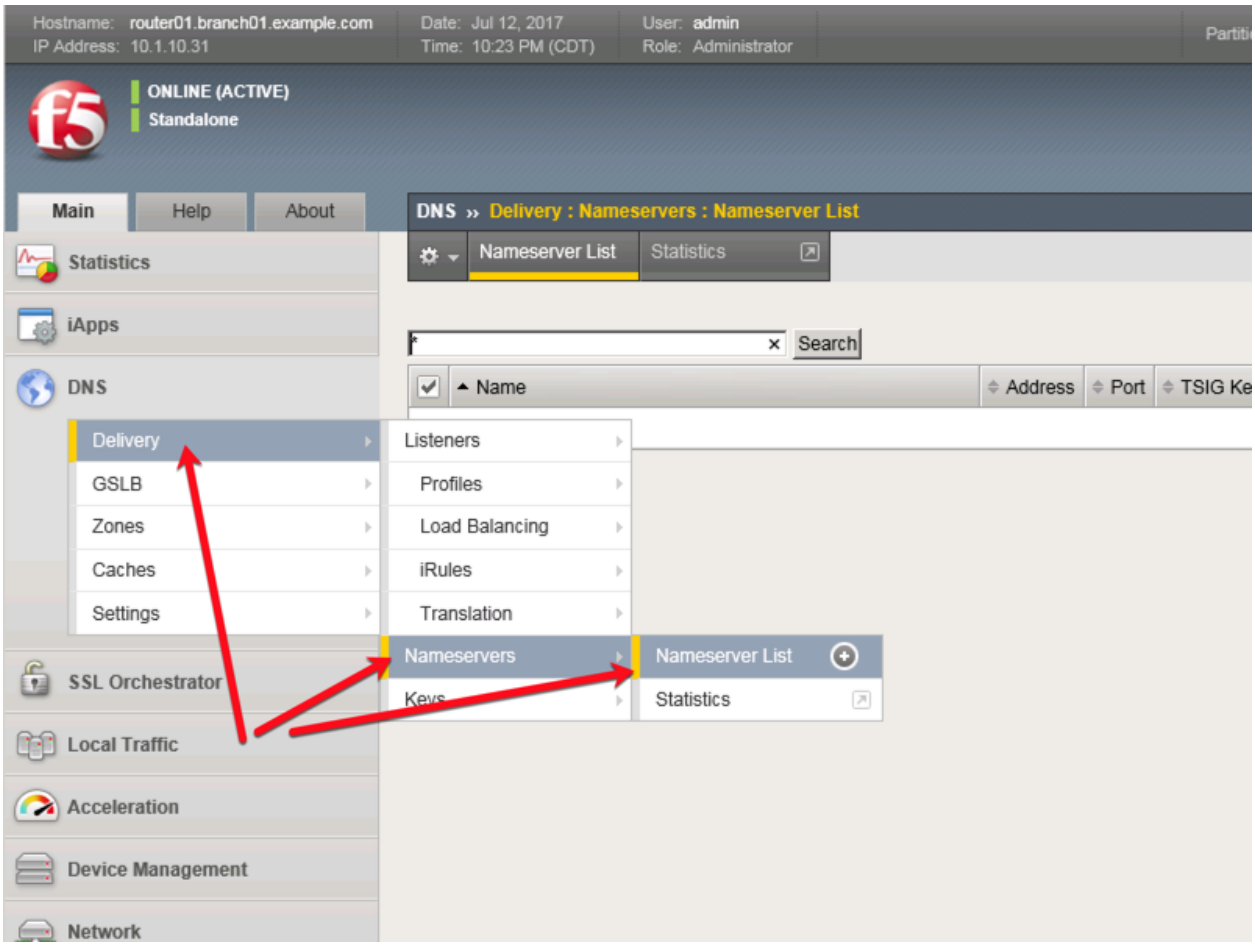



https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/dns-services-implementations-11-6-0/2.html#unique_1658664851

### 3.3.1 Name Server

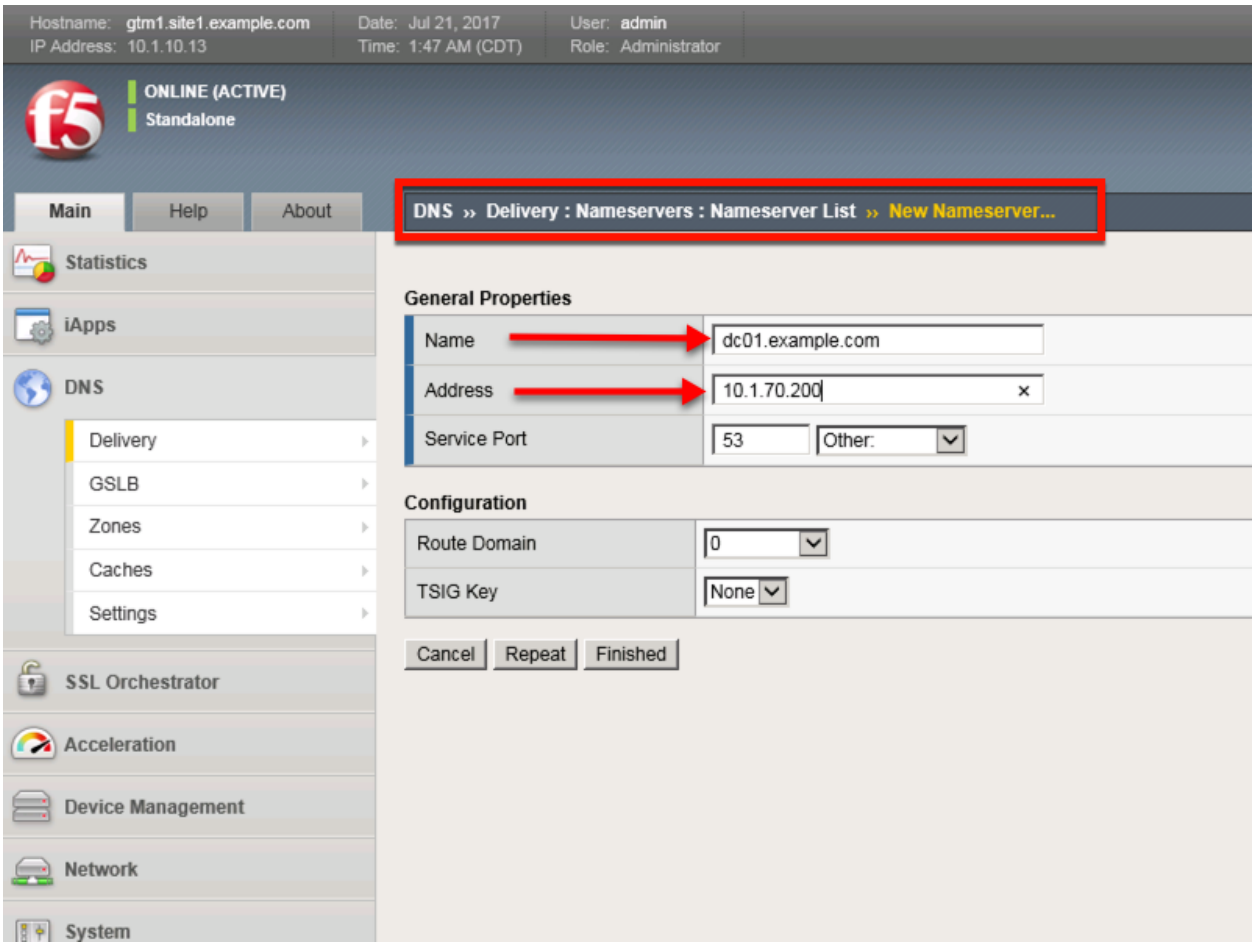
Define the Active Directory server as a nameserver and initiate a zone transfer.

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




Create a nameserver according to the following table:

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




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

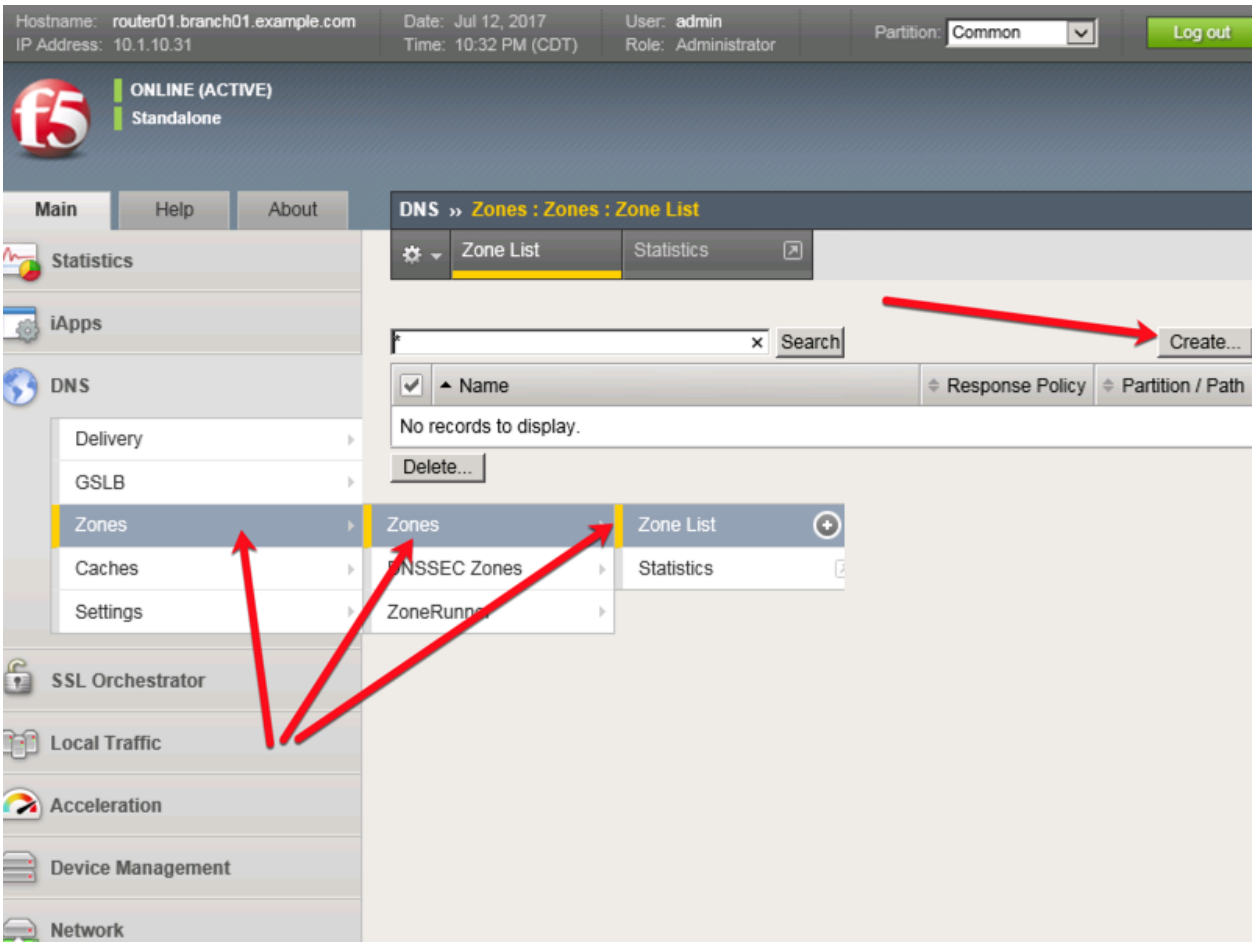
**TMSH**

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

### 3.3.2 DNS Express

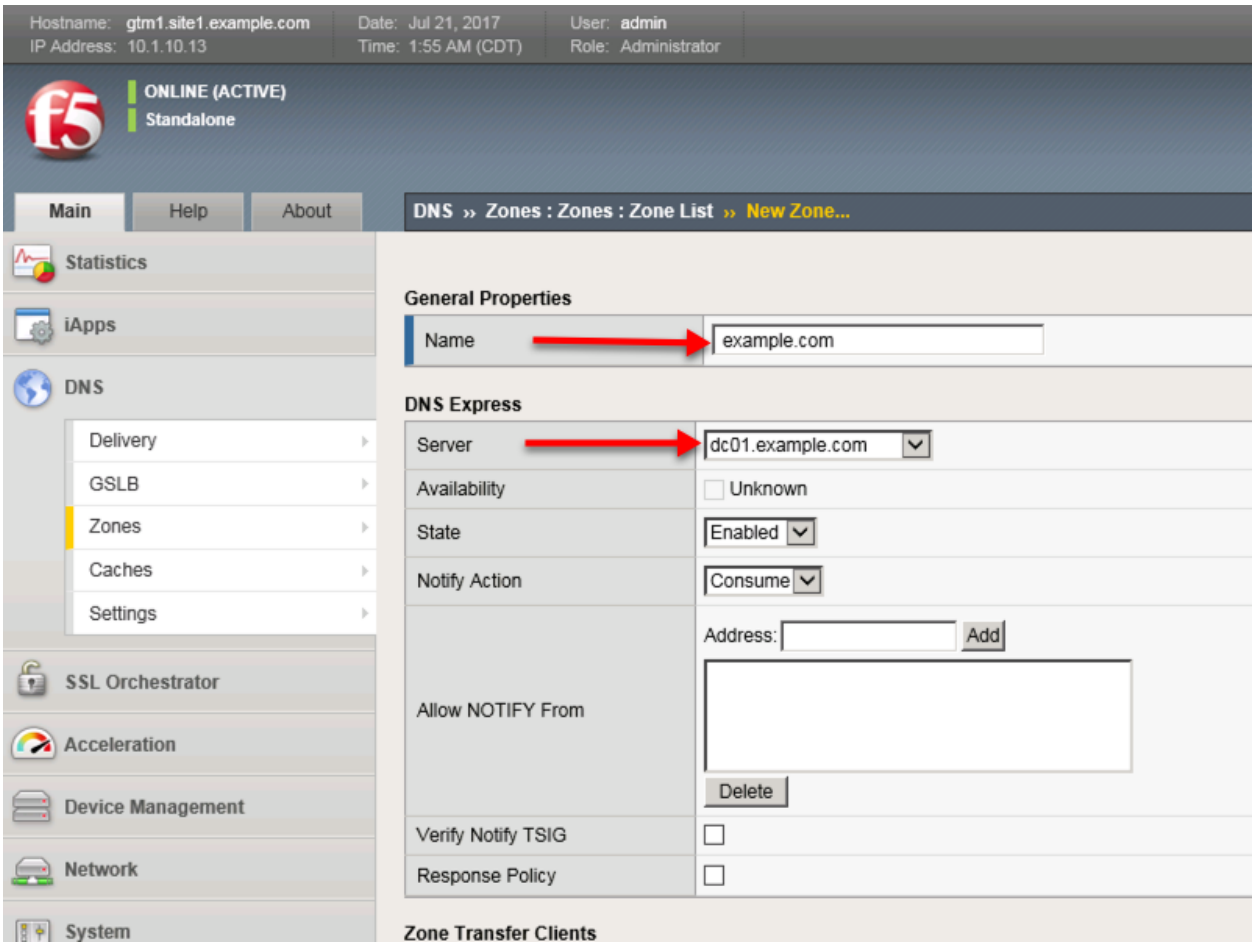
The zone example.com is served from the high performance authoritative resolver.

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




Create a DNS Express zone according to the following table:

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




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

---

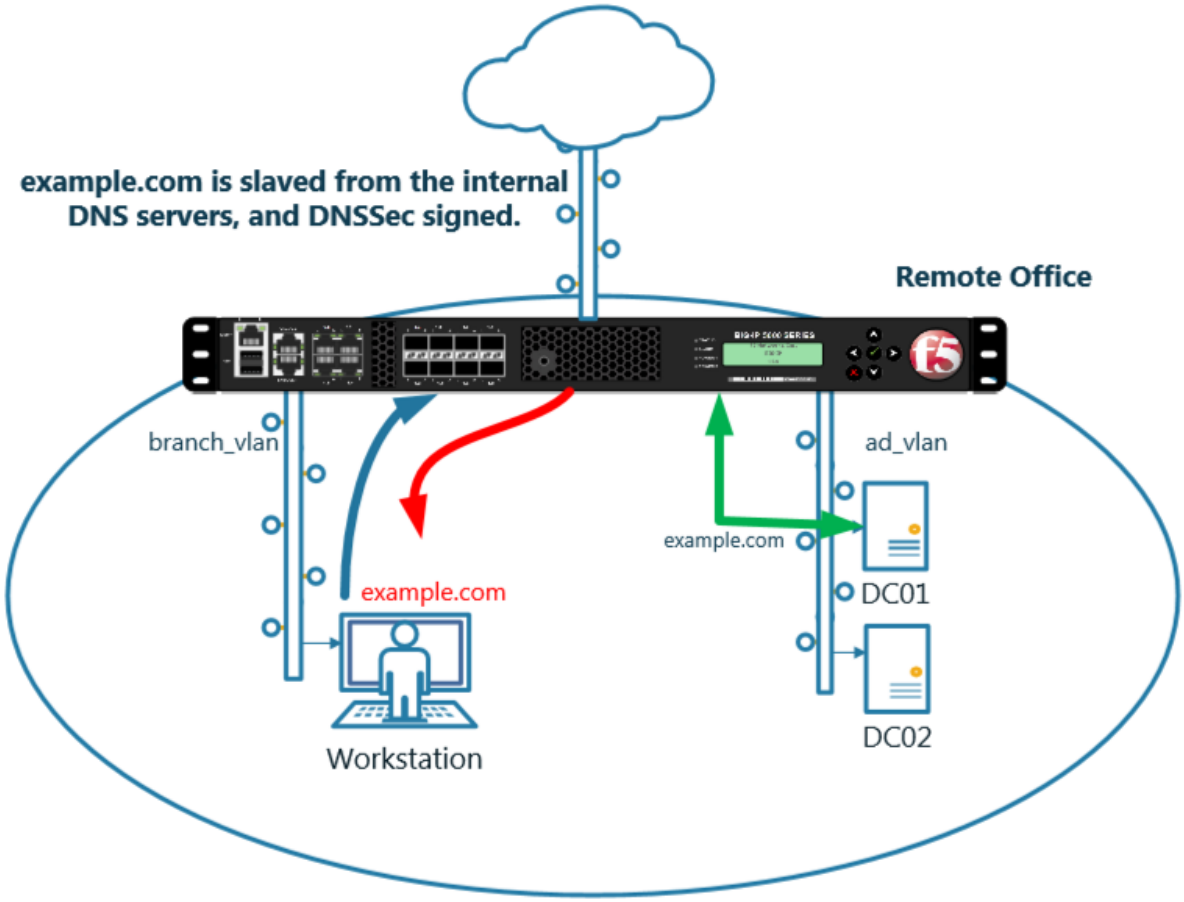
**TMSH**

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

---

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

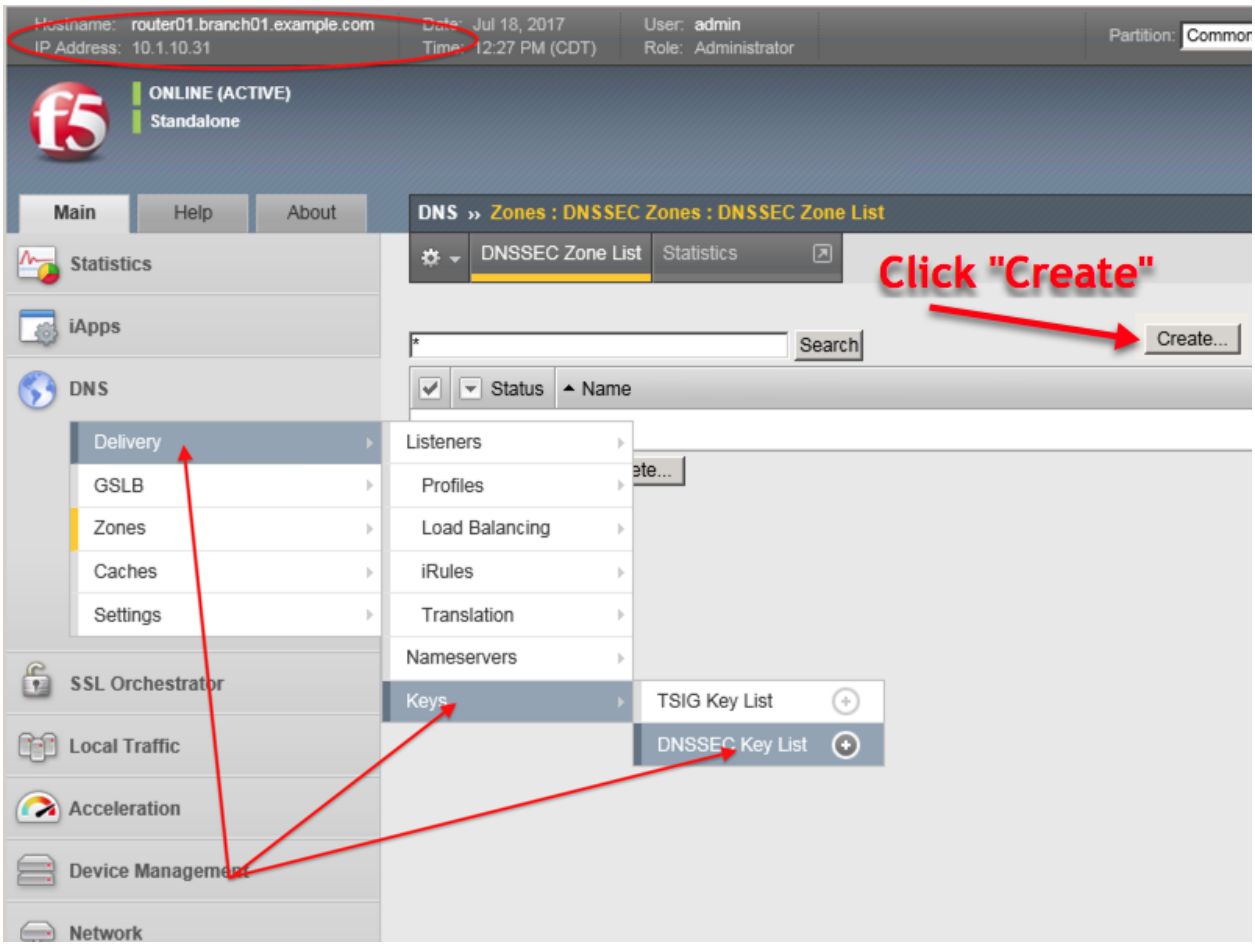
## 3.4 DNSSec




https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/dns-services-implementations-11-6-0/2.html#unique_1658664851

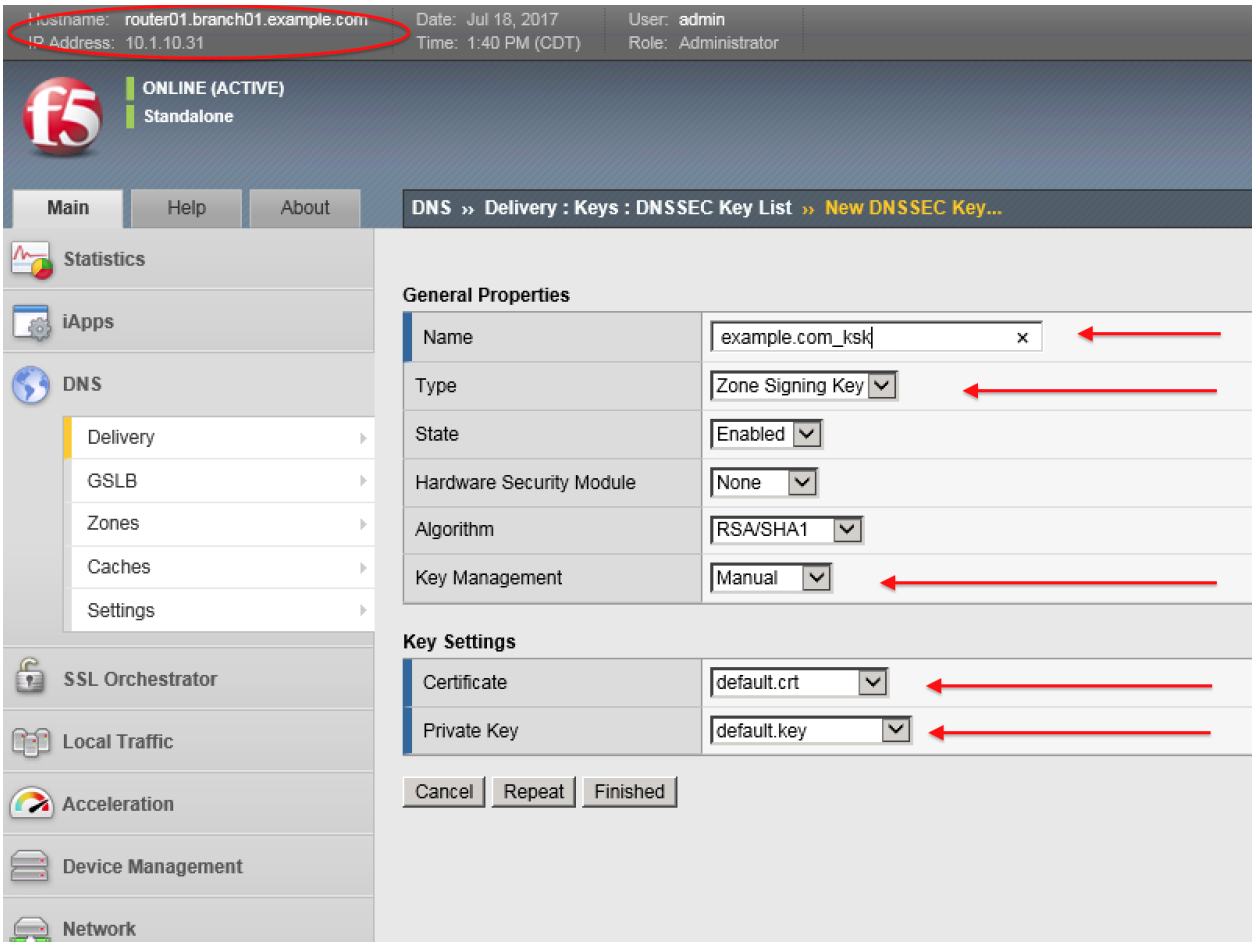
### 3.4.1 Zone Signing Key

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 |



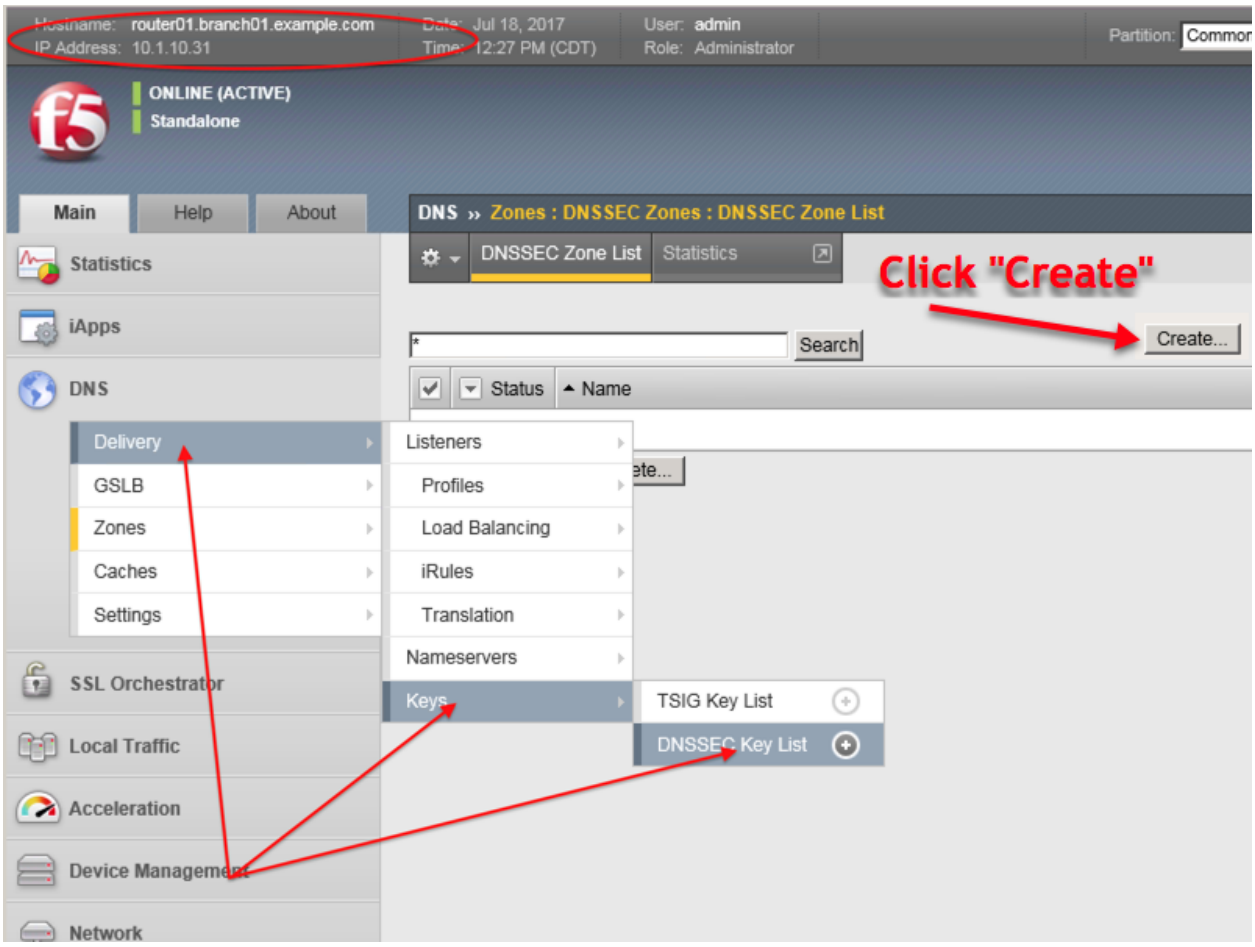

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/dnssec_key/create.jsp

**TMSH**

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

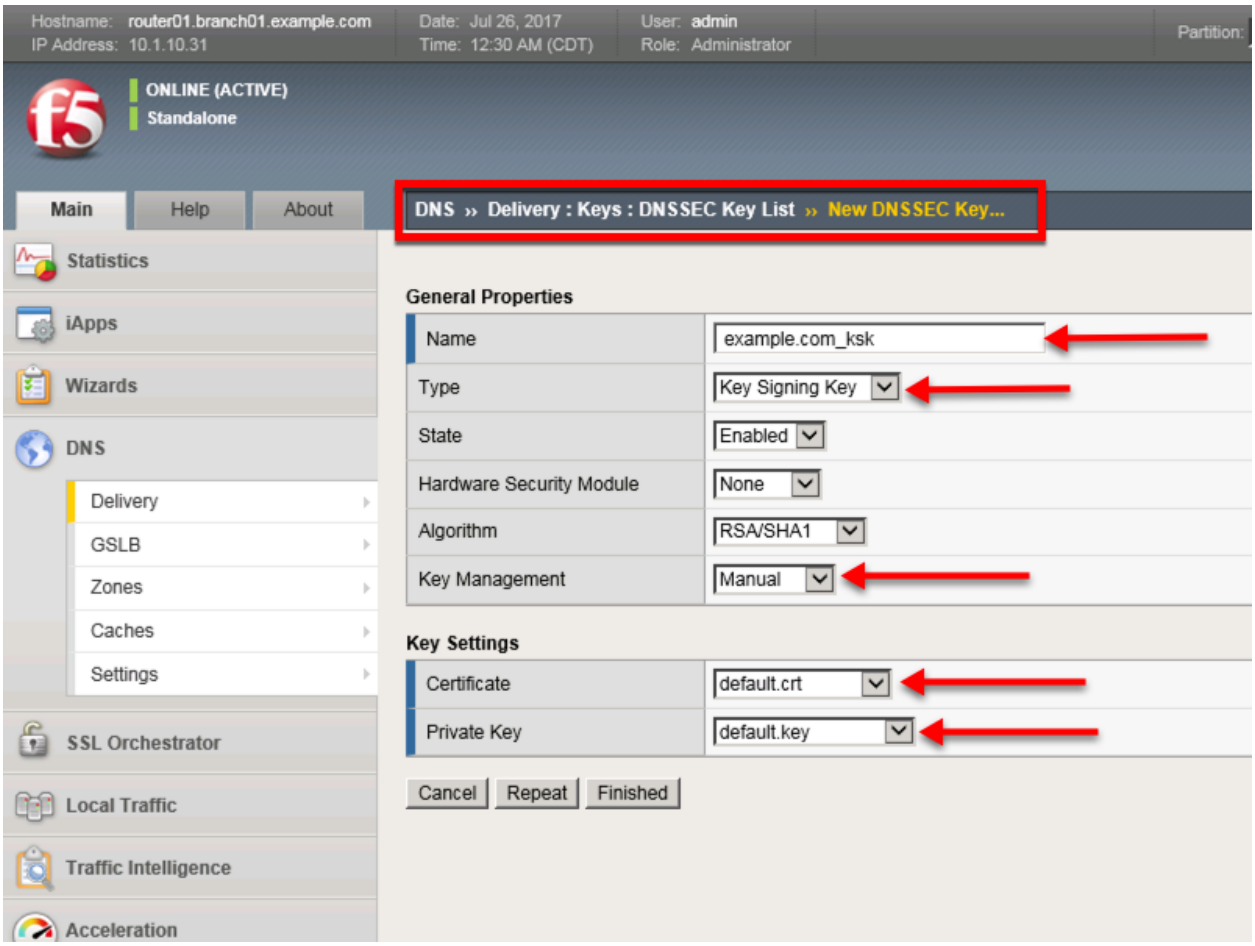
## 3.4.2 Key Signing Key

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 |




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

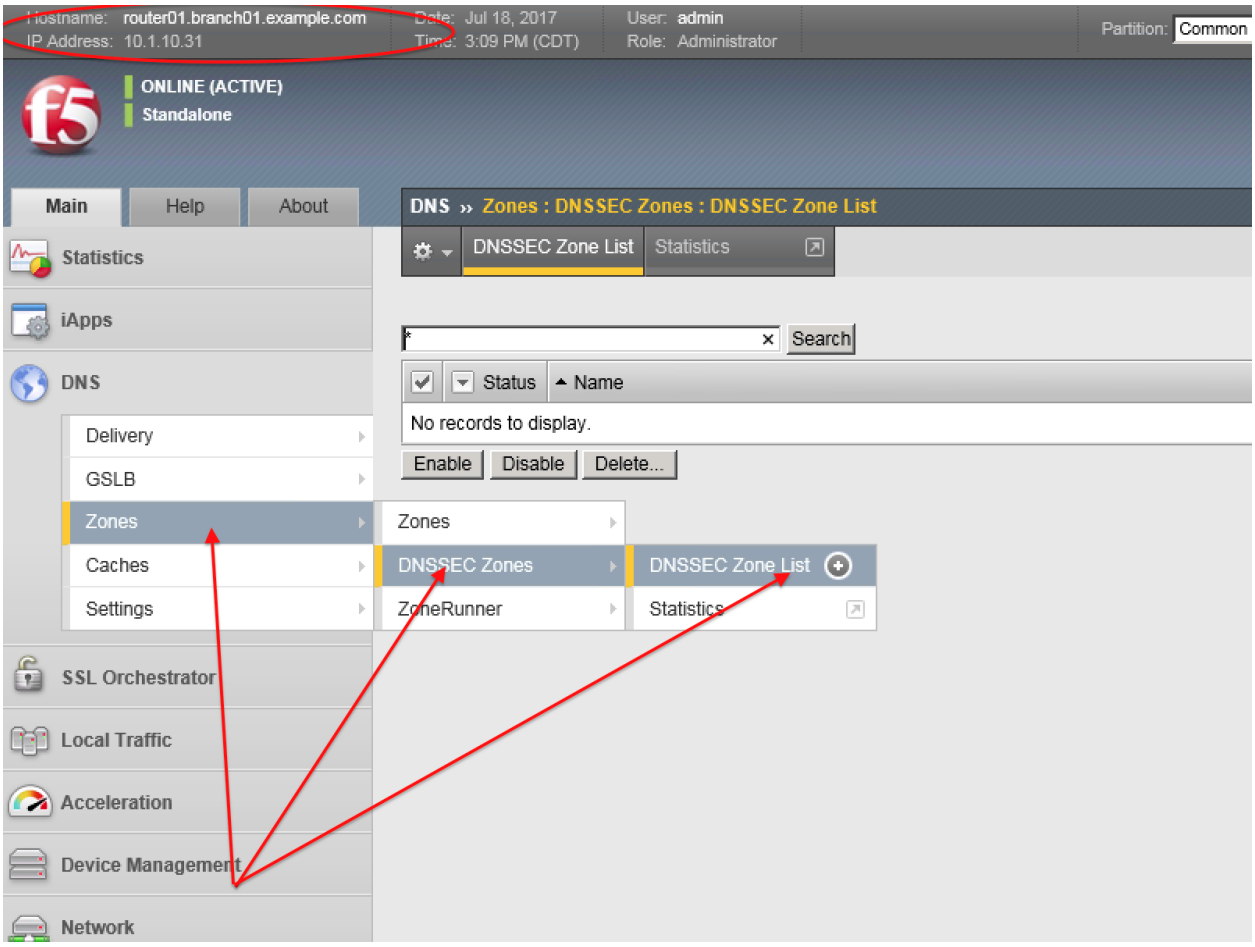
TMSH commands for Key Signing key creation:

**TMSH**

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

### 3.4.3 Signed Zone

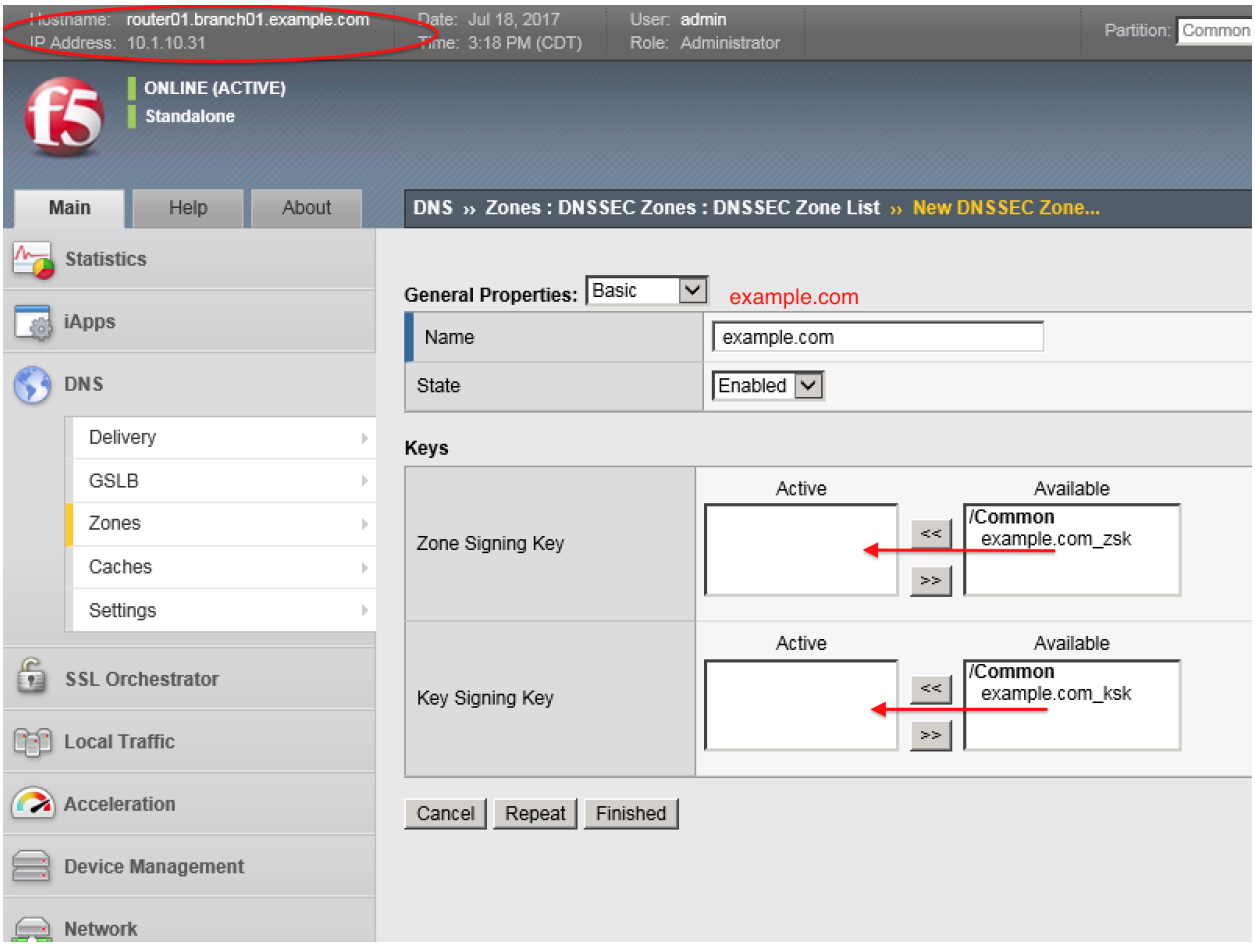
Navigate to: **DNS ›› Zones : DNSSEC Zones : DNSSEC Zone List**




https://router01.branch01.example.com/tmui/Control/form?__handler=/tmui/dns/dnssec_zone/list&__source=delete_confirm&__linked=false&__fromError=false

Create DNS Express zone signed by DNSSEC

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




TMSH commands for DNSSEC signed zone creation:

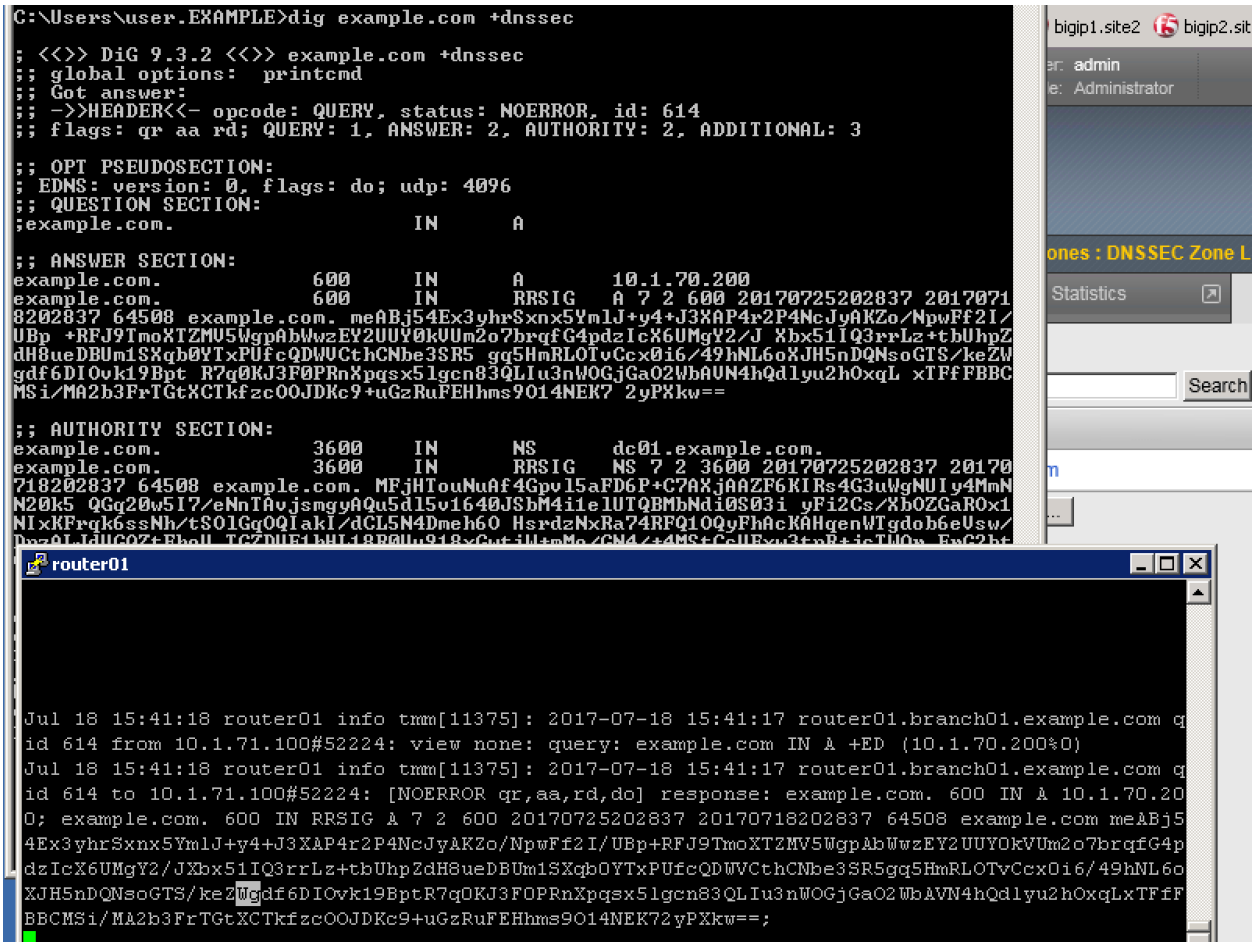
**TMSH**

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

### 3.4.4 Results

From the CLI on the router01.branch01 BIGIP run tail -f /var/log/ltm

From the Workstation CMD prompt run: “dig example.com +dnssec”




## 3.5 Validating Resolver

### 3.5.1 Trust Anchors

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

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

---

**TMSH**

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

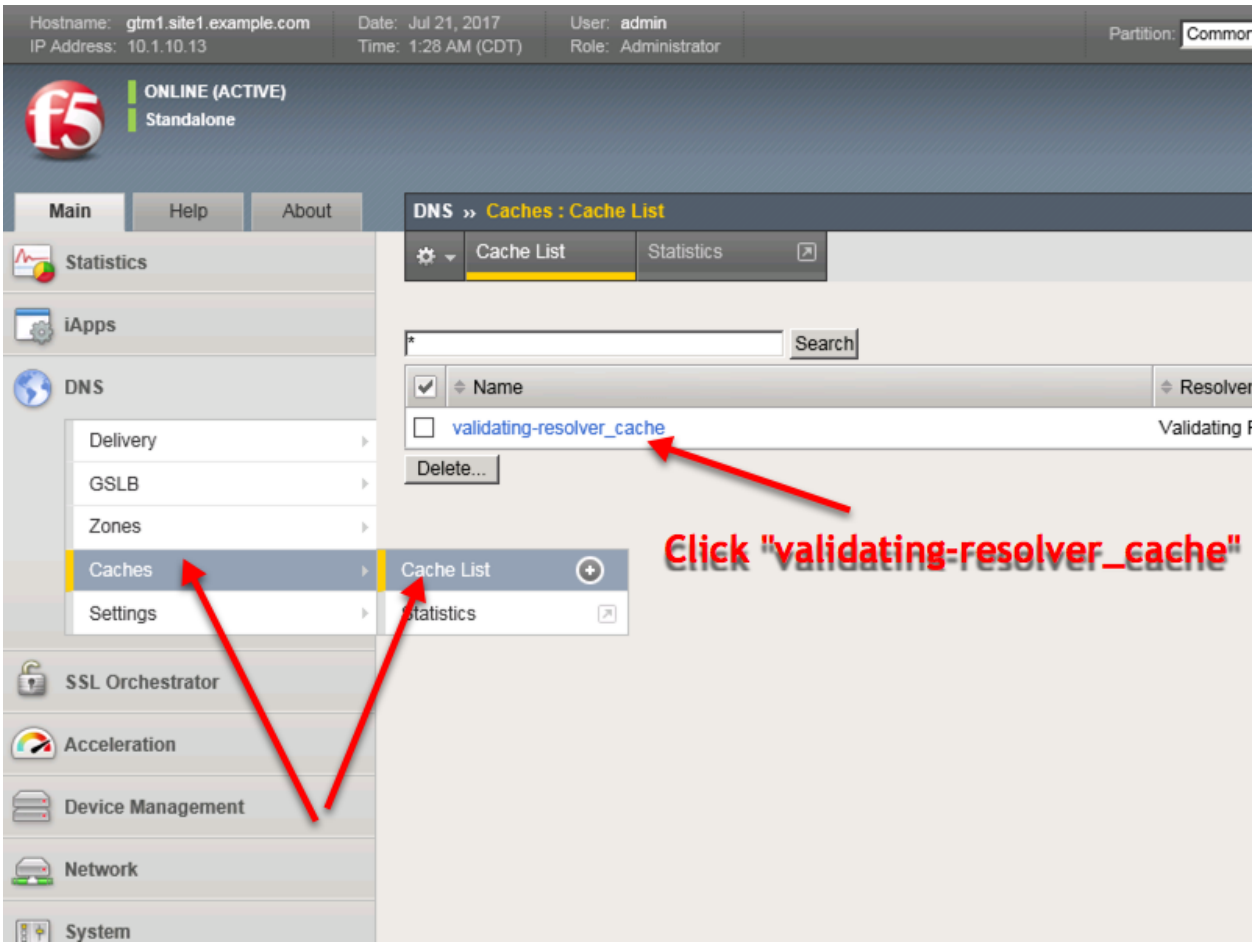
dnssec-dsfromkey -f /root/dnskey.txt .

---

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

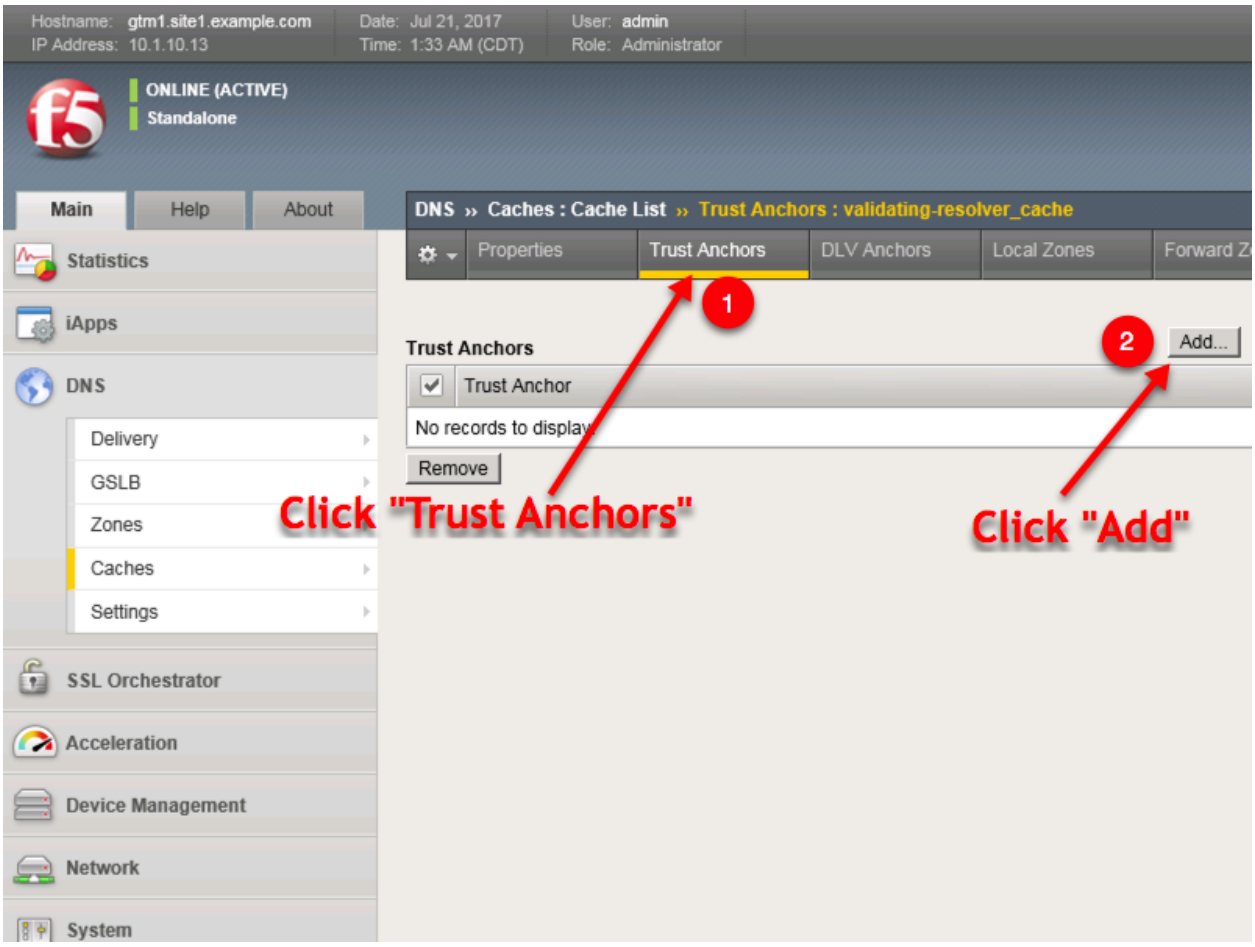
Navigate to: **DNS ›› Caches : Cache List ›› validating-resolver_cache : Trust Anchors**

Select the validating-resolver_cache and click “Trust Anchors”

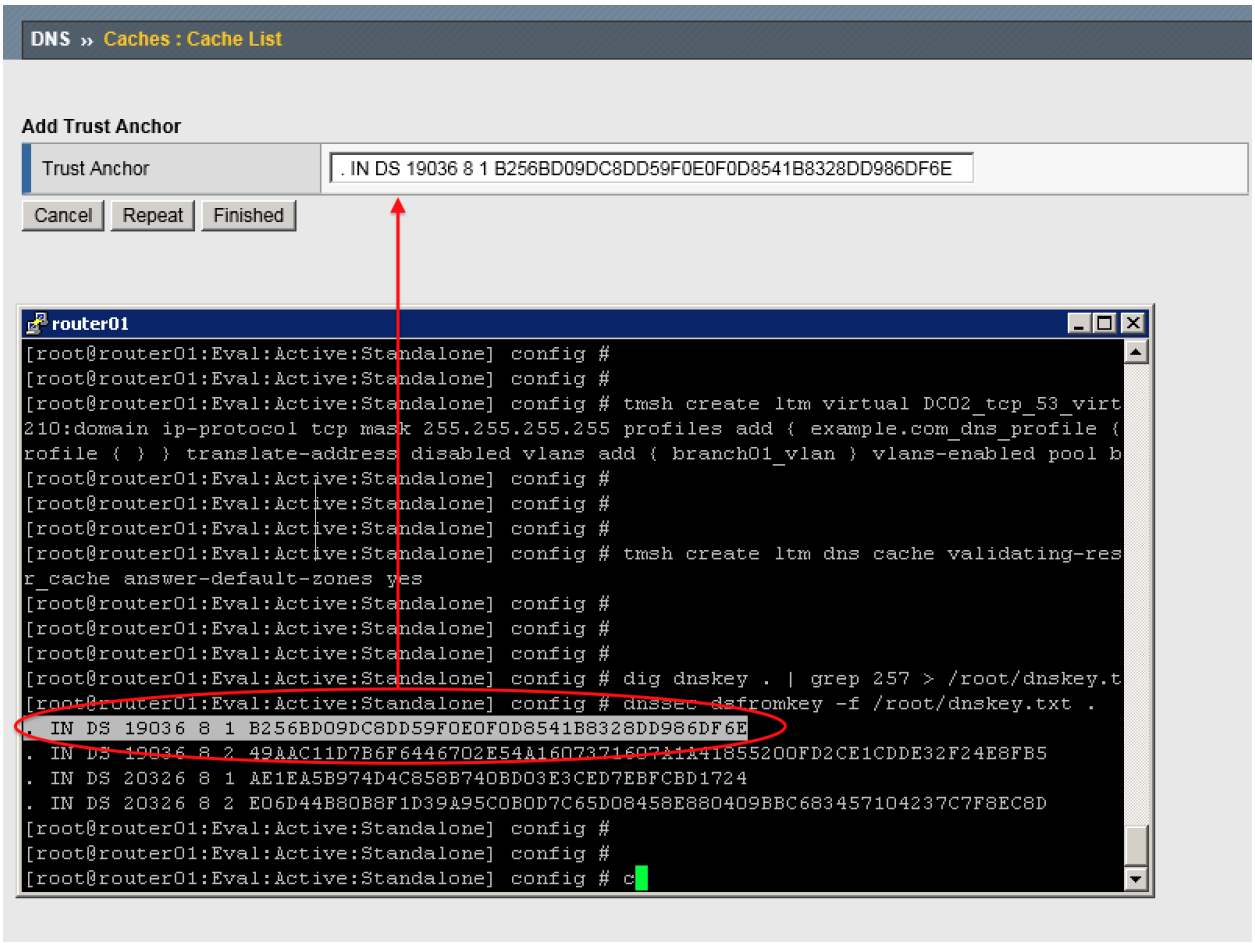


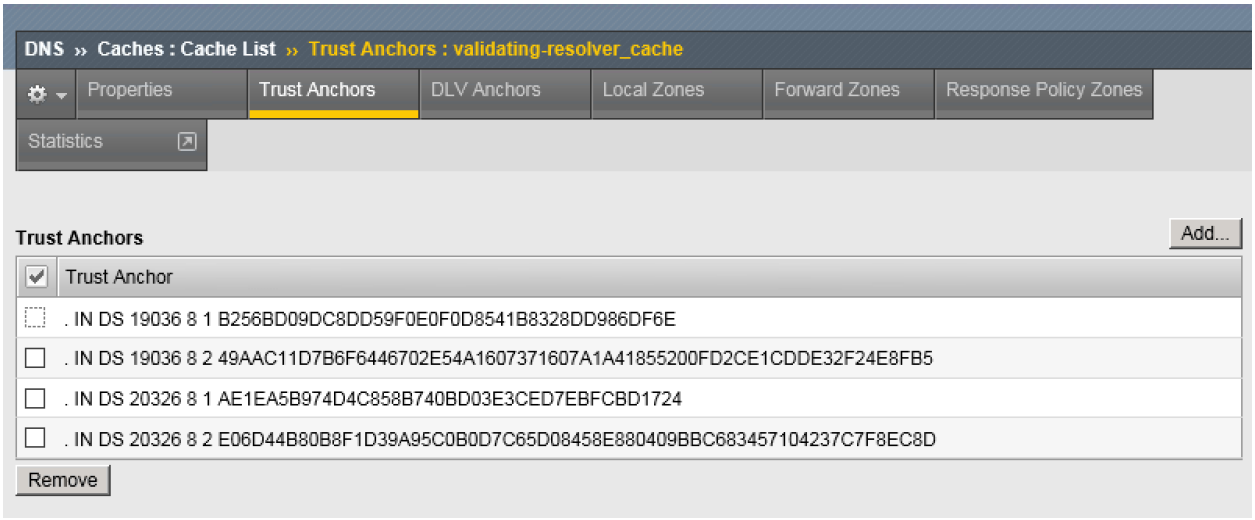

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/trust_anchor/list.jsp?name=

%2FCommon%2Fvalidating-resolver_cache&tab=dns_cache_validating_config




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




```
tmsh modify ltm dns cache validating-resolver validating-resolver_cache trust-anchors␣
↪replace-all-with { ". IN DS 19036 8 1 B256BD09DC8DD59F0E0F0D8541B8328DD986DF6E" ".␣
↪IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5" ".
↪ IN DS 20326 8 1 AE1EA5B974D4C858B740BD03E3CED7EBFCBD1724" ". IN DS 20326 8 2␣
↪E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D" }
```

### 3.5.2 DLV Anchors

To cache a validated response for the signed zones, you need to obtain a trust and DLV anchor.

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

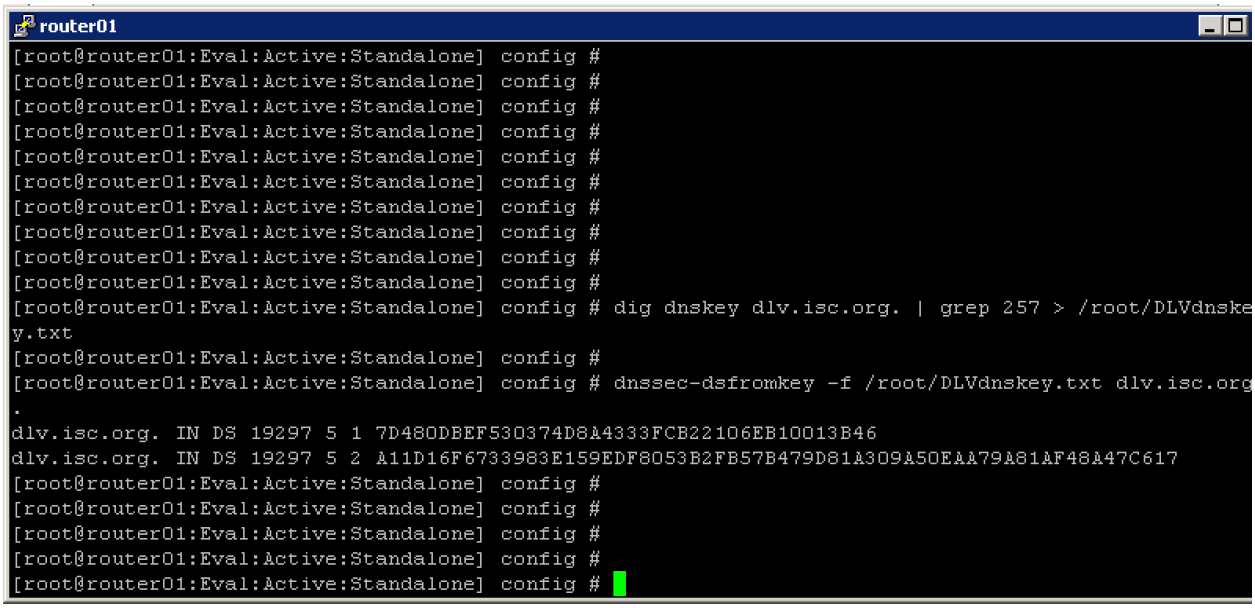
---

**TMSH**

dig dnskey dlv.isc.org. | grep 257 > /root/DLVdnskey.txt

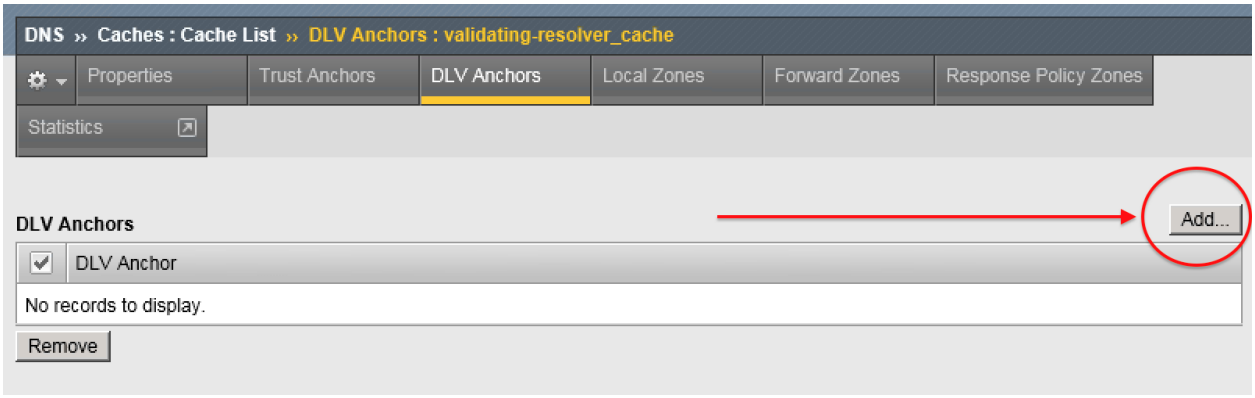
dnssec-dsfromkey -f /root/DLVdnskey.txt dlv.isc.org.

---

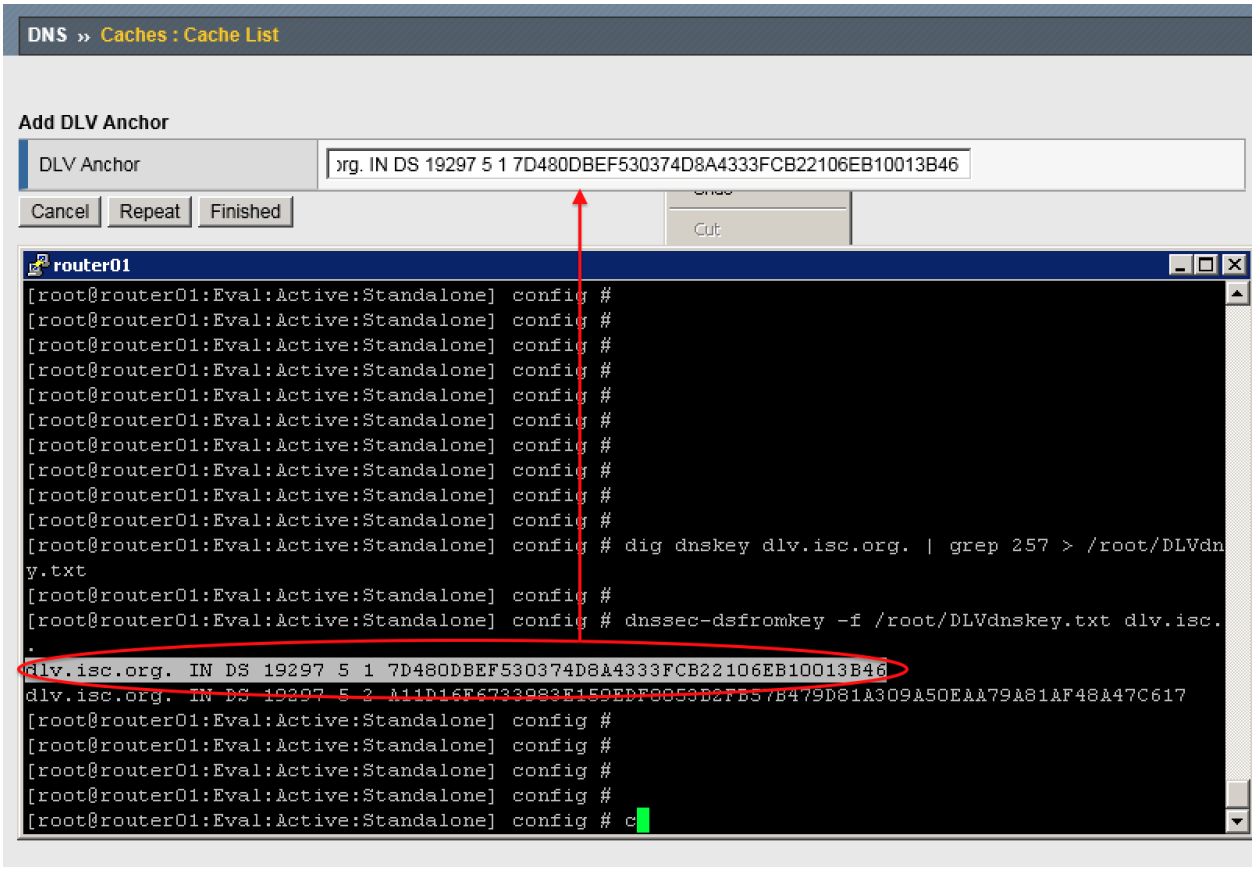


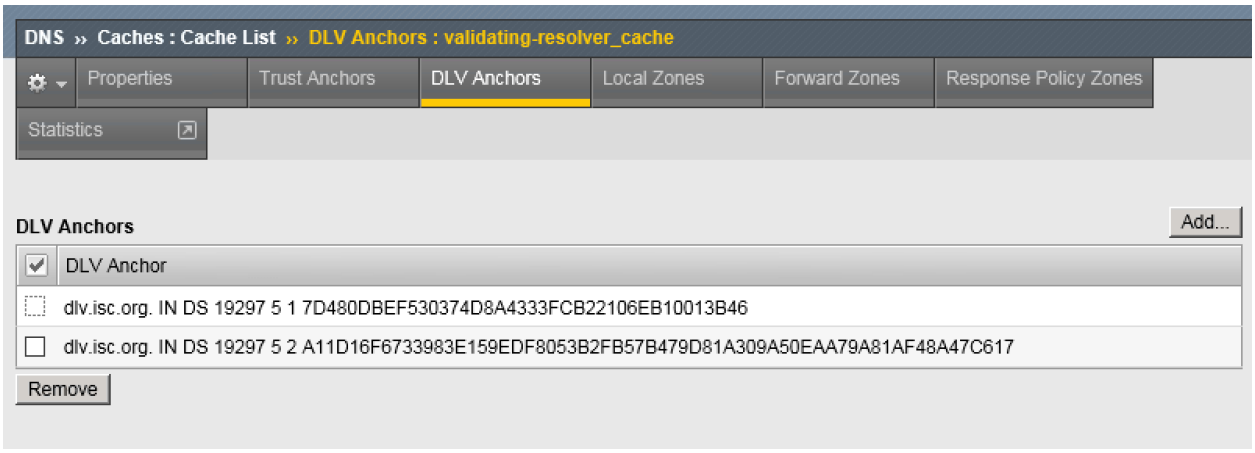

Navigate to: **DNS ›› Caches : Cache List ›› validating-resolver_cache : DLV Anchors**

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/trust_anchor/list.jsp?name=%2FCommon%2Fvalidating-resolver_cache&tab=dns_cache_validating_config




For each line of output from the preceding command create a “DLV Anchor”



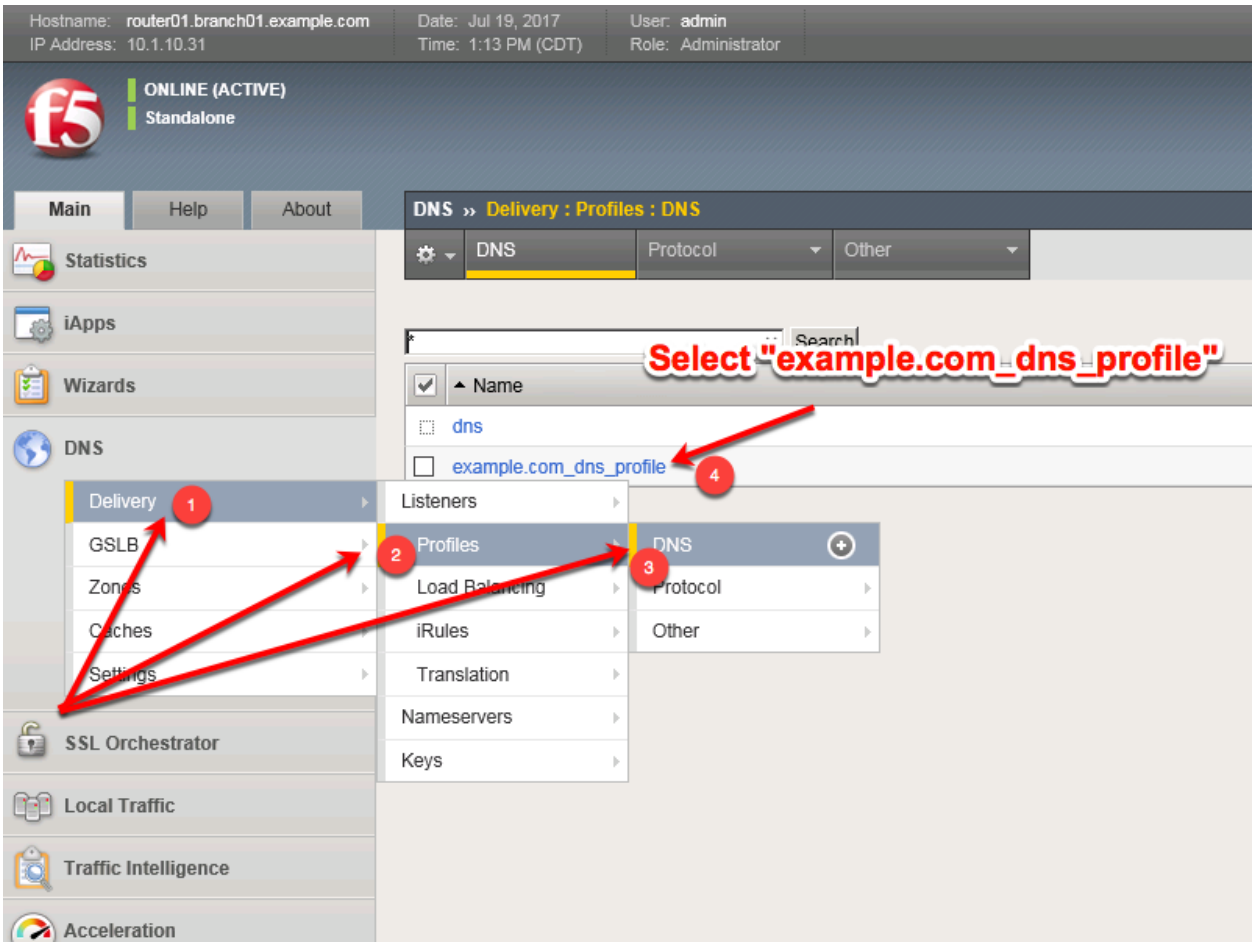




```
tmsh modify ltm dns cache validating-resolver validating-resolver_cache dlv-anchors␣
↪replace-all-with { "dlv.isc.org. IN DS 19297 5 1␣
↪7D480DBEF530374D8A4333FCB22106EB10013B46" "dlv.isc.org. IN DS 19297 5 2␣
↪A11D16F6733983E159EDF8053B2FB57B479D81A309A50EAA79A81AF48A47C617" }
```

### 3.5.3 Modify DNS Profile

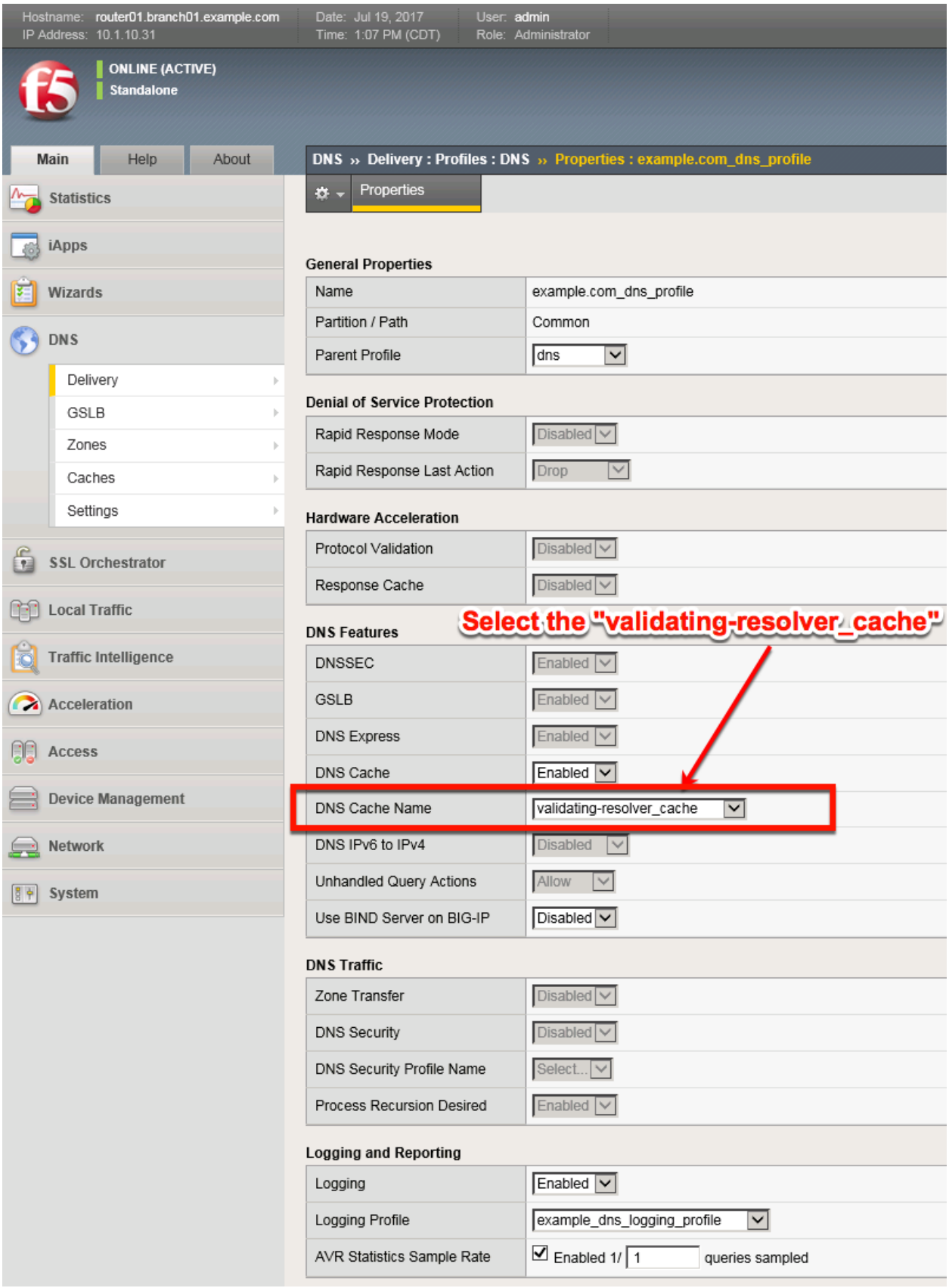
In order to activate the new “Validating Resolver”, modify the DNS profile example.com_dns_profile.

Navigate to: **DNS ›› Delivery : Profiles : DNS**




Select the profile “example.com_dns_profile”

Modify the DNS profile to activate the new validating-resolver_cache.


Hostname: router01.branch01.example.com
IP Address: 10.1.10.31
Date: Jul 19, 2017
Time: 1:07 PM (CDT)
User: admin
Role: Administrator
ONLINE (ACTIVE)
Standalone
Main
Help
About
DNS » Delivery : Profiles : DNS » Properties : example.com_dns_profile
Statistics
iApps
Wizards
DNS
Delivery
GSLB
Zones
Caches
Settings
SSL Orchestrator
Local Traffic
Traffic Intelligence
Acceleration
Access
Device Management
Network
System
Properties
General Properties
Name
example.com_dns_profile
Partition / Path
Common
Parent Profile
dns
Denial of Service Protection
Rapid Response Mode
Disabled
Rapid Response Last Action
Drop
Hardware Acceleration
Protocol Validation
Disabled
Response Cache
Disabled
DNS Features
Select the "validating-resolver_cache"
DNSSEC
Enabled
GSLB
Enabled
DNS Express
Enabled
DNS Cache
Enabled
DNS Cache Name
validating-resolver_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

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

**TMSH**

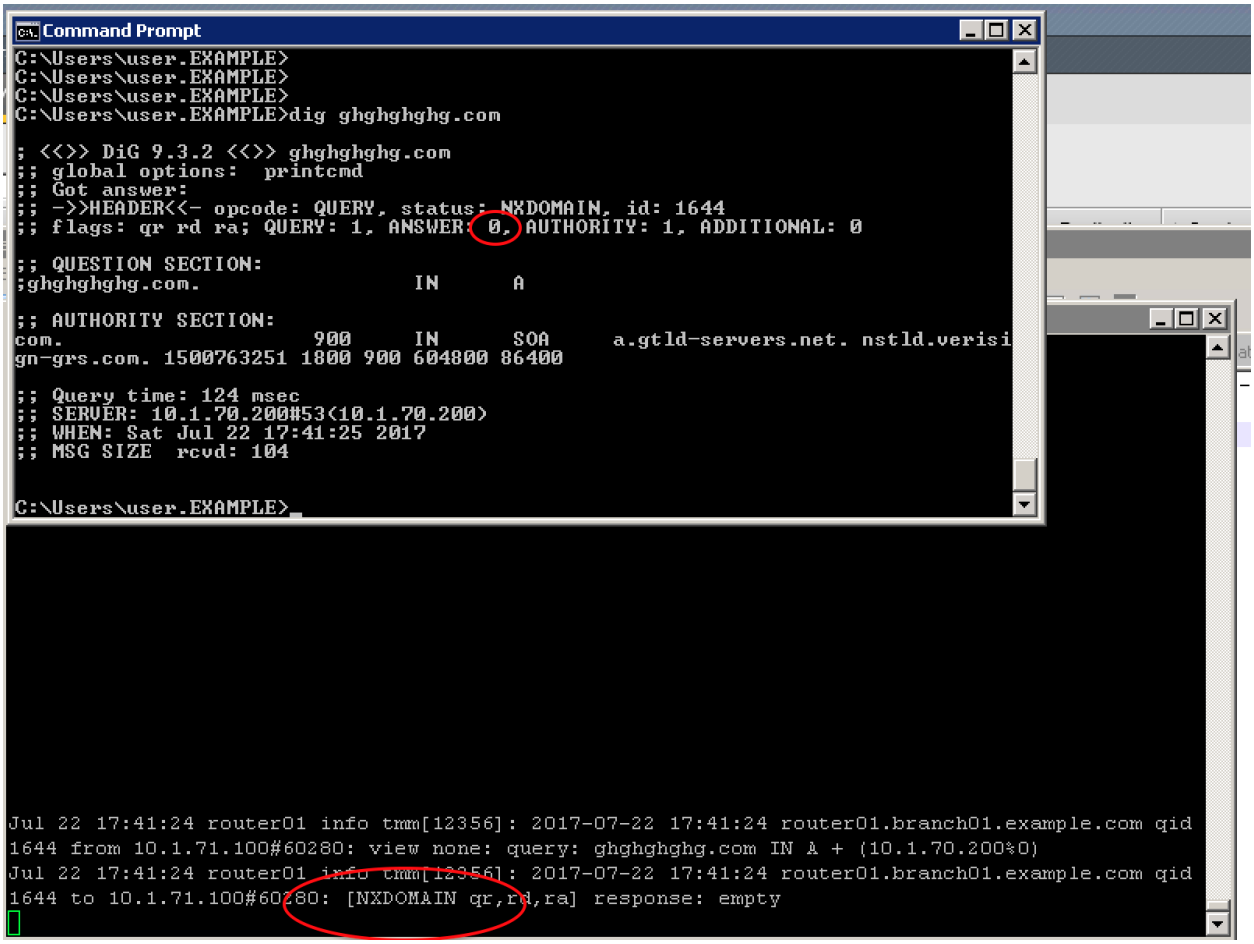
tmsh modify ltm profile dns example.com_dns_profile cache validating-resolver_cache

### 3.5.4 Results

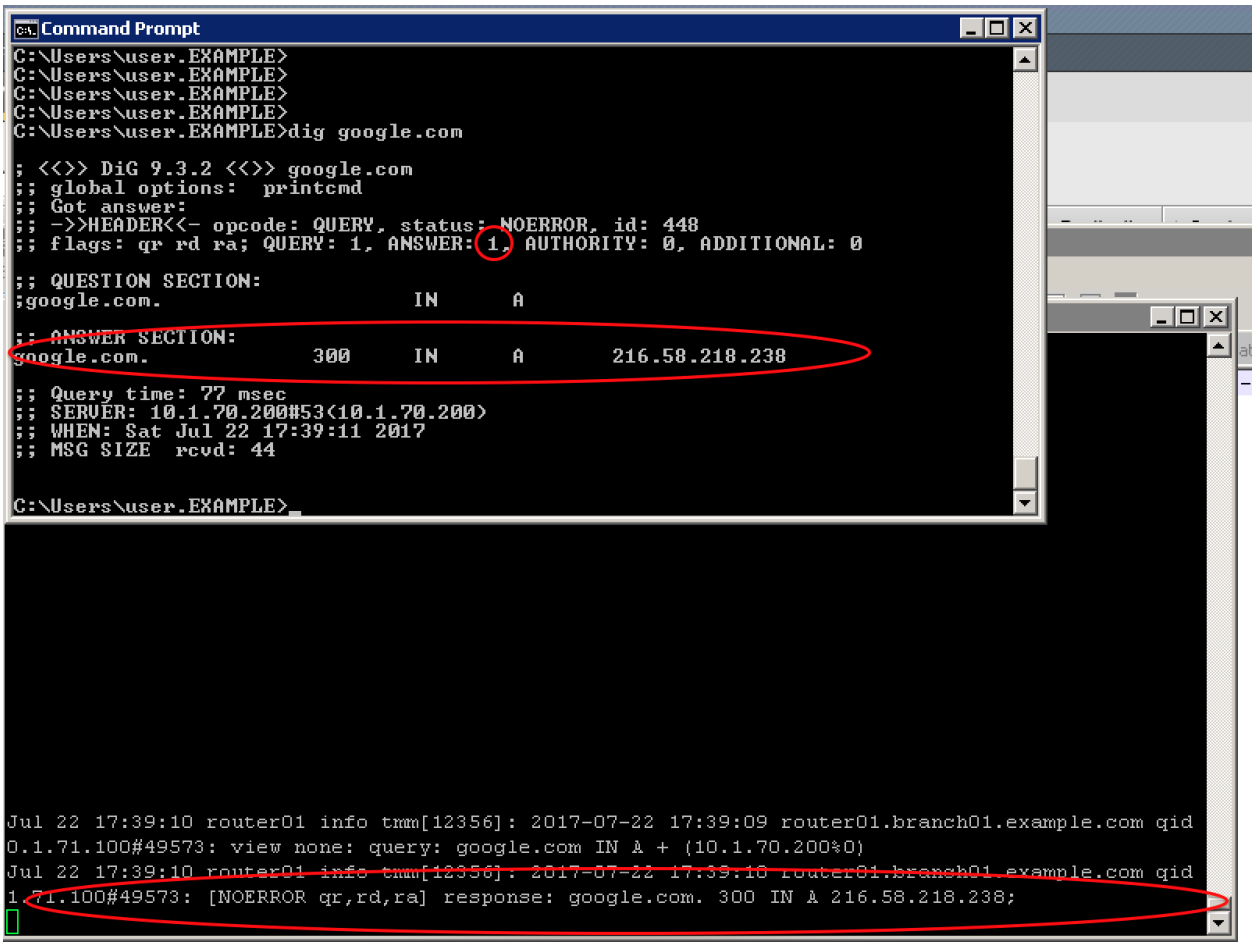
From the CLI on the router01.branch01 BIGIP run

tail -f /var/log/ltm

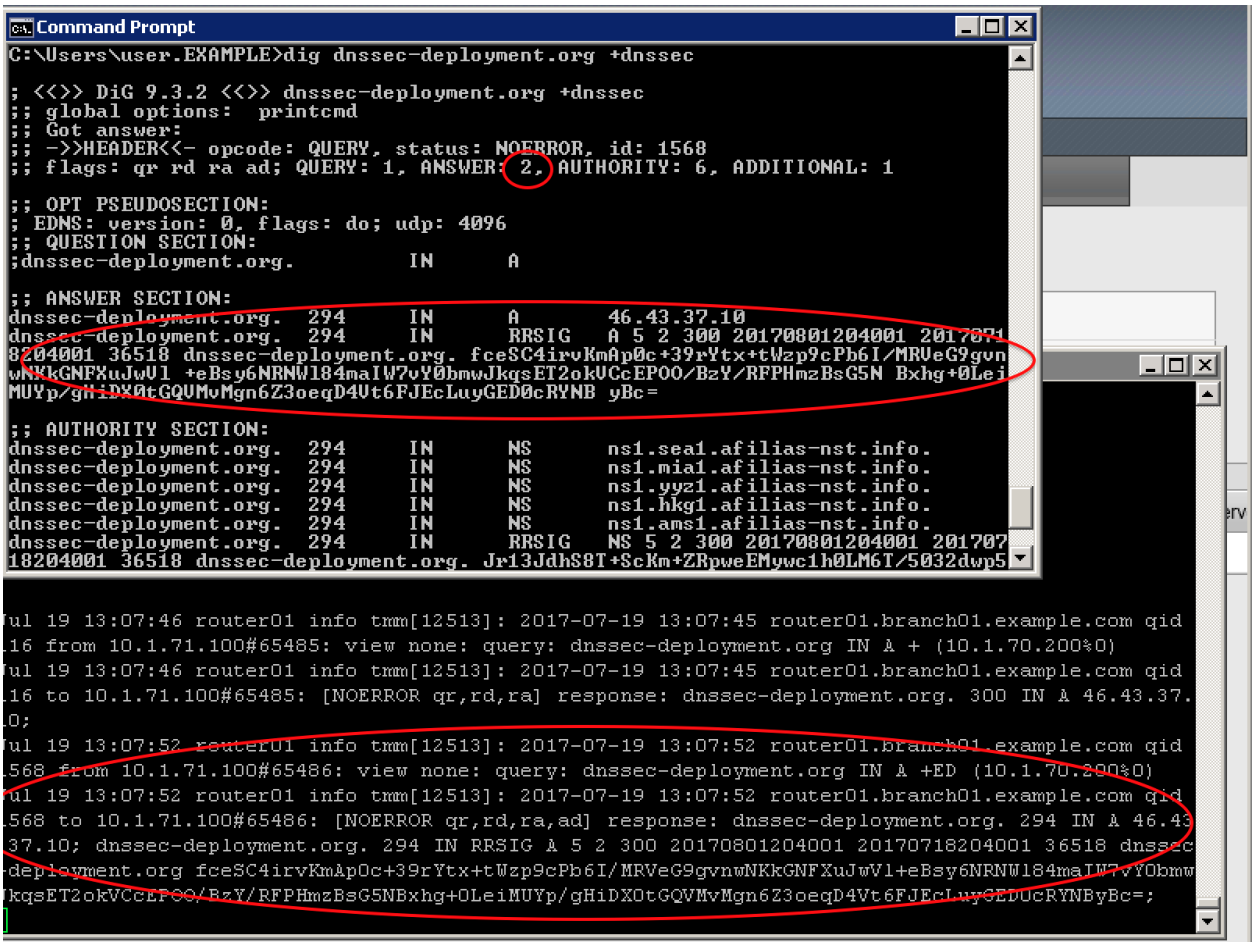
From the Workstation CMD prompt run: “dig ghghghghg.com”



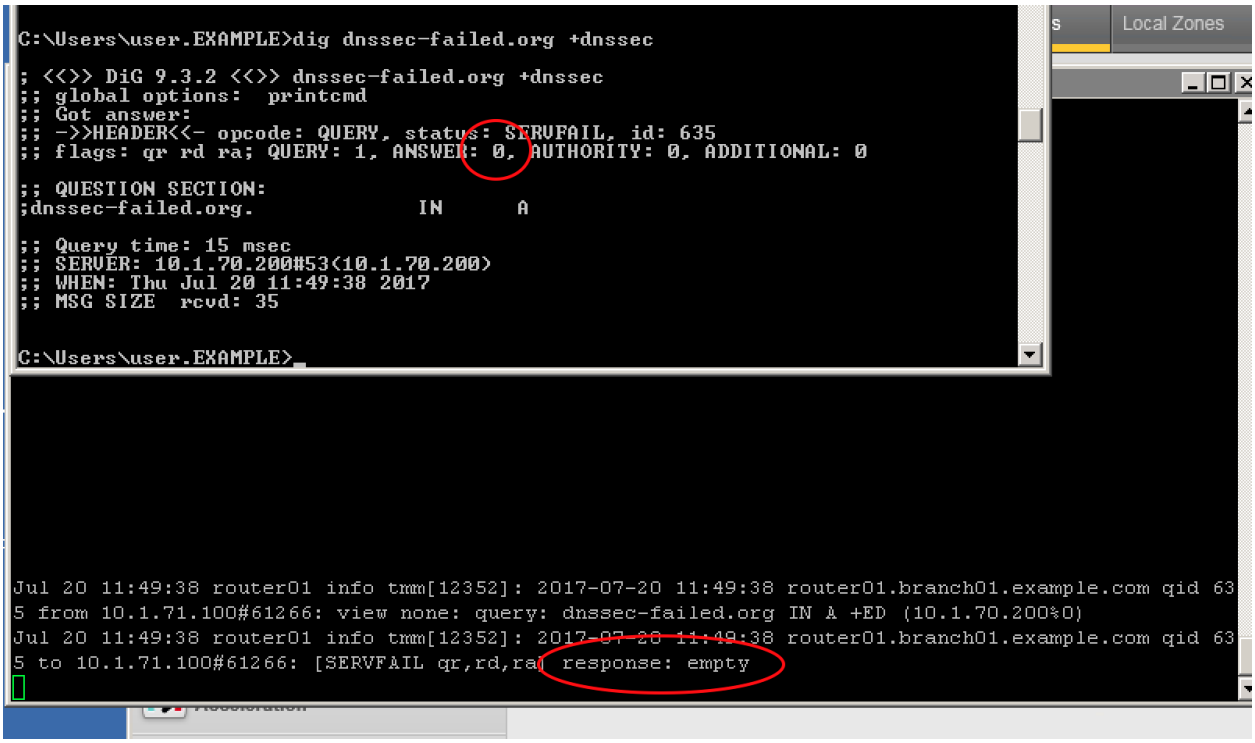

From the Workstation CMD prompt run: “dig google.com”




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



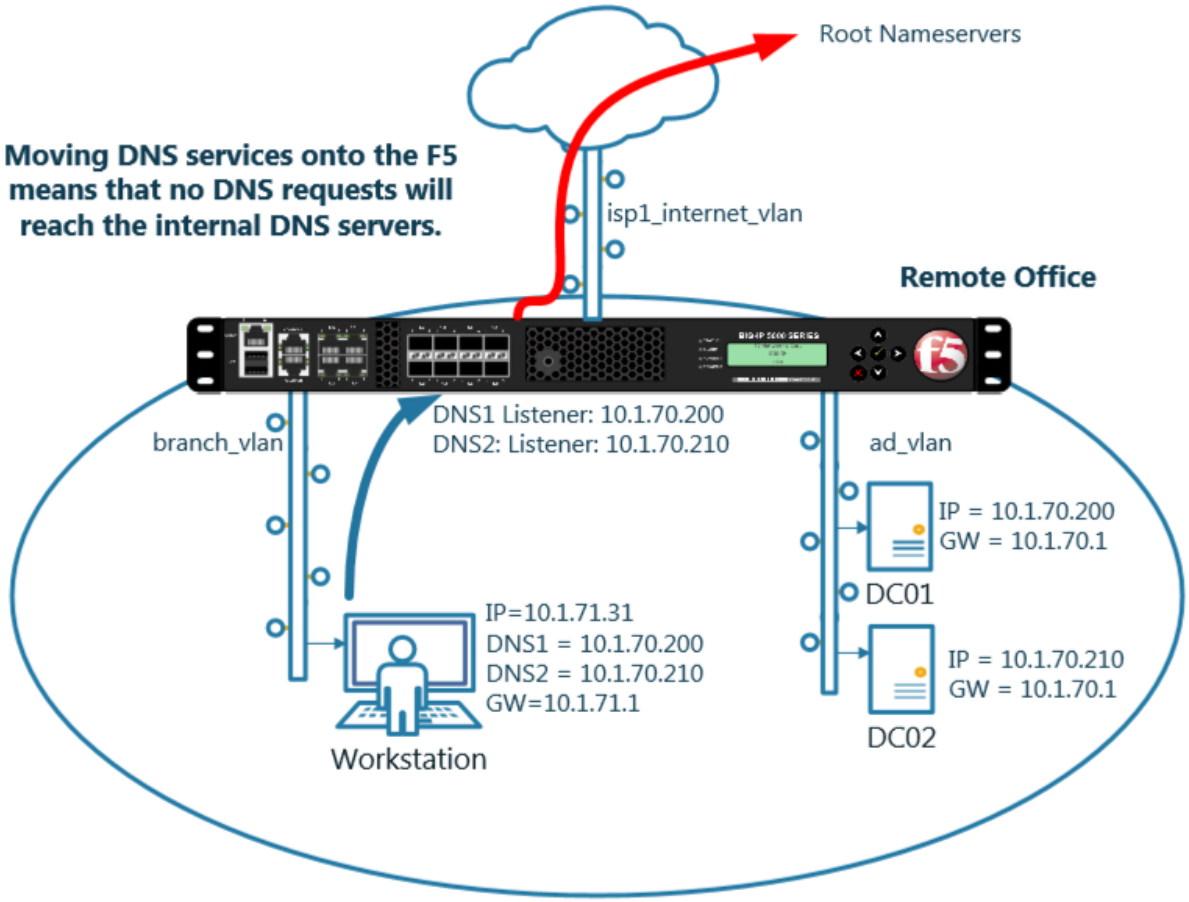

From the Workstation CMD prompt run: “dig dnssec-failed.org +dnssec”

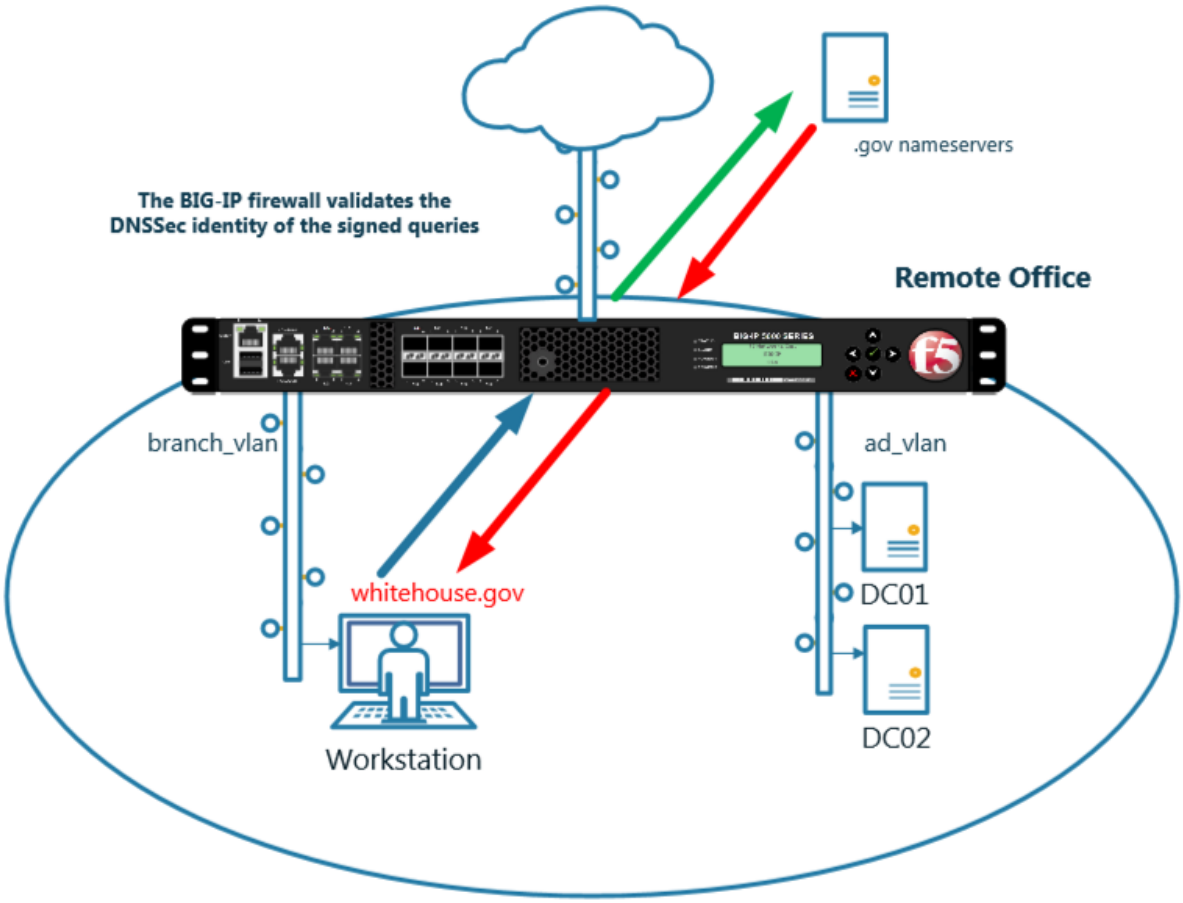



http://www.internetsociety.org/deploy360/resources/dnssec-test-sites/

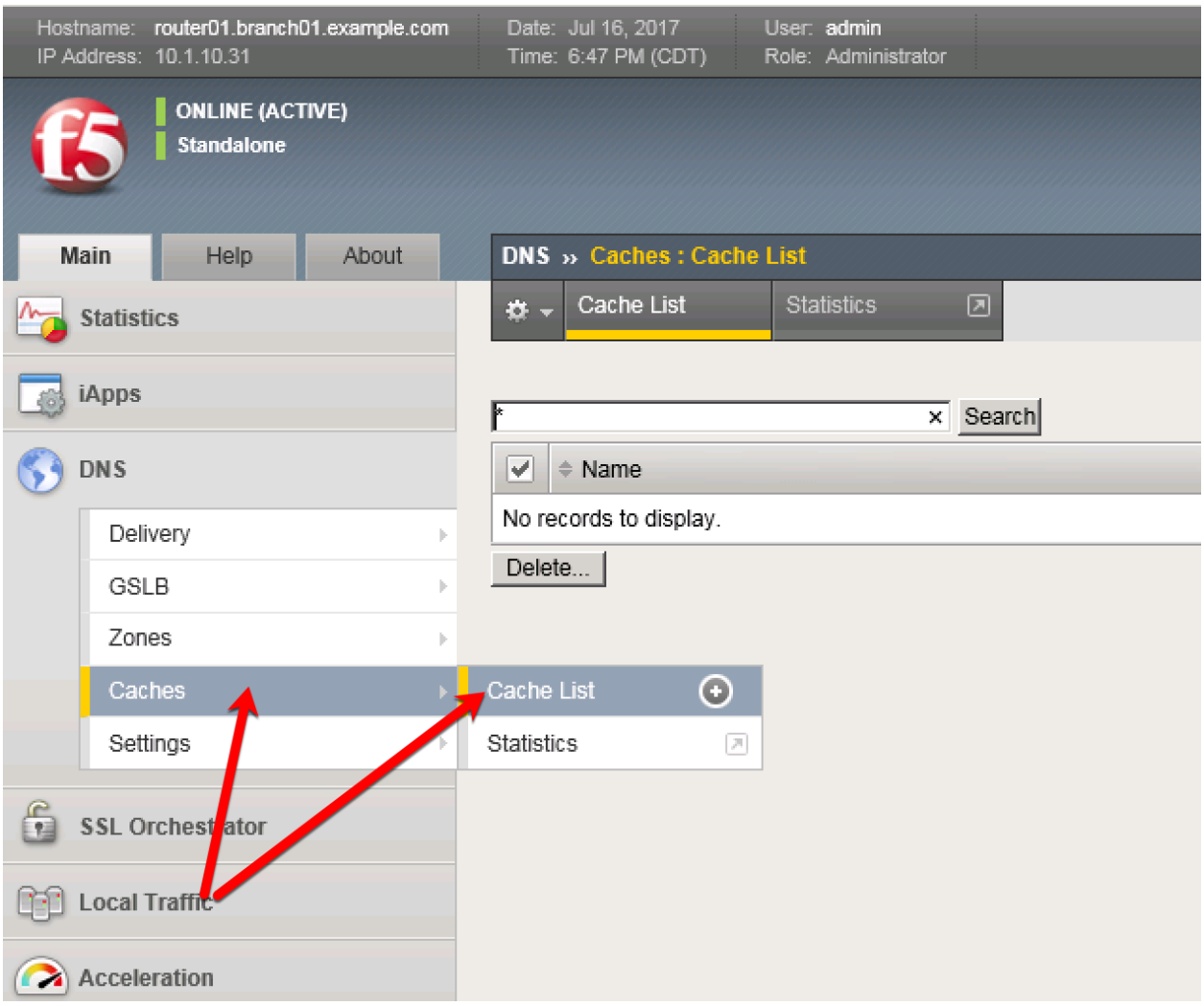
Configure a validating resolver cache on the BIG-IP® system to recursively query public DNS servers, validate the identity of the DNS server sending the responses, and then cache the responses.

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


Root Nameservers
Moving DNS services onto the F5 means that no DNS requests will reach the internal DNS servers.
isp1_internet_vlan
Remote Office
DNS1 Listener: 10.1.70.200
DNS2: Listener: 10.1.70.210
branch_vlan
ad_vlan
IP = 10.1.70.200
GW = 10.1.70.1
DC01
IP=10.1.71.31
DNS1 = 10.1.70.200
DNS2 = 10.1.70.210
GW=10.1.71.1
IP = 10.1.70.210
GW = 10.1.70.1
DC02
Workstation




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




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

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 | validating-resolver_cache |
| Resolver Type | Validating Resolver |
| Route Domain Name | 0 |

**DNS Cache**

| | |
|---|---|
| Message Cache Size | 1048576 bytes |
| Resource Record Cache Size | 10485760 bytes |
| Name Server Cache Count | 16536 entries |
| DNSSEC Key Cache Size | 1048576 bytes |
| Answer Default Zones | ☑ Enabled |
| RRSet Rotate | none |

**DNS Resolver**

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

**DNSSEC Validator**

| | |
|---|---|
| Prefetch Key | ☑ Enabled |

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

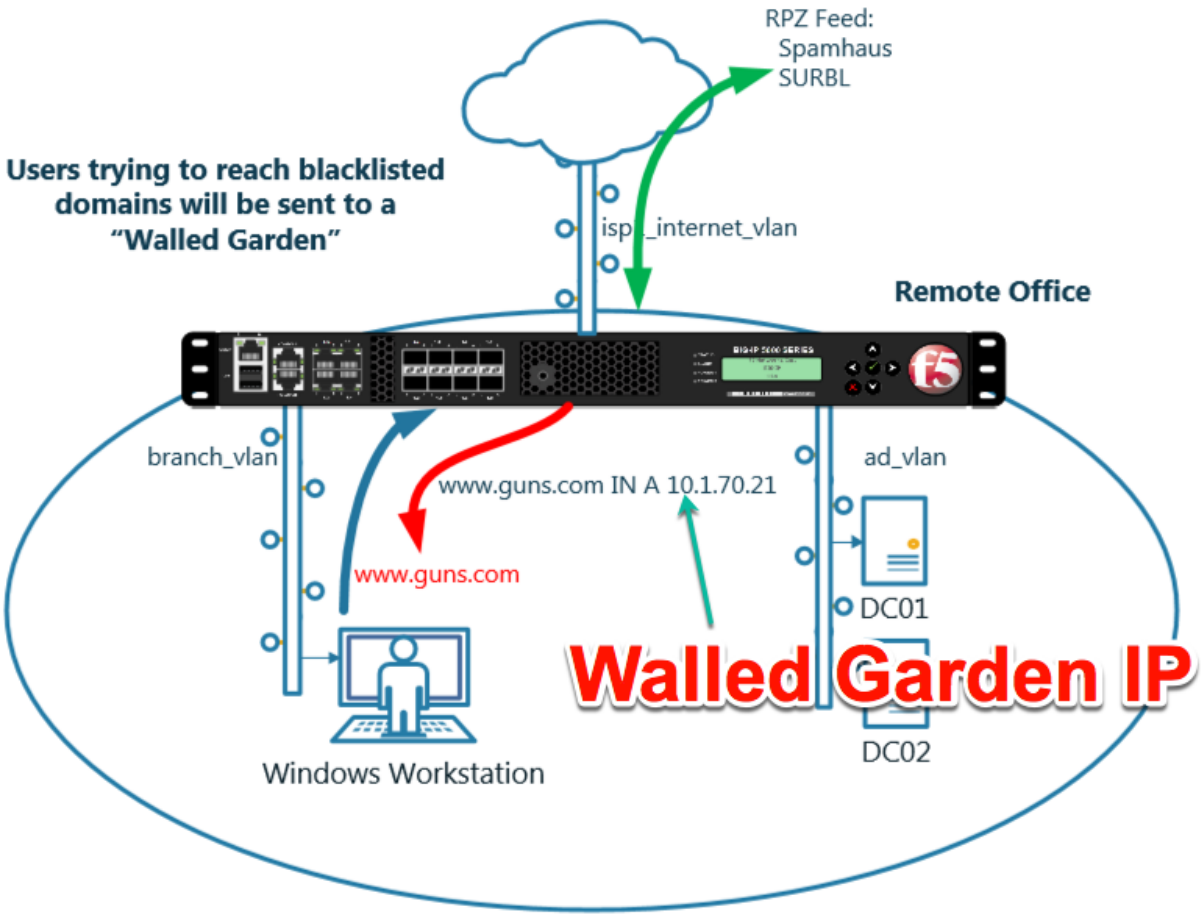
**TMSH**

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

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

## 3.6 RPZ

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




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

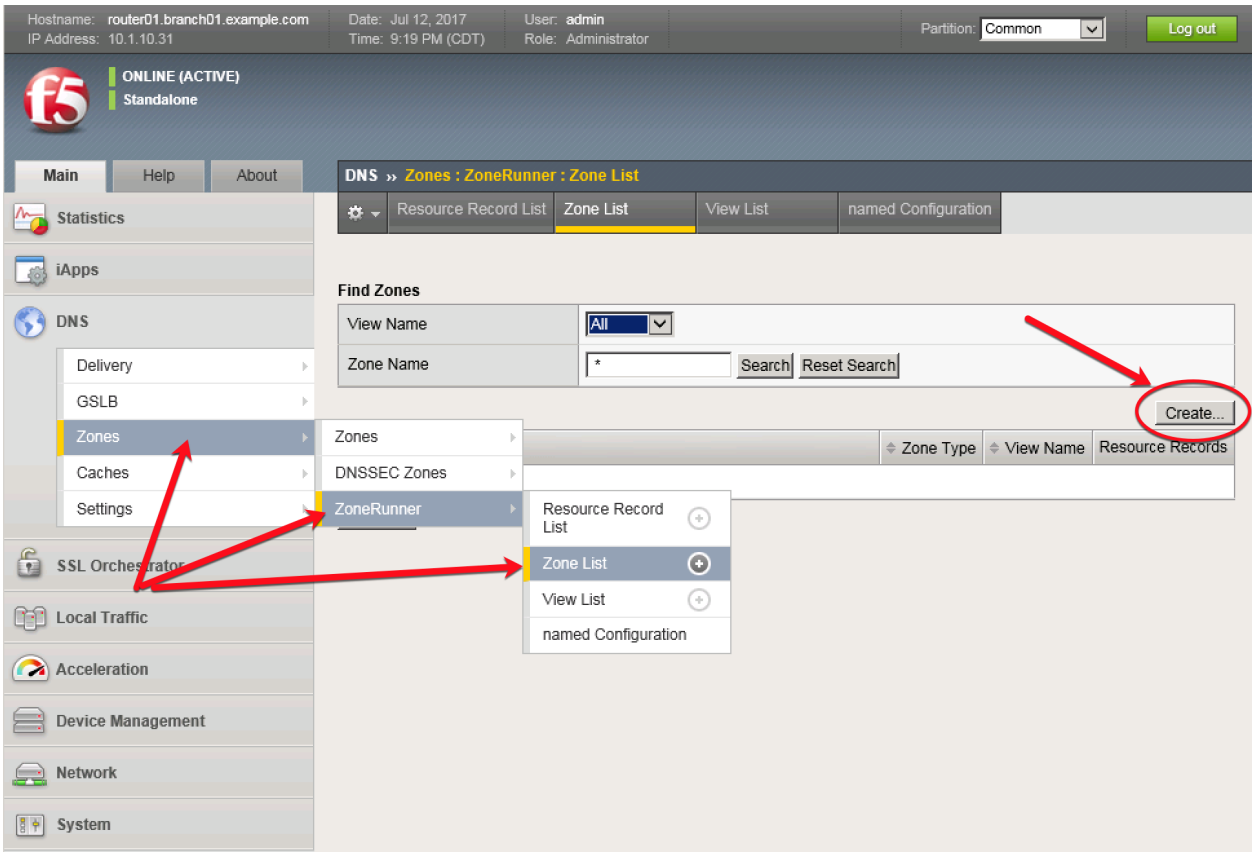
### 3.6.1 Zone Runner

Customers will subscribe to their RPZ vendor of choice.

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

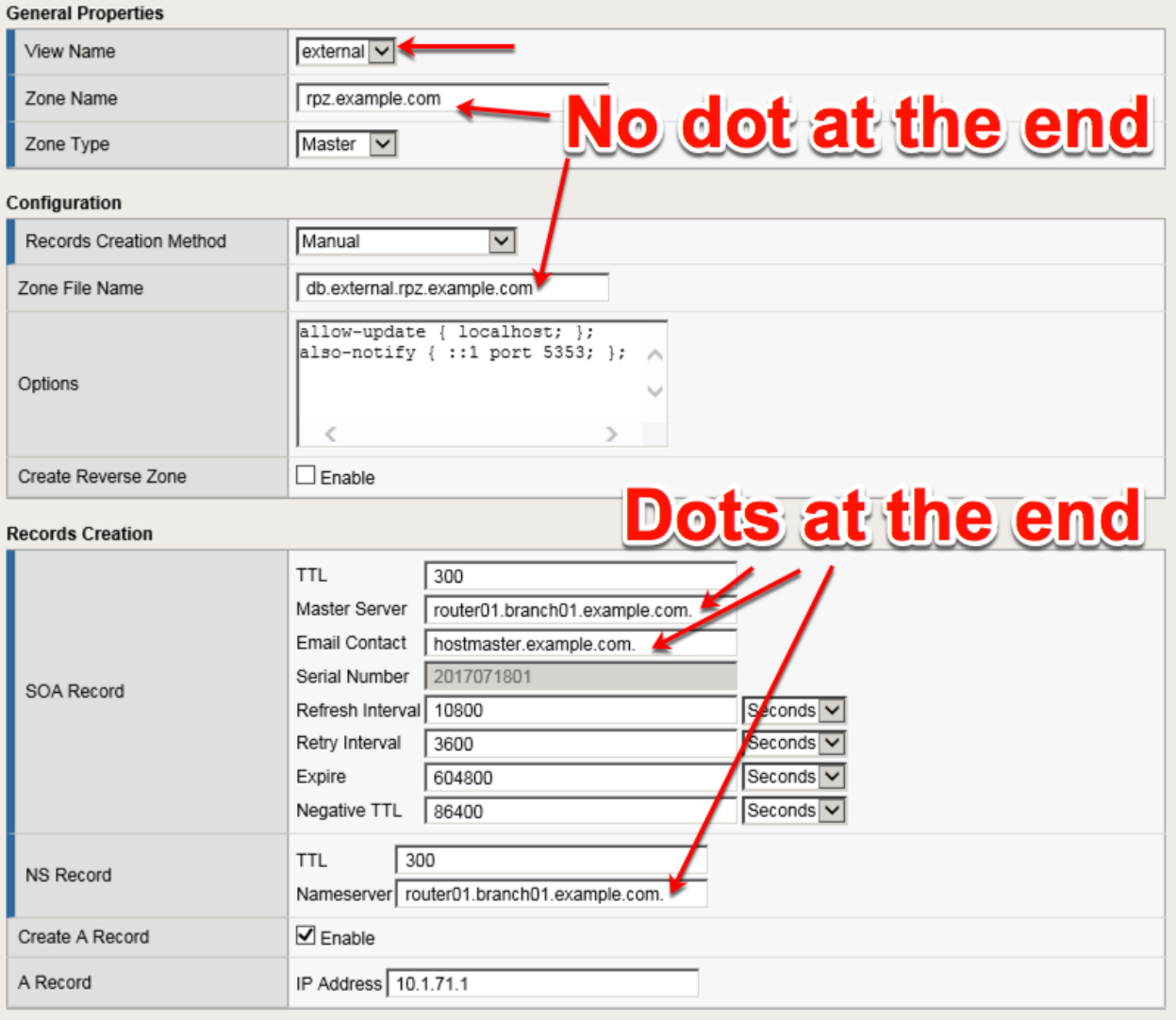
Navigate to **DNS ›› Zones : ZoneRunner : Zone List**

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



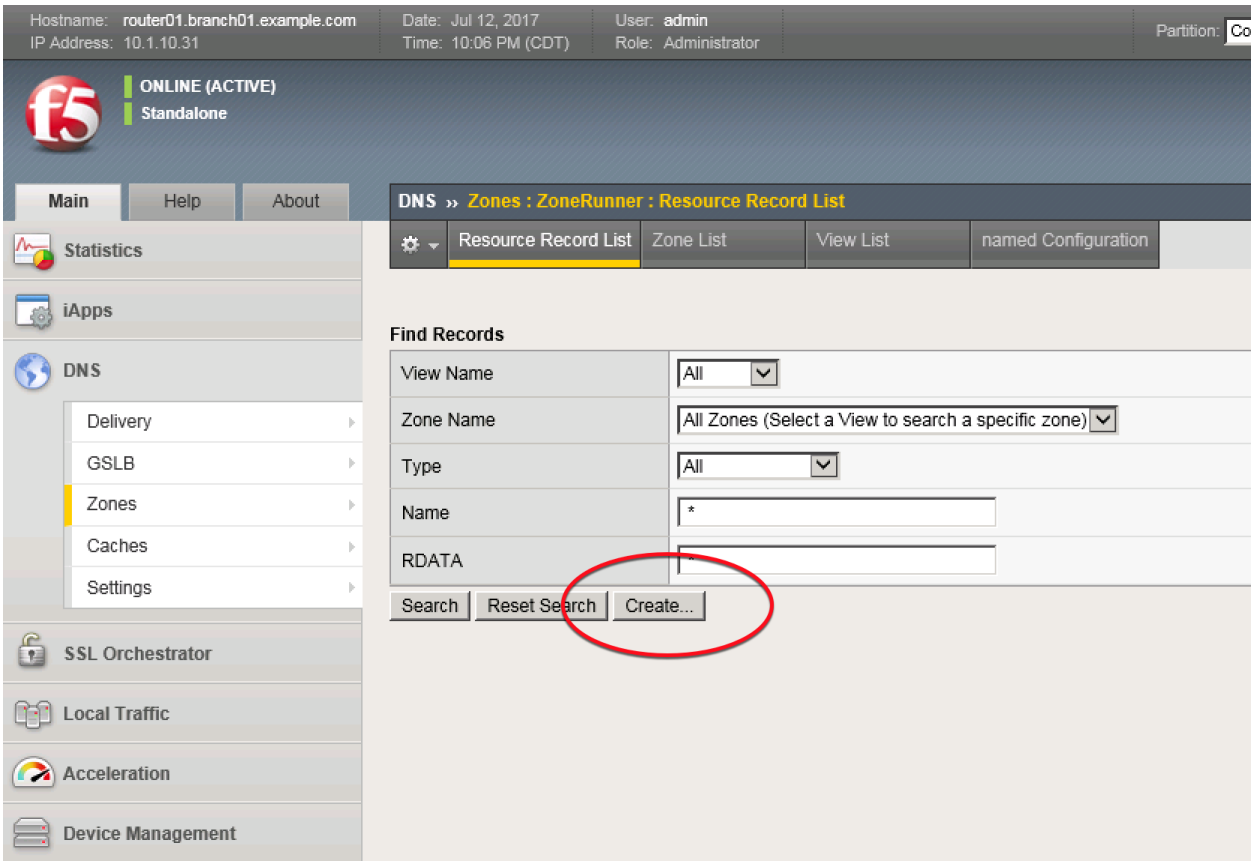

Create a zone according to the following table:

| 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 | router01.branch01.example.com. |
| Email Contact | hostmaster.example.com. |
| NS Record: TTL | 300 |
| NS Record: Nameserver | router01.branch01.example.com. |
| Create A Record | Checked - Enabled |
| A Record: IP Address | 10.1.71.1 |



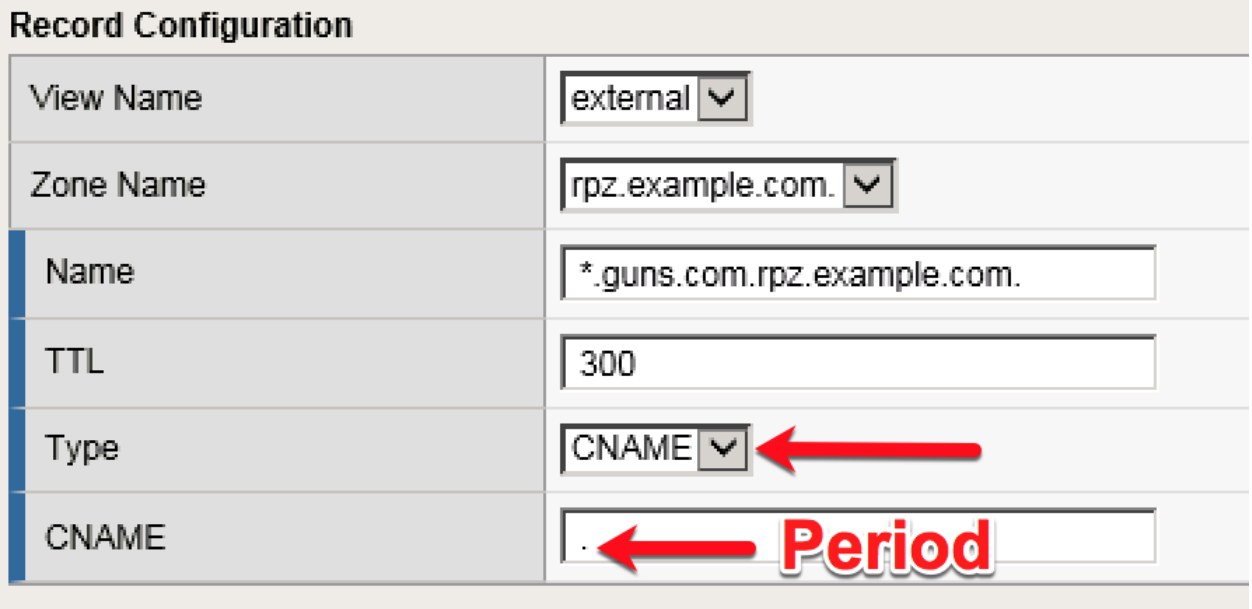

Navigate to: **DNS ›› Zones : ZoneRunner : Resource Record List**

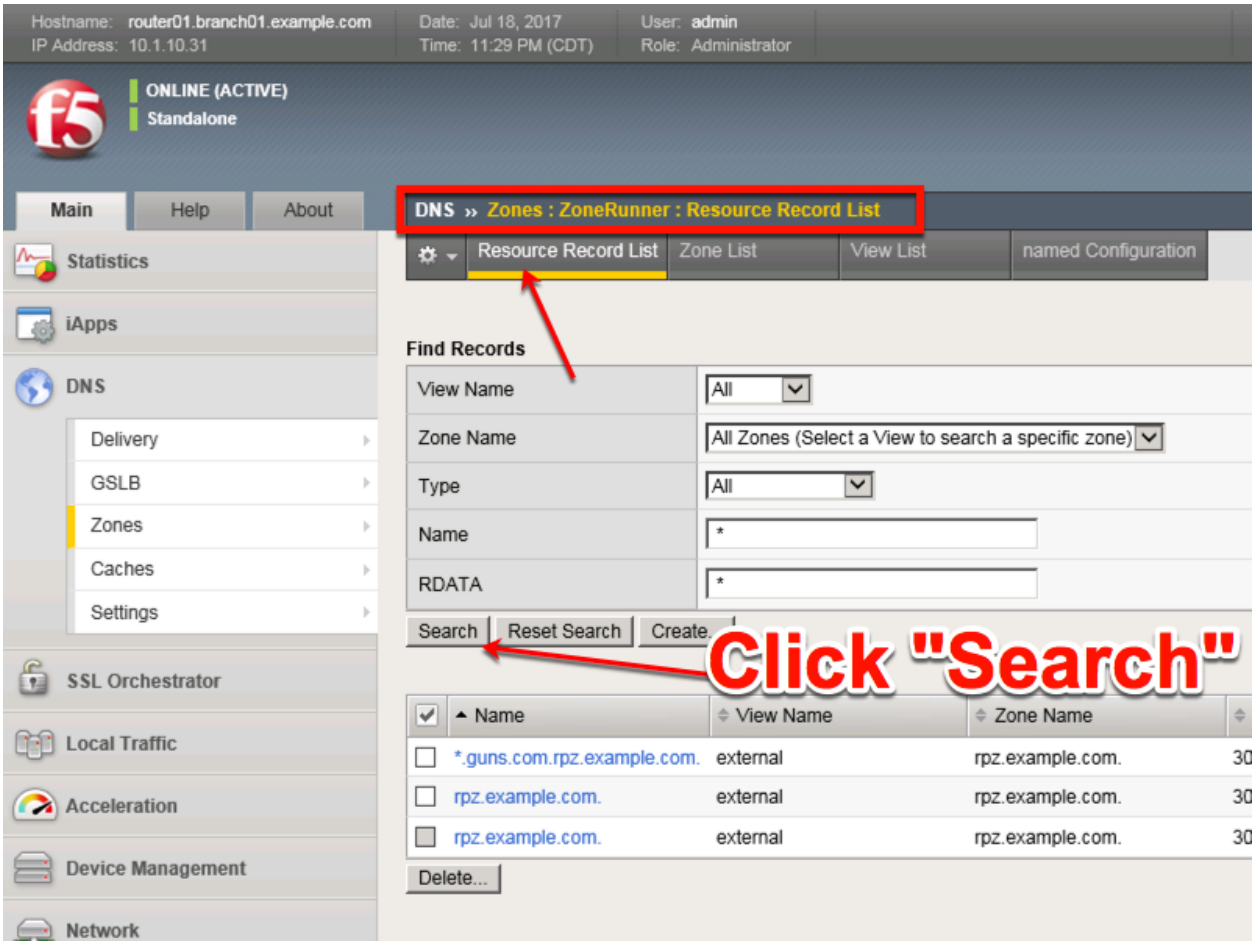
https://router01.branch01.example.com/tmui/Control/jspmap/tmui/globallb/zfd/record/create.jsp




Create a resource record according to the following table:

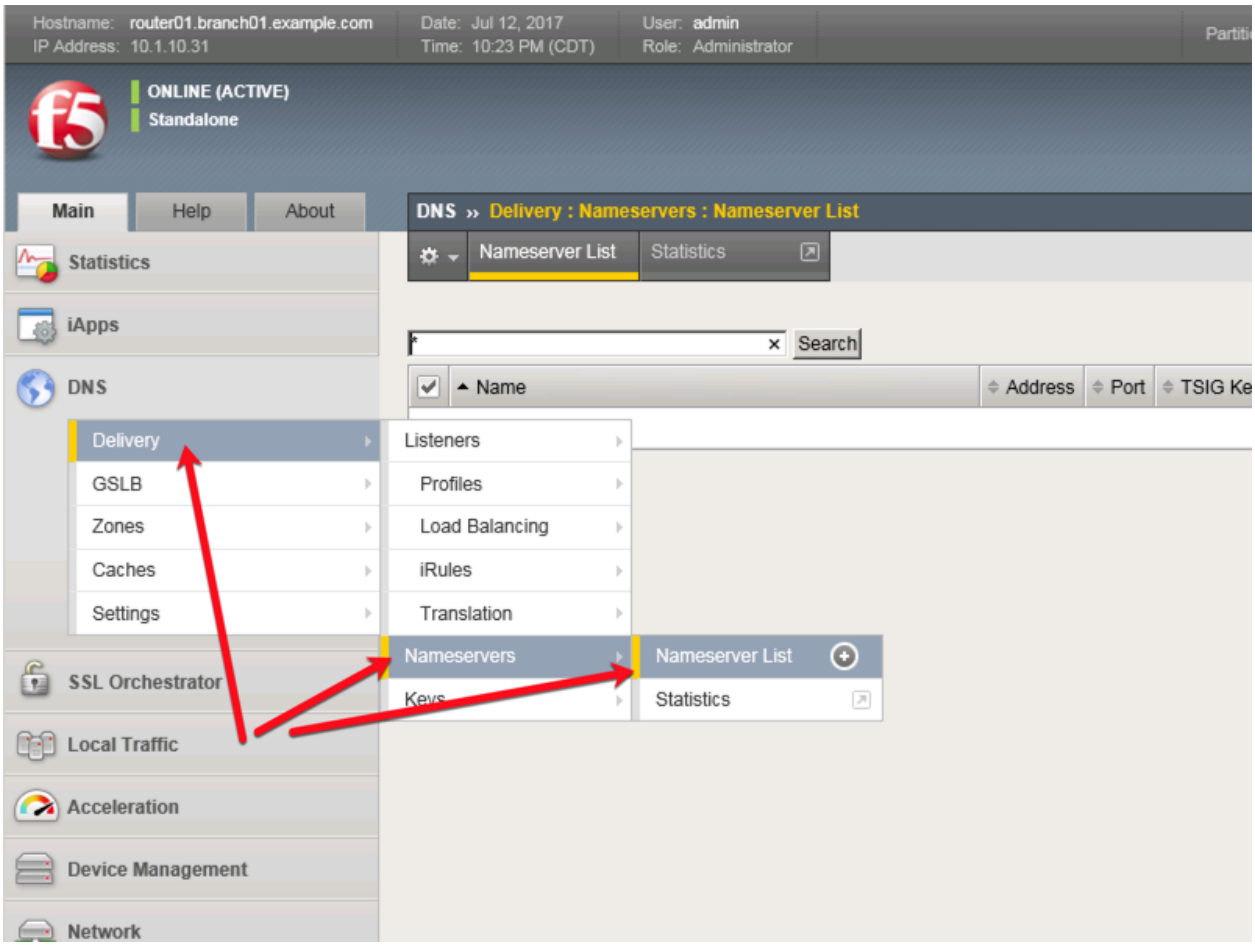
| Setting | Value |
|---|---|
| View Name | external |
| Zone Name | rpz.example.com |
| Name | *.guns.com.rpz.example.com. |
| TTL | 300 |
| Type | CNAME |
| CNAME | . |




### 3.6.2 Name Server

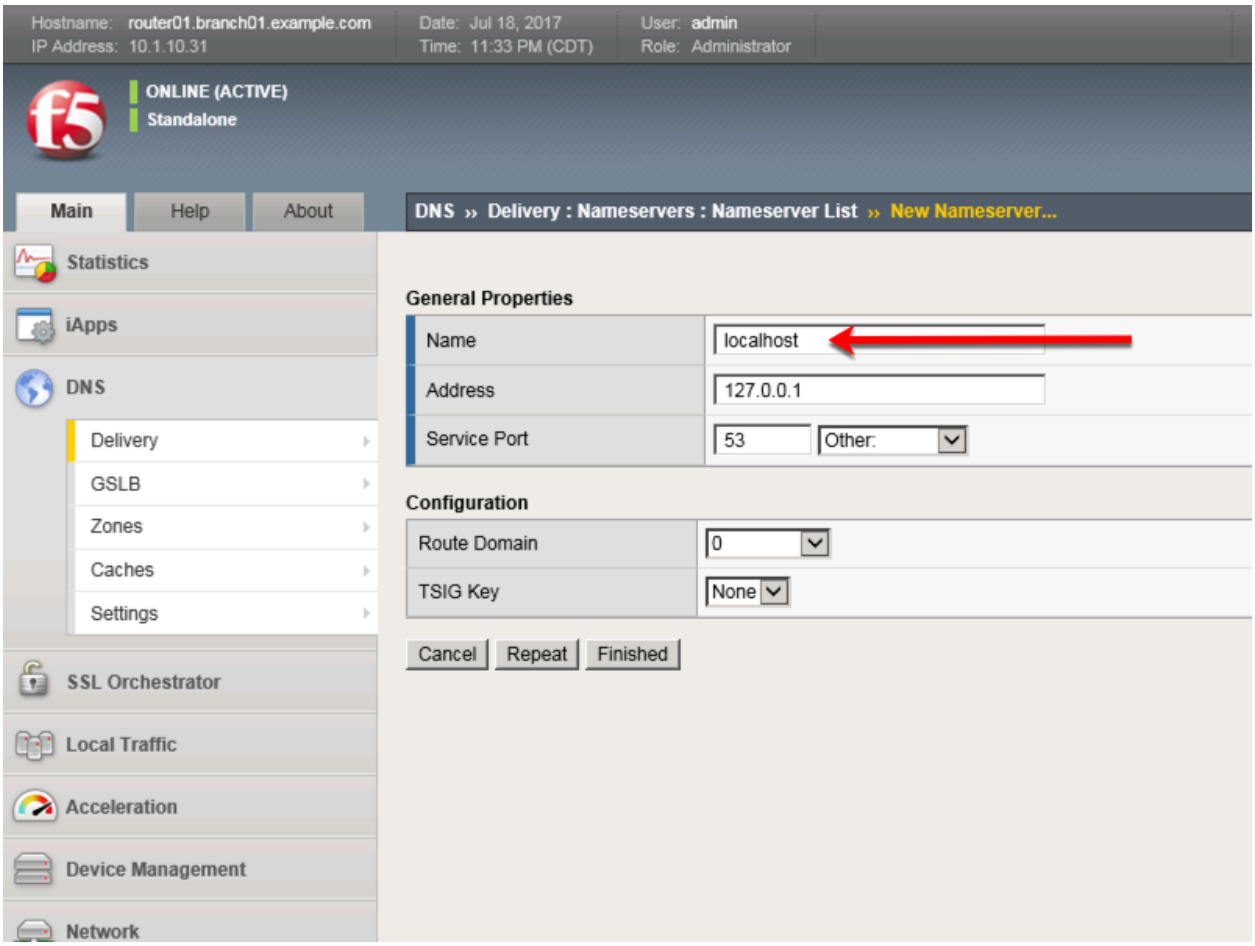
Navigate to **DNS ›› Delivery : Nameservers : Nameserver List**




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

Create a nameserver according to the following table:

| Setting | Value |
|---|---|
| Name | localhost |




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

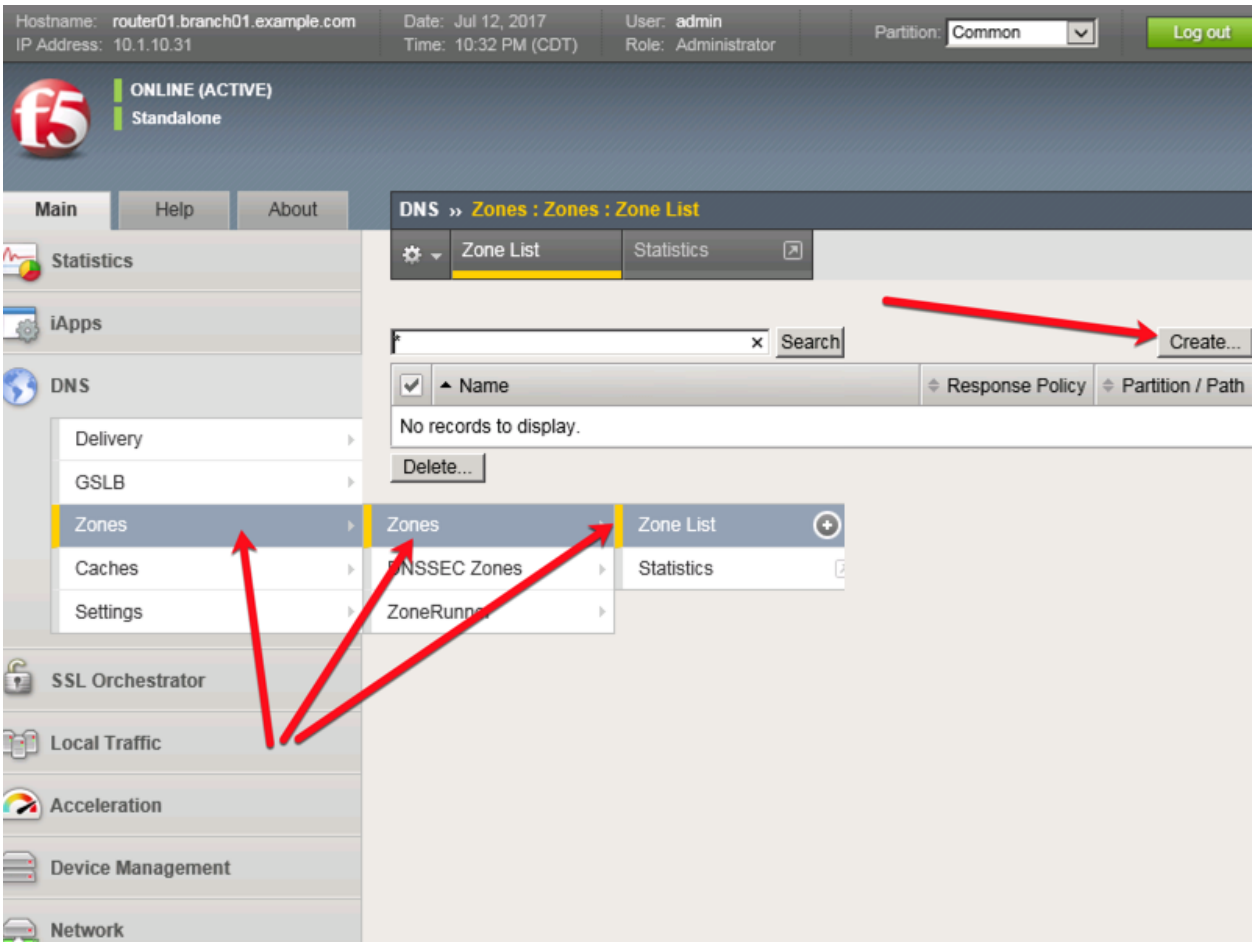
**TMSH**

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

### 3.6.3 DNS Express

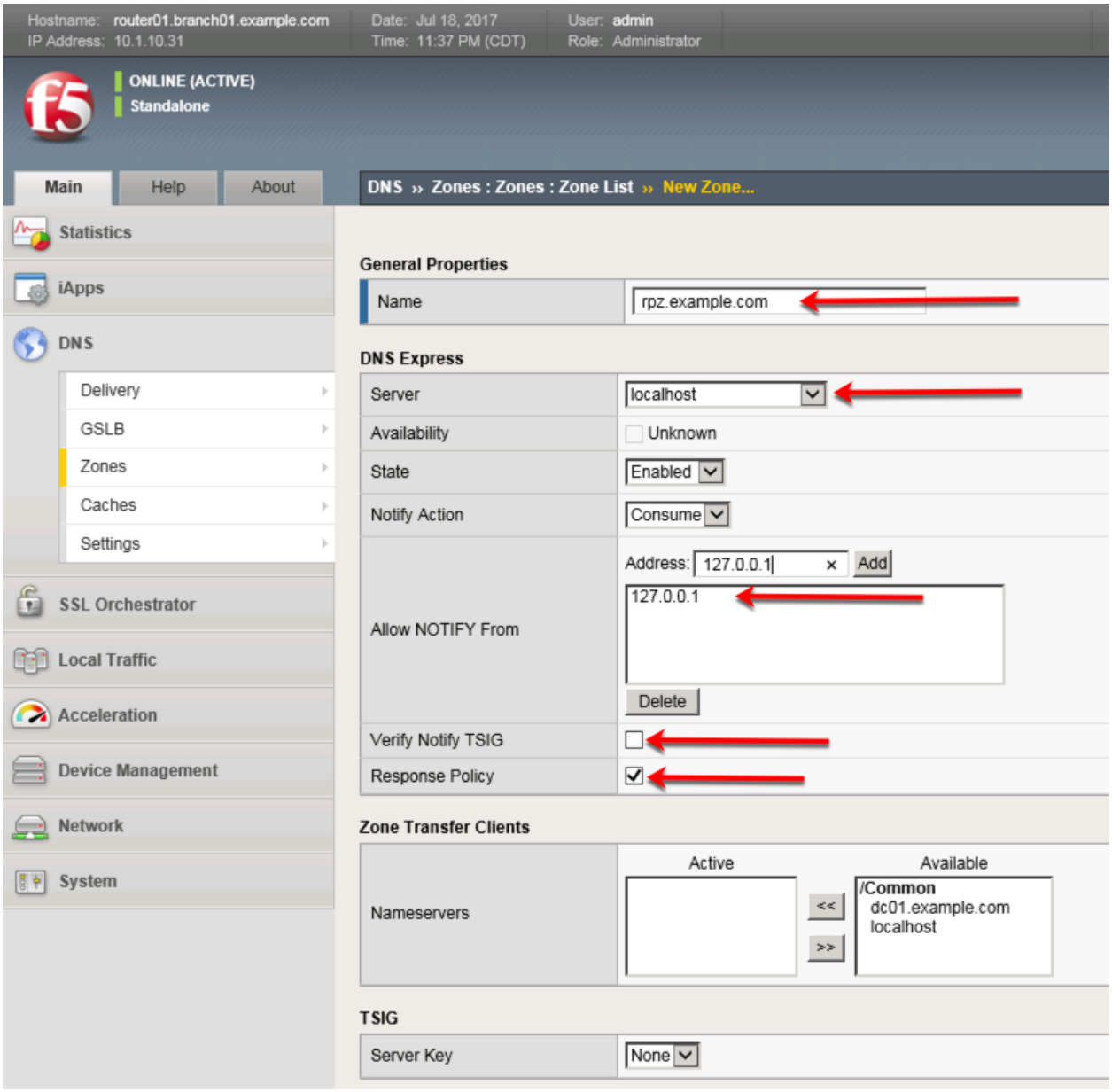
Navigate to **DNS ›› Zones : Zones : Zone List**

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




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 |
| Response Policy | checked |



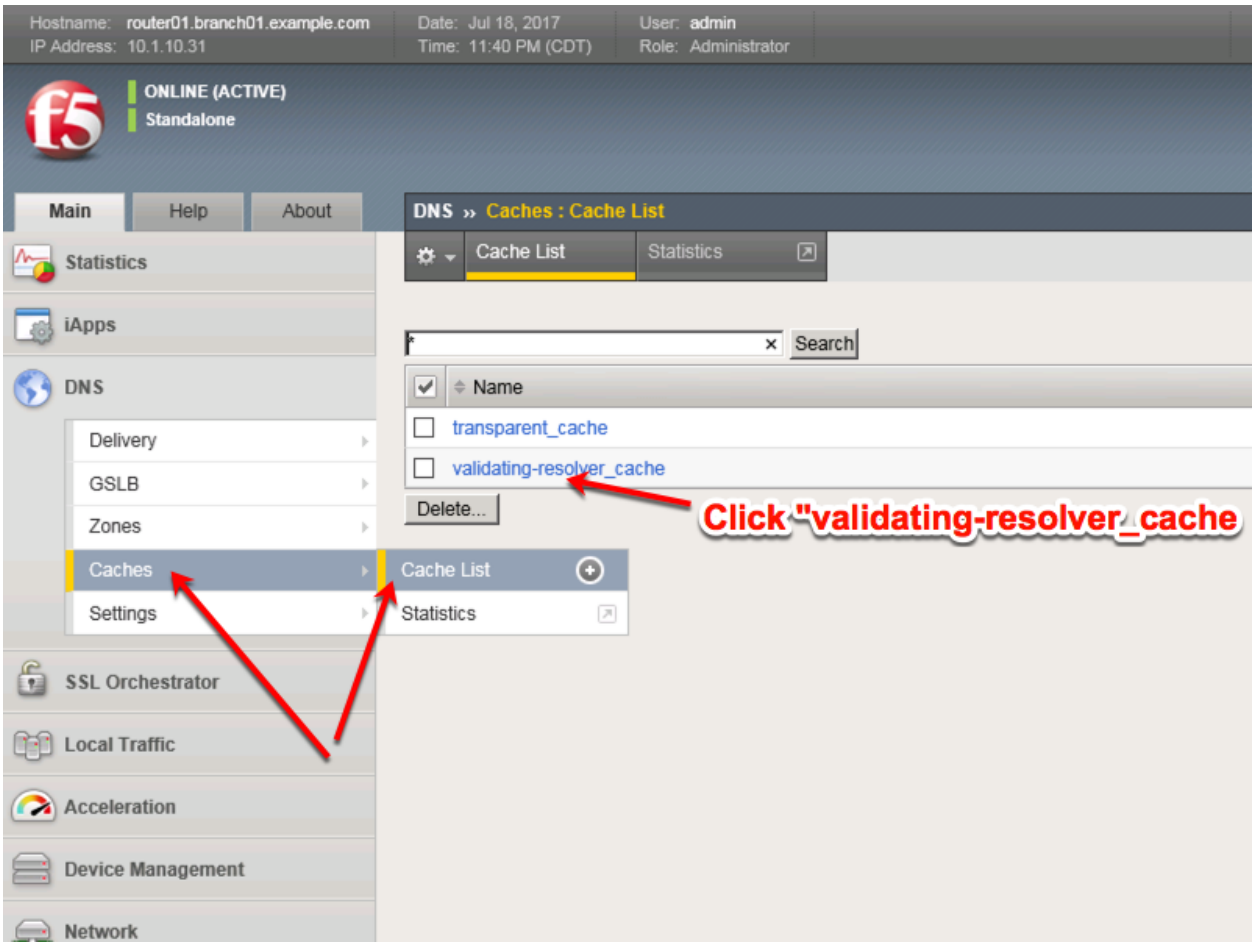

**TMSH**

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 }

### 3.6.4 Local Zone

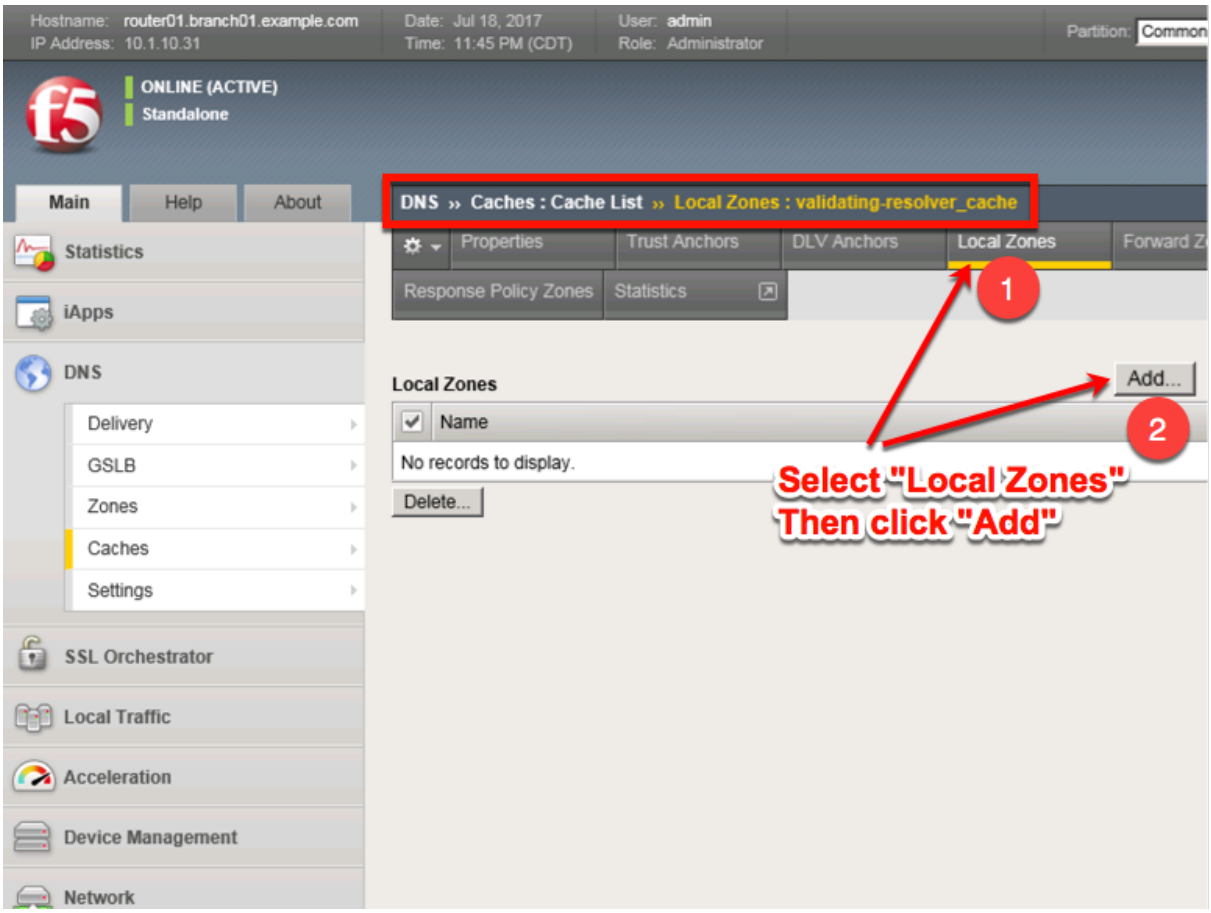
Navigate to: **DNS ›› Caches : Cache List**

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



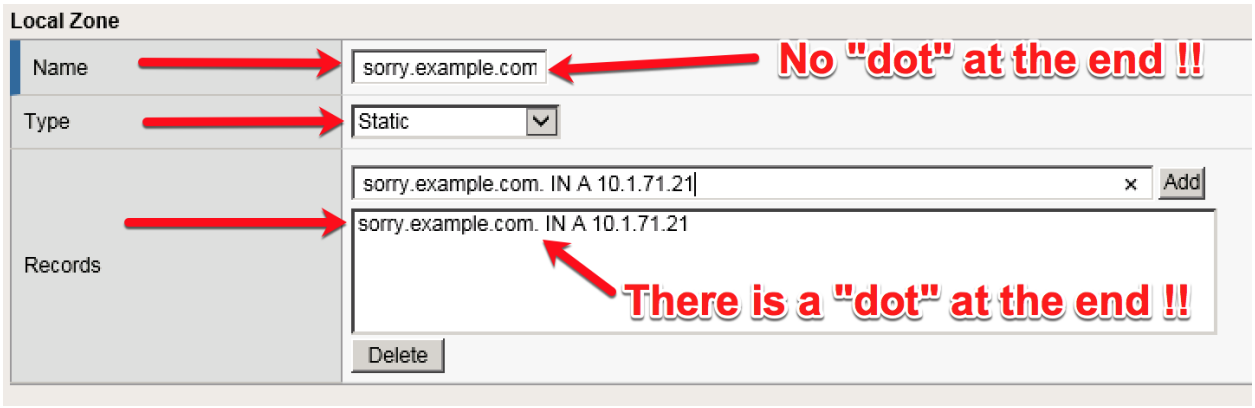

Select validating-resolver_cache, click “Local Zones”, and click “Add”

https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/local_zone/list.jsp?name=%2FCommon%2Fvalidating-resolver_cache&tab=dns_cache_config




Create a local zone entry according to the following table:

| Setting | Value |
|---|---|
| Name | sorry.example.com |
| Type | Static |
| Records | sorry.example.com. IN A 10.1.71.21 |




TMSH commands for router01.branch01:

**TMSH**

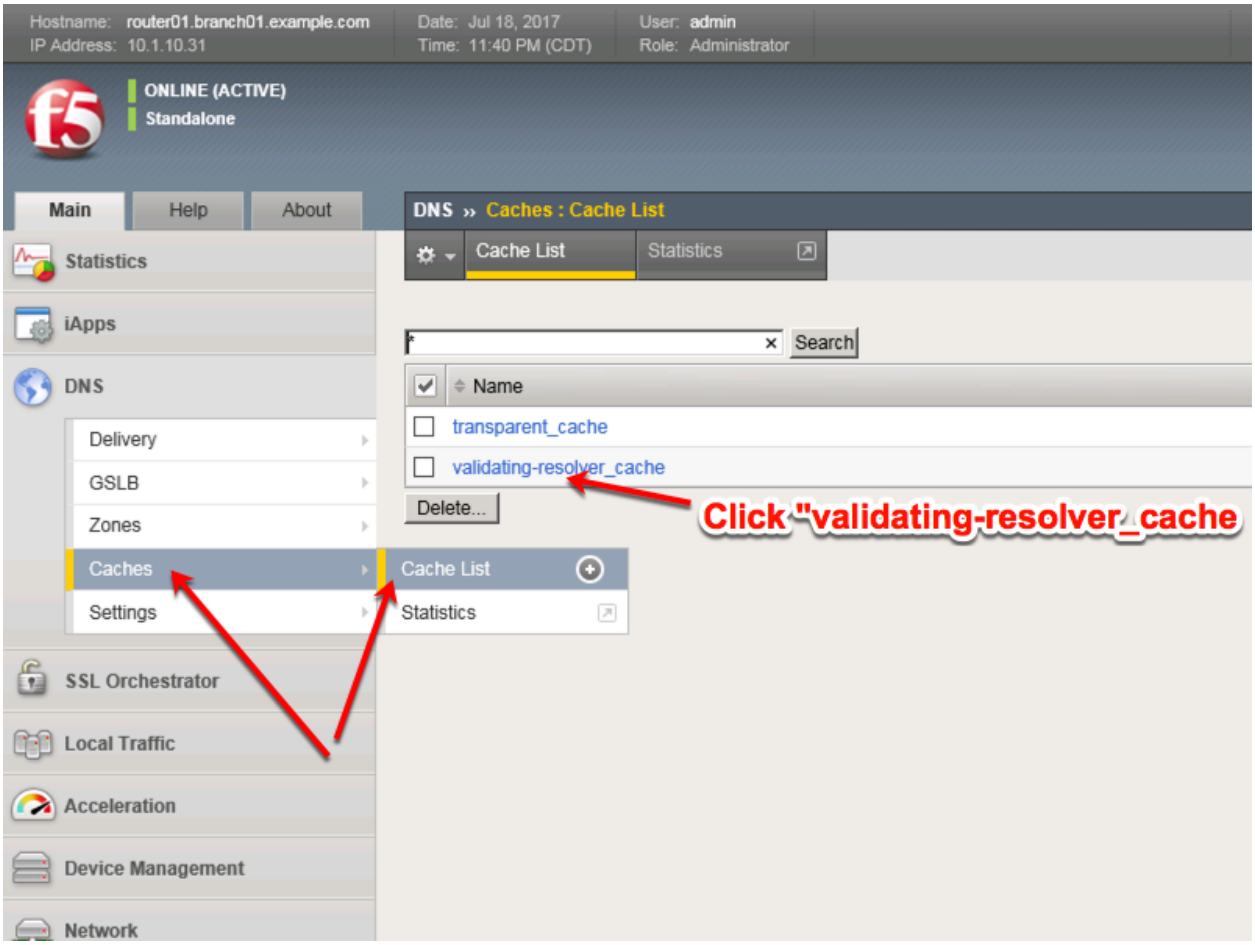
tmsh modify ltm dns cache validating-resolver validating-resolver_cache local-zones { { name sorry.example.com records add { “sorry.example.com. IN A 10.1.71.21” } type static } }

### 3.6.5 Walled Garden

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

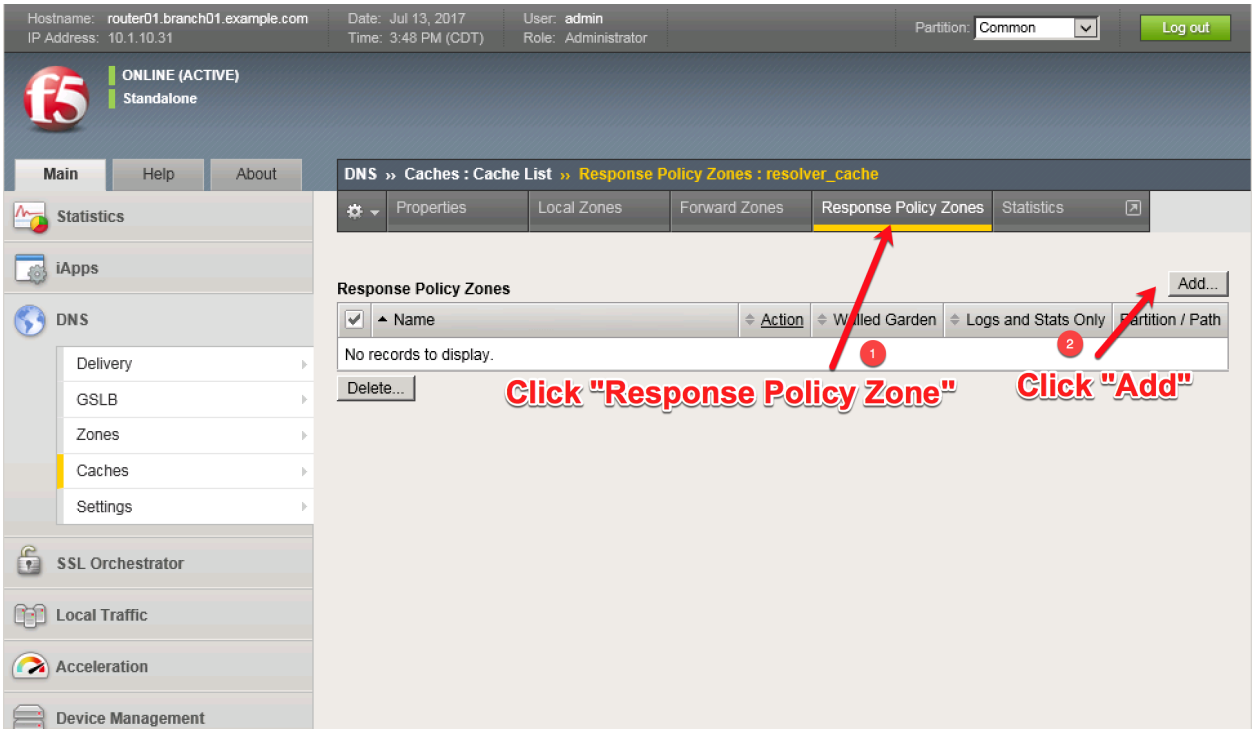
https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/list.jsp

Click “validating-resolver_cache”



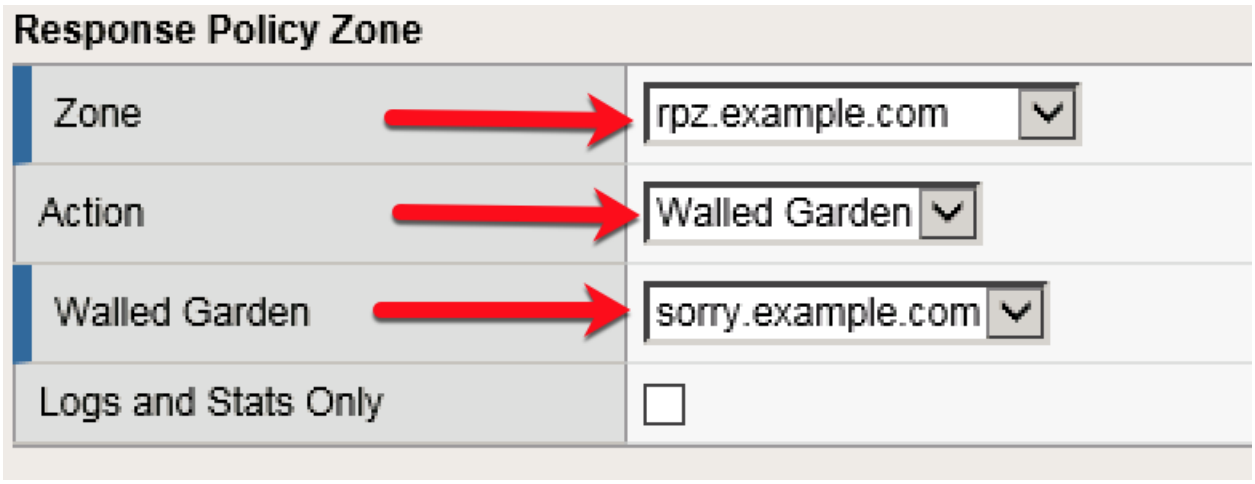

Select validating-resolver_cache, click “Response Policy Zones”, and then click “Add”

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




Create a local zone entry according to the following table:

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



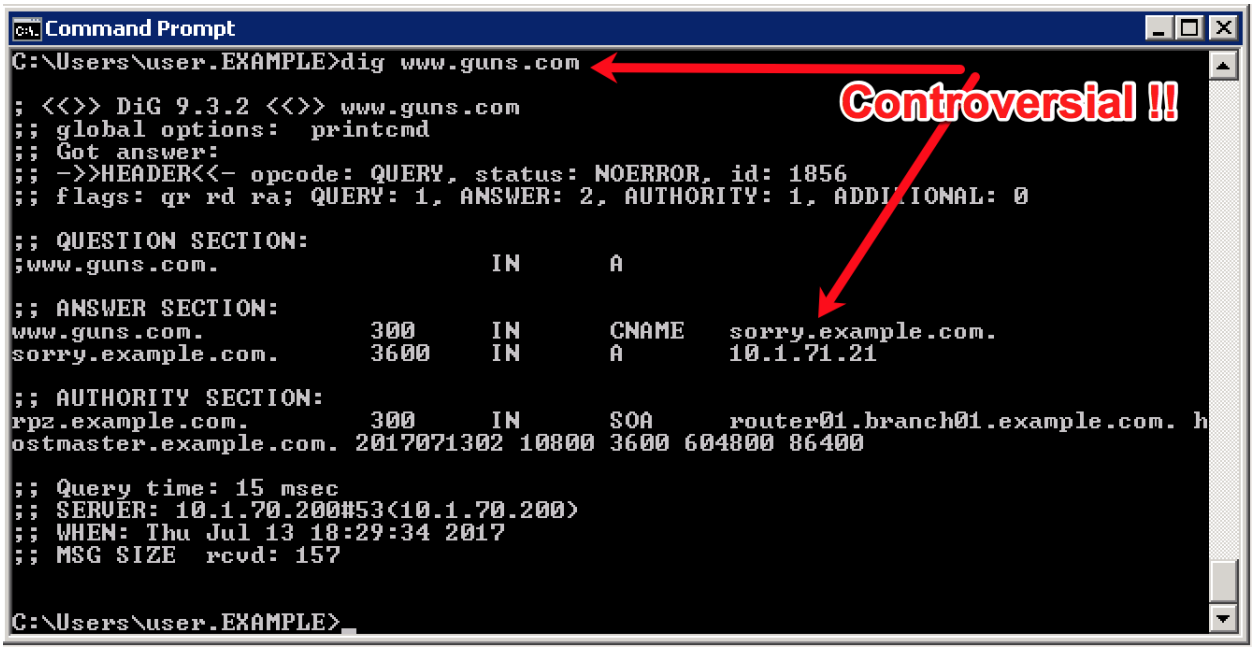

TMSH commands for router01.branch01:

**TMSH**

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

### 3.6.6 Results

From a Workstation command prompt run “dig www.guns.com”

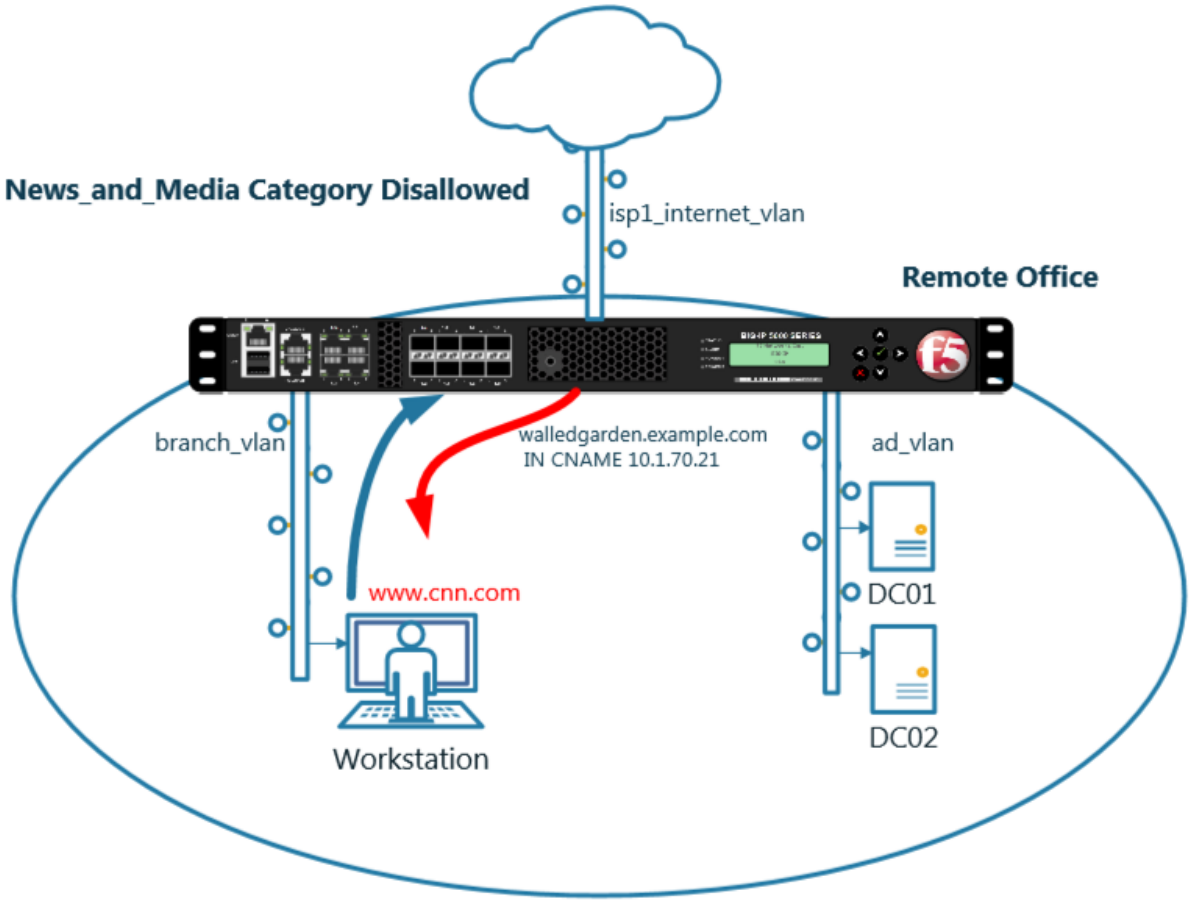



Try running additional dig commands to verify that other domains still resolve as expected.

dig www.f5.com

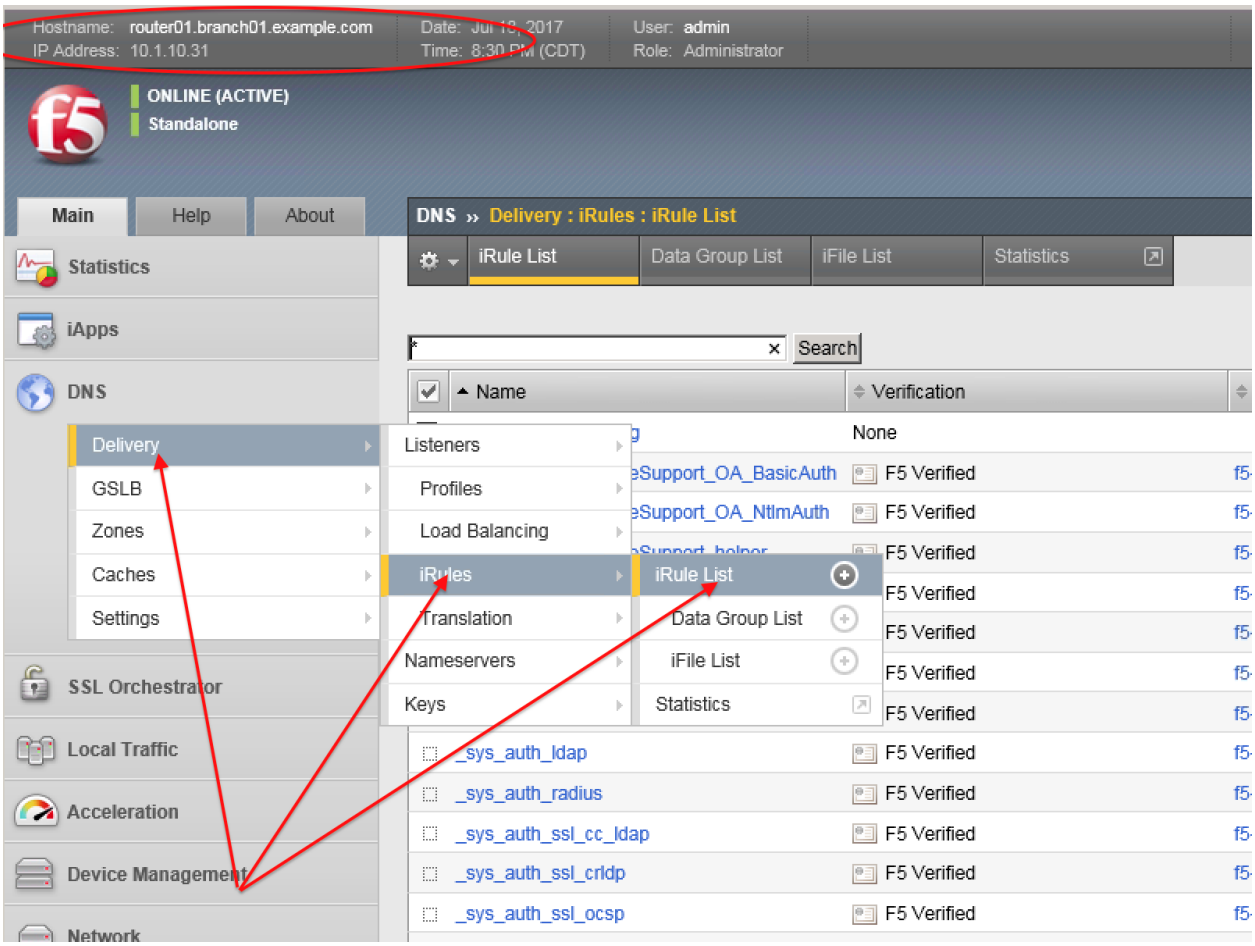
## 3.7 URL Categorization

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




### 3.7.1 Create an iRule

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




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

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

| 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/Sex
  }


  # 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 "10.1.71.21"
```

```
  # Toggle for debug logs
  set static::request_debug 1
}


when DNS_REQUEST {
  if { $static::request_check } {
    set lookup_category [getfield [CATEGORY::lookup "http://[DNS::question name]"] "
↪" 1]
    if { [lsearch -exact $static::blocked_categories $lookup_category] >= 1 } {
      if { $static::request_debug } {
         log local0. "BLOCKED: Category $lookup_category matching [DNS::question␣
↪name] is filtered."
      }
      DNS::answer clear
      if { $static::request_return_nxdomain } {
         DNS::header opcode QUERY
         DNS::header rcode NXDOMAIN
      } else {
         if { [DNS::question type] equals "A" } {
            DNS::answer insert "[DNS::question name]. 111 [DNS::question class]␣
↪[DNS::question type] $static::request_redirect_to"
         }
      }
      DNS::return
 } else {
    if { $static::request_debug } {
      log local0. "Category $lookup_category matching [DNS::question name] is not␣
↪filtered"
      }
    }
  }
}
```

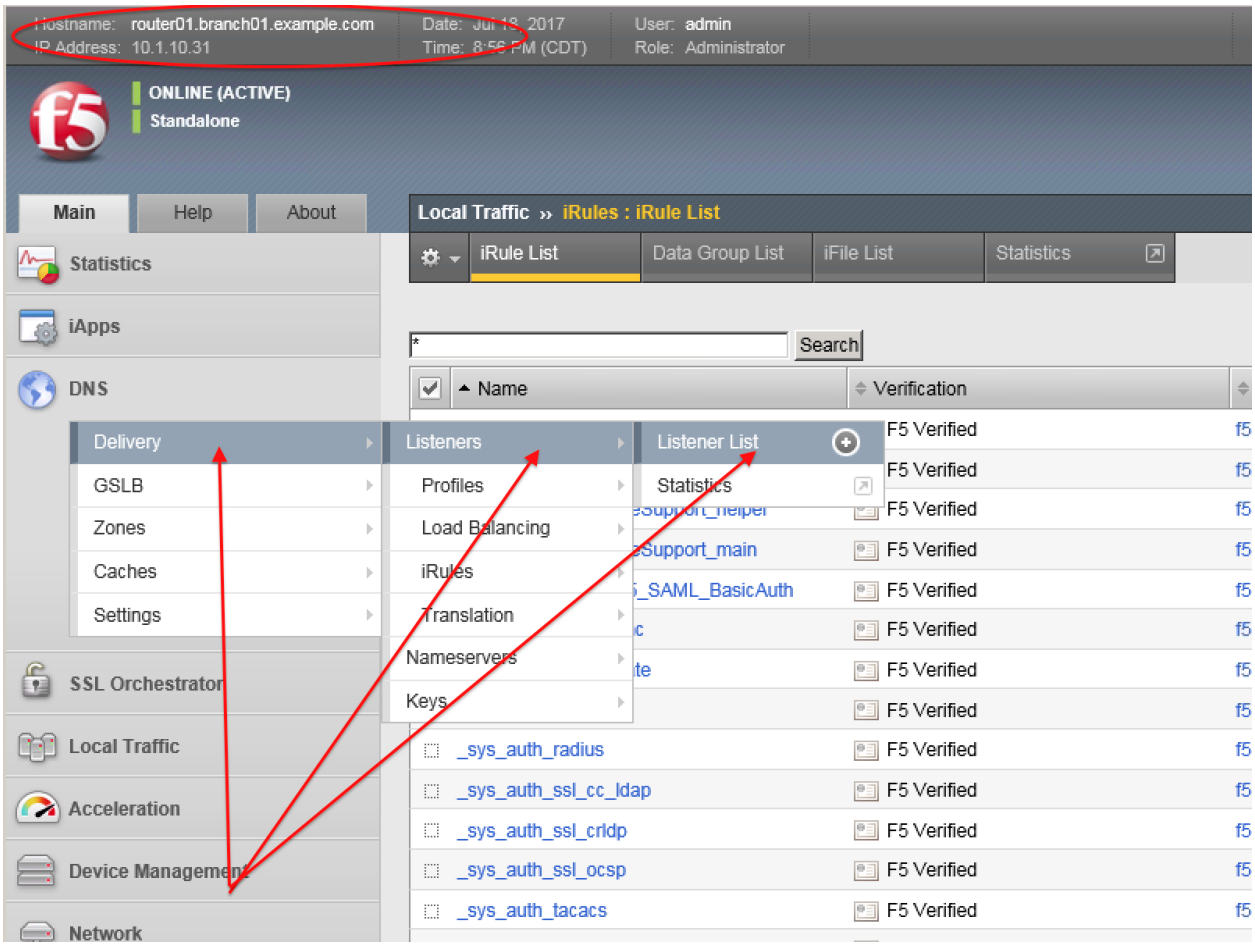
TMSH commands for router01.branch01 (Make sure you use text editor to copy content above and paste it)

**TMSH**

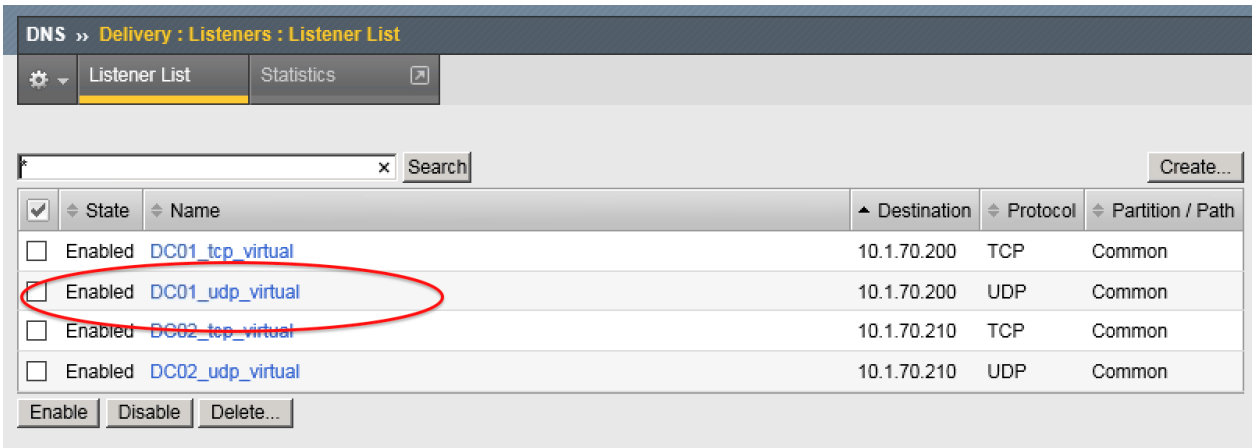
tmsh create ltm rule DNS-query-filtering

### 3.7.2 iRule assignment

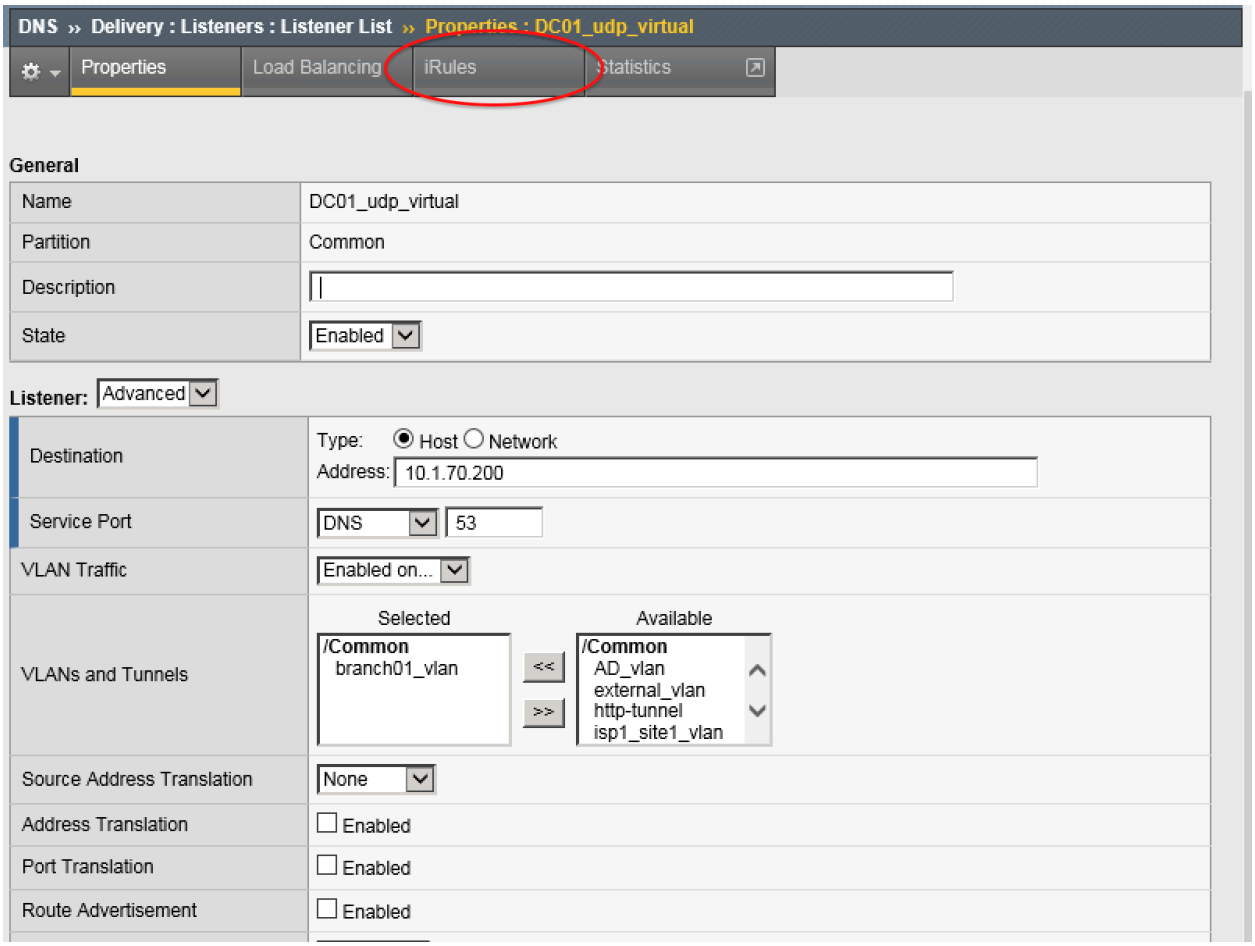
Navigate to: **DNS ›› Delivery : Listeners : Listener List**



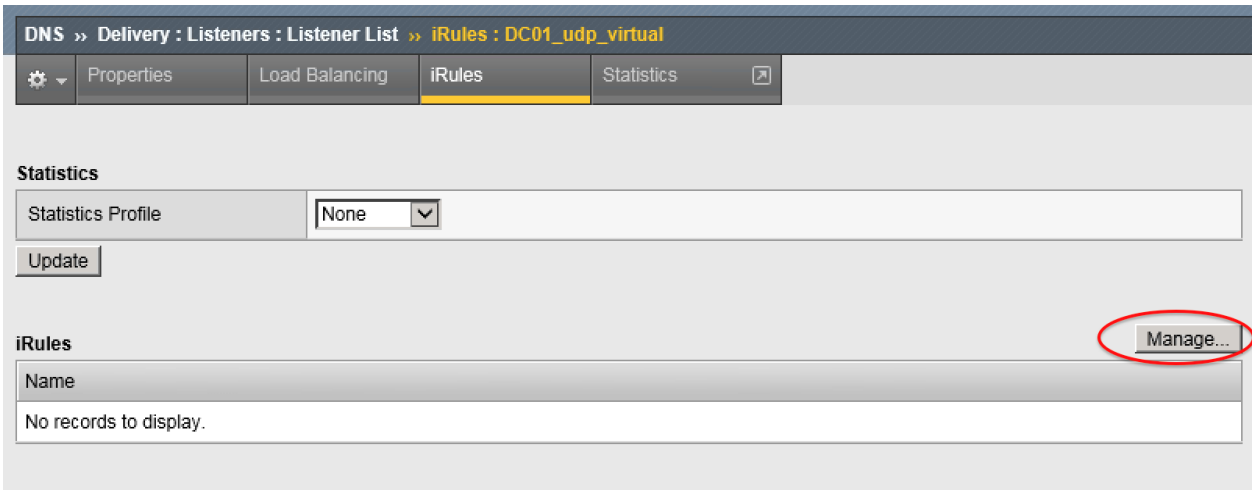

Navigate to the listener DC01_udp_virtual




Navigate to iRules section

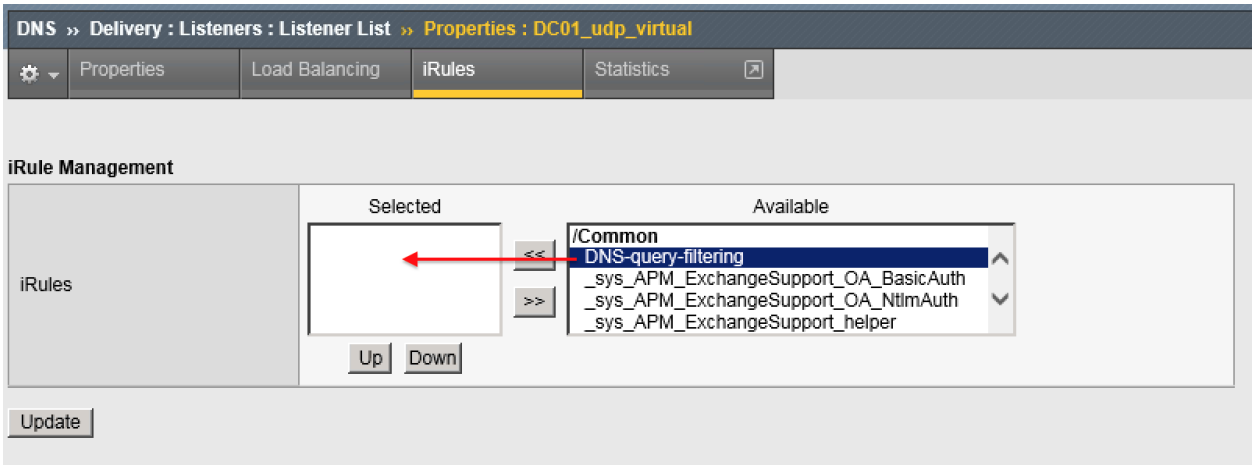



Navigate to Manage




https://router01.branch01.example.com/tmui/Control/form?__handler=/tmui/dns/listener/irules&__source=Manage. . . &__lin

Highlight DNS-query-filtering iRule and move it to Selected column




TMSH commands for router01.branch01

**TMSH**

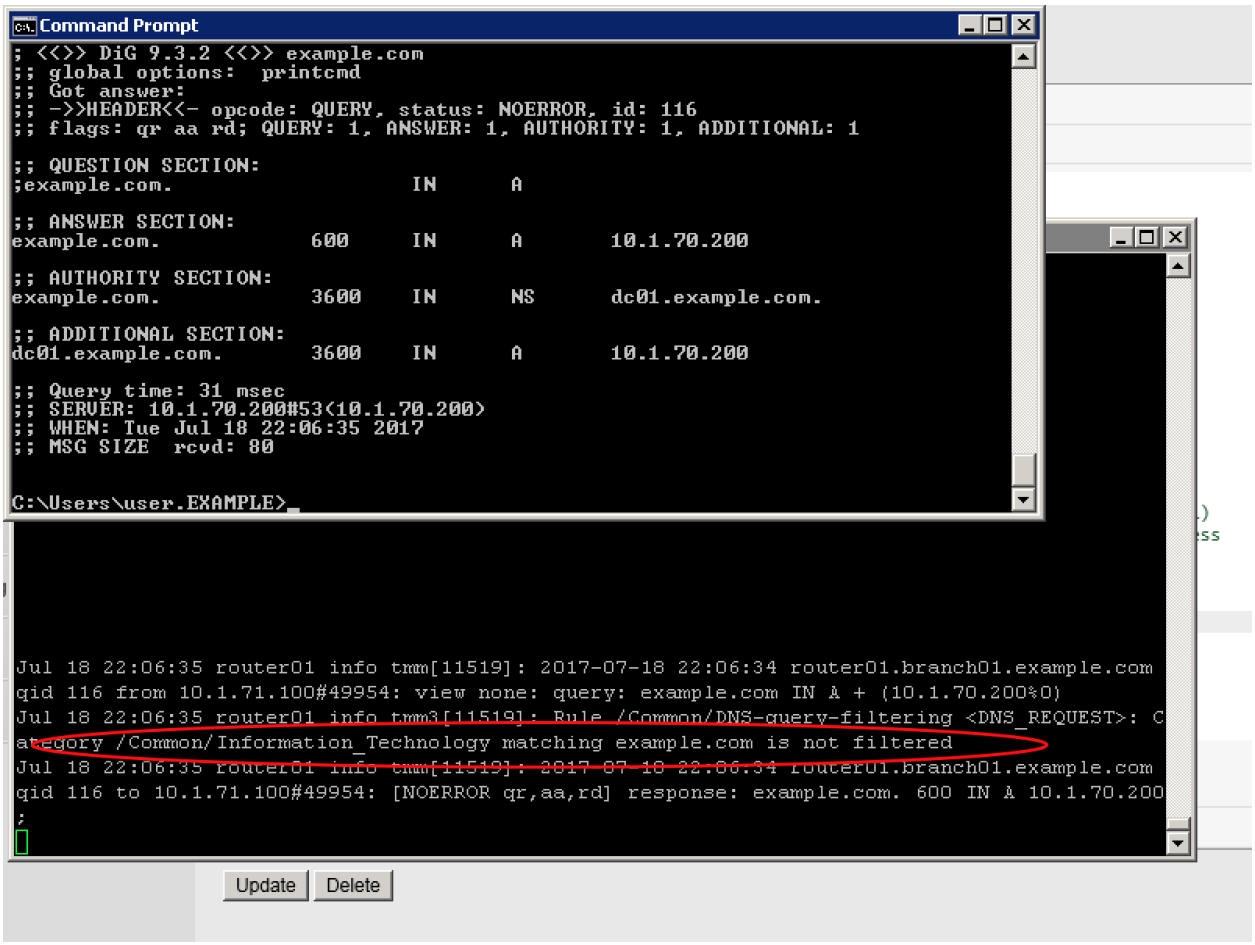
tmsh modify ltm virtual branch01_udp_53_virtual rules { DNS-query-filtering }

### 3.7.3 Results

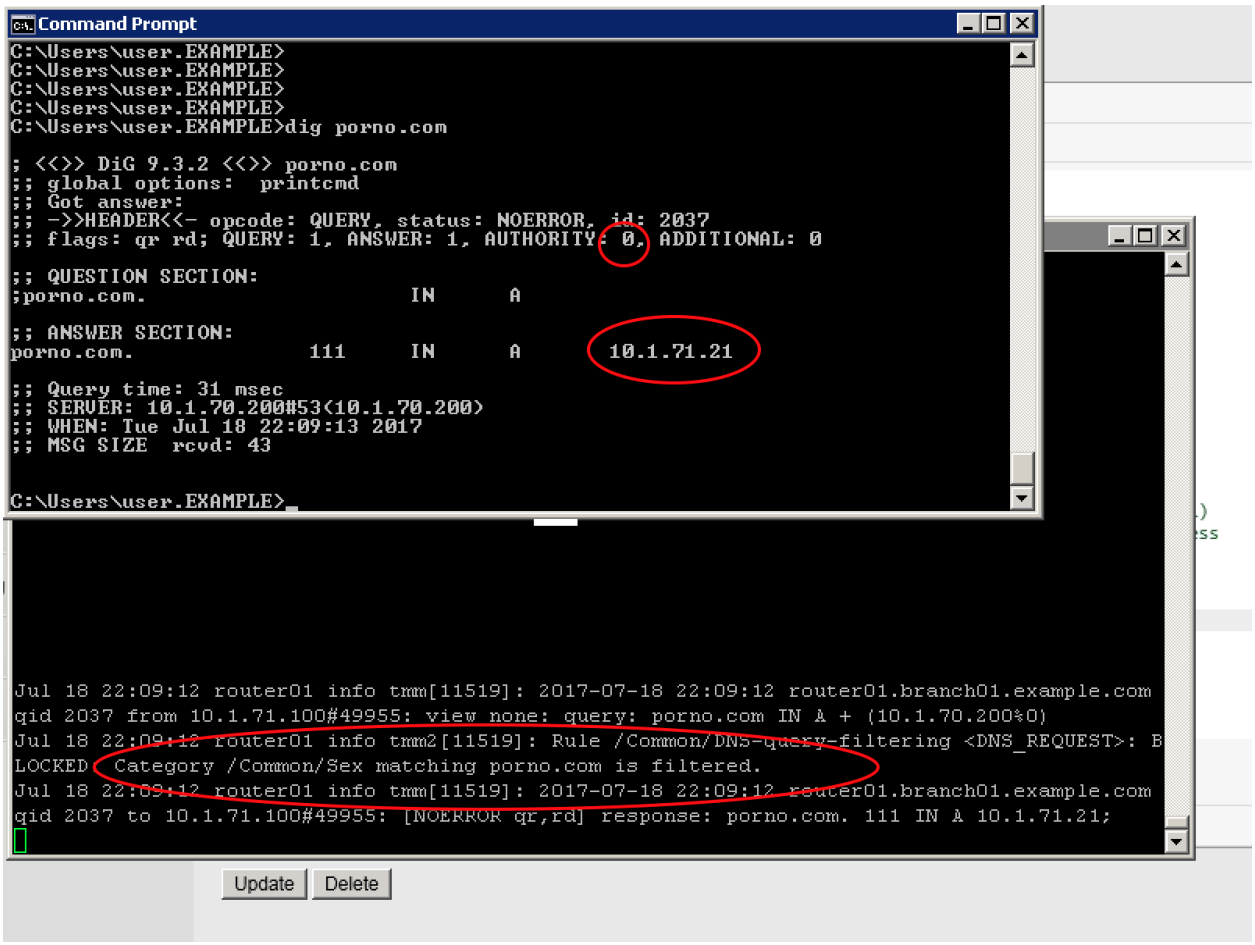
From the CLI on the router01.branch01 BIGIP run

tail -f /var/log/ltm

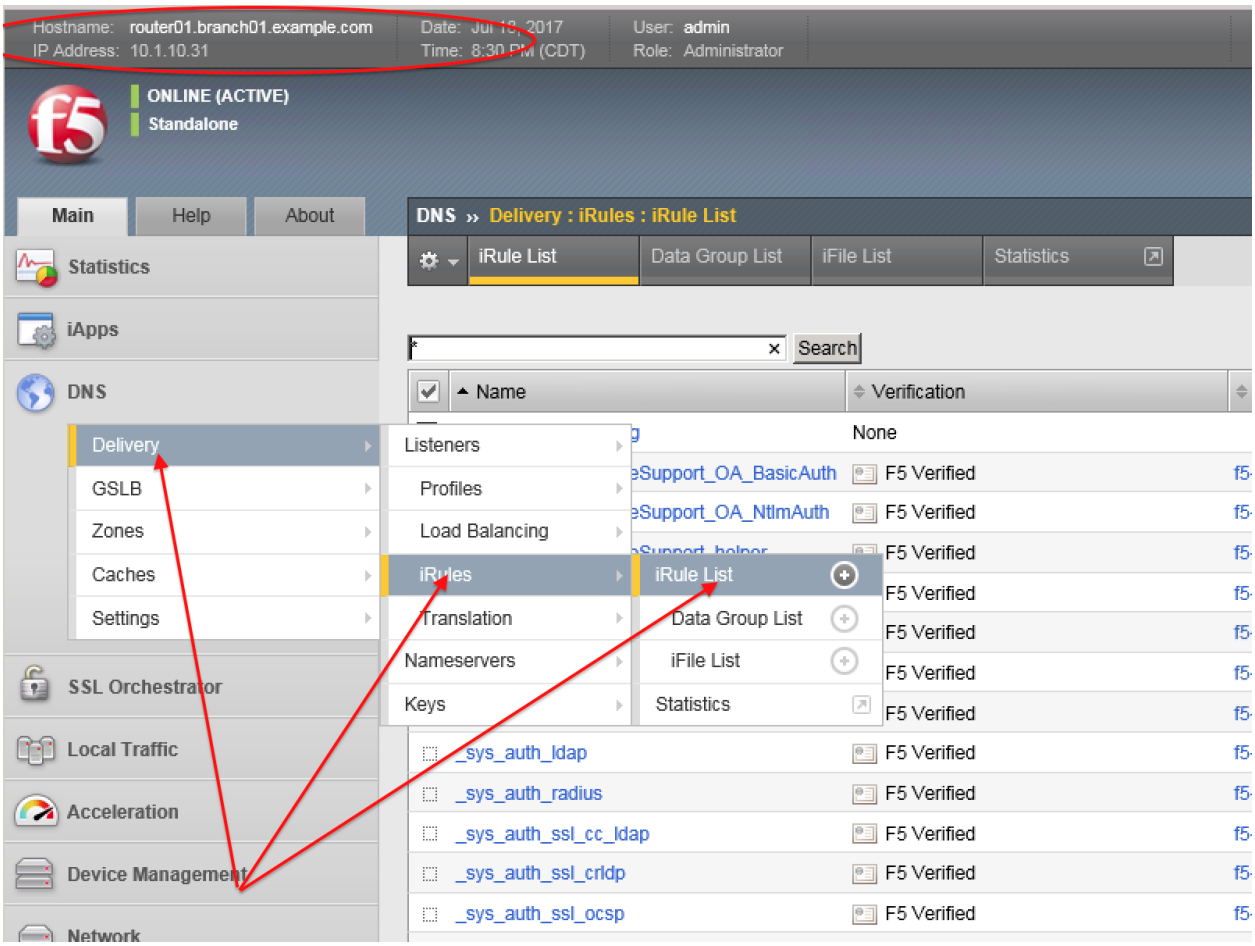
From the Workstation command prompt run “dig example.com” and check for the results




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

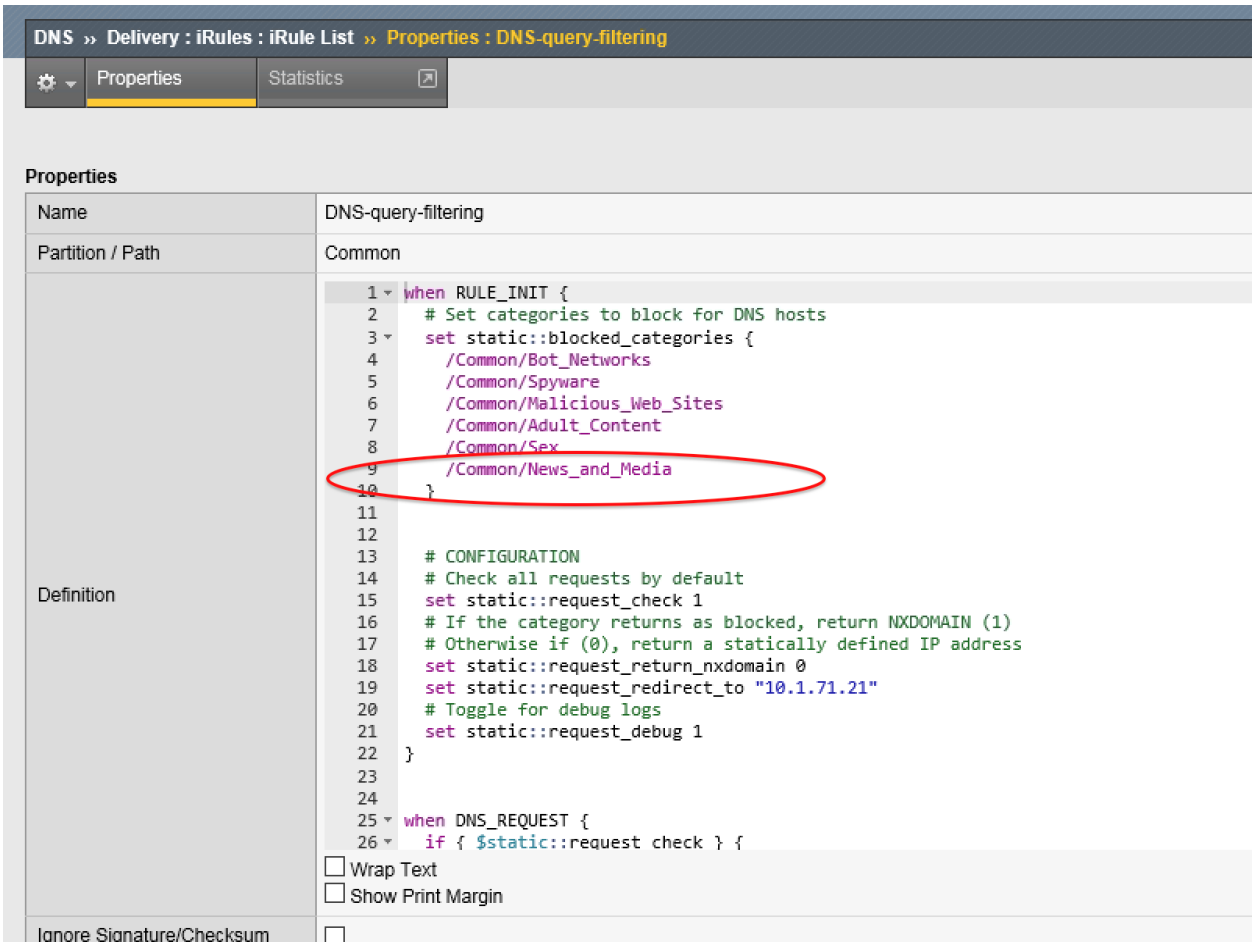



Navigate to: **DNS ›› Delivery : iRules : iRules List**

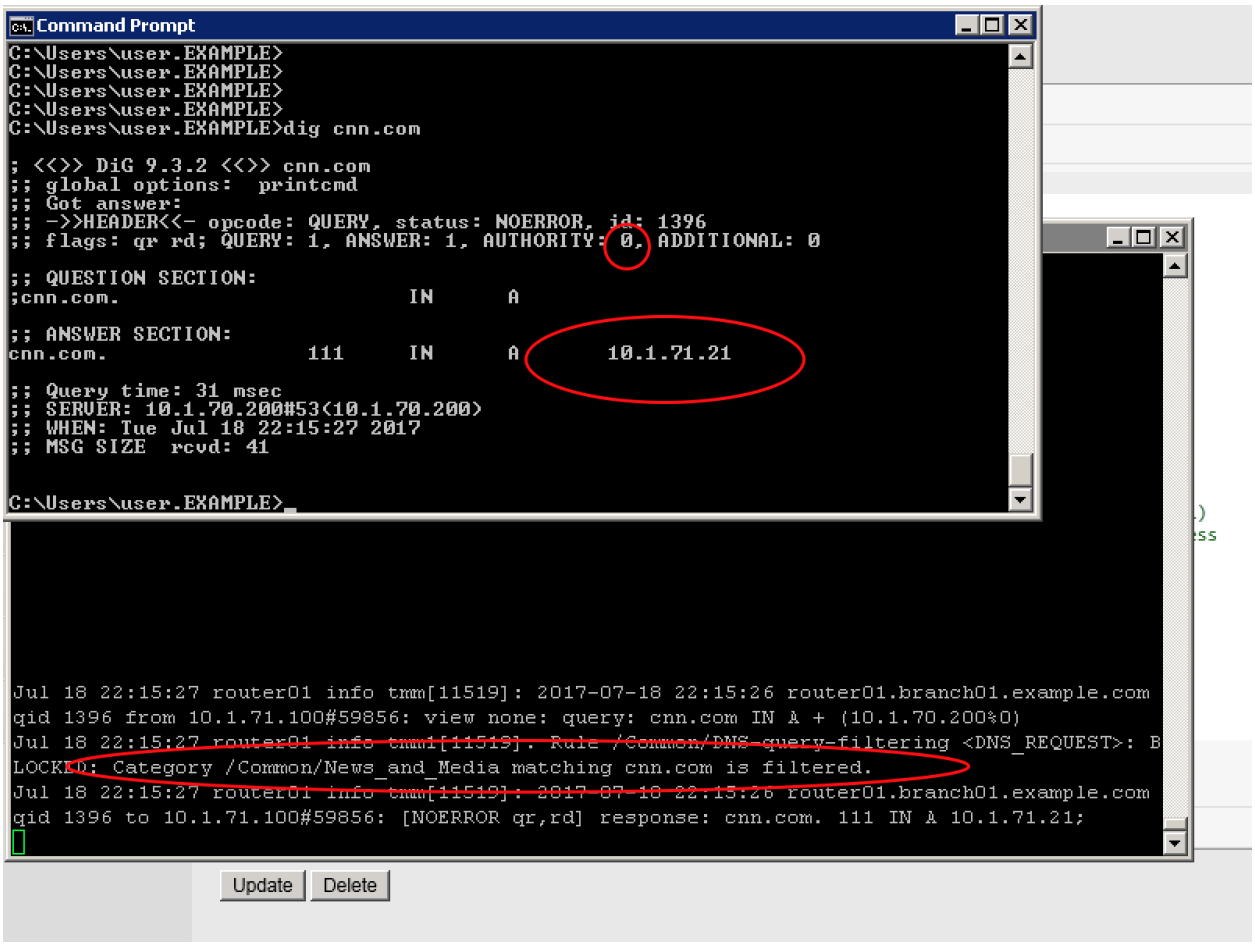



https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/rule/list.jsp

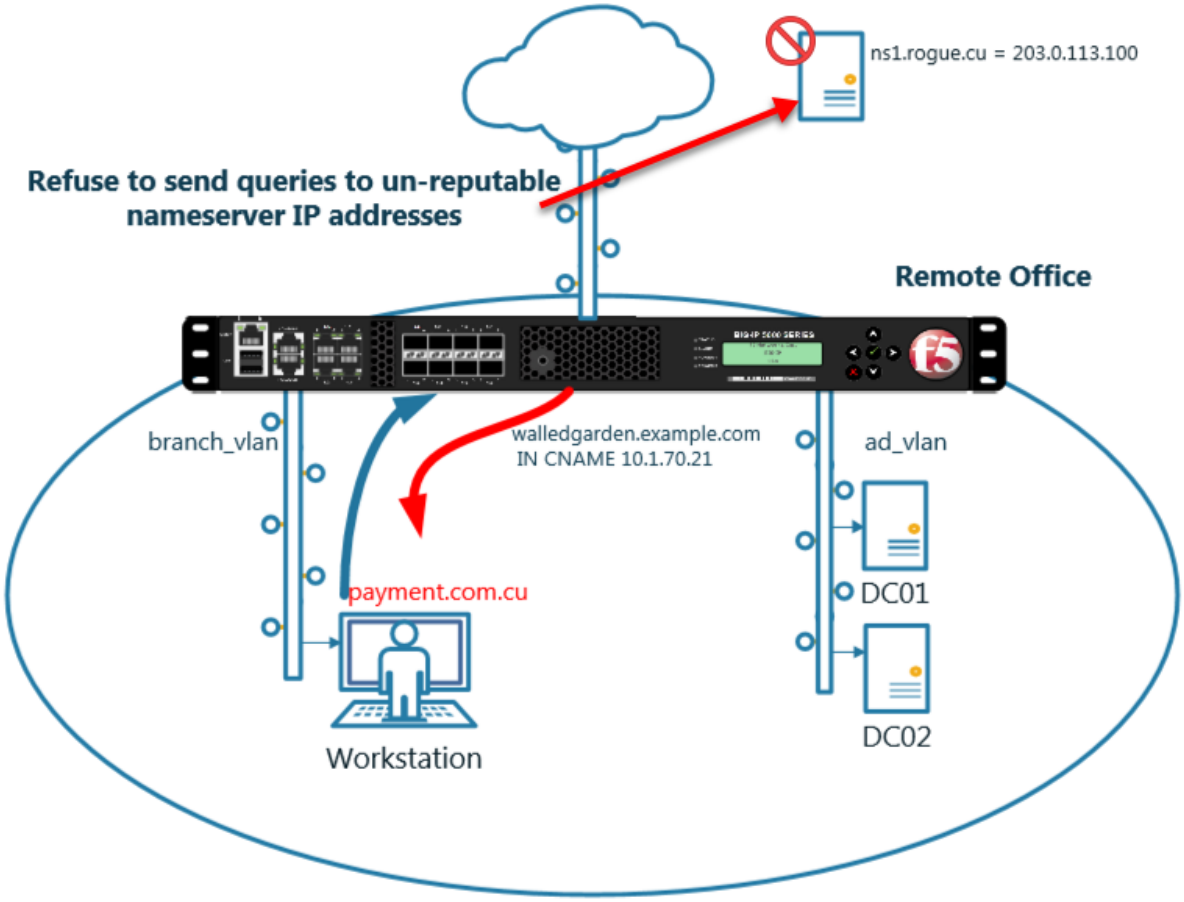
Click on the DNS-query-filtering iRule and add new filtering category “News_and_Media”




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

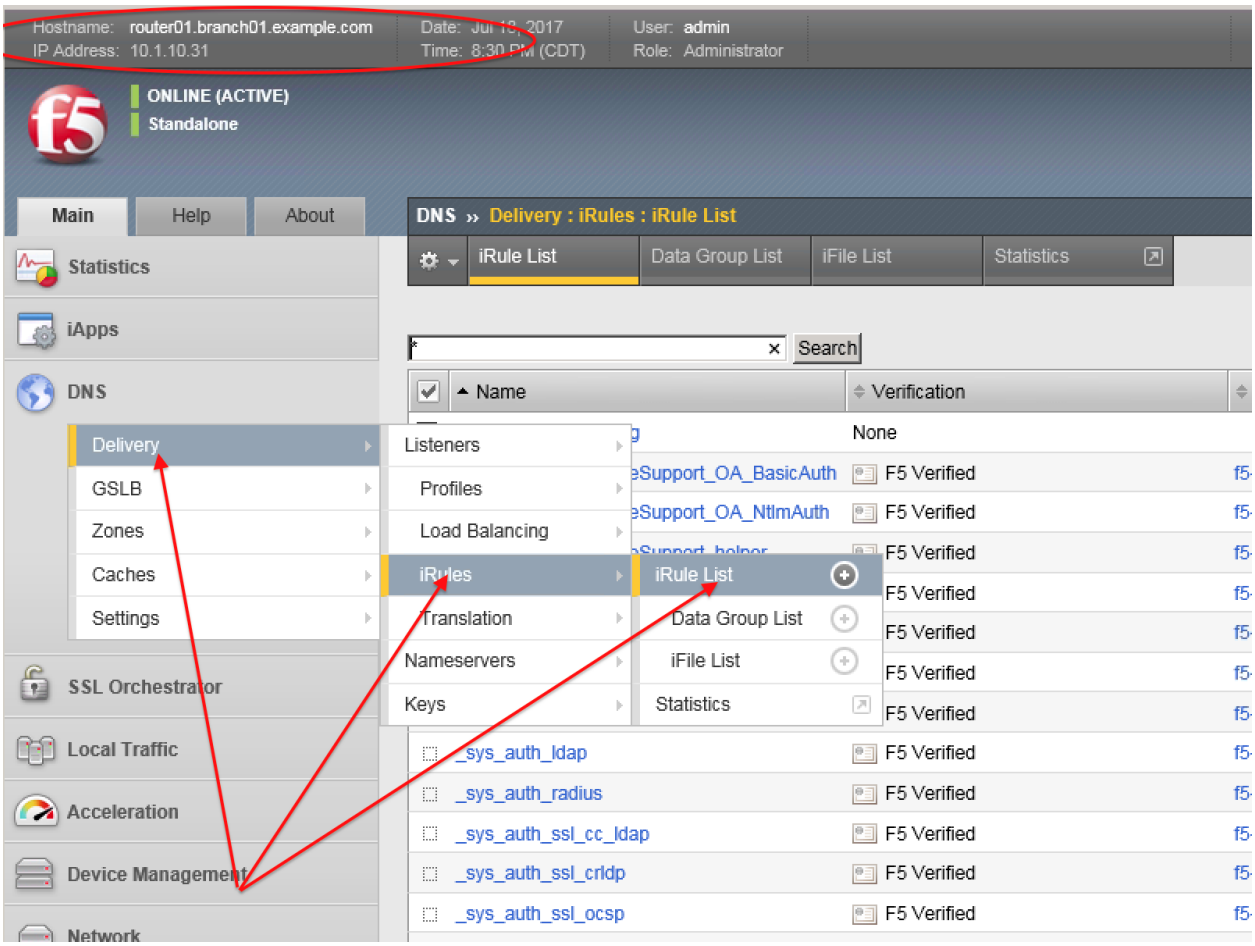

Command Prompt
C:\Users\user.EXAMPLE>
C:\Users\user.EXAMPLE>
C:\Users\user.EXAMPLE>
C:\Users\user.EXAMPLE>
C:\Users\user.EXAMPLE>dig cnn.com
; <<>> DiG 9.3.2 <<>> cnn.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1396
;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;cnn.com. IN A
;; ANSWER SECTION:
cnn.com. 111 IN A 10.1.71.21
;; Query time: 31 msec
;; SERVER: 10.1.70.200#53(10.1.70.200)
;; WHEN: Tue Jul 18 22:15:27 2017
;; MSG SIZE rcvd: 41
C:\Users\user.EXAMPLE>
Jul 18 22:15:27 router01 info tmm[11519]: 2017-07-18 22:15:26 router01.branch01.example.com
qid 1396 from 10.1.71.100#59856: view none: query: cnn.com IN A + (10.1.70.200%0)
Jul 18 22:15:27 router01 info tmm1[11519]: Rule /Common/DNS-query-filtering <DNS_REQUEST>: B
LOCK 0: Category /Common/News_and_Media matching cnn.com is filtered.
Jul 18 22:15:27 router01 info tmm[11519]: 2017-07-18 22:15:26 router01.branch01.example.com
qid 1396 to 10.1.71.100#59856: [NOERROR qr,rd] response: cnn.com. 111 IN A 10.1.71.21;
Update
Delete

## 3.8 IP Intelligence




### 3.8.1 Create an iRule

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




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

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

```
when DNS_RESPONSE {
    # If Query type was A and response is an answer. if { ([DNS::question type] eq “A”) and ([DNS::ptype] == “ANSWER”) } {
        set rrs [DNS::answer] foreach rr $rrs {
            if { [DNS::type $rr] eq “A” } {
            if {[llength [IP::reputation [DNS::rdata $rr]]] != 0} {
                # Bad IP Reputation for destination detected log local0.  “$rr: “[IP::reputation $ip]”, count: [llength [IP::reputation $rr]]”
            } }
        }
    }
}
```

| Setting | Value |
|---|---|
| Name | IPI_irule |

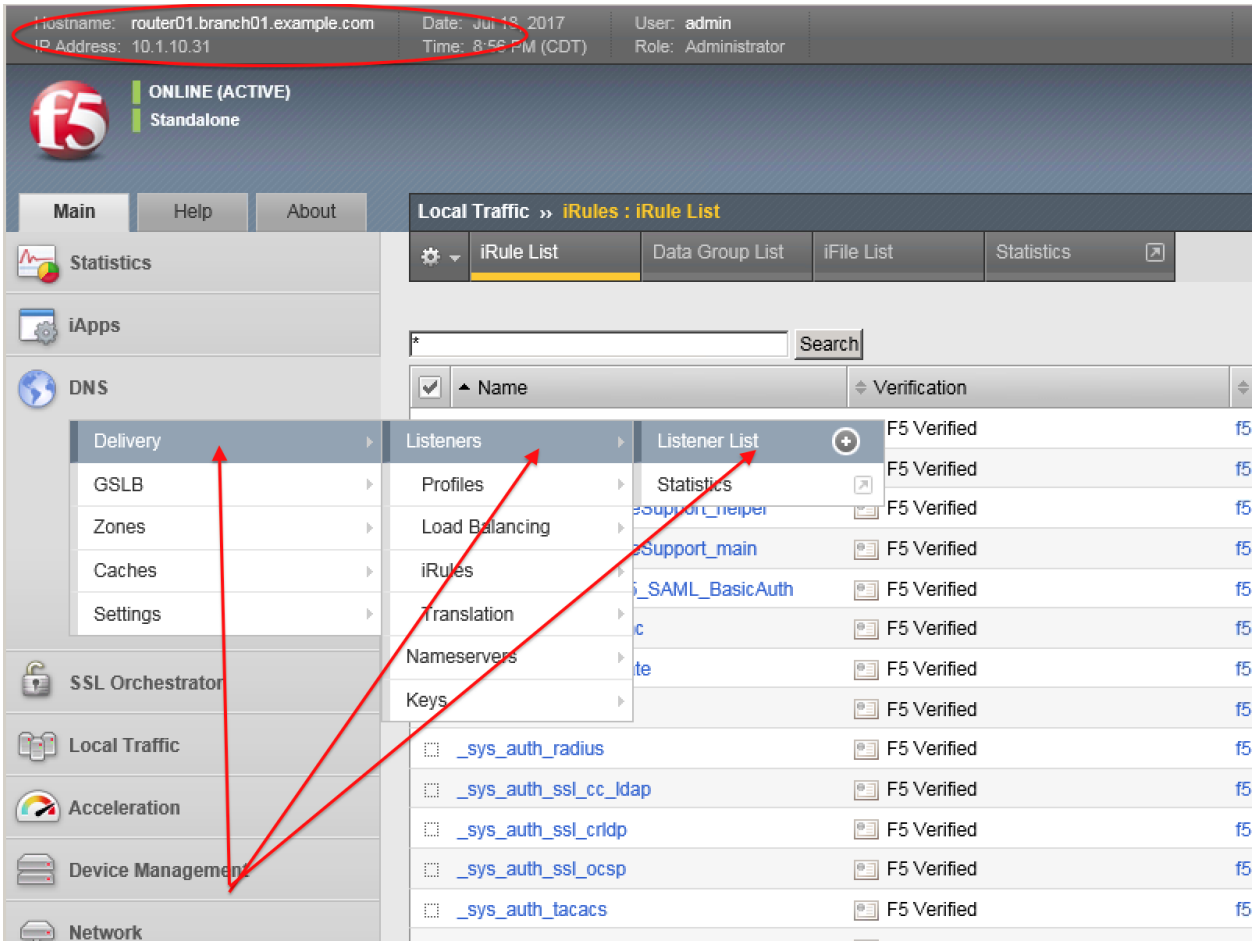
TODO: get updated irule from Brian Van Lieu

**TMSH**

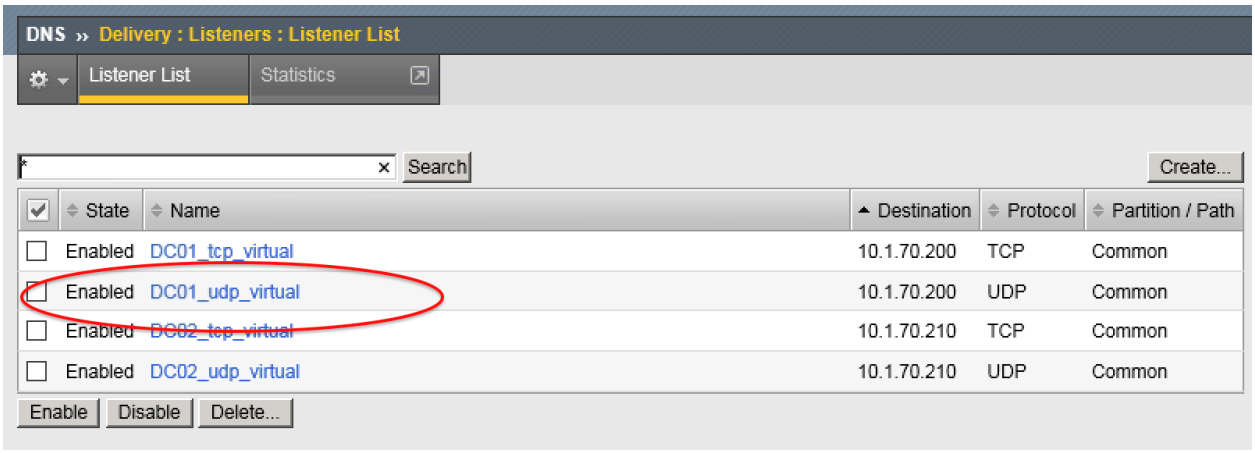
tmsh create ltm rule IPI_irule

### 3.8.2 iRule assignment

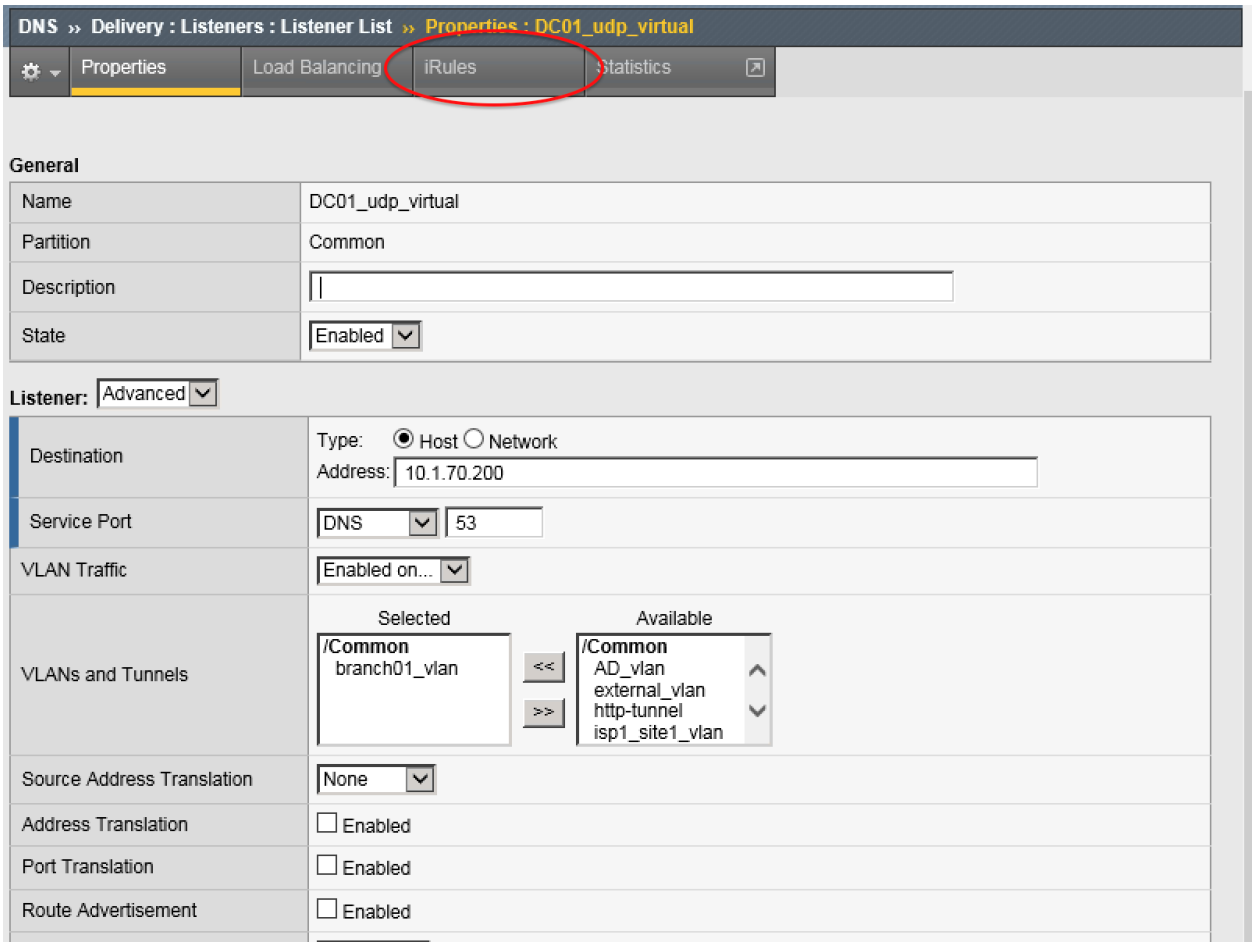
Navigate to: **DNS ›› Delivery : Listeners : Listener List**



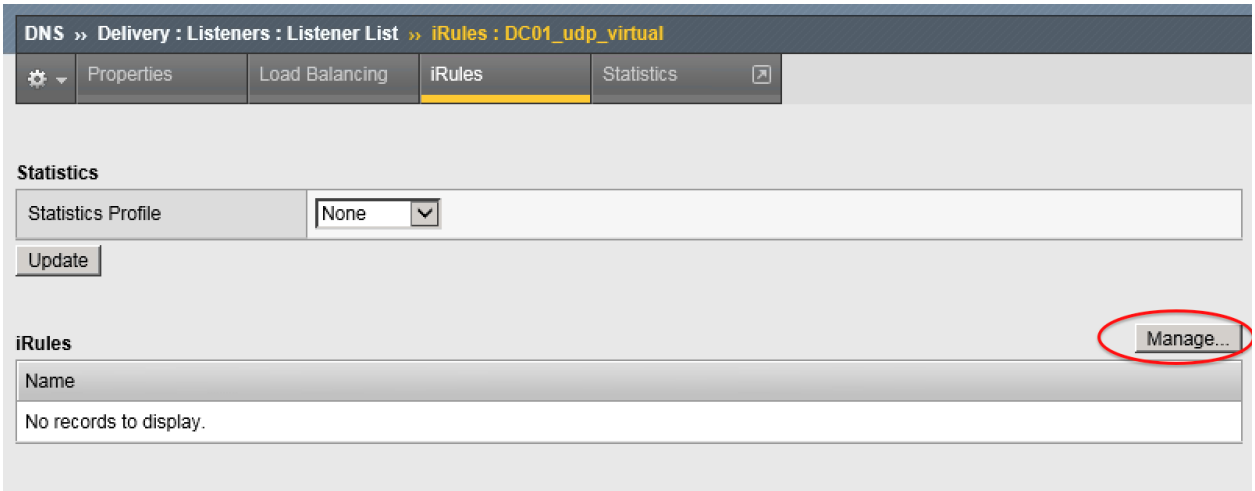

Navigate to the listener DC01_udp_virtual




Navigate to iRules section




Navigate to Manage




https://router01.branch01.example.com/tmui/Control/form?__handler=/tmui/dns/listener/irules&__source=Manage. . . &__lin

Highlight IPI iRule and move it to Selected column

TMSH commands for router01.branch01

**TMSH**

tmsh modify ltm virtual branch01_udp_53_virtual rules add { IPI_irule }

### 3.8.3 Results

From the CLI on the router01.branch01 BIGIP run

tail -f /var/log/ltm

TODO: put the results screenshots here

# 4 Credits

- Agility 2017:
    - Bill Wester
    - Boris Gekhtman
    - Brendan Gladney
    - Brian Buback
    - Dave Doucette
    - Emilio Torres
    - Josh Anderson
    - Robin Mordasiewicz
- Advisors:
    - Brian Van Lieu
    - Hitesh Patel
    - Joe Hermes
    - Jonathan Dehaan
    - Pat Chang
    - Pat Fiorino

F5 Networks, Inc. | f5.com

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com
©2017 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. These training materials and documentation are F5 Confidential Information and are subject to the F5 Networks Reseller Agreement. You may not share these training materials and documentation with any third party without the express written permission of F5.