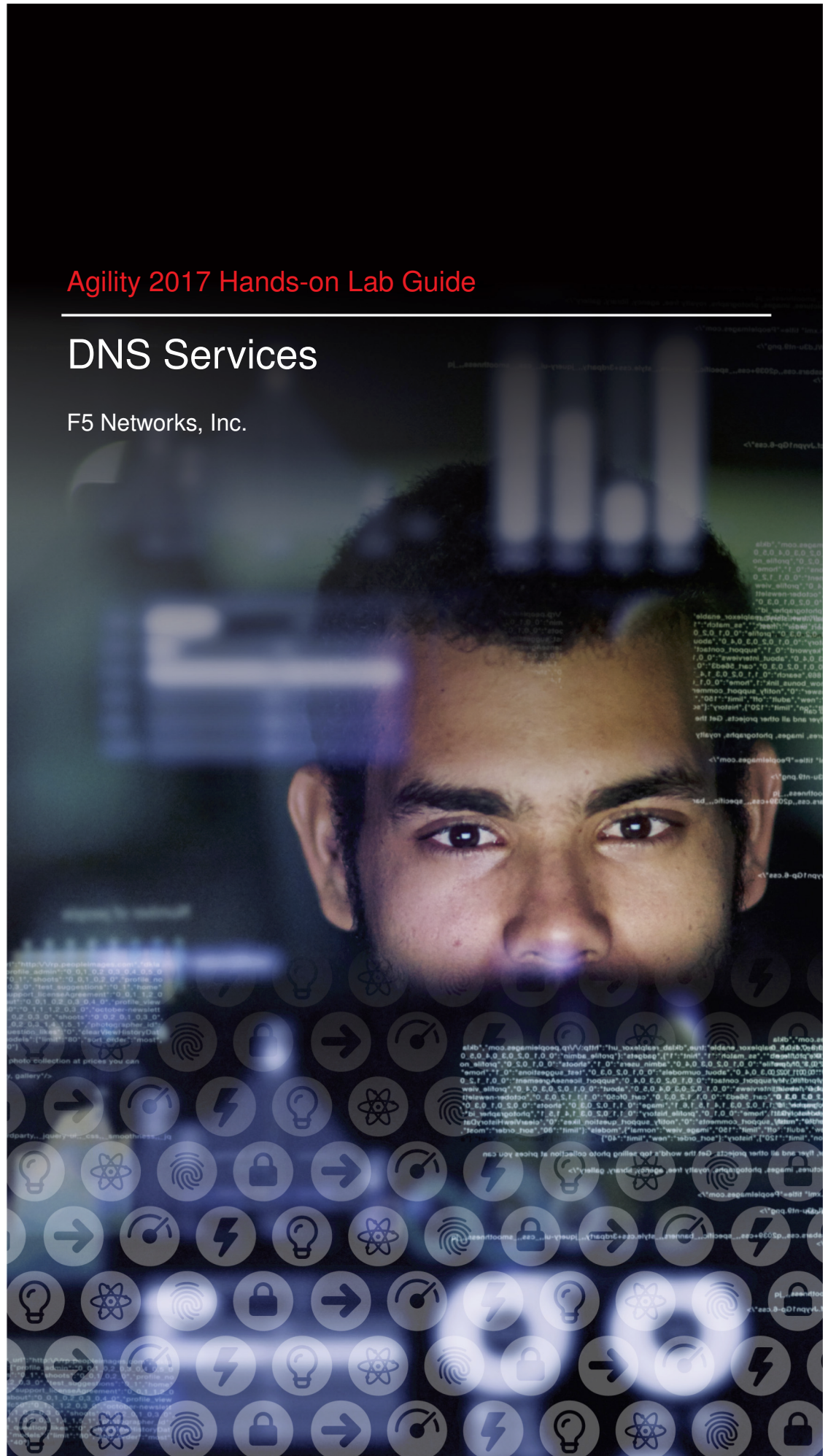




Agility 2017 Hands-on Lab Guide

DNS Services

F5 Networks, Inc.

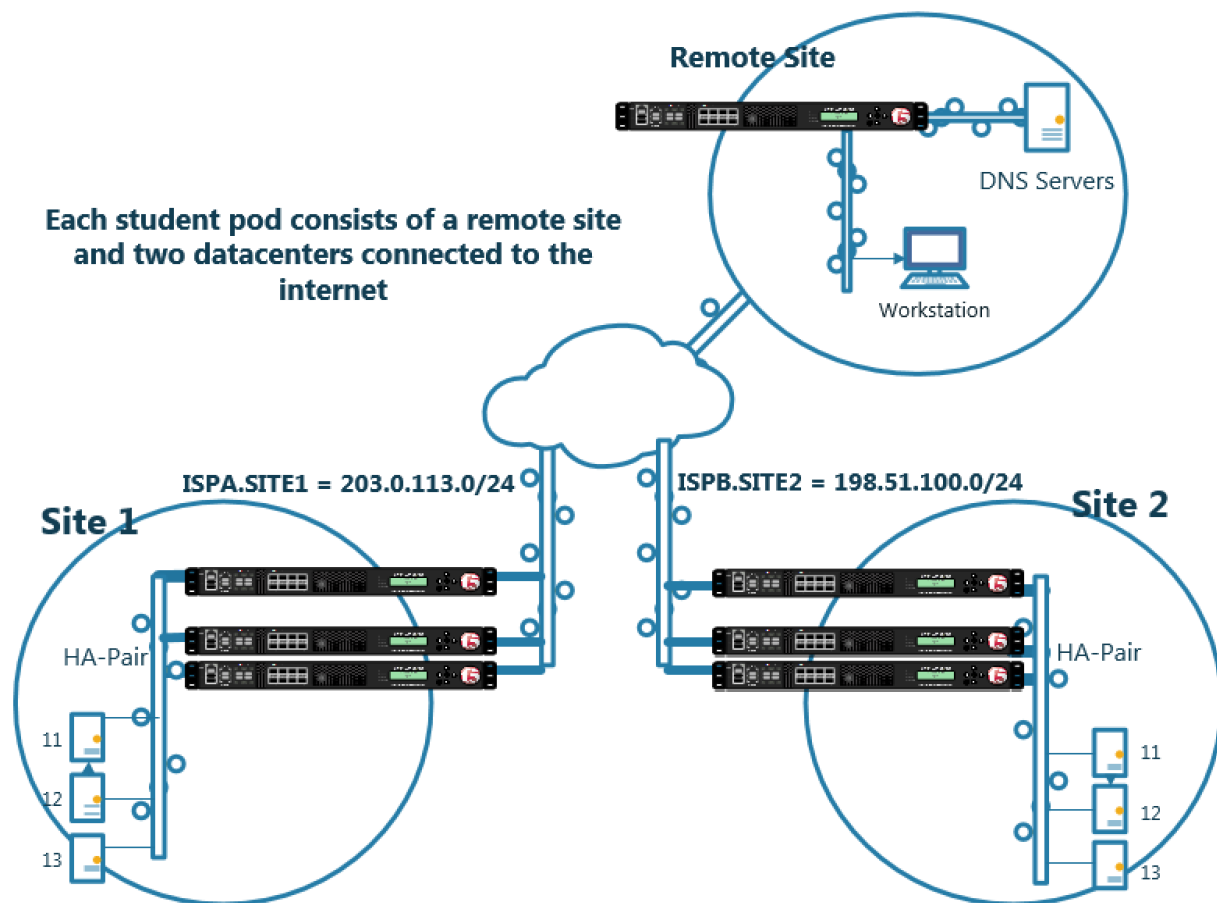


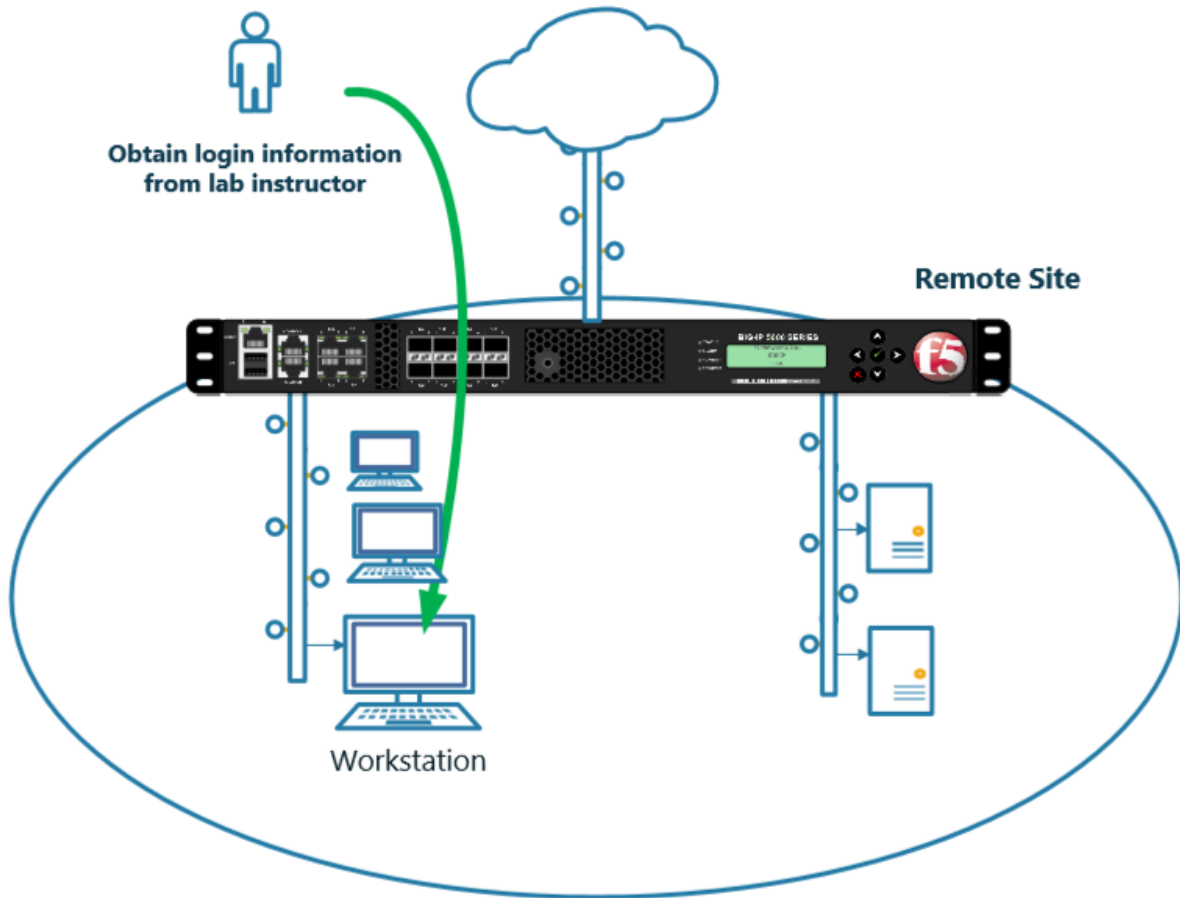
Contents:

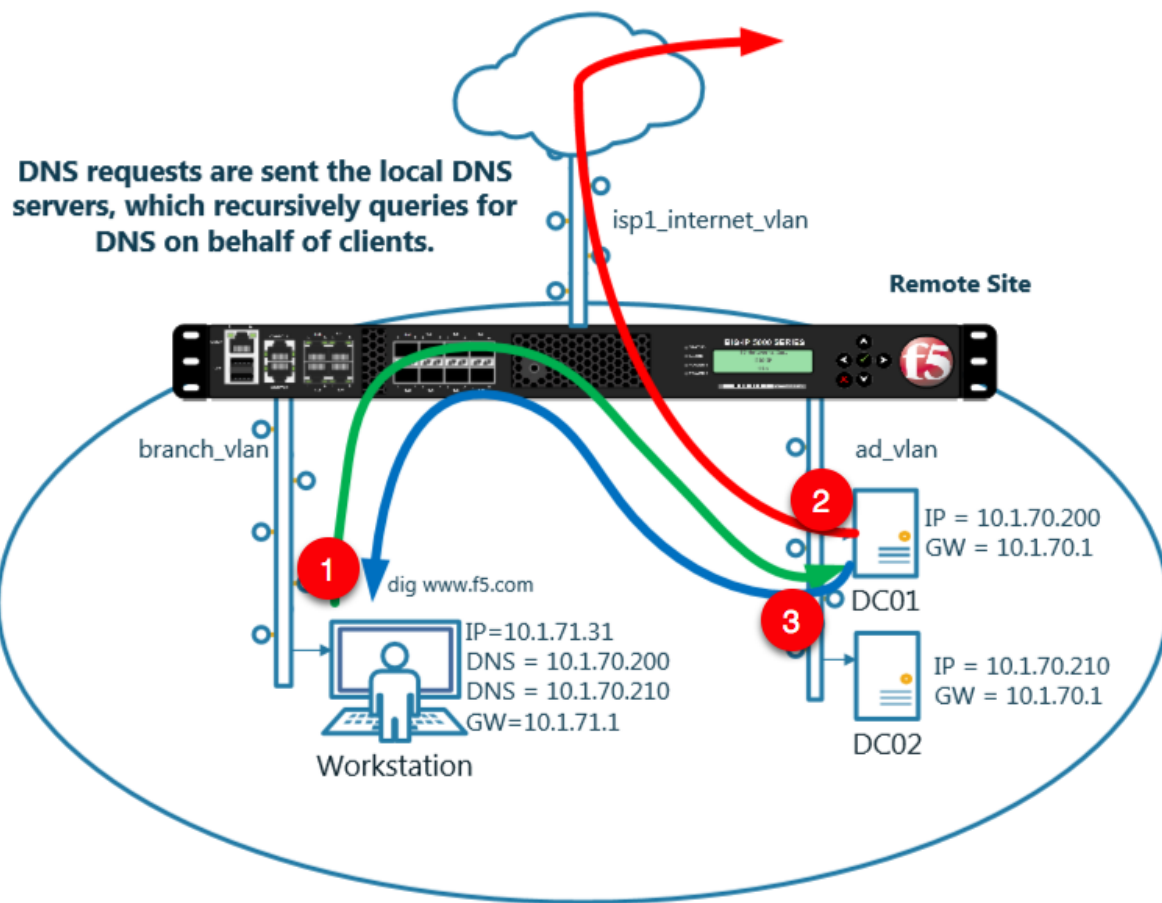
1	Lab Environment	5
2	Class 1 - Intro to GSLB	11
2.1	Settings	12
2.2	Listeners	13
2.2.1	Logging	13
2.2.2	DNS Profile	17
2.2.3	UDP Profile	20
2.2.4	TCP Profile	21
2.2.5	UDP IP Address	23
2.2.6	TCP IP Address	26
2.3	Datacenters	28
2.3.1	Servers	29
2.3.1.1	gtm1.site1	30
2.3.1.2	gtm1.site2	35
2.3.1.3	site1_ha-pair	39
2.3.1.4	site2_ha-pair	45
2.3.2	Device Trust	51
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 - Advanced GSLB	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

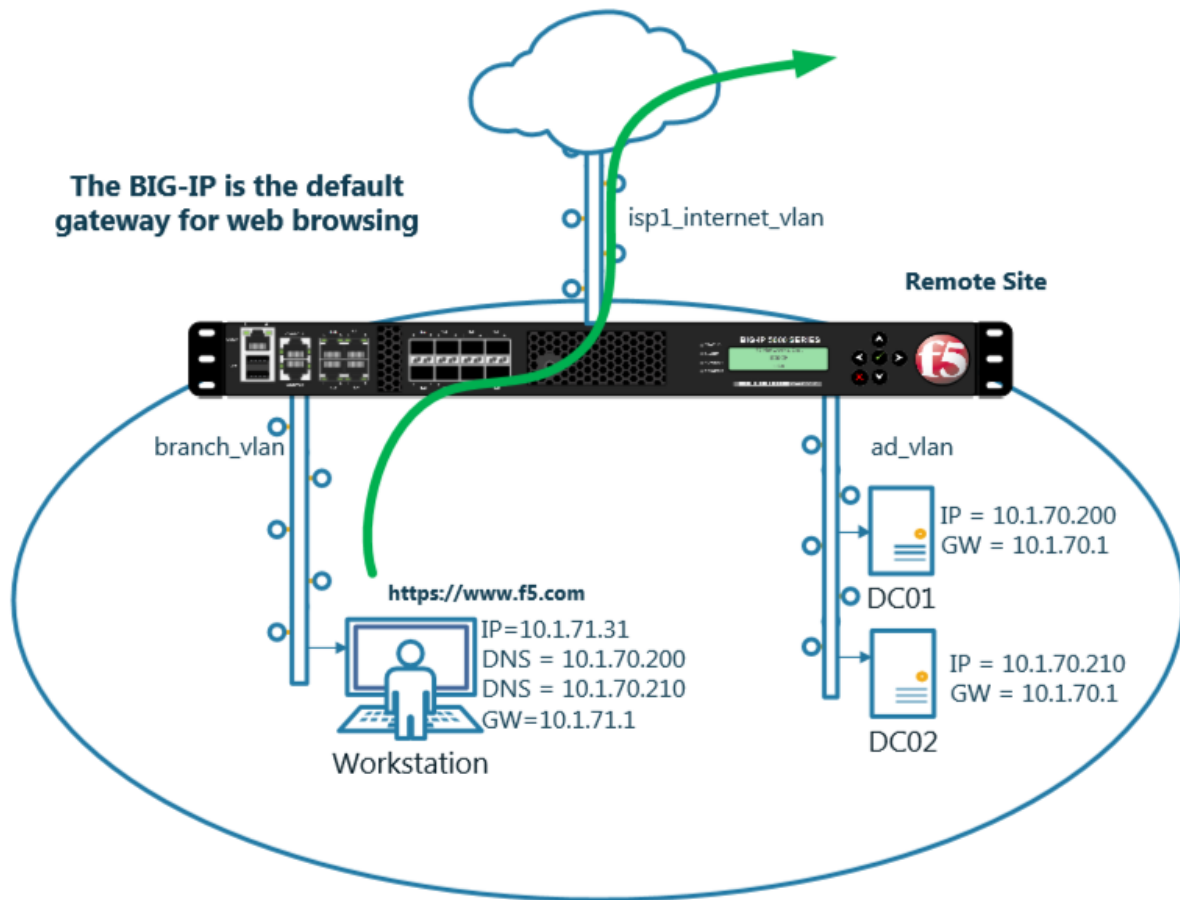
3.2.1	Log Profile	96
3.2.2	DNS Profile	100
3.2.3	UDP Profile	103
3.2.4	TCP Profile	104
3.2.5	UDP Listener	106
3.2.6	TCP Listeners	109
3.2.7	Results	112
3.3	Hidden Master	115
3.3.1	Name Server	115
3.3.2	DNS Express	117
3.3.3	Results	119
3.4	DNSSec	120
3.4.1	Zone Signing Key	121
3.4.2	Key Signing Key	122
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	Modify DNS Profile	131
3.5.3	Results	133
3.6	RPZ	141
3.6.1	Zone Runner	141
3.6.2	Name Server	145
3.6.3	DNS Express	147
3.6.4	Local Zone	149
3.6.5	Walled Garden	152
3.6.6	Results	154
3.7	URL Categorization	154
3.7.1	Create an iRule	155
3.7.2	iRule assignment	157
3.7.3	Results	160
4	Credits	167

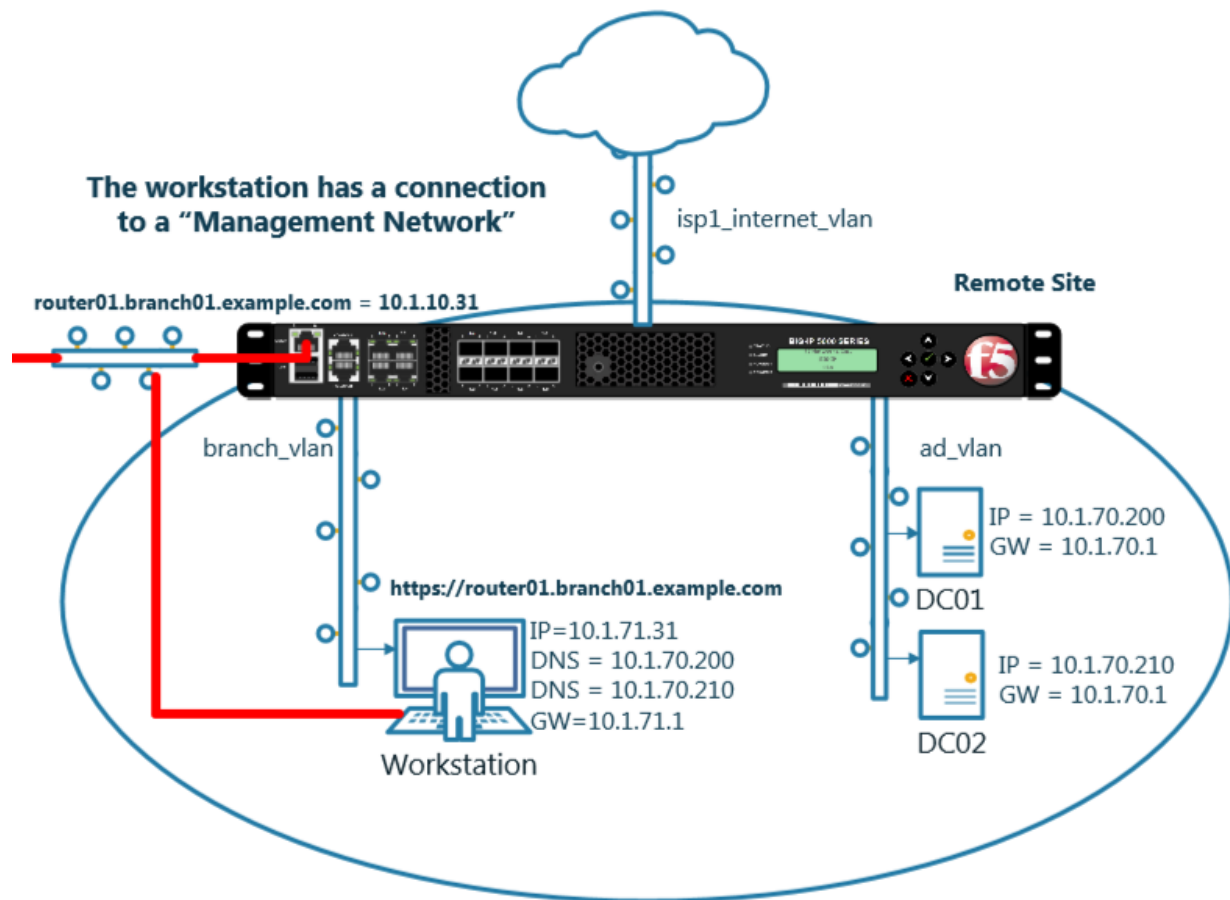
Lab Environment



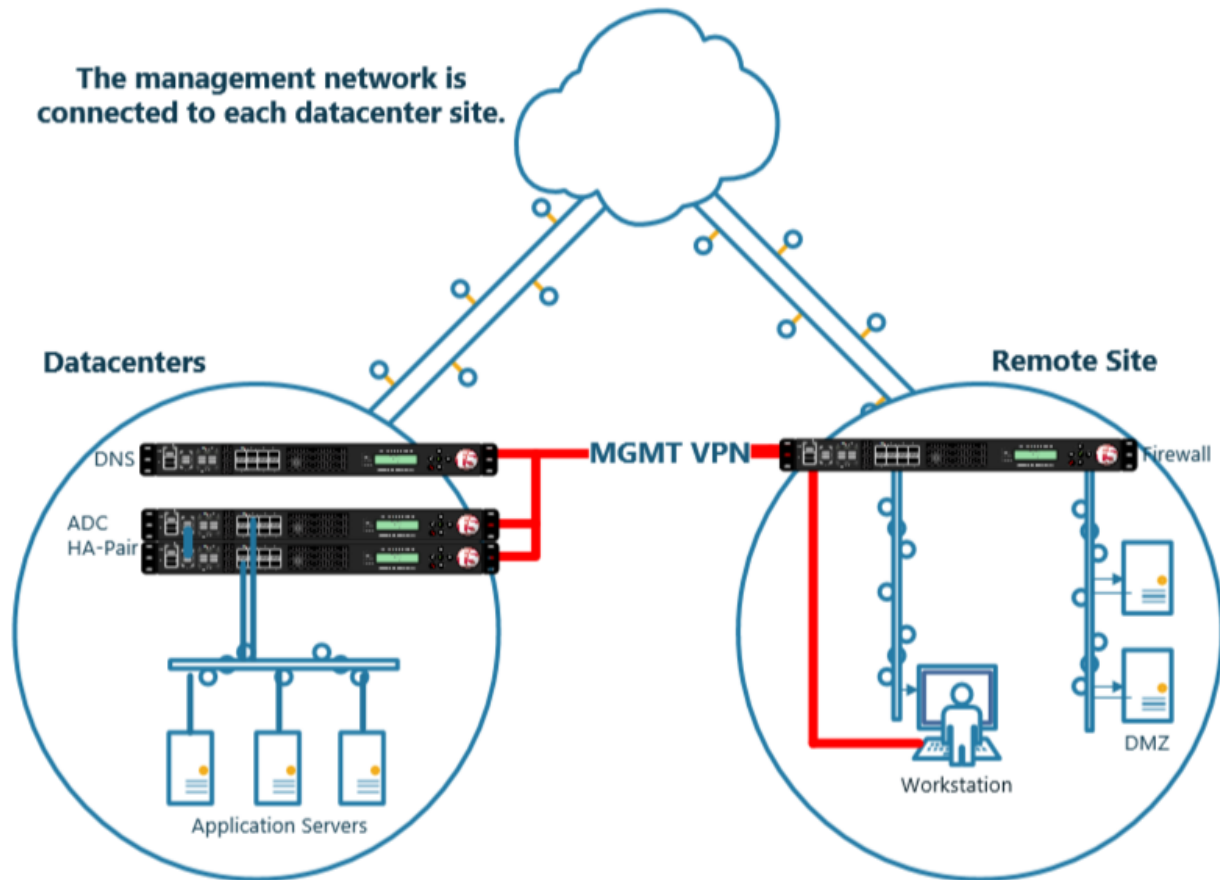








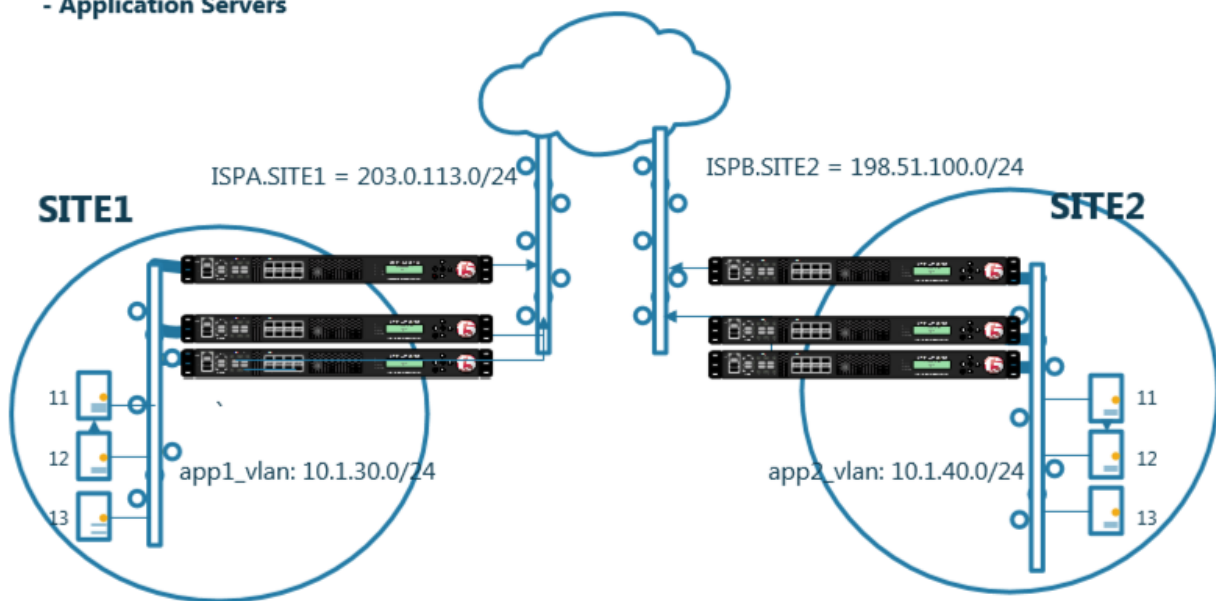
The management network is connected to each datacenter site.



Class 1 - Intro to GSLB

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

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



- Students will configure F5 DNS servers to support GSLB services on a single device in site1.
- Join an additional F5 DNS server in site2 to the GSLB cluster.
- An Internal group of DNS servers is authoritative for the zone example.com and contains a static A record for “www.example.com”, which resolves to 203.0.113.9.
- Students will add glue records and delegate gslb.example.com to the F5 GSLB DNS servers.

- Convert the A record “www.example.com” to be a CNAME record pointing to *www.gslb.example.com*.

At the end of the lab students will have configured F5 GSLB DNS servers to alternately resolve www.example.com to 203.0.113.9 and 198.51.100.41

2.1 Settings

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

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

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

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

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

ONLINE (ACTIVE)
Standalone

Main Help About

DNS » Settings : GSLB : General

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

Configuration Synchronization

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

Configuration Save

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

Auto-Discover ☒ Enabled

Request Interval 30 seconds

Monitoring

Heartbeat Interval 10 seconds

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

TMSH

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

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

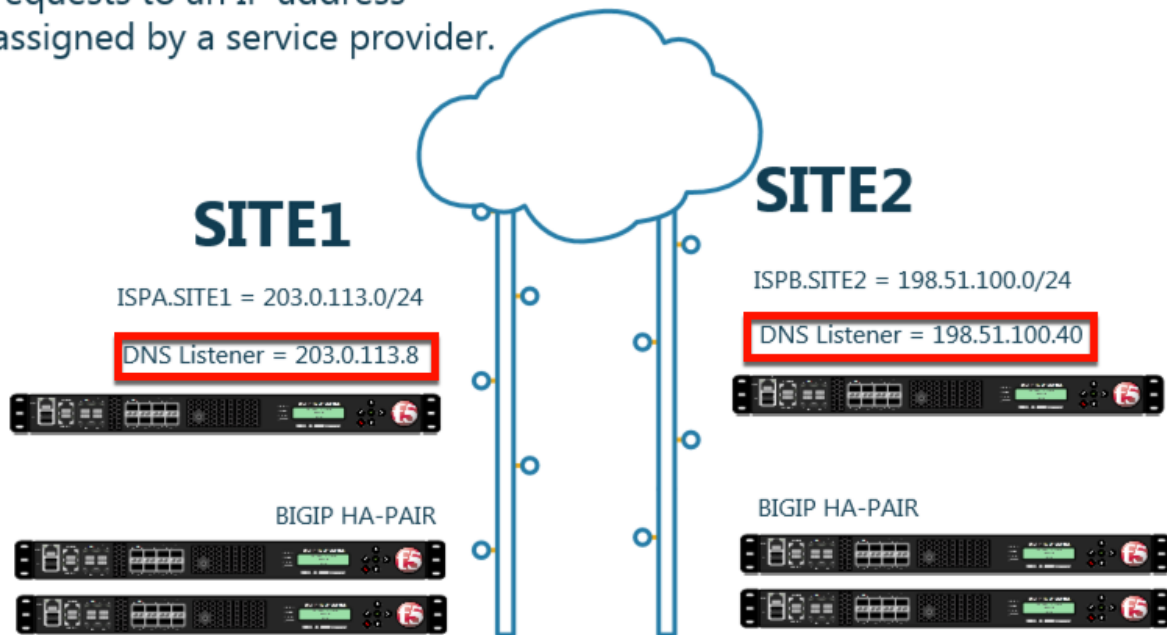
<https://support.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-implementations-12-0-0/4.html>

2.2 Listeners

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

We will be creating both TCP and UDP based listeners.

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

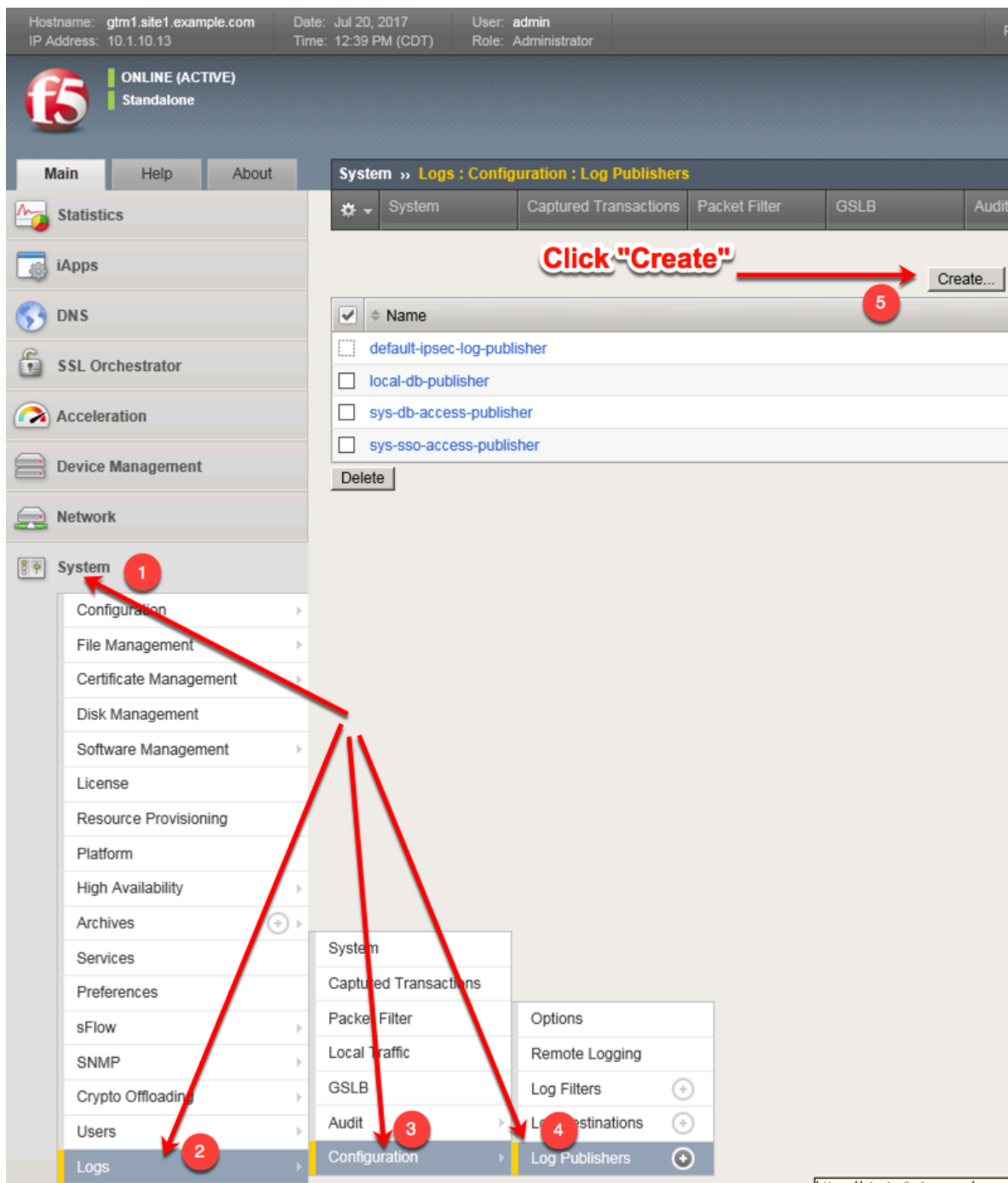


2.2.1 Logging

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

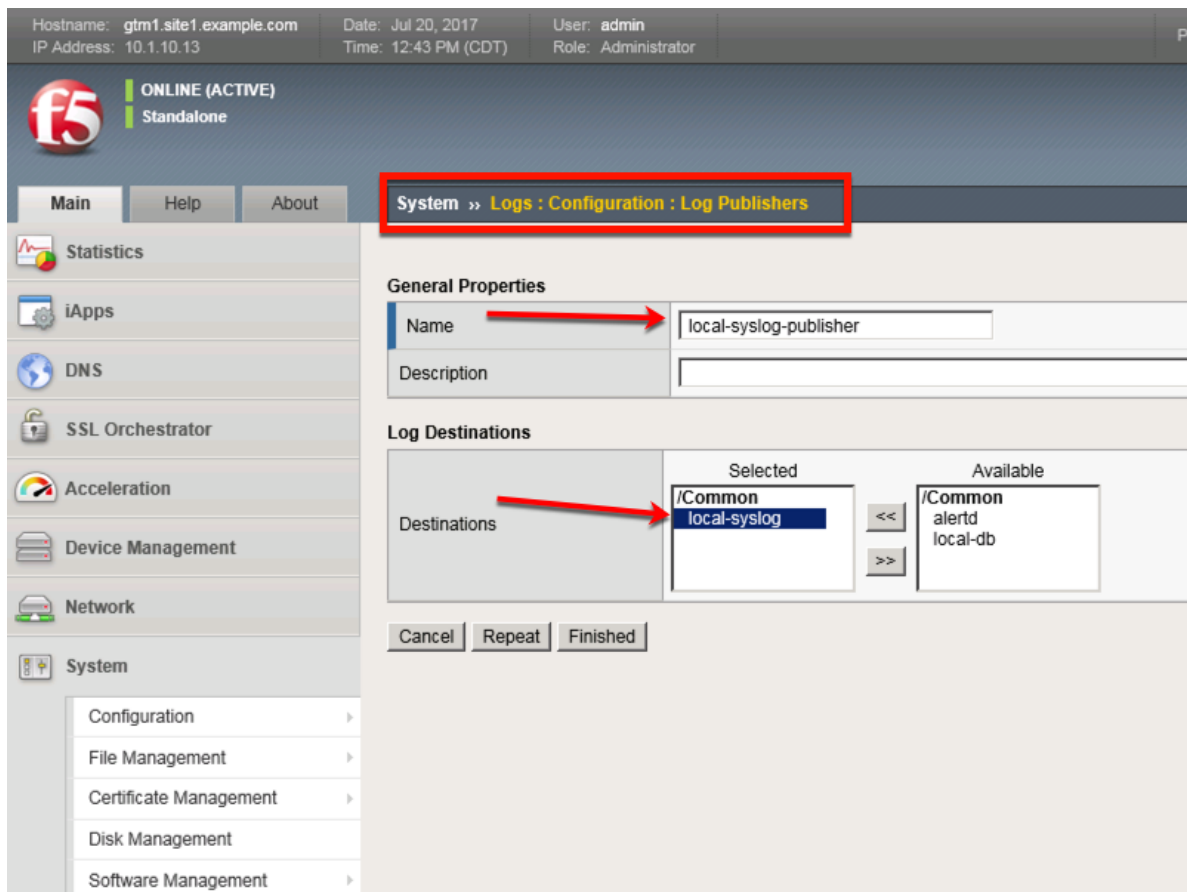
Note: It is required to complete the following task on both gtm1.site1 and gtm1.site2

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



Create a local syslog publisher according to the table below:

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



https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/system/log/create_publisher.jsp

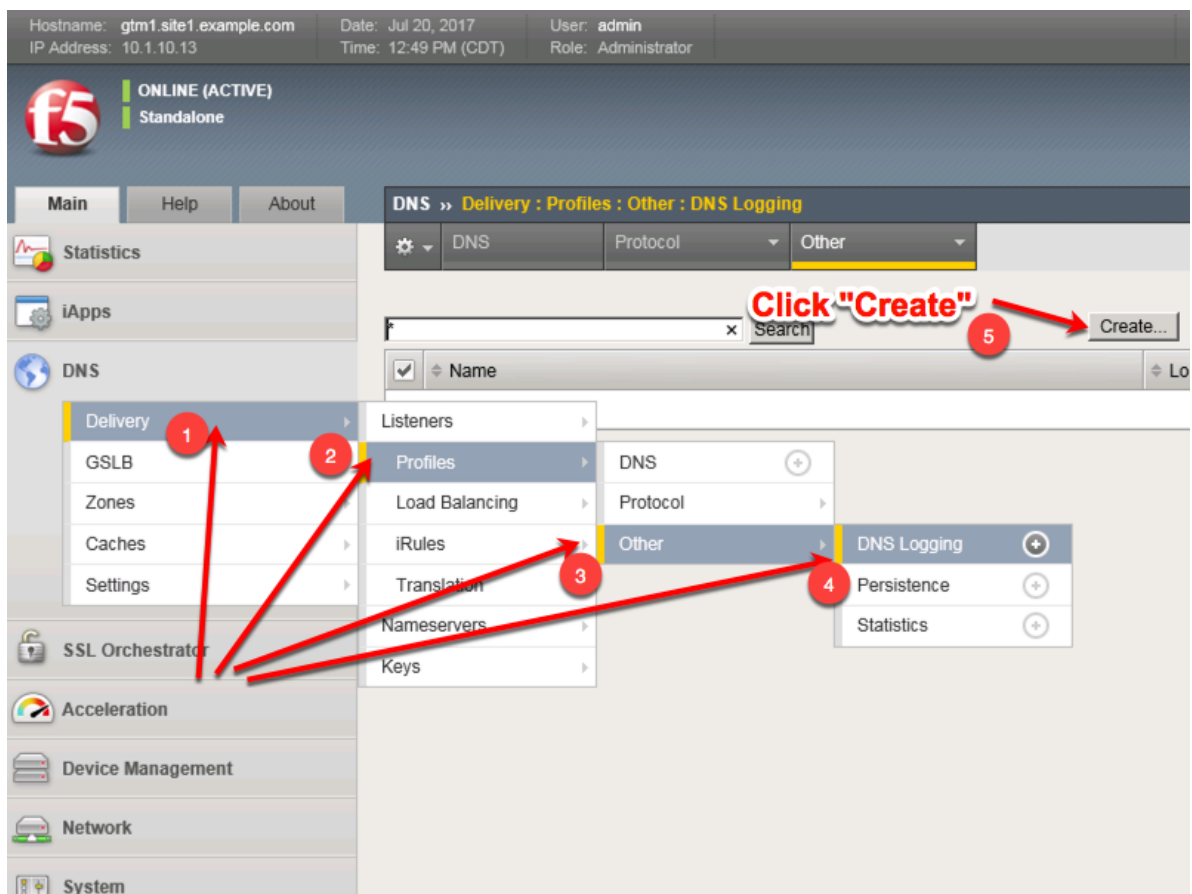
https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/system/log/create_publisher.jsp

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

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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

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

General Properties

Name
Description

Configuration

Log Publisher
Log Queries ☒ Enabled
Log Responses ☒ Enabled

Log Fields

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

Cancel Repeat Finished

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

https://gtm1.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
```

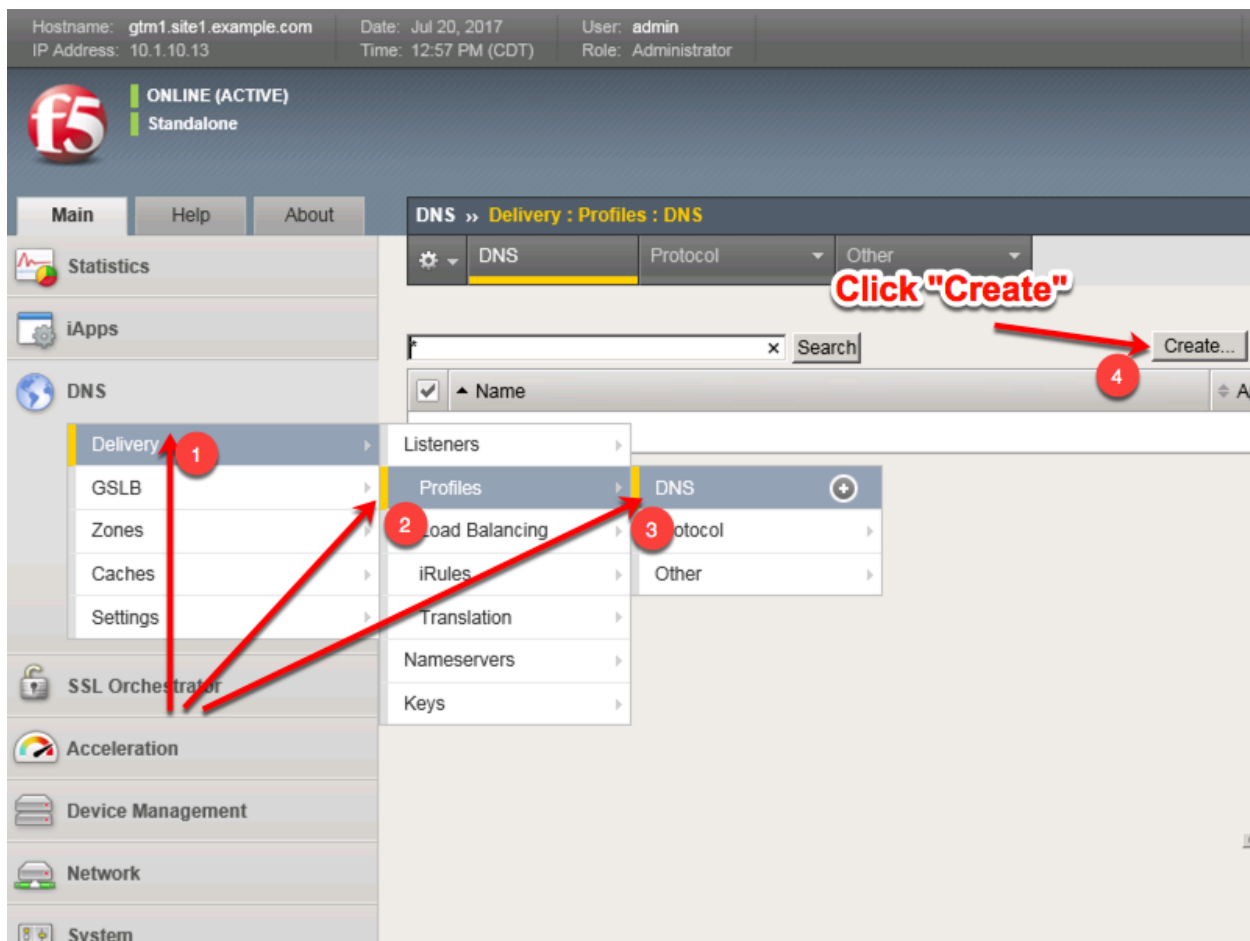
https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-12-0-0/5.html

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

Hostname: gtm1.site1.example.com

IP Address: 10.1.10.13

Date: Jul 20, 2017

Time: 1:02 PM (CDT)

User: admin

Role: Administrator

ONLINE (ACTIVE)

Standalone

Main

Help

About

DNS » Delivery : Profiles : DNS » New DNS Profile...

Statistics

iApps

DNS

Delivery

GSLB

Zones

Caches

Settings

SSL Orchestrator

Acceleration

Device Management

Network

System

General Properties

Name

example.com_dns_

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

DNSSEC

Enabled

GSLB

Enabled

DNS Express

Enabled

DNS Cache

Disabled

DNS Cache Name

Select...

DNS IPv6 to IPv4

Disabled

Unhandled Query Actions

Drop

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://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

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

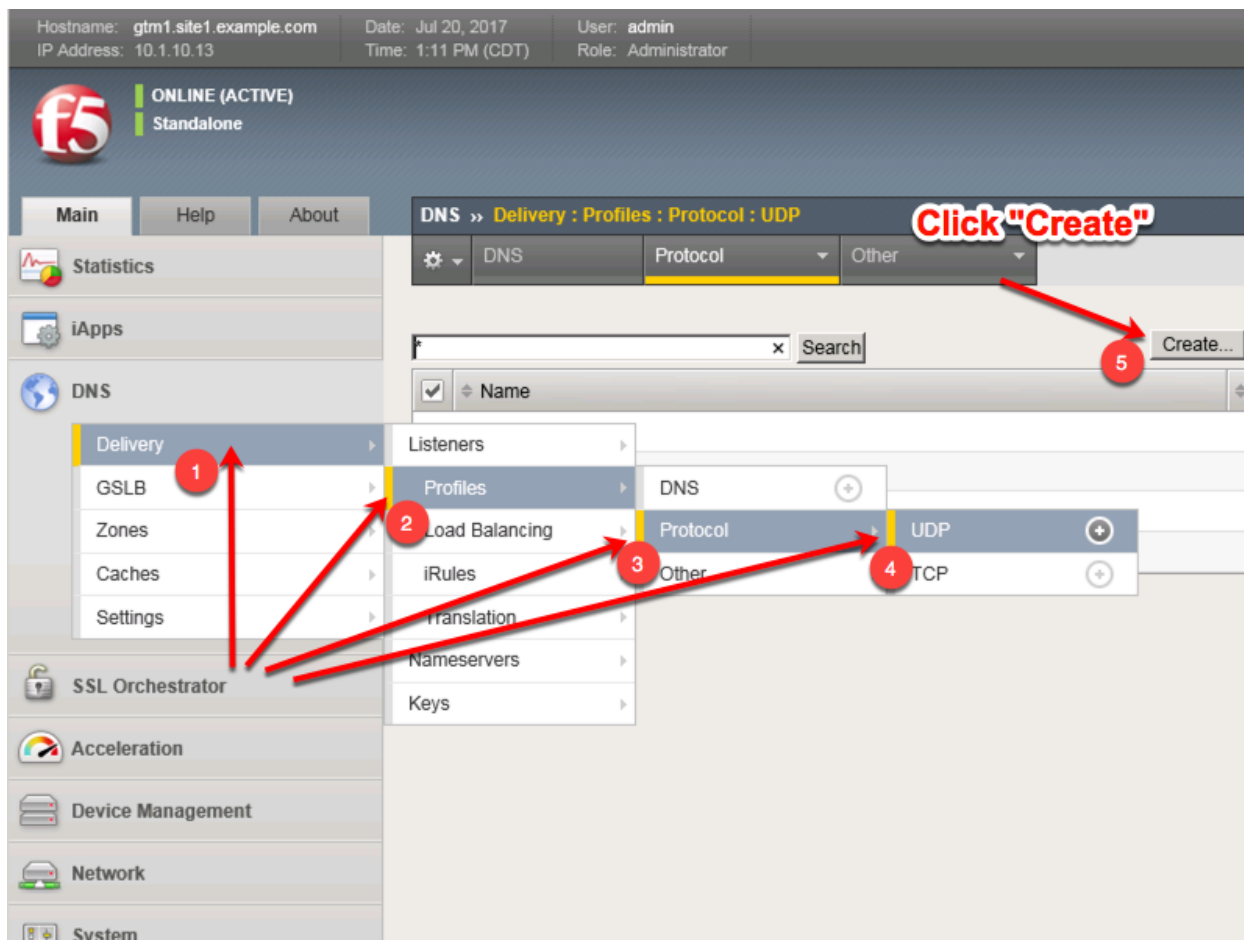
<https://support.f5.com/csp/article/K14510>

2.2.3 UDP Profile

A UDP profile is associated with a listener.

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

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



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

Setting	Value
Name	example.com_udp-dns_profile
Parent Profile	udp_gtm_dns

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin
 IP Address: 10.1.10.13 Time: 1:15 PM (CDT) Role: Administrator Partition: Common

f5 ONLINE (ACTIVE)
 Standalone

Main Help About

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

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

General Properties

Name example.com_udp
 Parent Profile udp

Settings Custom ☐

Proxy Maximum Segment	<input type="checkbox"/>	<input type="checkbox"/>
Idle Timeout	Specify... 60 seconds	<input type="checkbox"/>
IP ToS	Specify... 0	<input type="checkbox"/>
Link QoS	Specify... 0	<input type="checkbox"/>
Datagram LB	<input type="checkbox"/>	<input type="checkbox"/>
Allow No Payload	<input type="checkbox"/>	<input type="checkbox"/>
TTL Mode	Proxy	<input type="checkbox"/>
Don't Fragment Mode	PMTU	<input type="checkbox"/>

Cancel Repeat Finished

<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

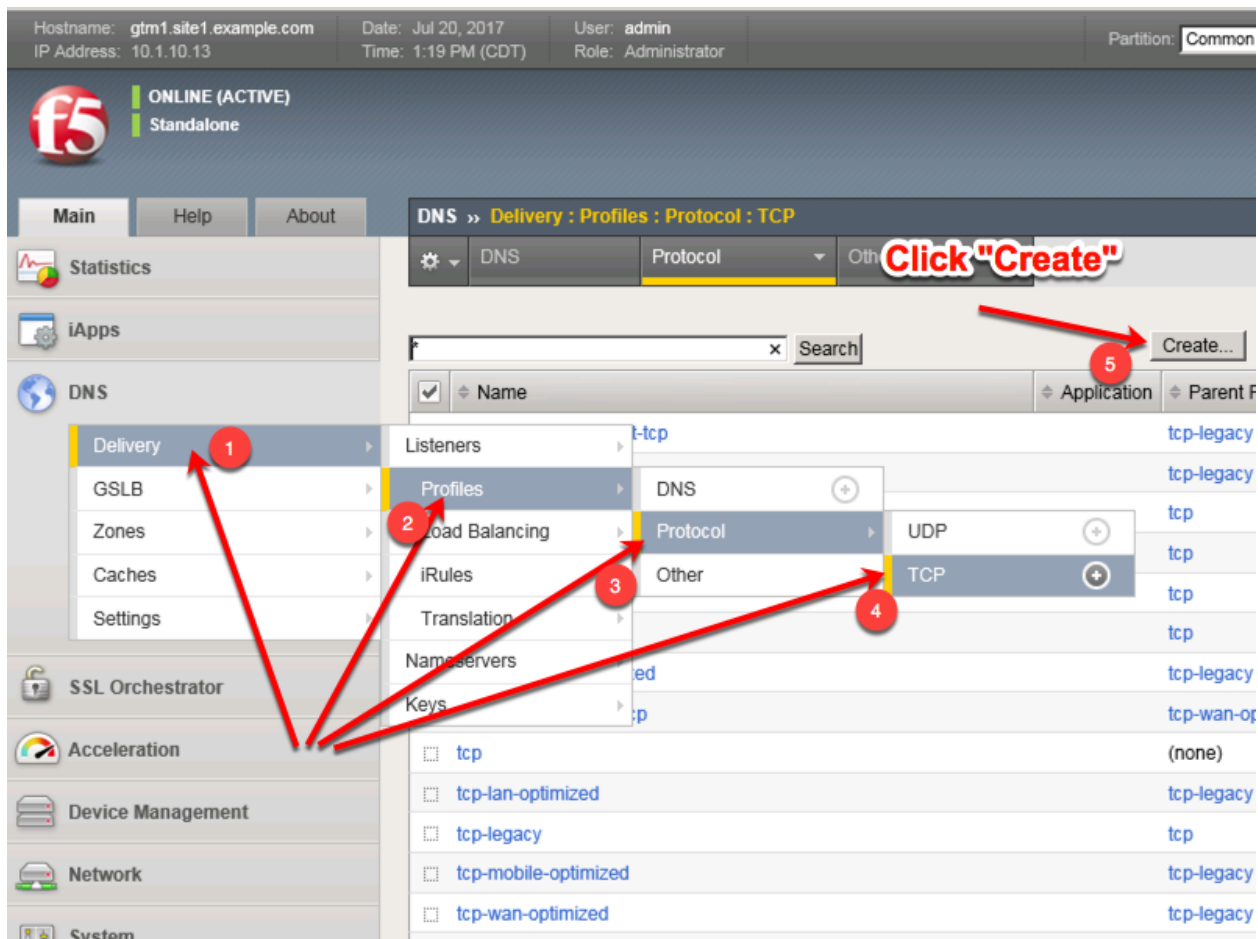
```
tms create ltm profile udp example.com_udp-dns_profile defaults-from udp_gtm_dns
```

2.2.4 TCP Profile

A TCP profile is associated with a listener.

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

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



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

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

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

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

Name example.com_tcp_x
Parent Profile f5-tcp-wan

Timer Management

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

Scroll way down to find the "Finish" button

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

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

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

TMSH

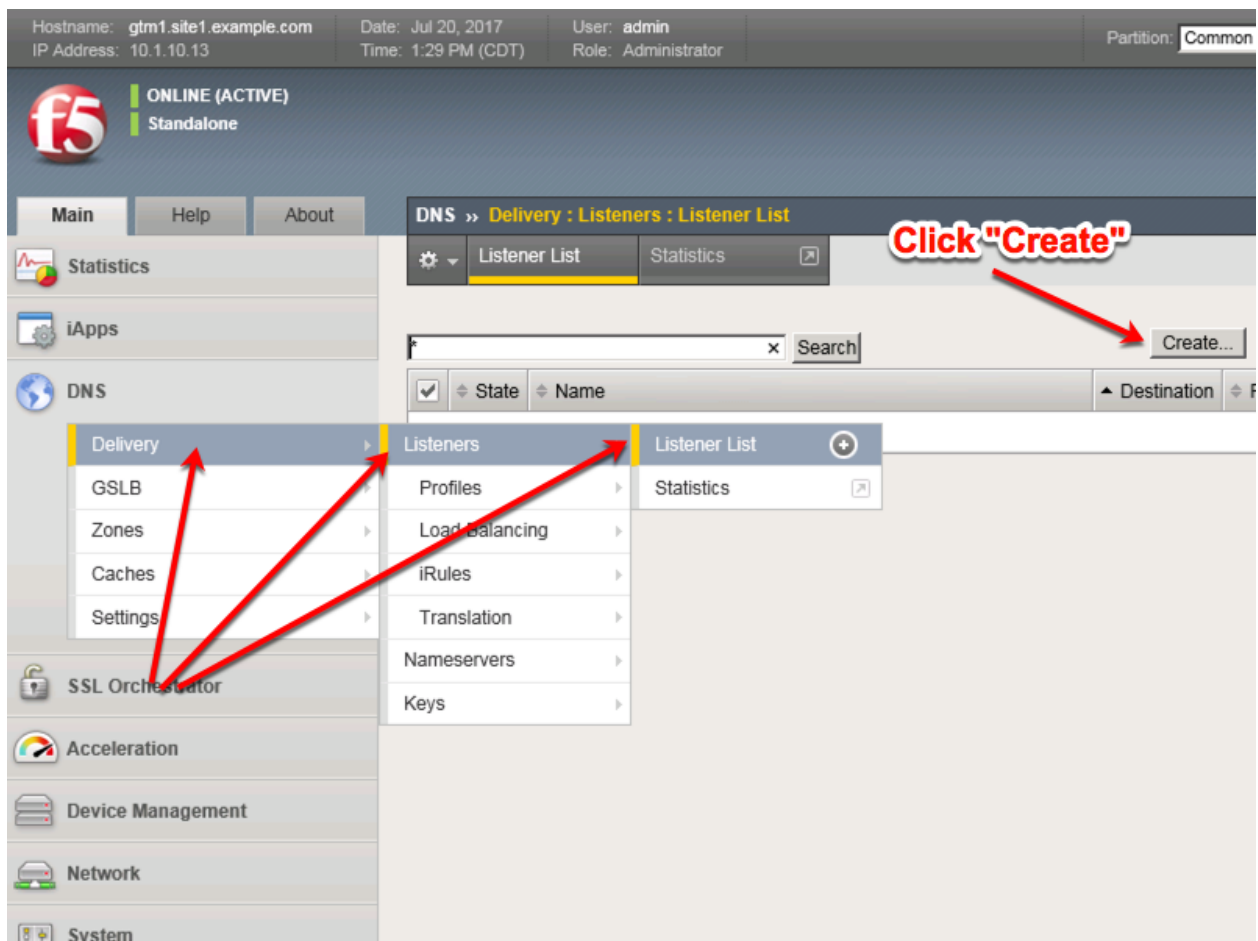
tmsh create ltm profile tcp example.com_tcp-dns_profile defaults-from tcp-wan-optimized

2.2.5 UDP IP Address

A UDP listener will receive and process DNS queries.

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

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



Create a UDP listener according to the following table:

Setting	gtm1.site1	gtm1.site2
Name	isp1_site1_ns1.example.com_udp_53_virtual	isp1_site2_ns2.example.com_udp_53_virtual
Destination	203.0.113.8	198.51.100.40
Protocol 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>

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

f5 ONLINE (ACTIVE)
Standalone

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

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

General

Name: isp1_site1_ns1.example.com_udp_53
Description:
State: Enabled

Listener: Advanced

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

Service: Advanced

Protocol: UDP
Protocol Profile (Client): example.com_udp-dns_profile
Protocol Profile (Server): (Use Client Profile)
DNS Profile: example.com_dns_profile

gtm1.site1 TMSH command:

TMSH

```
tmsh create gtm listener isp1_site1_ns1.example.com_udp_53_virtual address 203.0.113.8 ip-protocol udp
mask 255.255.255.255 port 53 profiles add { example.com_dns_profile example.com_udp-dns_profile }
```

gtm1.site2 TMSH command:

TMSH

```
tmsh create gtm listener isp1_site2_ns2.example.com_udp_53_virtual address 198.51.100.40 ip-protocol
udp mask 255.255.255.255 port 53 profiles add { example.com_dns_profile example.com_udp-dns_profile }
```

}

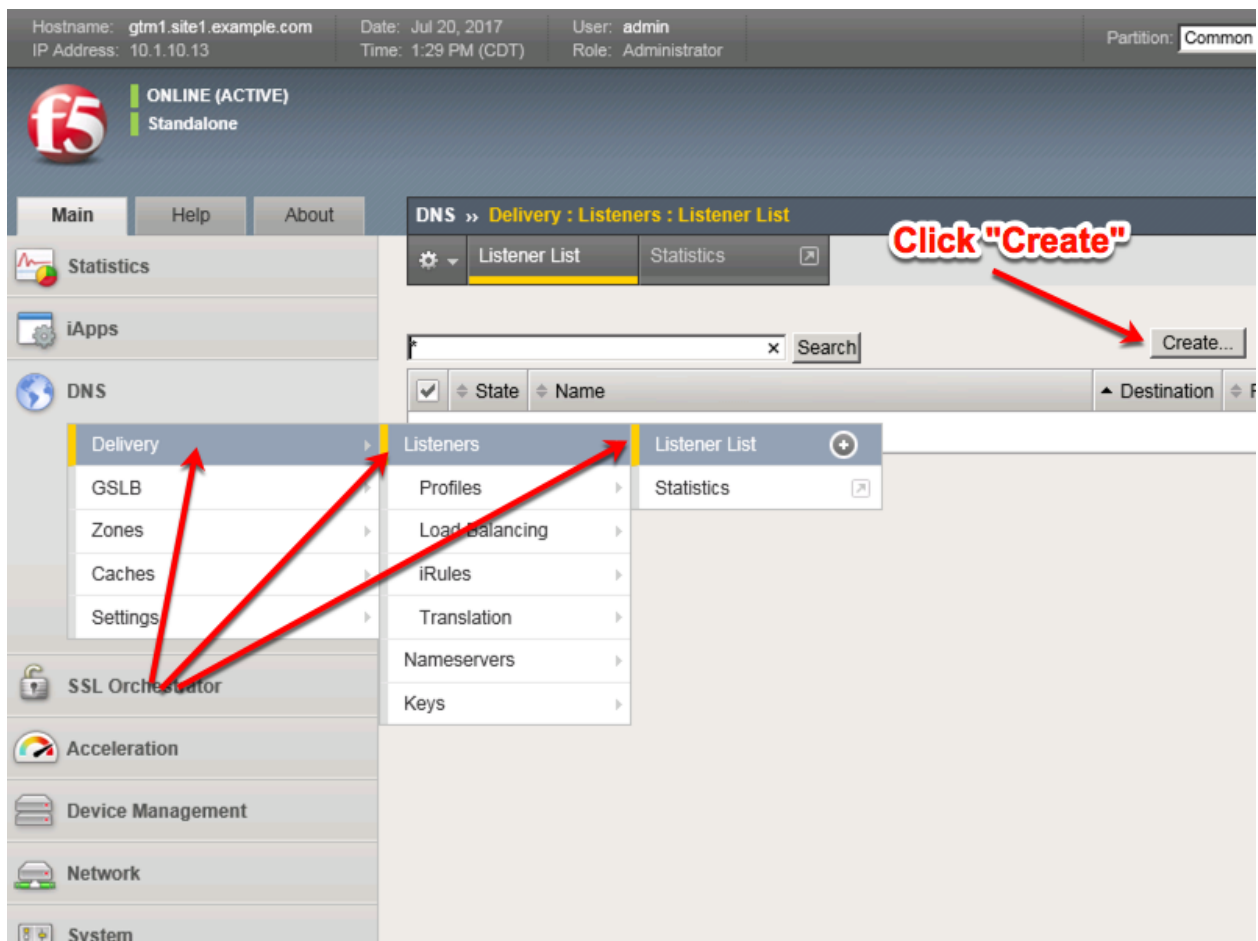
<https://support.f5.com/csp/article/K14923>

2.2.6 TCP IP Address

A TCP listener will receive and process DNS queries.

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

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



Create a TCP listener.

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

Hostname: gtm1.site1.example.com

IP Address: 10.1.10.13

Date: Jul 20, 2017

Time: 2:18 PM (CDT)

User: admin

Role: Administrator

Partition: Common

f5

ONLINE (ACTIVE)

Standalone

Main

Help

About

Statistics

iApps

DNS

- Delivery
- GSLB
- Zones
- Caches
- Settings

SSL Orchestrator

Acceleration

Device Management

Network

System

DNS » Delivery : Listeners : Listener List » New...

General

Name

isp1_site1_ns1.example.com_udp_53

Description

State

Enabled

Listener: Advanced

Destination

Type: Host Network

Address: 203.0.113.8

Service Port

DNS 53

VLAN Traffic

All VLANs

Source Address Translation

None

Address Translation

Enabled

Port Translation

Enabled

Route Advertisement

Enabled

Auto Last Hop

Default

Last Hop Pool

None

Service: Advanced

Protocol

TCP

Protocol Profile (Client)

example.com_tcp-dns_profile

Protocol Profile (Server)

(Use Client Profile)

DNS Profile

example.com_dns_profile

Load Balancing

Default Pool

None

Default Persistence Profile

None

Fallback Persistence Profile

None

<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

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

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

gtm1.site2 TMSH command:

TMSH

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

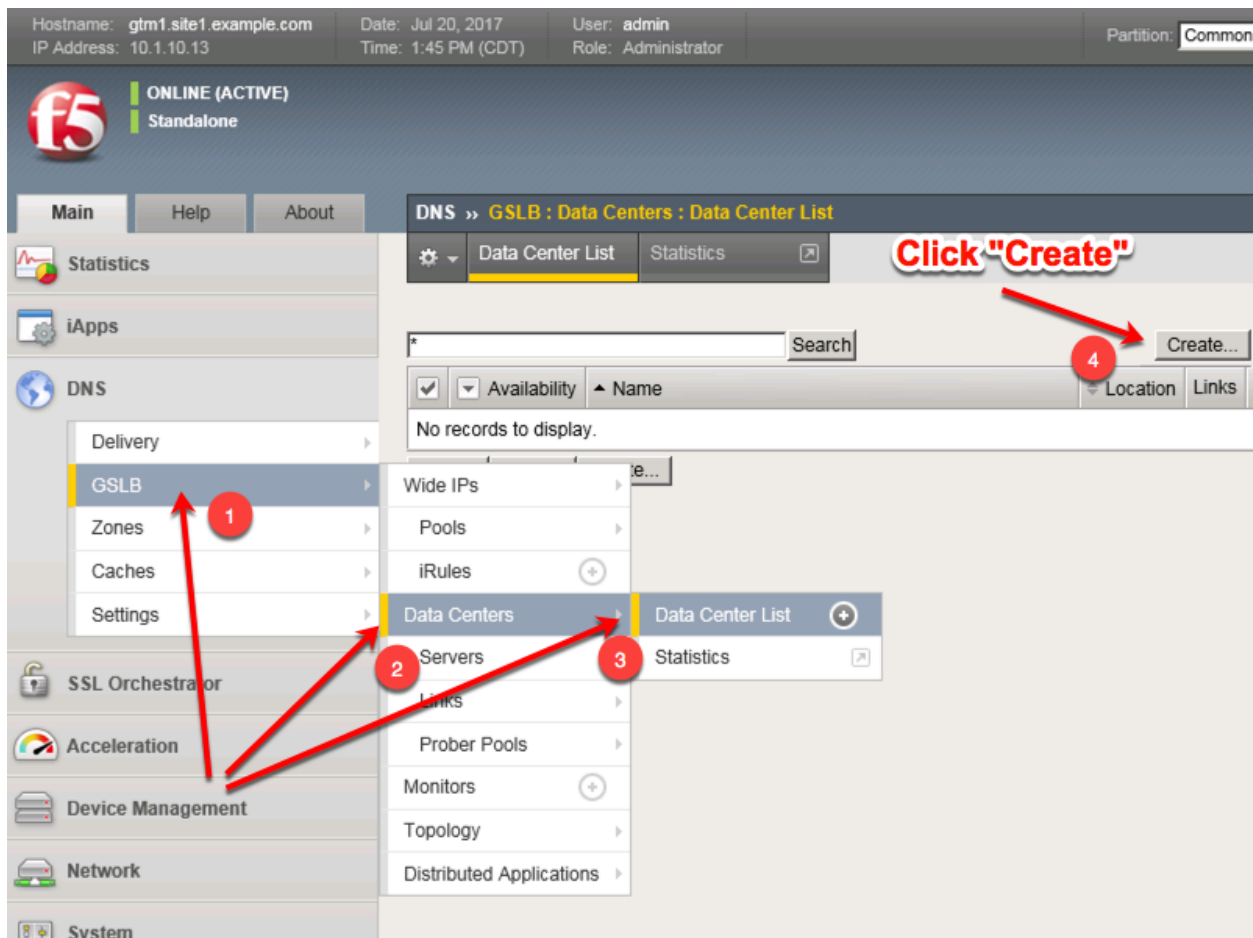
<https://support.f5.com/csp/article/K14923>

2.3 Datacenters

Datacenters are logical groupings of devices that share a gateway.

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

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



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

Create two data centers according to the table below:

Setting	Value
Name	site1_datacenter
Name	site2_datacenter

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

ONLINE (ACTIVE)
Standalone

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

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

General Properties

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

Cancel Repeat Finished

Repeat this step to create "site2_datacenter"

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

TMSH command for only site1.gtm1:

TMSH

```
tmsh create gtm datacenter site1_datacenter
```

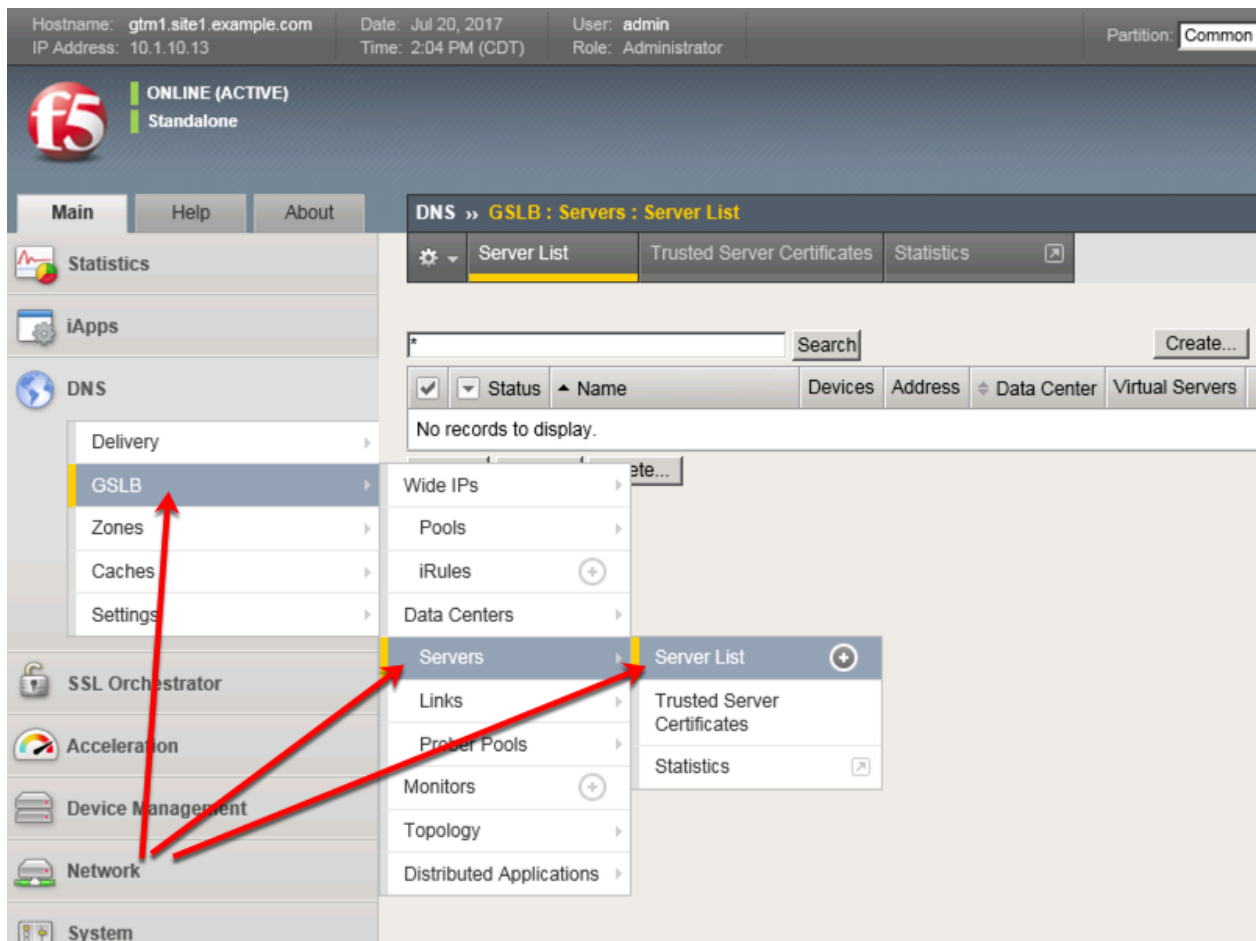
TMSH

```
tmsh create gtm datacenter site2_datacenter
```

2.3.1 Servers

Server objects need to be defined and grouped into a Datacenter

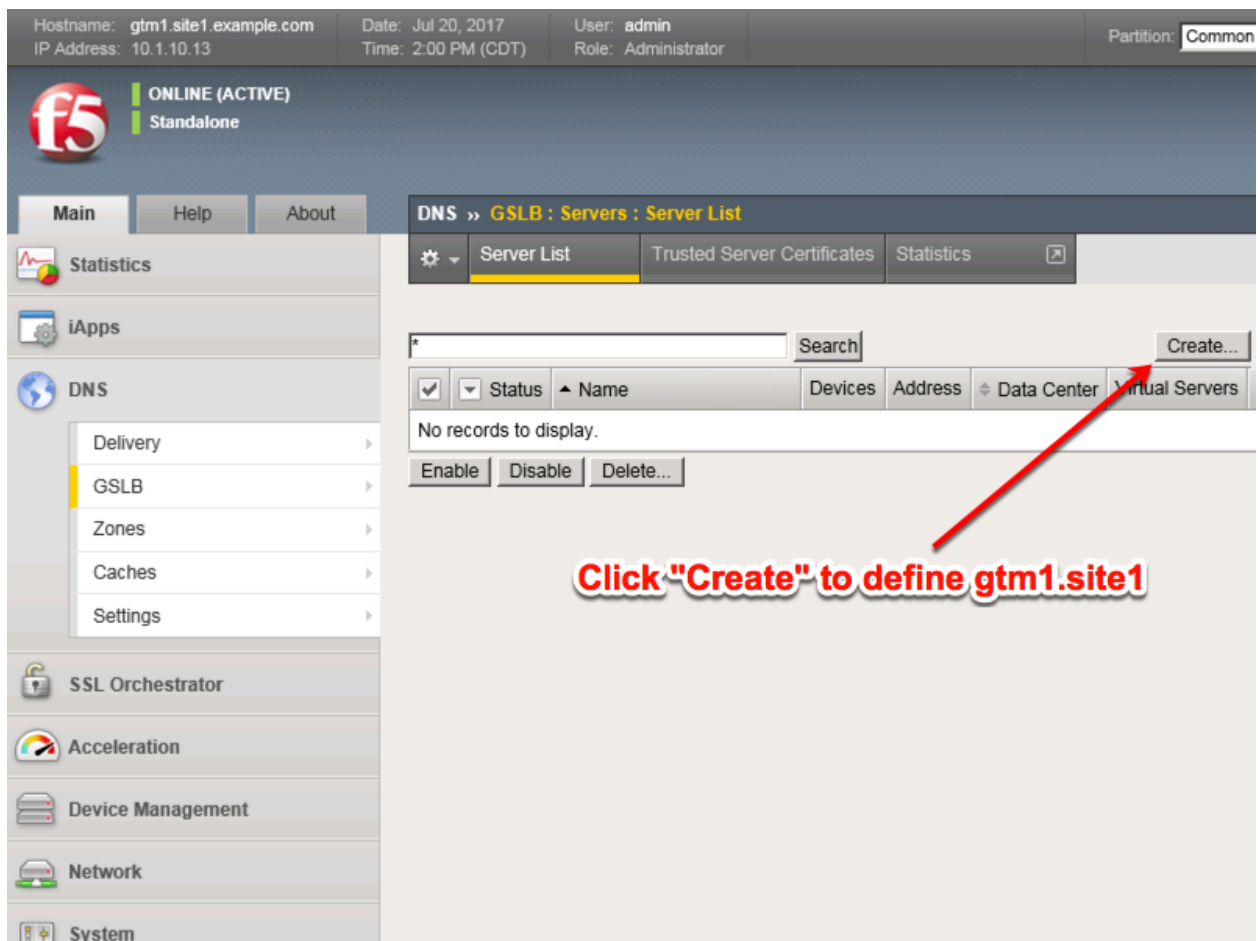
Navigate to: **DNS » GSLB : Servers : Server List**



<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

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin
IP Address: 10.1.10.13 Time: 2:29 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

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

Devices

Click "Add" → Add

Device Name	Address
No data available in table	

Big-IP System Devices

Edit Delete

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

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

f5 ONLINE (ACTIVE)
 Standalone

Main Help About

Statistics
 iApps
 DNS
 Delivery
GSLB
 Zones
 Caches
 Settings

SSL Orchestrator
 Acceleration
 Device Management
 Network
 System

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

Add BIG-IP System Device

General Properties

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

OK Cancel **4**
Click "OK"

Devices

Add
 Delete
 BIG-IP System Devices
 No data available in table
 Edit Delete

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

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

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

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

Devices

Device Name	Address
gtm1.site1.example.com	203.0.113.7

Add Edit Delete

Configuration: Advanced

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

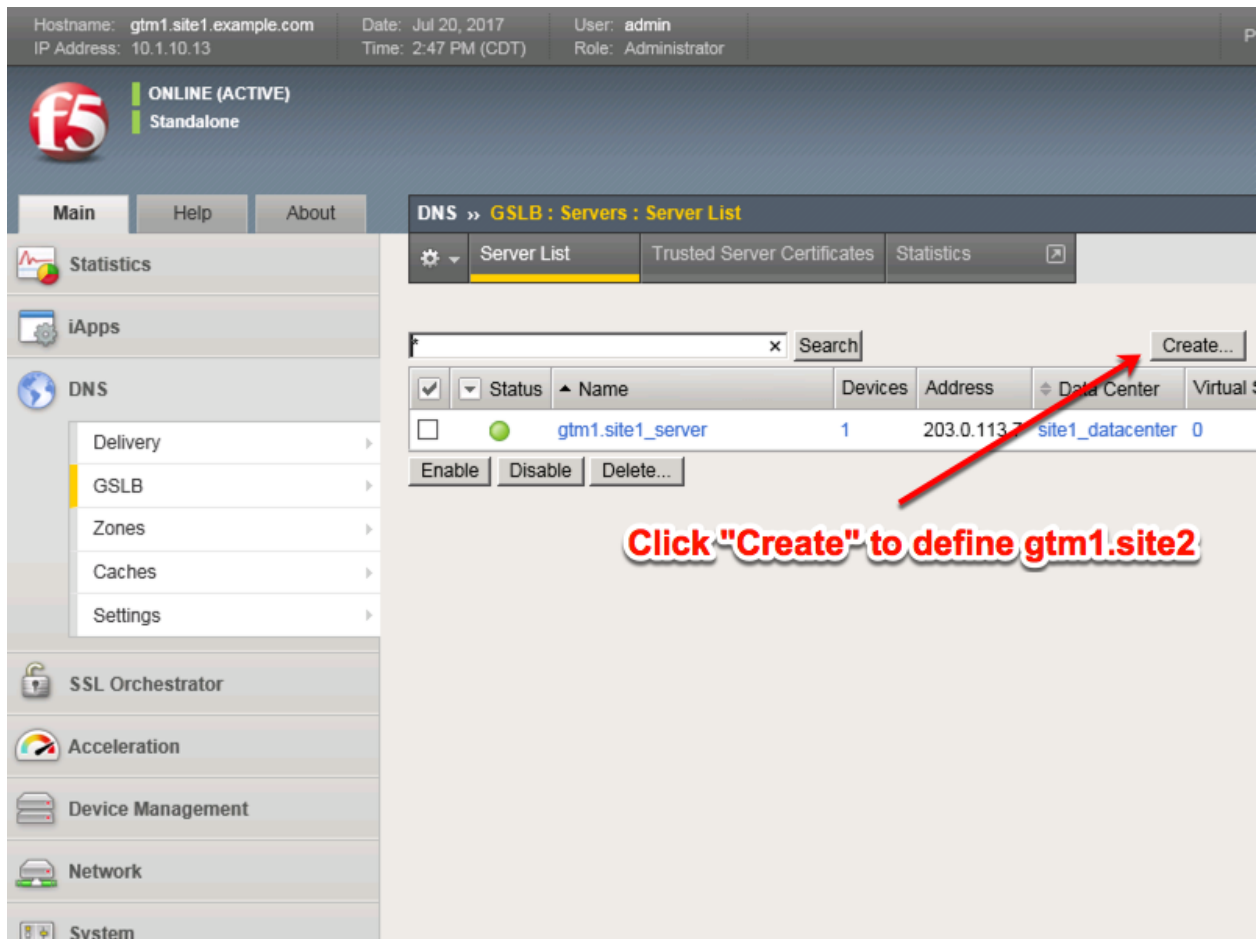
<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/server/create.jsp>

TMSH

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

2.3.1.2 gtm1.site2

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



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

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

1. Fill in the Name and Datacenter

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin
IP Address: 10.1.10.13 Time: 3:18 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

Name
Product
Data Center
Prober Preference
Prober Fallback
State

Devices

Click "Add"

Device Name	Address
No data available in table	

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

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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

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

Add BIG-IP System Device

General Properties

Device Name: gtm1.site2.example.com
Address: 198.51.100.39
Translation: (Optional)
Link: Auto-Select
Prober Preference: Add
Prober Fallback: 198.51.100.39
State:
Delete

Click "Add"

Click "OK"

Devices

Add
Delete
Edit
Delete

BIG-IP System Devices

No data available in table

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

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

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

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

Devices

Device Name	Address
gtm1.site2.example.com	198.51.100.39

Add Edit Delete

Configuration: Advanced

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

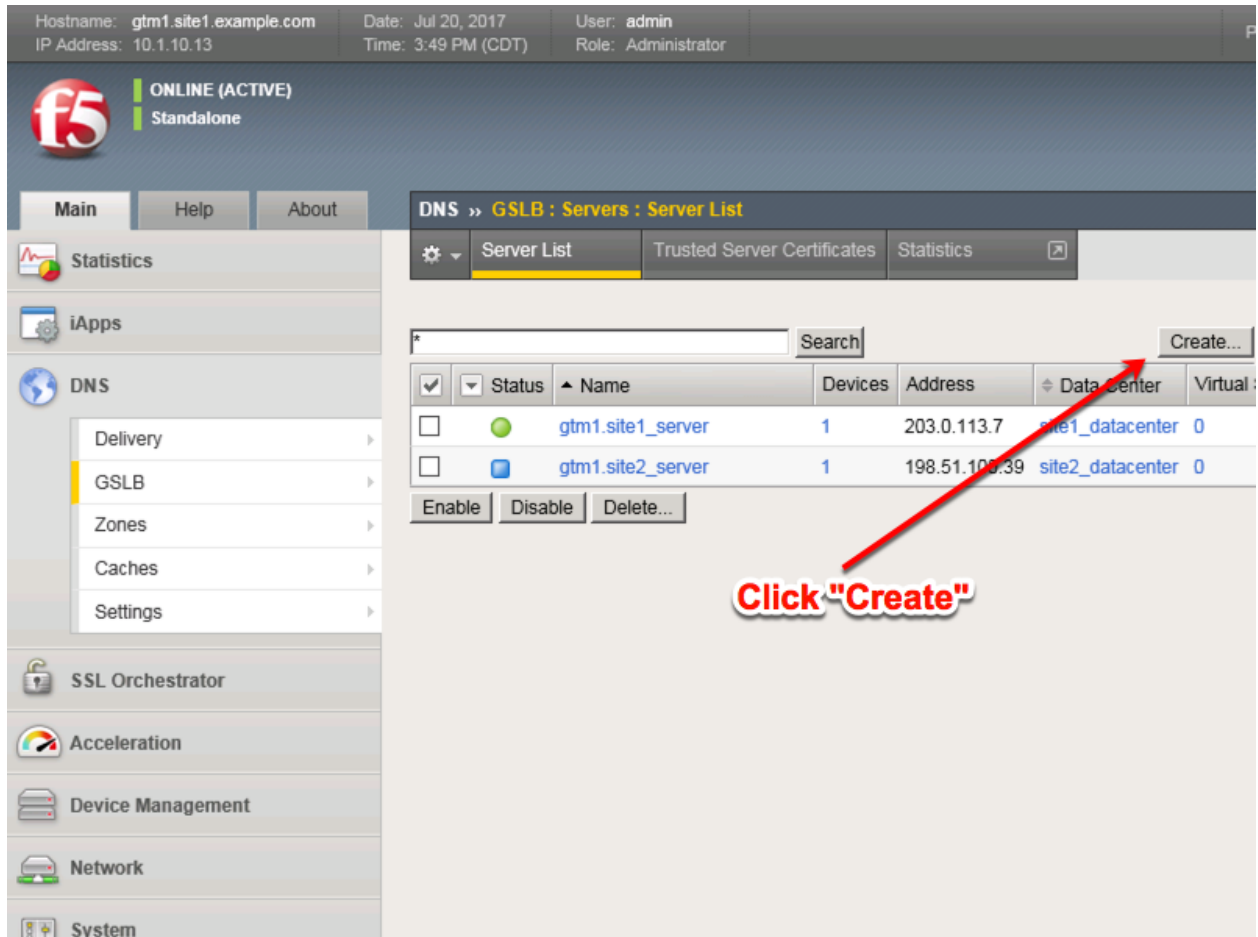
<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/server/create.jsp>

TMSH

```
tmsl 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

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin
IP Address: 10.1.10.13 Time: 3:58 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

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

General Properties

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

Devices

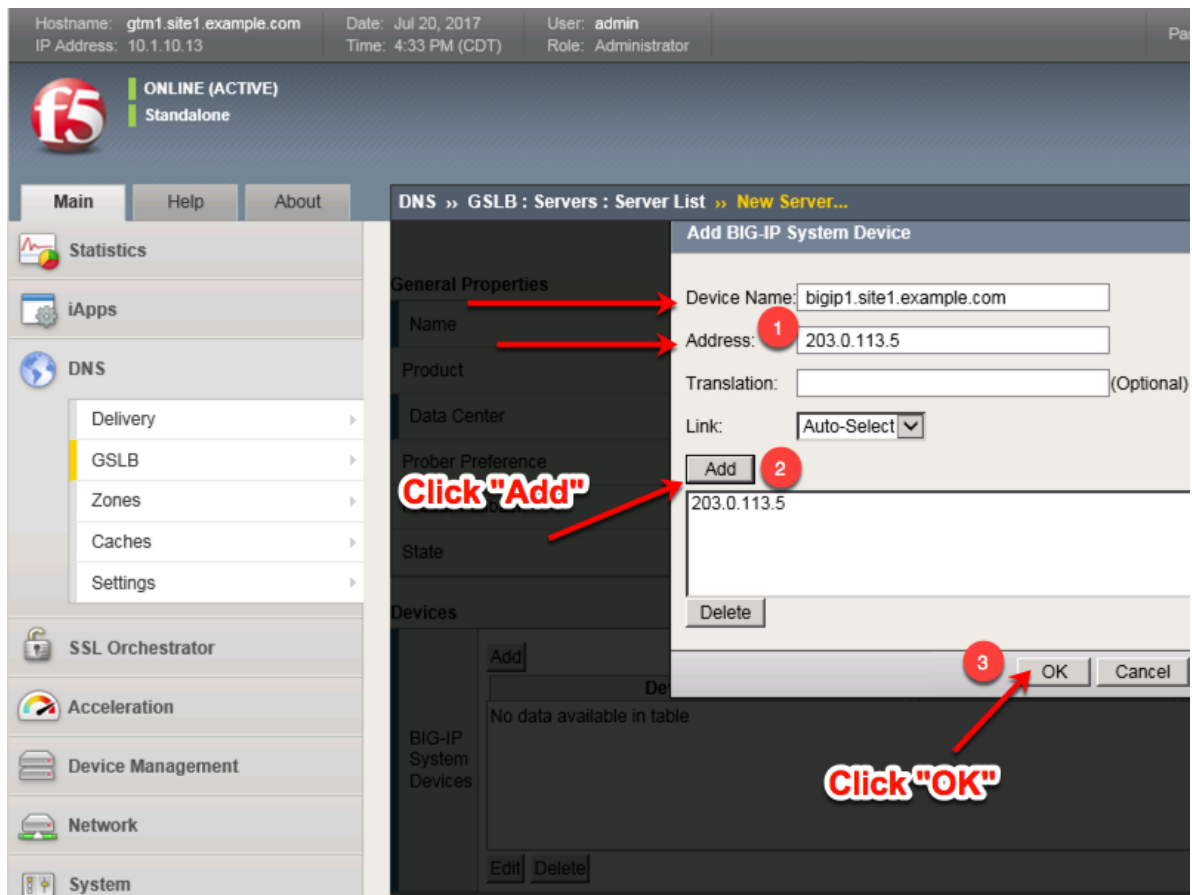
Click "Add"

Add

Device Name	Address
No data available in table	

Edit Delete

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



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

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

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

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

Devices

Add

Device Name	Address
bigip1.site1.example.com	203.0.113.5

Edit Delete

Click "Add"again

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

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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

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

Add BIG-IP System Device

General Properties

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

Click "Add"

Devices

Add
bigip1.site1.example.com 203.0.113.5
Delete

Click "OK"

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

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

ONLINE (ACTIVE)
Standalone

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

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

General Properties

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

Devices

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

Add the "bigip" Health Monitor

Configuration: Advanced

Health Monitors

Selected	Available
/Common bigip	/Common gateway_icmp gtp http http_head_f5

Availability Requirements: All Health Monitors

- Make sure to enable both "Virtual Server" and "Link" discovery

Resources

Virtual Server Discovery	Enabled
Link Discovery	Enabled

Cancel Repeat Finished

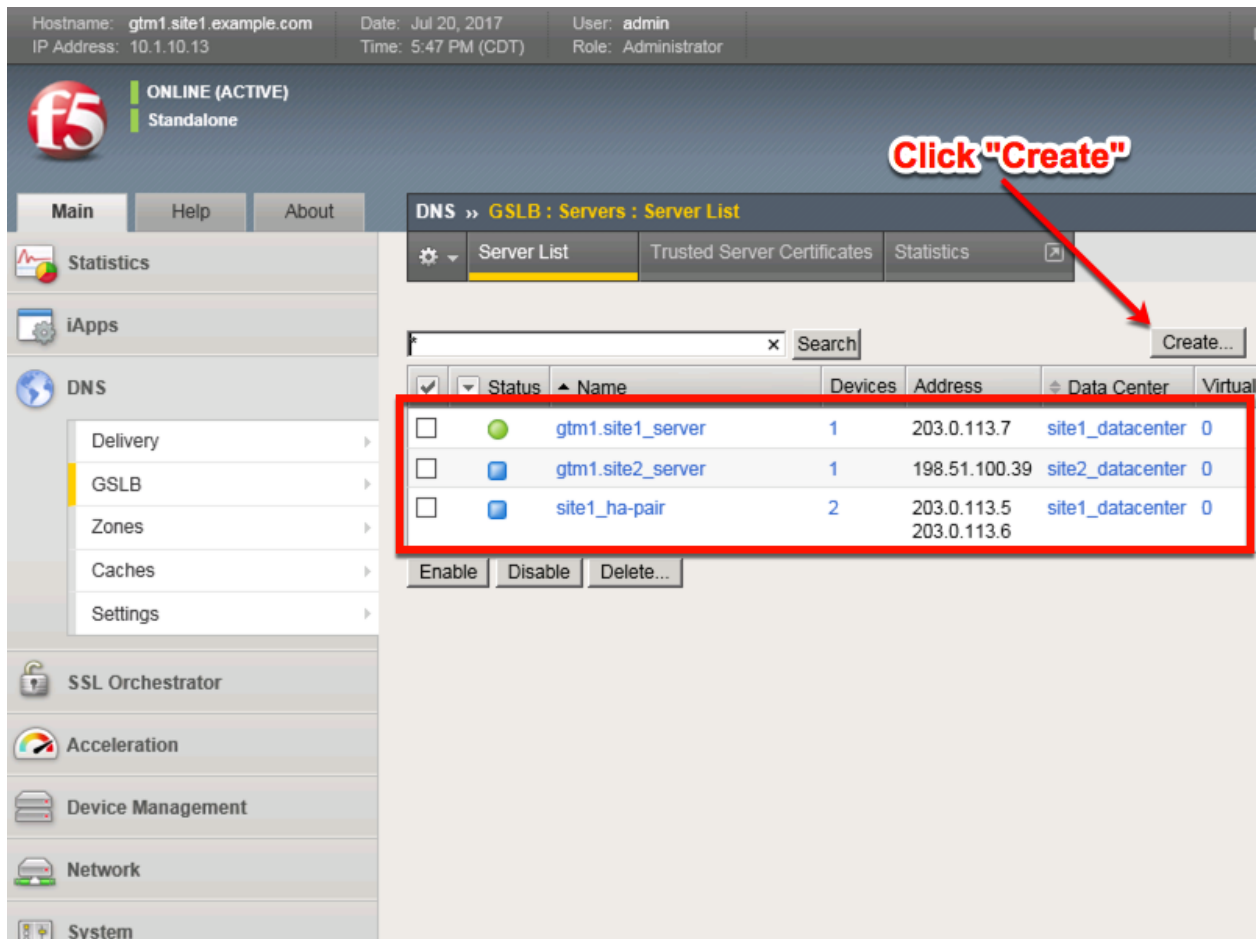
<https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/globallb/server/create.jsp>

TMSH

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


2.3.1.4 site2_ha-pair

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



Create a Server Object as defined in the table below:

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

1. Fill in the Name and Datacenter

Hostname: gtm1.site1.example.com Date: Jul 20, 2017 User: admin
IP Address: 10.1.10.13 Time: 5:52 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

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

Devices

Big-IP System Devices

Add

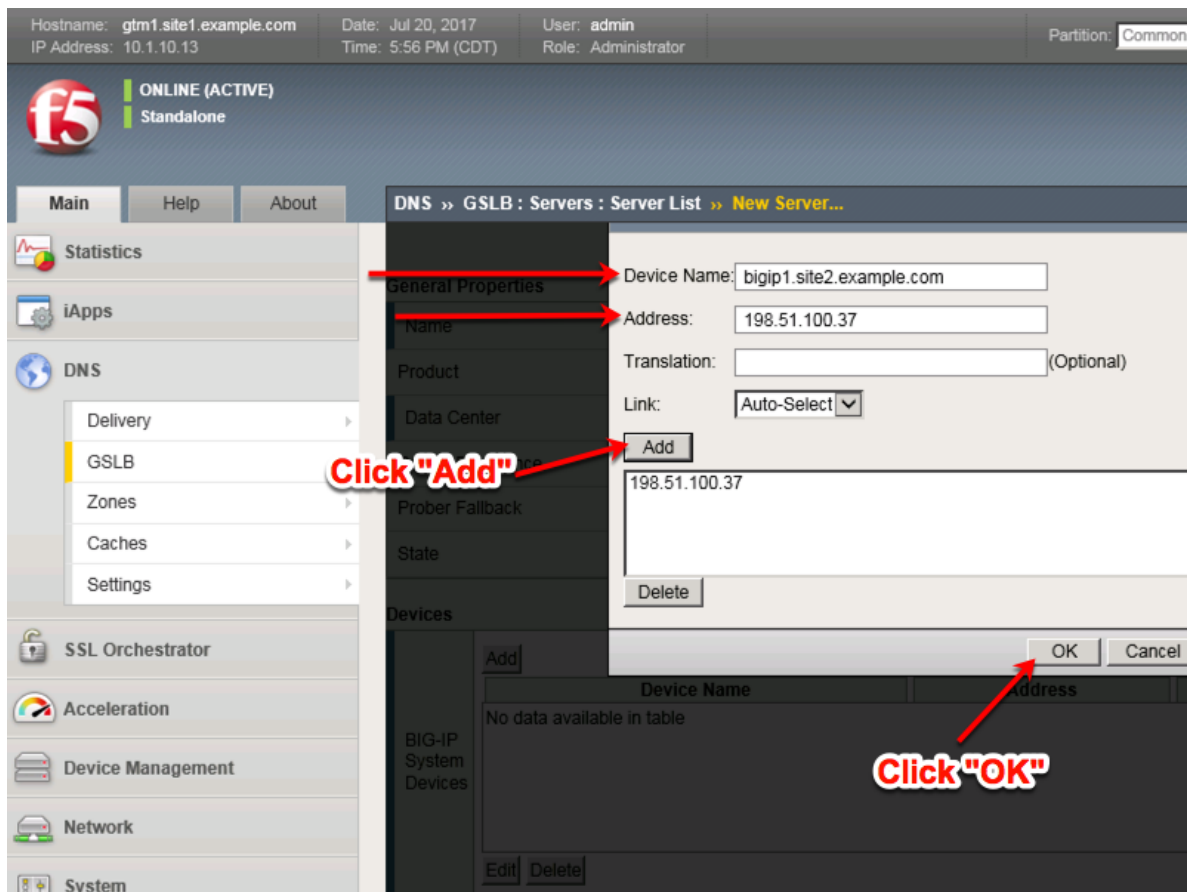
Device Name

No data available in table

Edit Delete

Click "Add"

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



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

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

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

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

Devices

Click "Add"

Device Name	Address
bigip1.site2.example.com	198.51.100.37

Edit Delete

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

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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

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

General Properties

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

Click "Add"

Devices

Device Name	Address
bigip1.site2.example.com	198.51.100.37

OK Cancel
3
Click "OK"

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

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

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

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

Devices

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

Add Edit Delete

Configuration: Advanced

Health Monitors

Selected: /Common bigip

Available: /Common gateway_icmp gtp http http_head_f5

Availability Requirements: All Health Monitors

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

Resources

Virtual Server Discovery	Enabled
Link Discovery	Enabled

Cancel Repeat Finished

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

TMSH

```
tmsh create gtm server site2_ha-pair datacenter site2_datacenter devices add { bigip1.site2.example.com
{ addresses add { 198.51.100.37 { } } bigip2.site2.example.com { addresses add { 198.51.100.38 { } } } }
link-discovery enabled monitor bigip product bigip virtual-server-discovery enabled
```

2.3.2 Device Trust

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

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

ONLINE (ACTIVE)
Standalone

Main Help About

DNS » GSLB : Servers : Server List

Server List Trusted Server Certificates Statistics

Search

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

Enable Disable Delete...

Three other servers need to "establish trust"

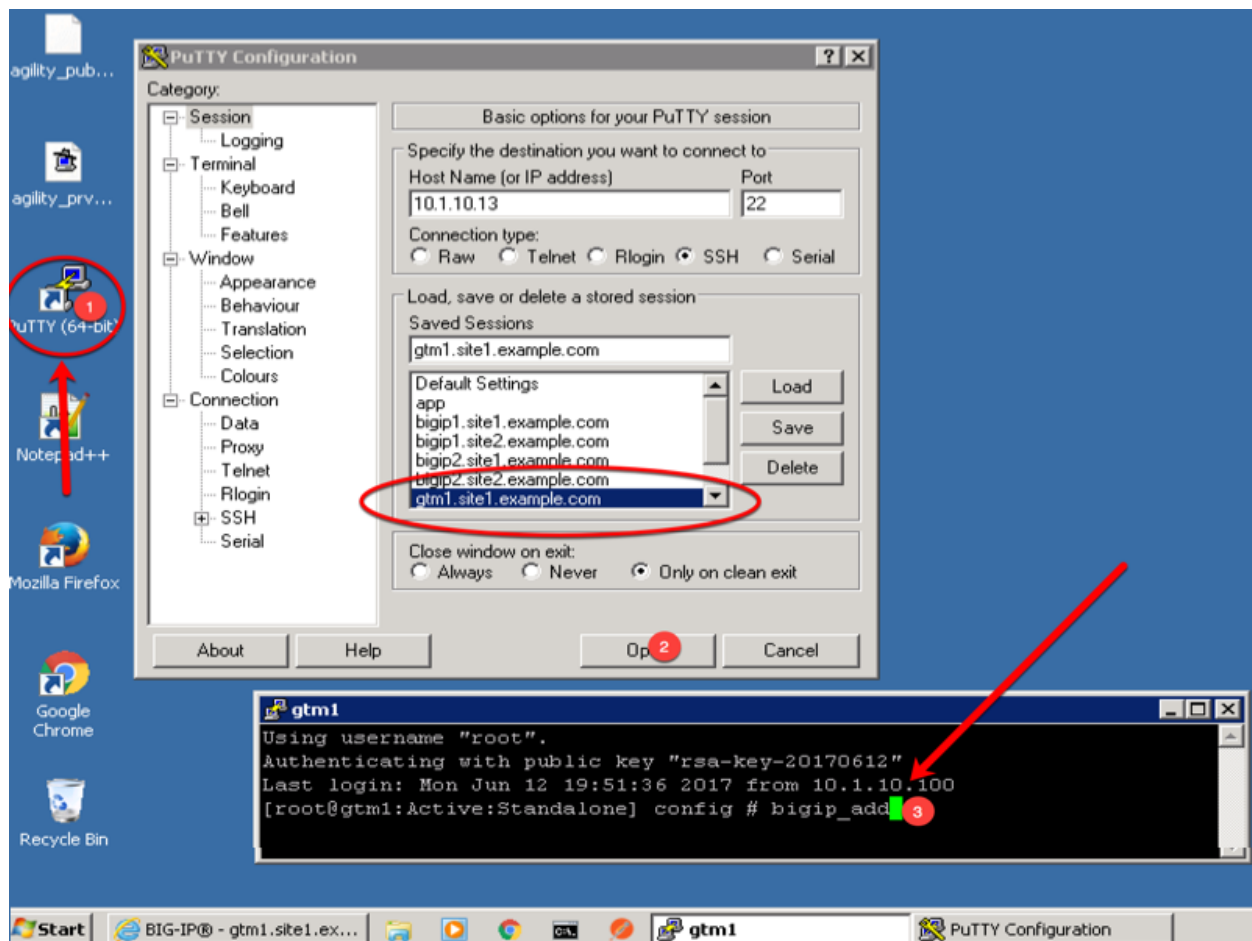
Launch Putty and login to gtm1.site1.example.com

Run the following command:

When prompted for a password use "default".

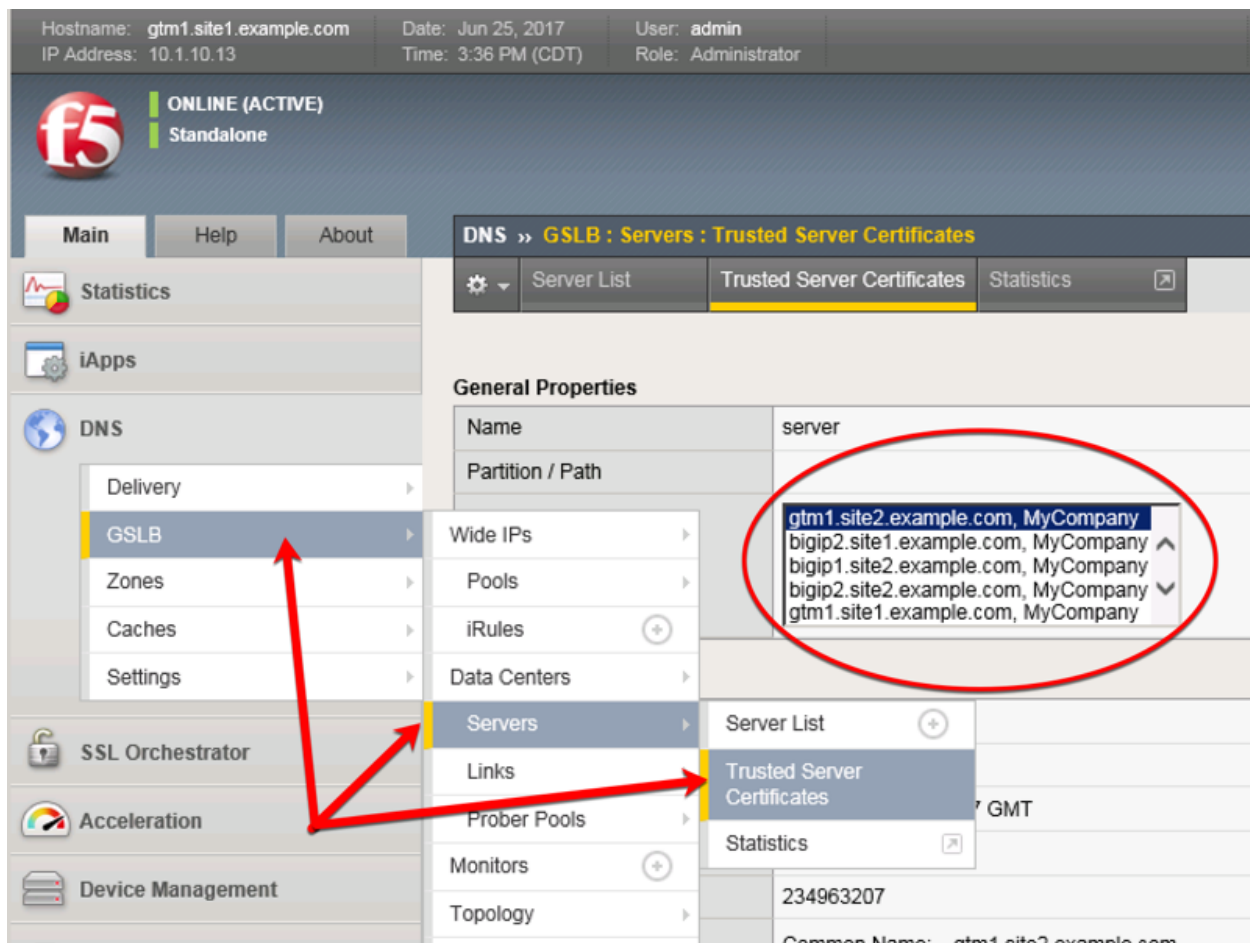
TMSH

bigip_add



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

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/localb/ssl_certificate/properties.jsp?certificate_name=server&store=iquery



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.

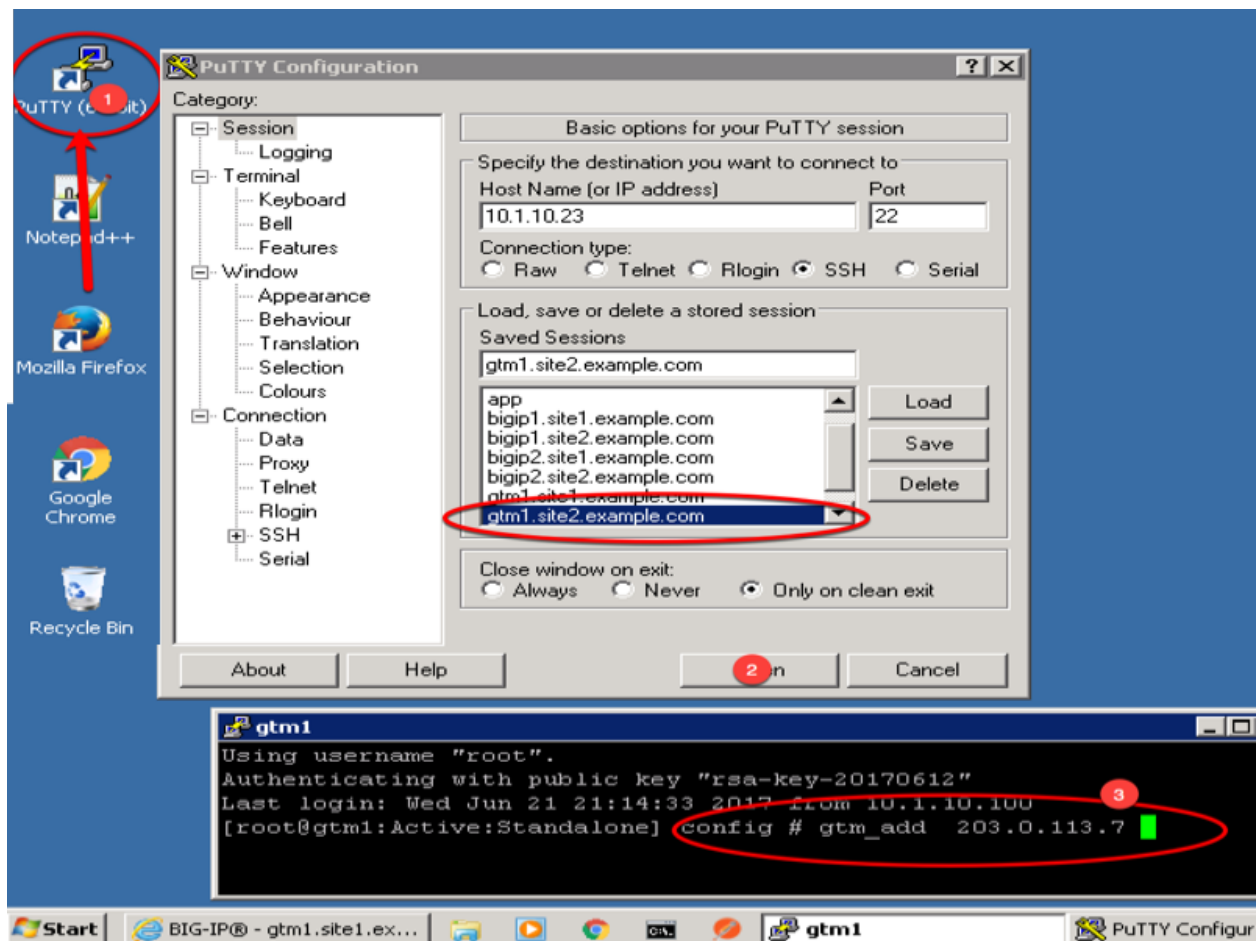
Launch Putty and log in to gtm1.site2

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

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

TMSH

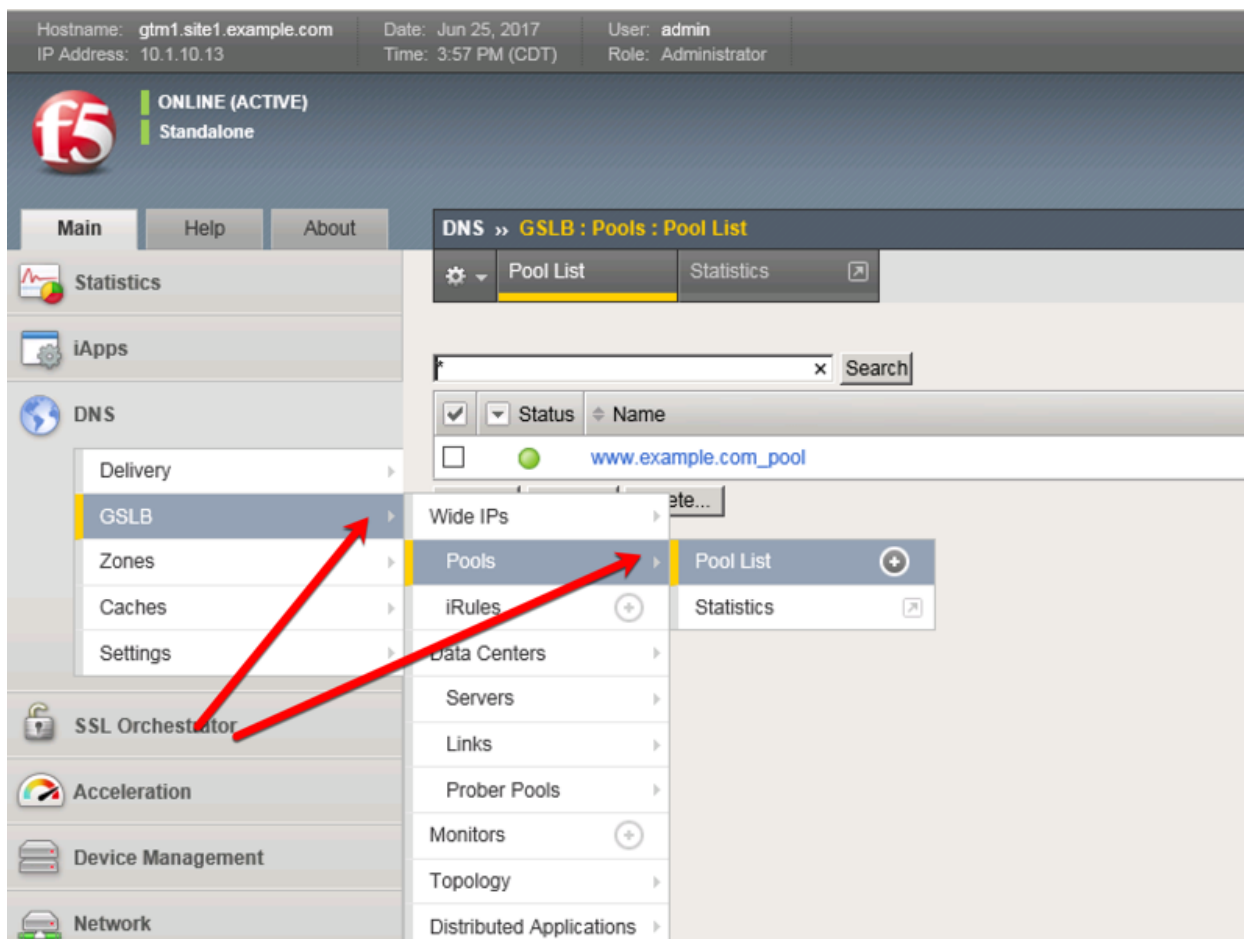
```
gtm_add 203.0.113.7
```



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>

DNS » GSLB : Pools : Pool List » New Pool...

General Properties

Name:

Type:

State:

Configuration

Health Monitors:
 Selected:
 Available:
 Up Down

Availability Requirements:

Limit Settings:
 Bits:
 Packets:
 Current Connections:

Manual Resume: ☐

TTL:

Dynamic Ratio: ☐

Maximum Answers Returned:

Verify Member Availability: ☒

Members

Load Balancing Method:
 Preferred:
 Alternate:
 Fallback:

Fallback IP:

Virtual Server:
 Ratio:

Add

Member List:

Delete Up Down

Cancel Repeat Finished

TMSH command to run on only gtm1.site1:

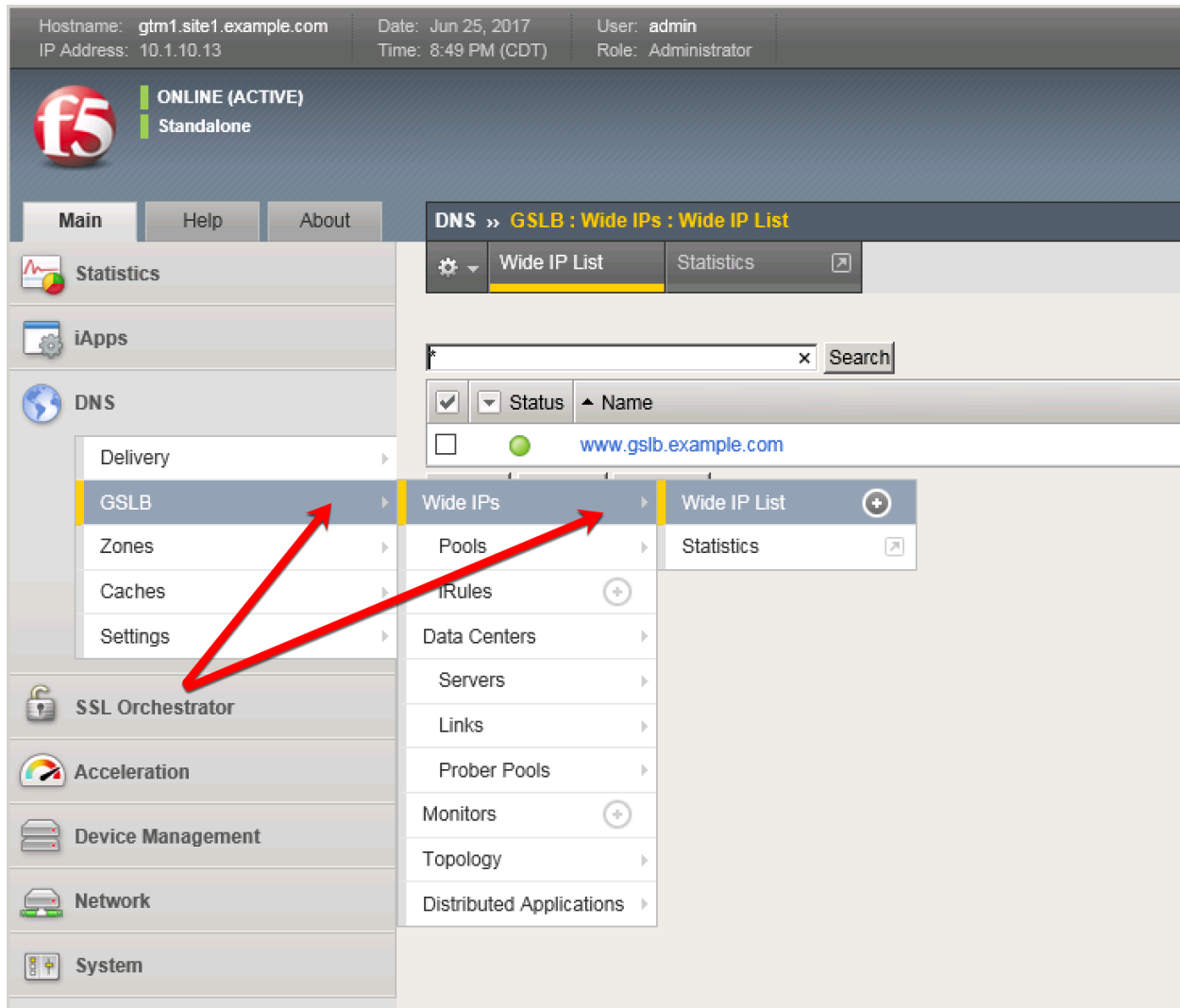
TMSH

```
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”.

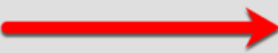

Navigate to: **DNS » GSLB : Wide IPs : Wide IP List**



Create an F5 “wide IP”

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

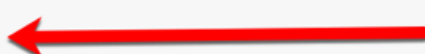
General Properties: Advanced ▾

Name	 <input type="text" value="www.example.com"/>
Type	 A ▾
Description	<input type="text"/>
Alias List	<div>Alias: <input type="text"/></div> <div>Add</div> <div><input type="text"/></div> <div>Delete</div>
State	Enabled ▾
Minimal Response	Enabled ▾
Return Code On Failure	Disabled ▾
Load-Balancing Decision Log	<div><input type="checkbox"/> Pool Selection</div> <div><input type="checkbox"/> Pool Traversal</div> <div><input type="checkbox"/> Pool Member Selection</div> <div><input type="checkbox"/> Pool Member Traversal</div>

iRules

iRule List	<div>Selected</div> <div><input type="text"/></div> <div>Available</div> <div><input type="text"/></div> <div><<</div> <div>>></div> <div>Up</div> <div>Down</div>
------------	--

Pools

Load Balancing Method	Round Robin ▾
58 Persistence	Disabled ▾
	Pool Select... ▾ 

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

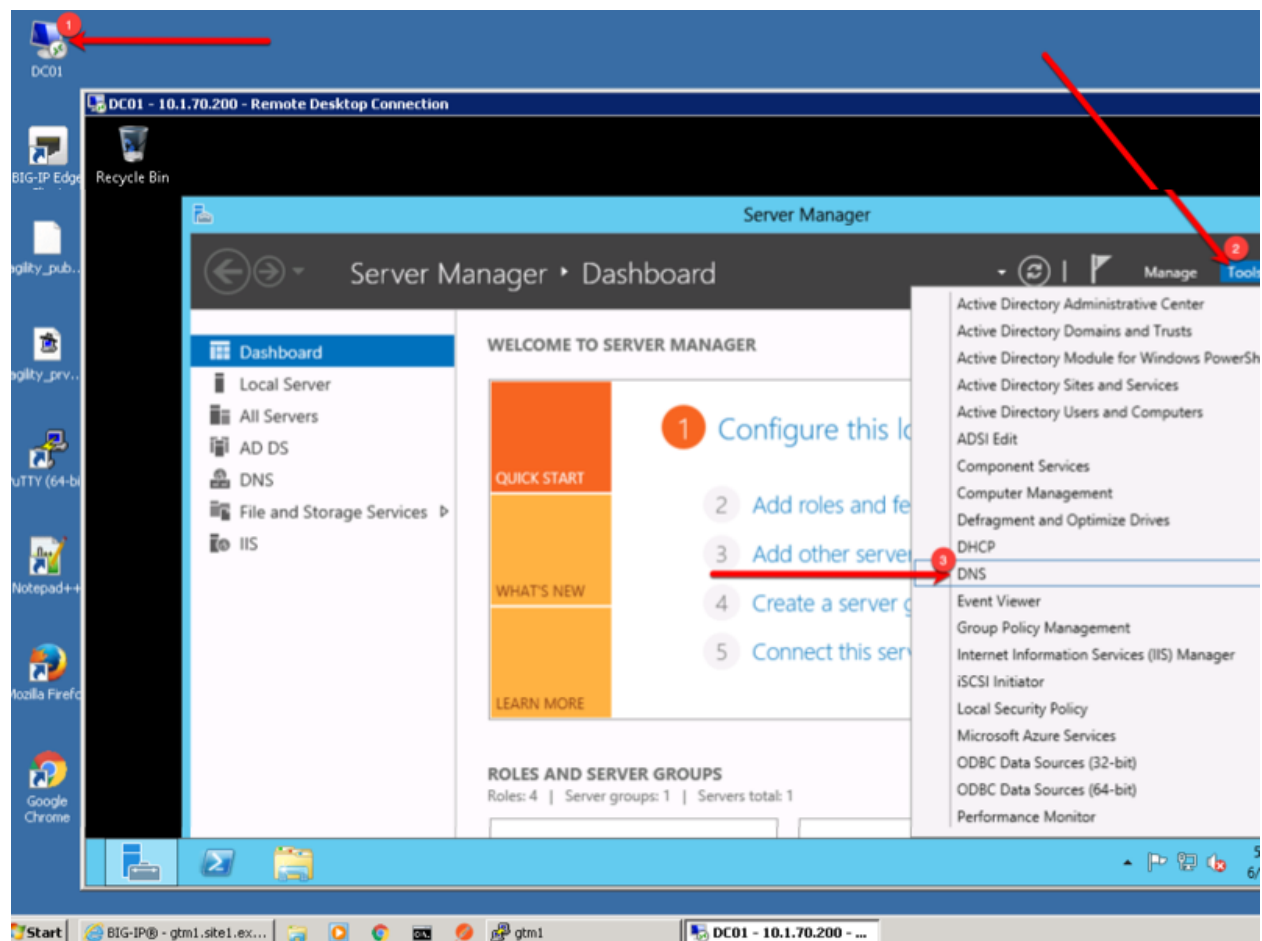
TMSH command to run on only gtm1.site1:

TMSH

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

2.6 Delegation

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

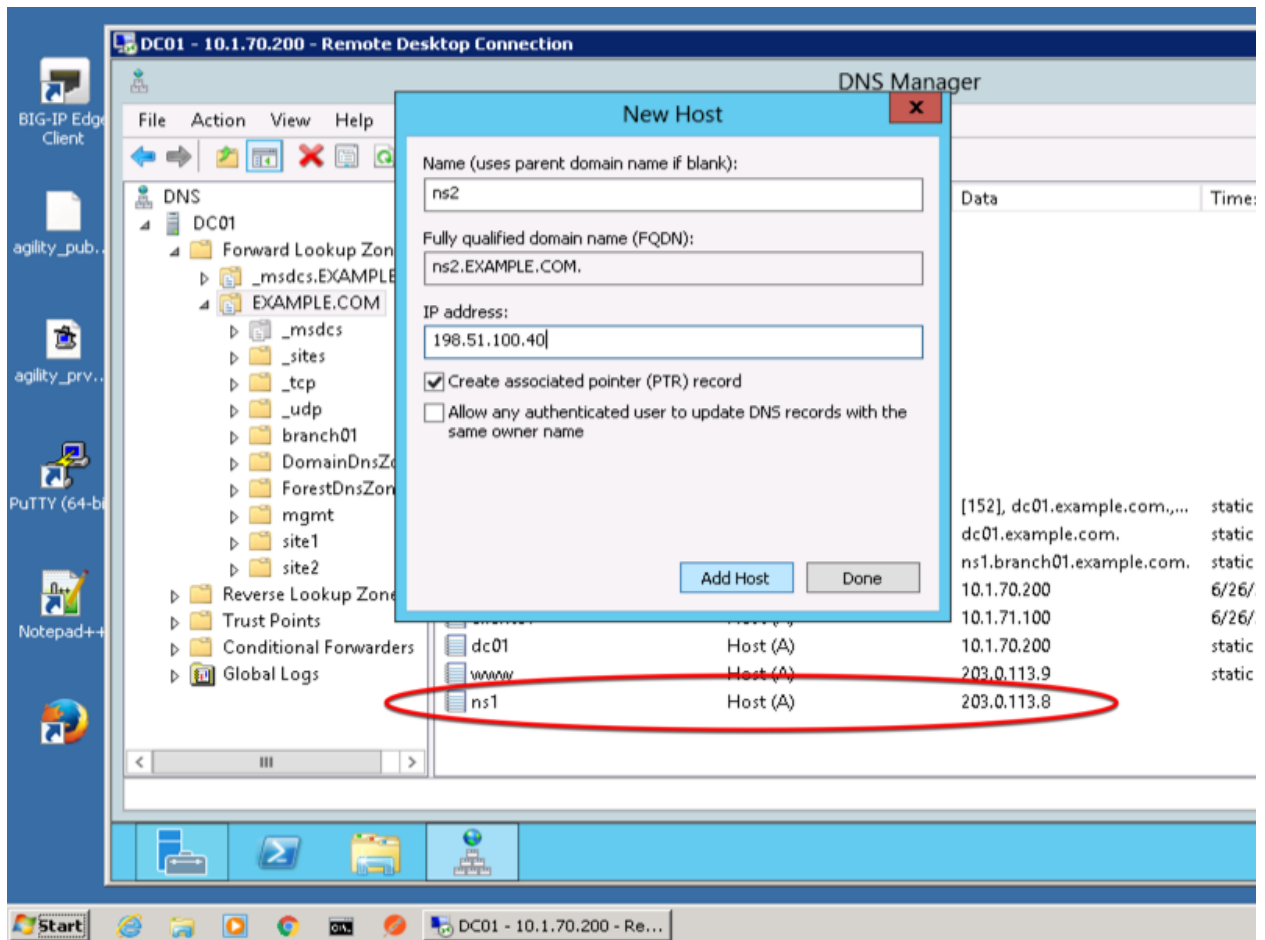


2.6.1 A Records

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

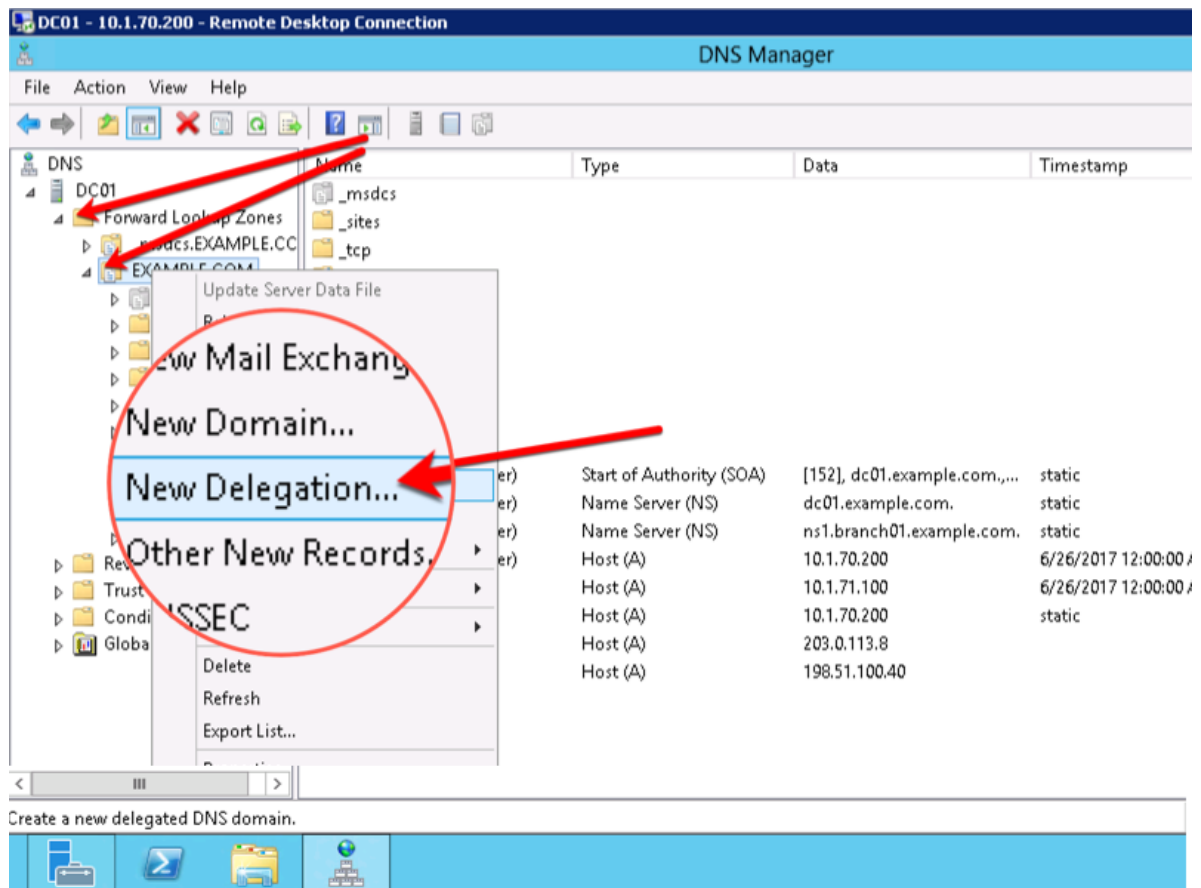
Setting	Value
ns1	203.0.113.8
ns2	198.51.100.40

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

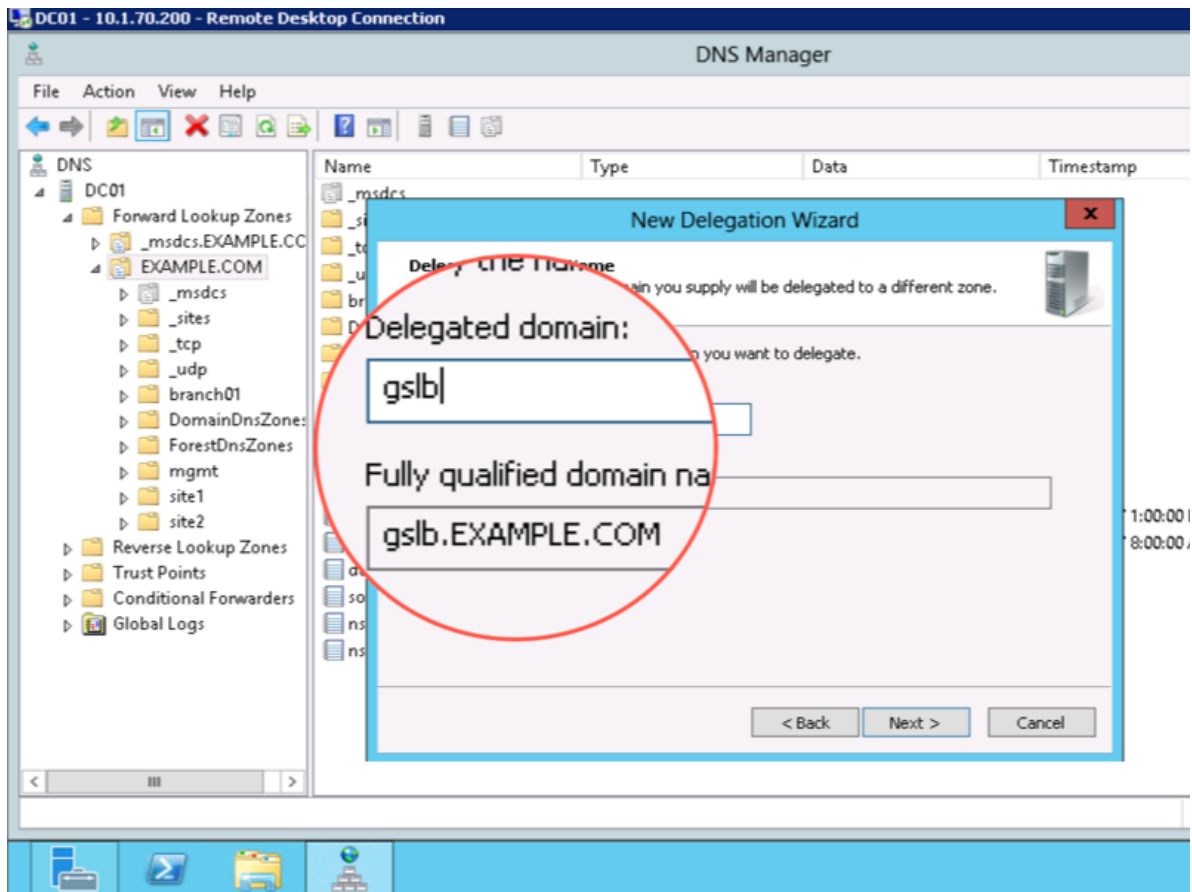


2.6.2 Sub Domain

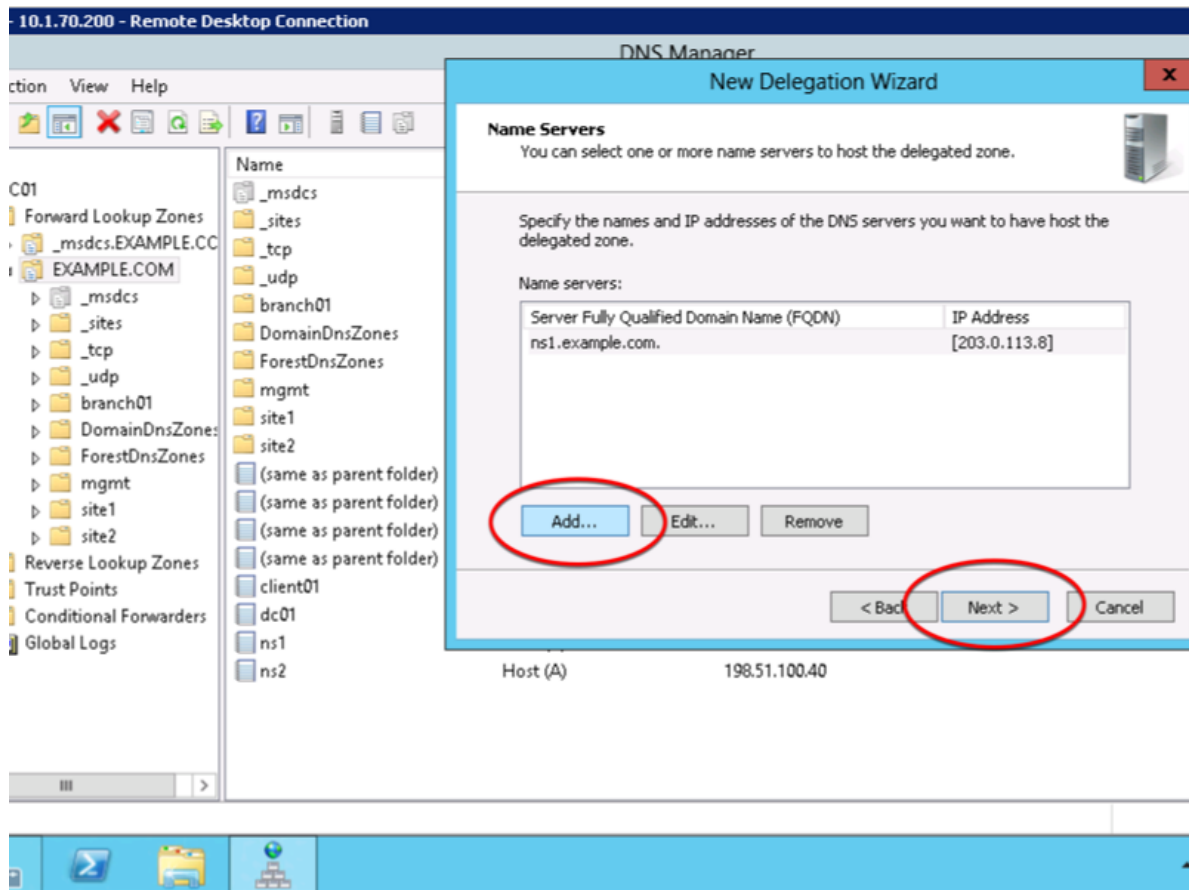
1. Expand “Forward Lookup Zones”, and right click on “EXAMPLE.com



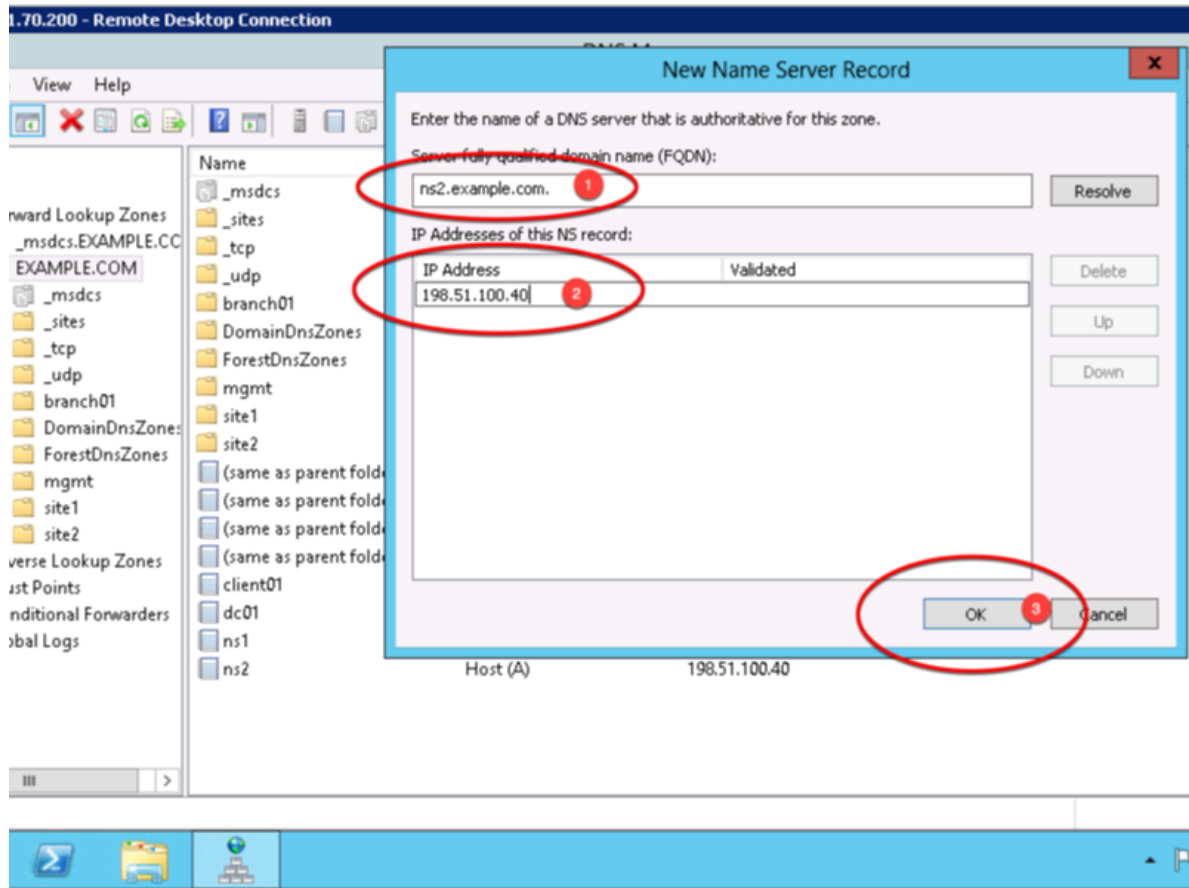
2. Create the "gslb" subdomain.



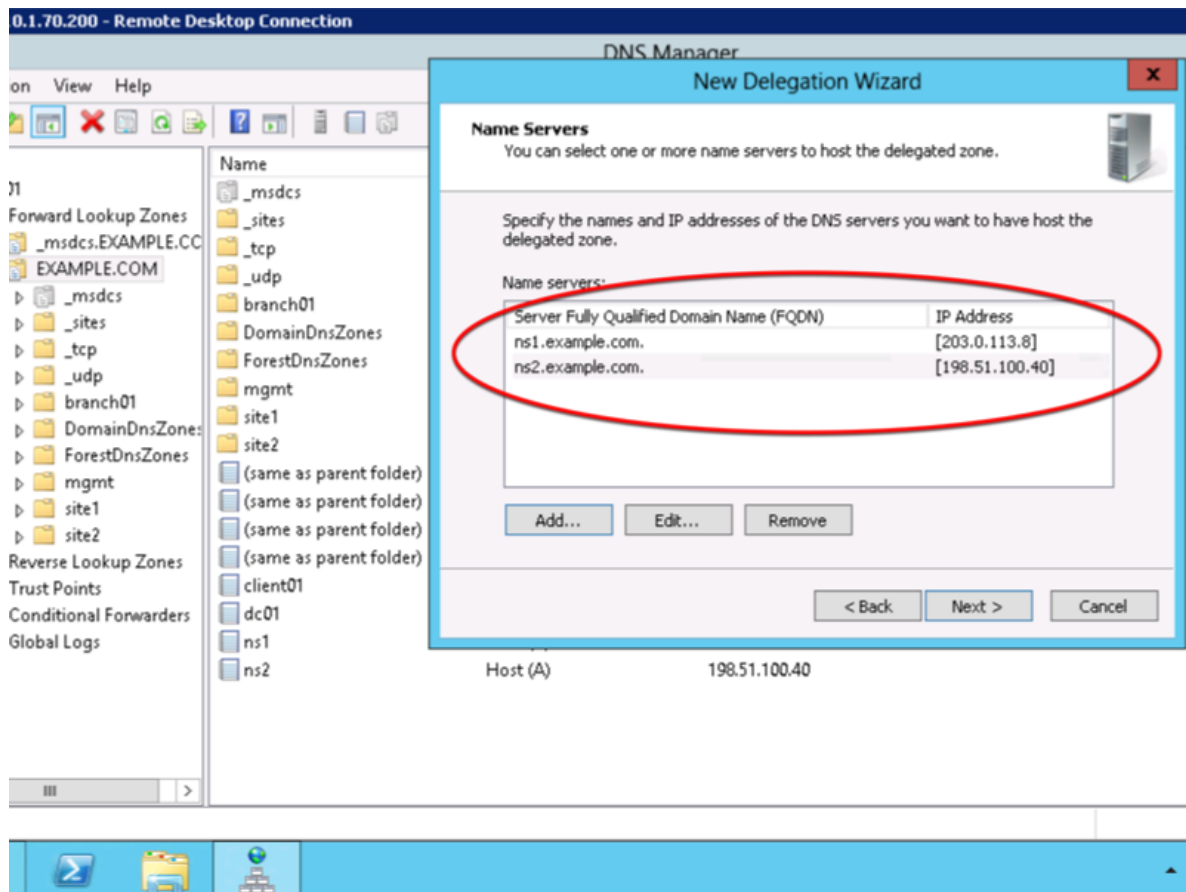
3. Step through the Delegation Wizard. Add "ns1.example.com - 203.0.113.8"



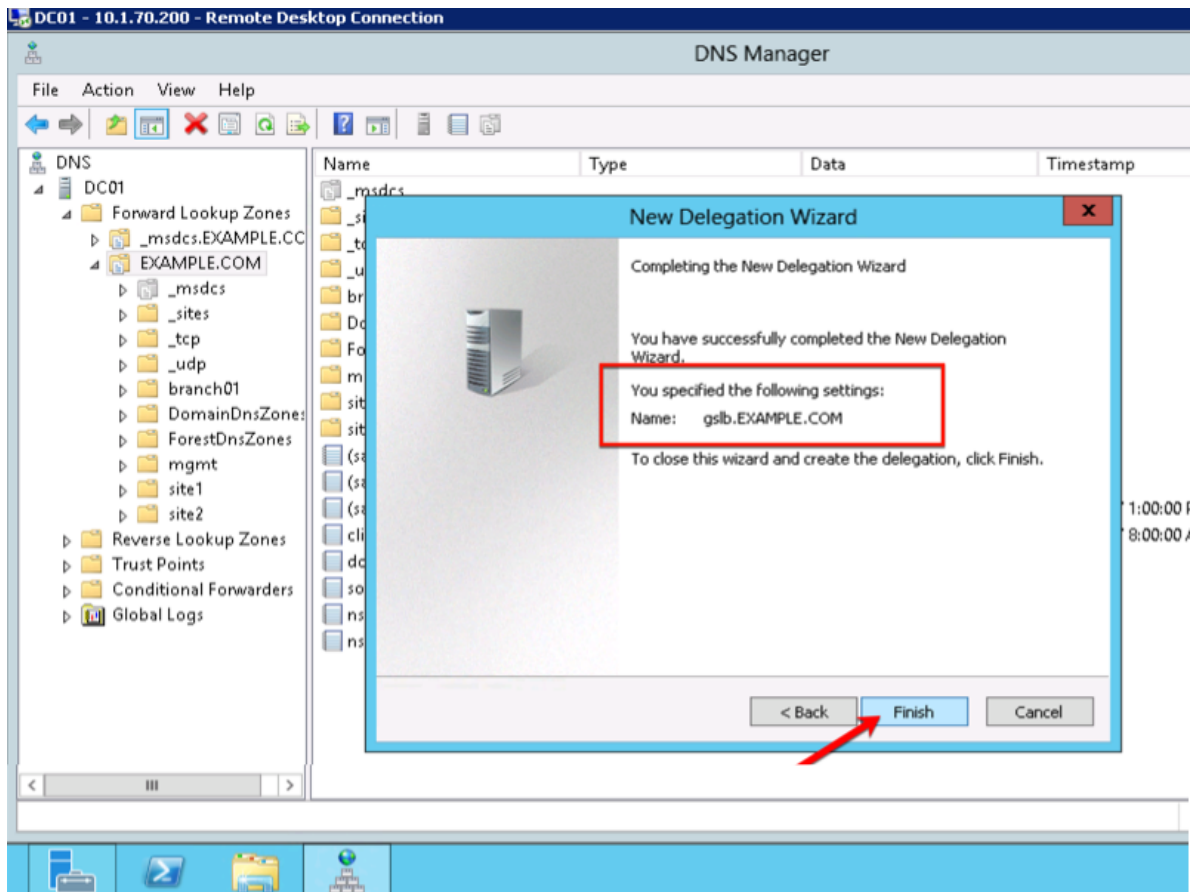
4. Also add "ns2.example.com - 198.51.100.40"



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

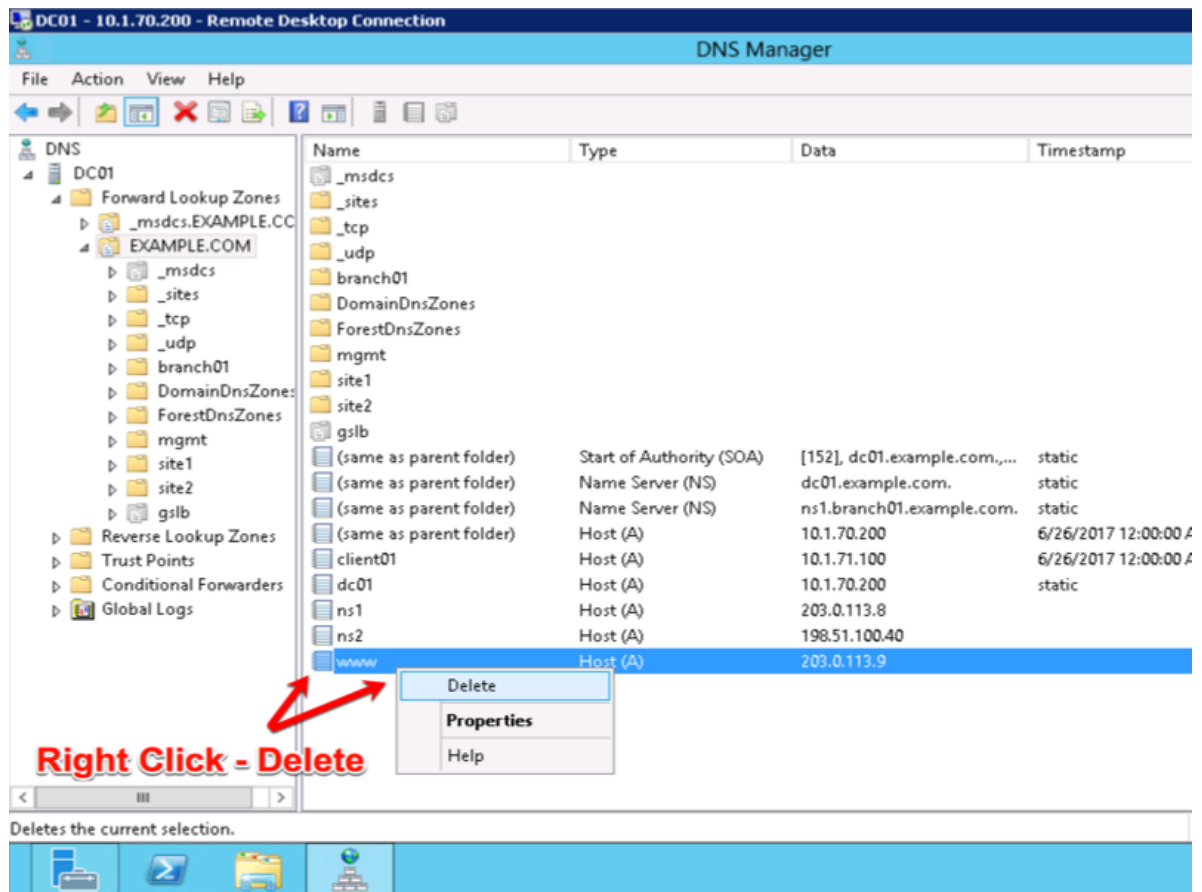


6. Click "Finish"

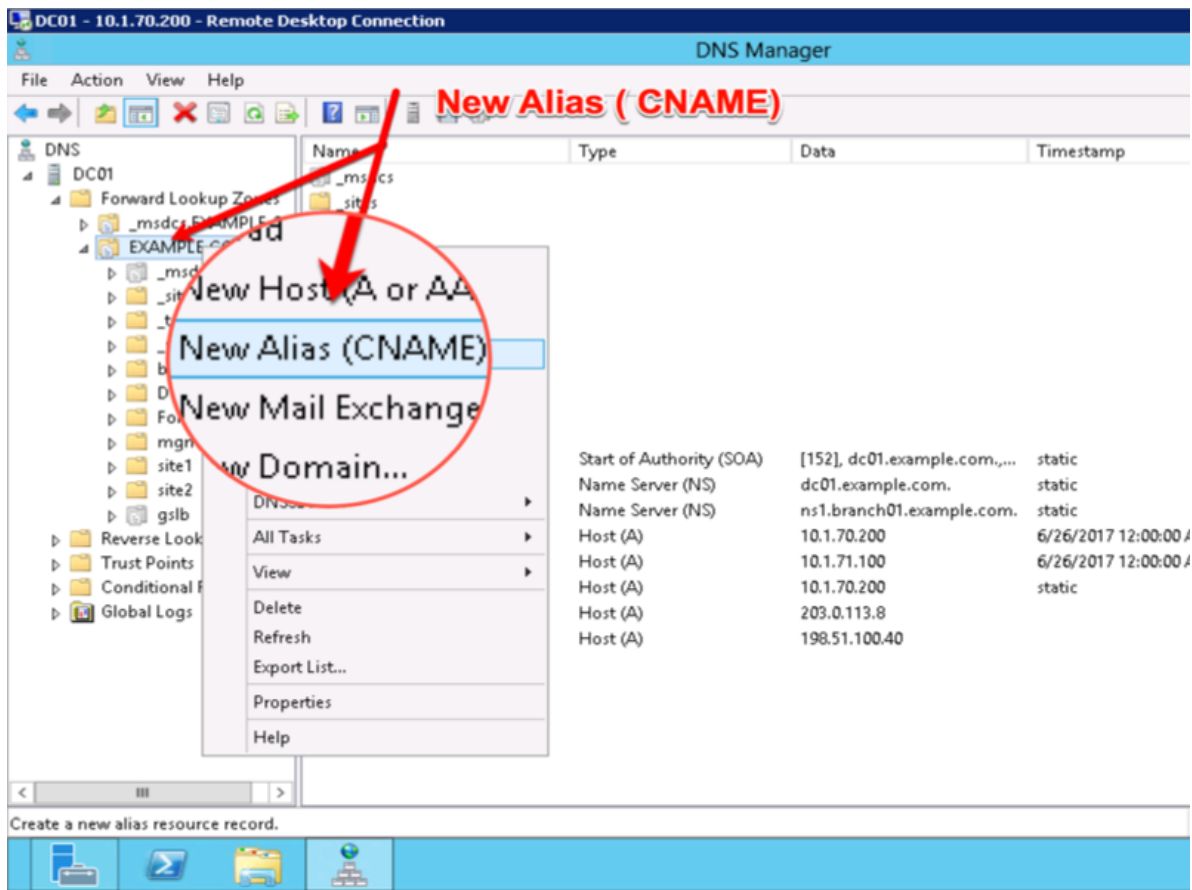


2.6.3 CNAME

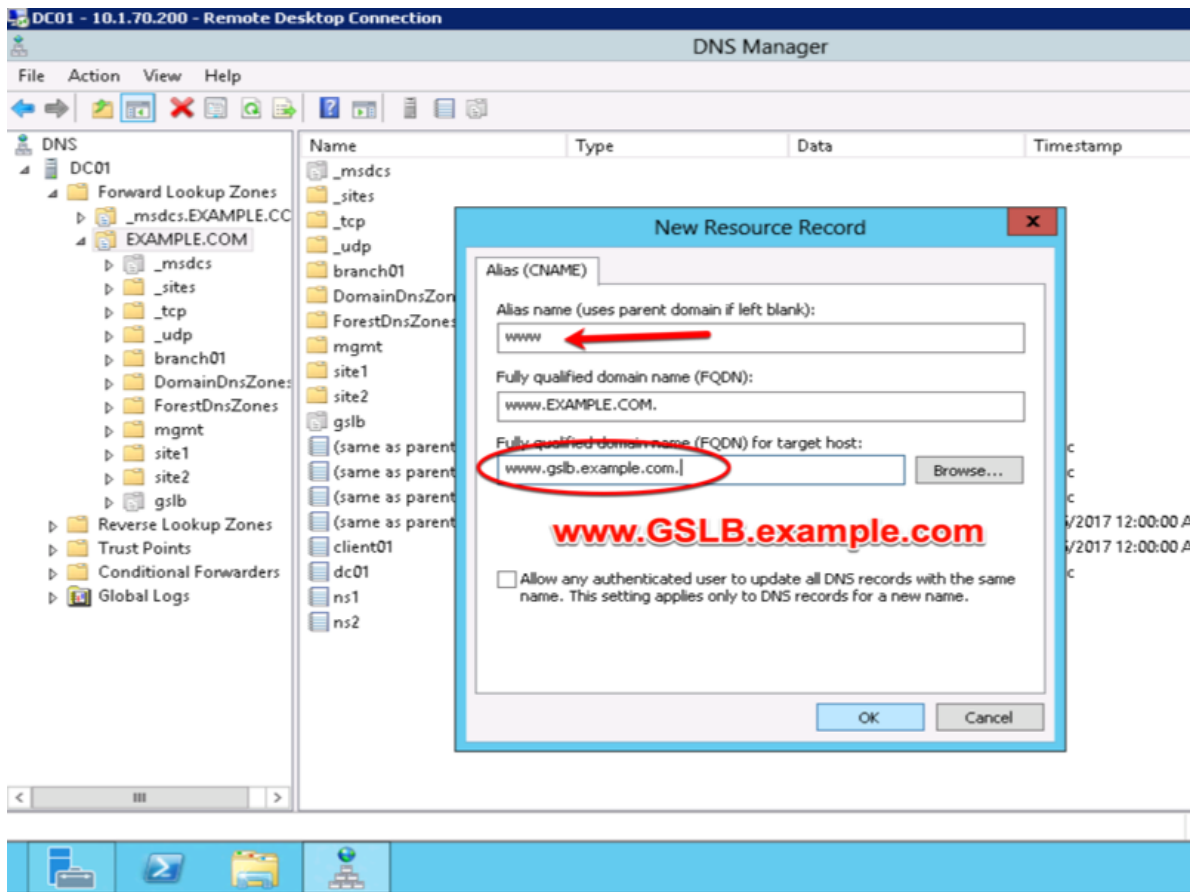
1. Make sure "Forward Lookup Zones" and "EXAMPLE.COM" is expanded. Right click on "www", and select delete.



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

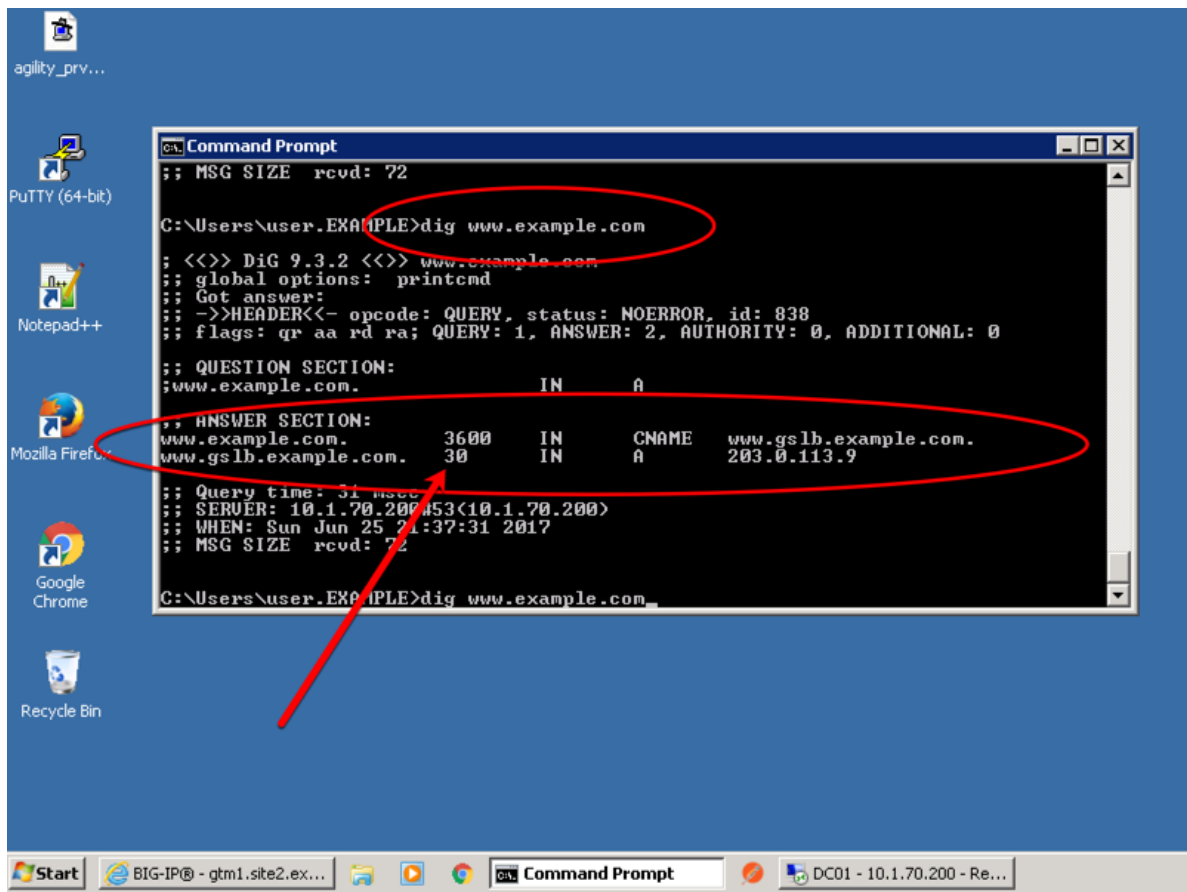


3. Add "www - www.gslb.example.com"



2.7 Results

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



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

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

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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

Statistics Properties iRules Pools Statistics

General Properties: Advanced

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

Click Statistics

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

Alias:

Add

Delete

Available (Enabled) - Available

Enabled

Enabled

Disabled

Hostname: gtm1.site1.example.com Date: Jul 17, 2017 User: admin
IP Address: 10.1.10.13 Time: 11:45 AM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About

Statistics » Module Statistics : DNS : GSLB » Wide IPs : www.gslb.example.com : A

Statistics

- Dashboard
- Module Statistics
- Analytics
- Performance

iApps

DNS

SSL Orchestrator

Acceleration

Device Management

Network

System

Display Options

Data Format: Normalized

Auto Refresh: Disabled Refresh

<< Back Clear Statistics

Requests

Total	12
Persisted	0
Resolved	12
Dropped	0

Load Balancing

Preferred	12
Alternate	0
Fallback	0
CNAME Resolutions	0

TMSH

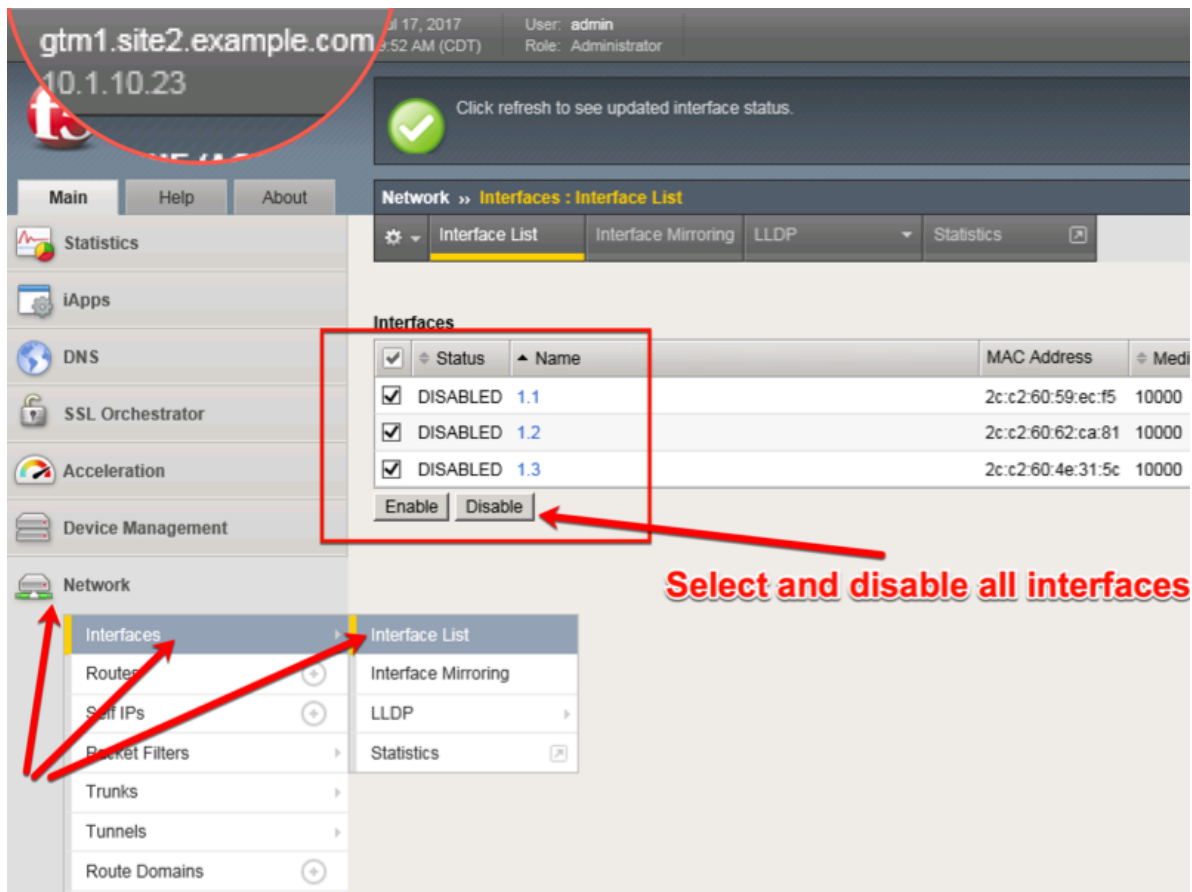
tmsh show gtm wideip a www.gslb.example.com

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

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

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

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

TMSH command to run on only gtm1.site2:

TMSH

tmsh modify net interface all enabled

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

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

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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

Statistics » Module Statistics : DNS : GSLB » Pools : www.example.com_pool : A

Traffic Summary DNS Network Memory

Display Options
Data Format: Normalized
Auto Refresh: Disabled Refresh
<< Back

Pool Details: "www.example.com_pool : A"

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

TMSH

show gtm pool a www.example.com_pool

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

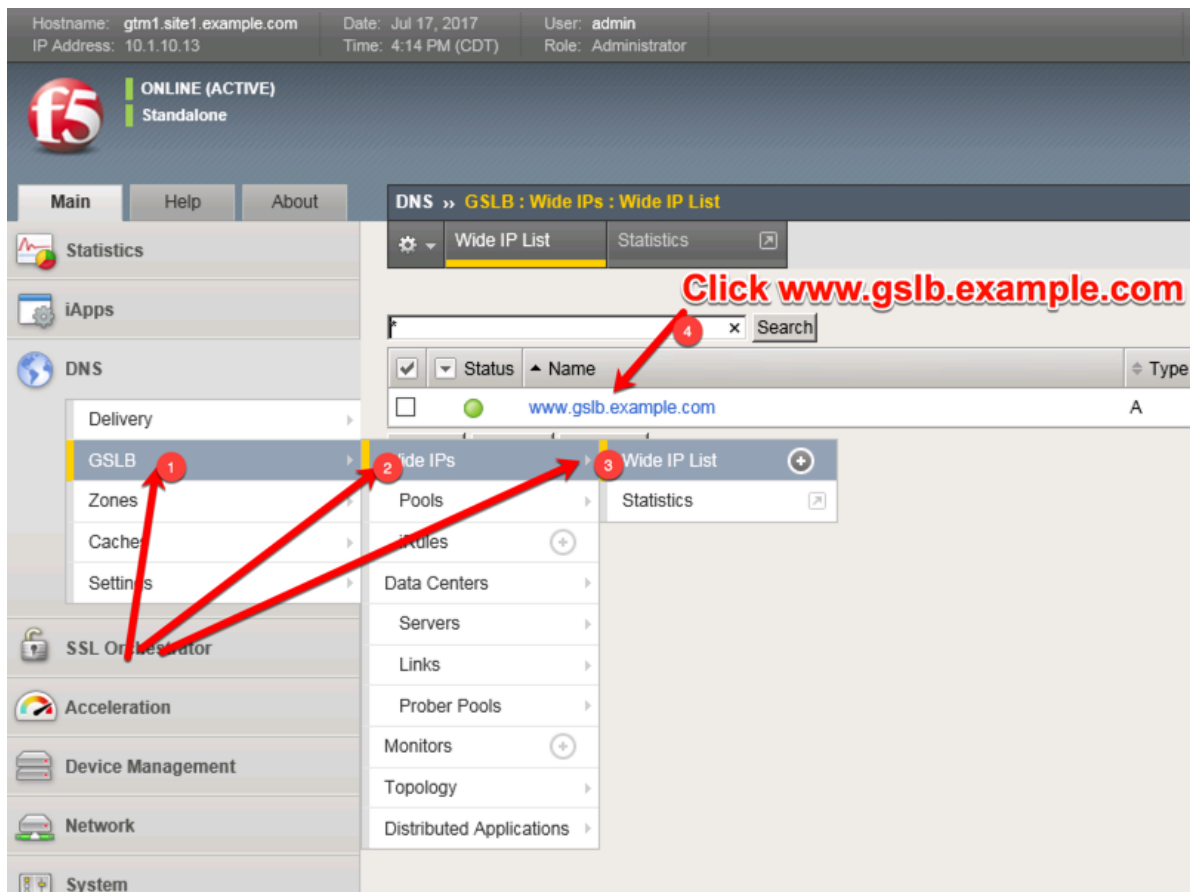
TMSH

tail -f /var/log/ltm

2.8 Persistence

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

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



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

2. Click into the "Pools" tab:

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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

Statistics iApps DNS SSL Orchestrator Acceleration Device Management Network System

General Properties: **Advanced**

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

Click "Pools"

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

3. Enable Persistence

Hostname: gtm1.site1.example.com Date: Jul 17, 2017 User: admin
IP Address: 10.1.10.13 Time: 4:53 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

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

Properties iRules Pools Statistics

Pools

Load Balancing Method	Round Robin
Persistence	Enabled
Persistence TTL	3600 seconds
Persist CIDR (IPv4)	32
Persist CIDR (IPv6)	128
Last Resort Pool	None

Update

Pools

<input checked="" type="checkbox"/>	▲ Order	▼ Status	Pool Name
<input type="checkbox"/>	0	●	www.example.com_pool

Delete...

TMSH

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

4. View Persistence Records

TMSH

tmsh show gtm persist

2.9 LB Methods

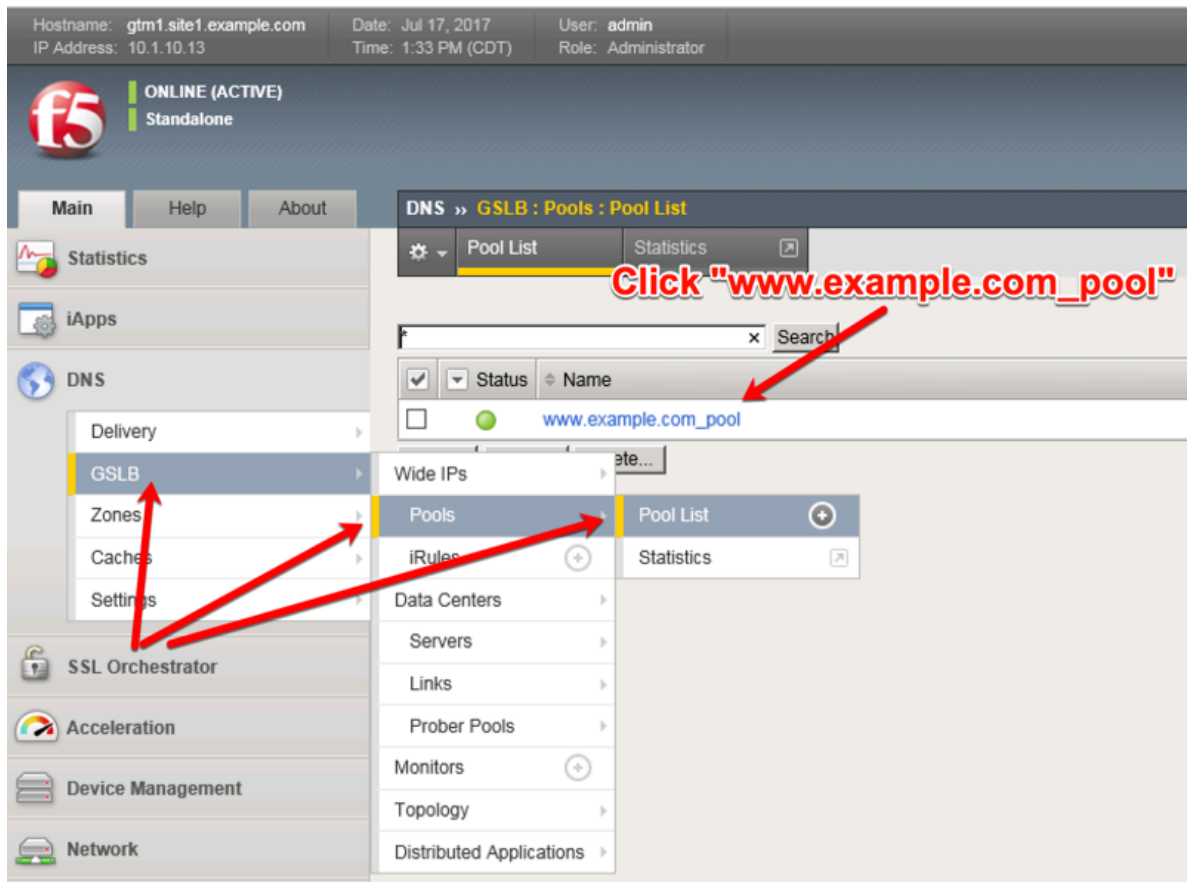
Modify the GSLB configuration so that site2 is a standby DR site.

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

An ISP network outage can automatically cause DR activation.

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

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



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

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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

DNS » GSLB : Pools : Pool List » Members : www.example.com_pool : A

Statistics iApps DNS

Delivery GSLB Zones Caches Settings

SSL Orchestrator Acceleration Device Management Network

Properties Members Statistics

Click "Members"

Load Balancing

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

Fallback IP 0.0.0.0

Update

Members

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

Enable Disable Remove

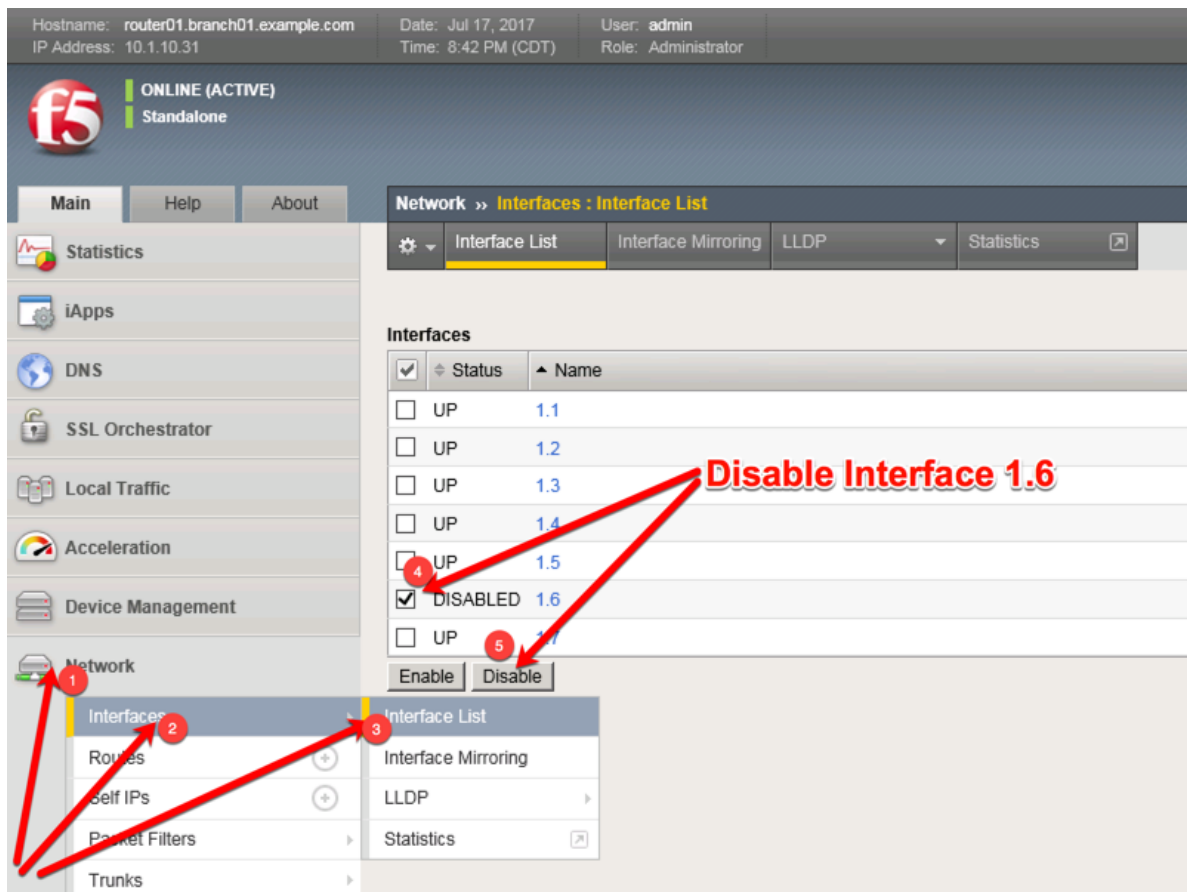
TMSH

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

- Introduce a network problem in the ISP at site1

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

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



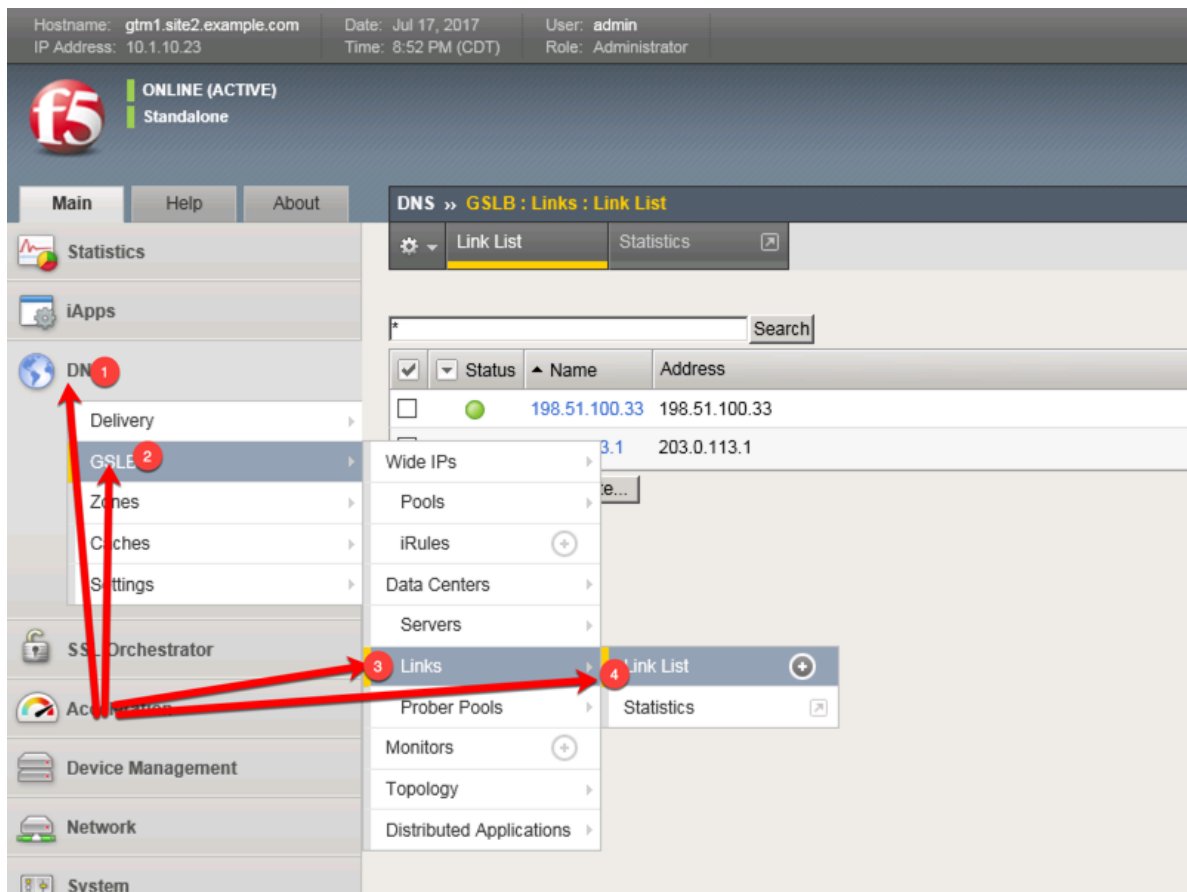
TMSH command to run on the router01 to simulate an ISP failure

TMSH

tmsh modify interface 1.6 disabled

4. View the effect

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



https://gtm1.site2.example.com/tmui/Control/jspmap/xsl/gtm_link/list

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>

Hostname: router01.branch01.example.com Date: Jul 17, 2017 User: admin
IP Address: 10.1.10.31 Time: 8:42 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About

Network » Interfaces : Interface List

Interface List Interface Mirroring LLDP Statistics

Statistics
iApps
DNS
SSL Orchestrator
Local Traffic
Acceleration
Device Management
Network

Interfaces

<input checked="" type="checkbox"/>	Status	Name
<input type="checkbox"/>	UP	1.1
<input type="checkbox"/>	UP	1.2
<input type="checkbox"/>	UP	1.3
<input type="checkbox"/>	UP	1.4
<input type="checkbox"/>	UP	1.5
<input checked="" type="checkbox"/>	DISABLED	1.6
<input type="checkbox"/>	UP	1.7

Enable Disable

1 2 3 4 5

Enable Interface 1.6

TMSH

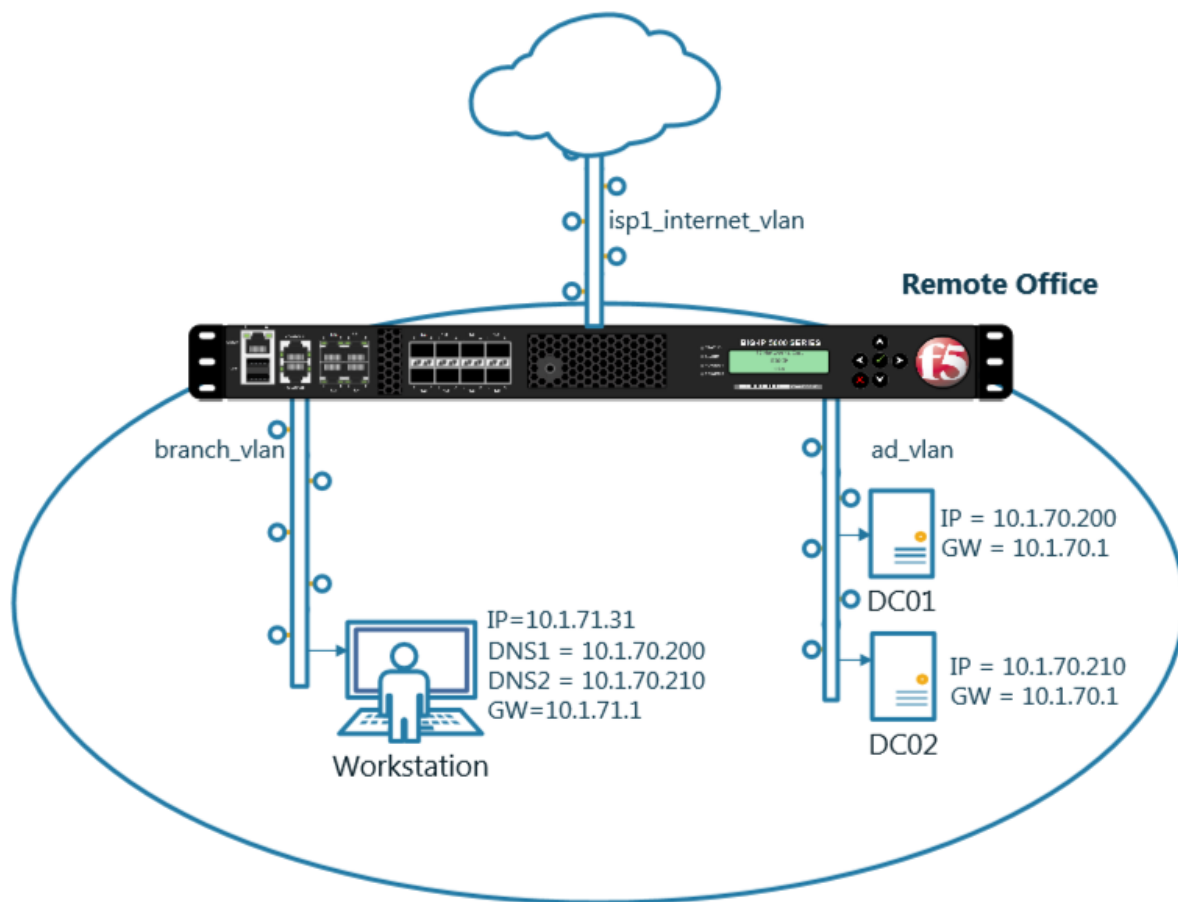
tmsh modify interface 1.6 enabled

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

Class 2 - Advanced GSLB

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.

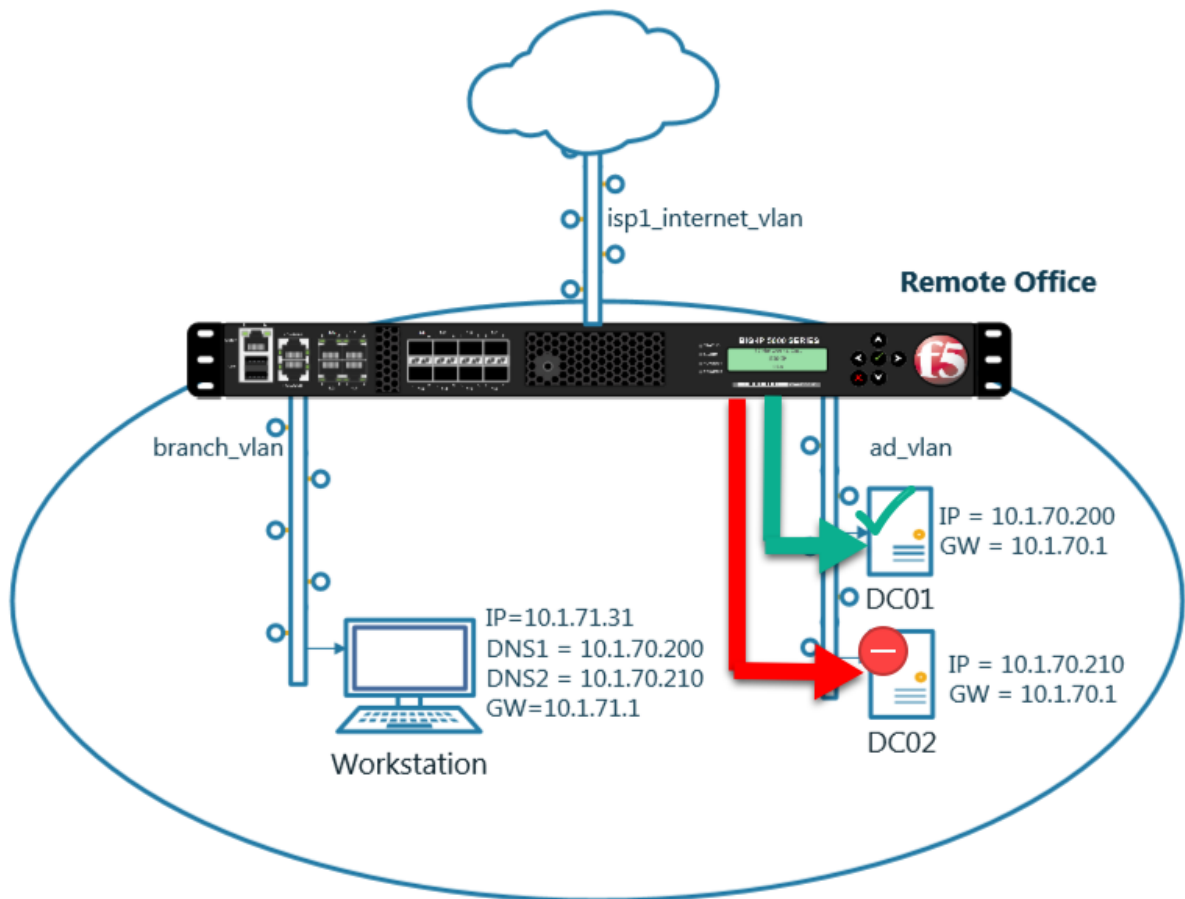
1. Transparent Cache

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

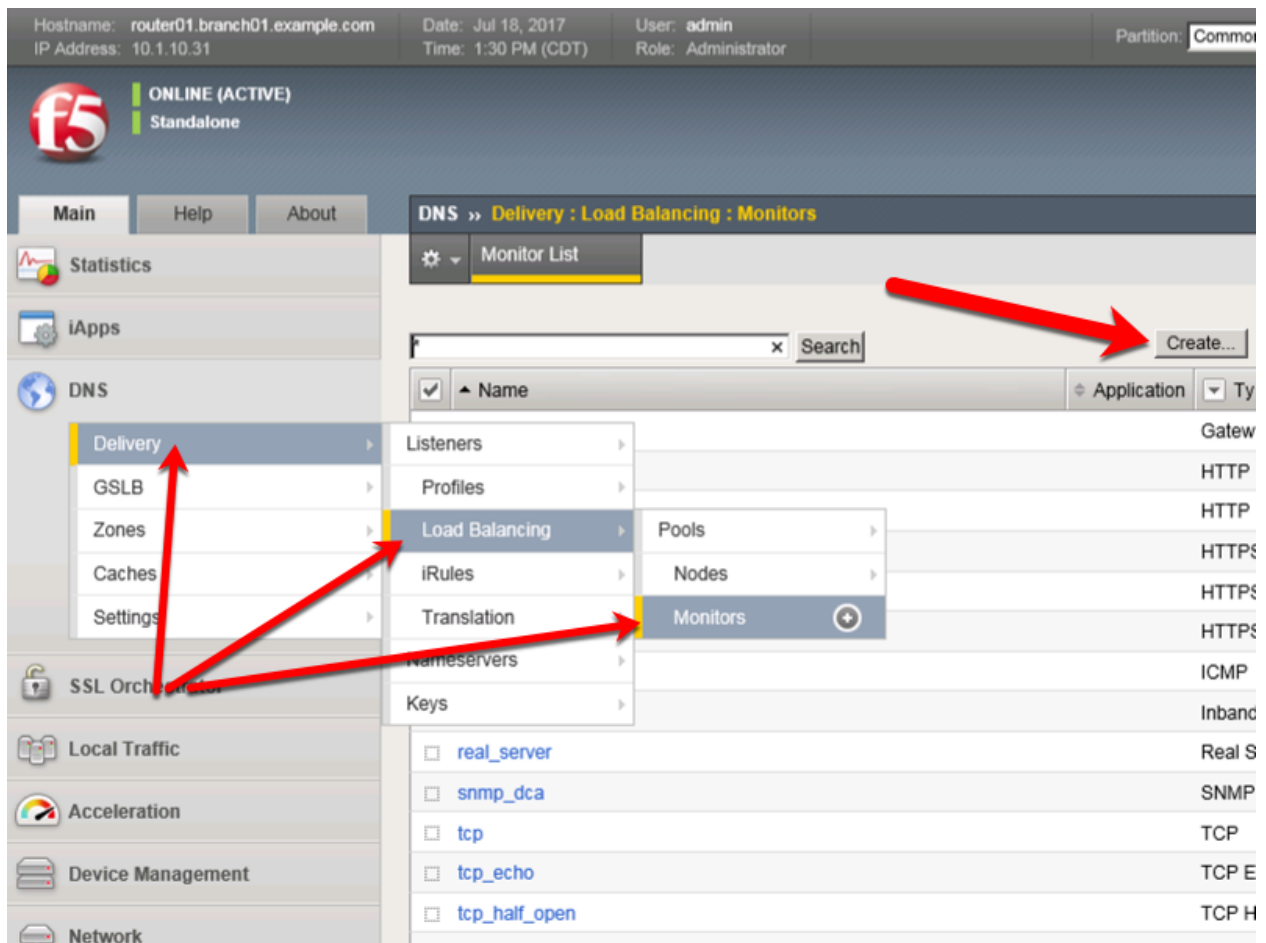
3.1 Transparent Cache

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

General Properties	
Name	example.com_dns_monitor
Description	
Type	DNS
Parent Monitor	dns

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

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

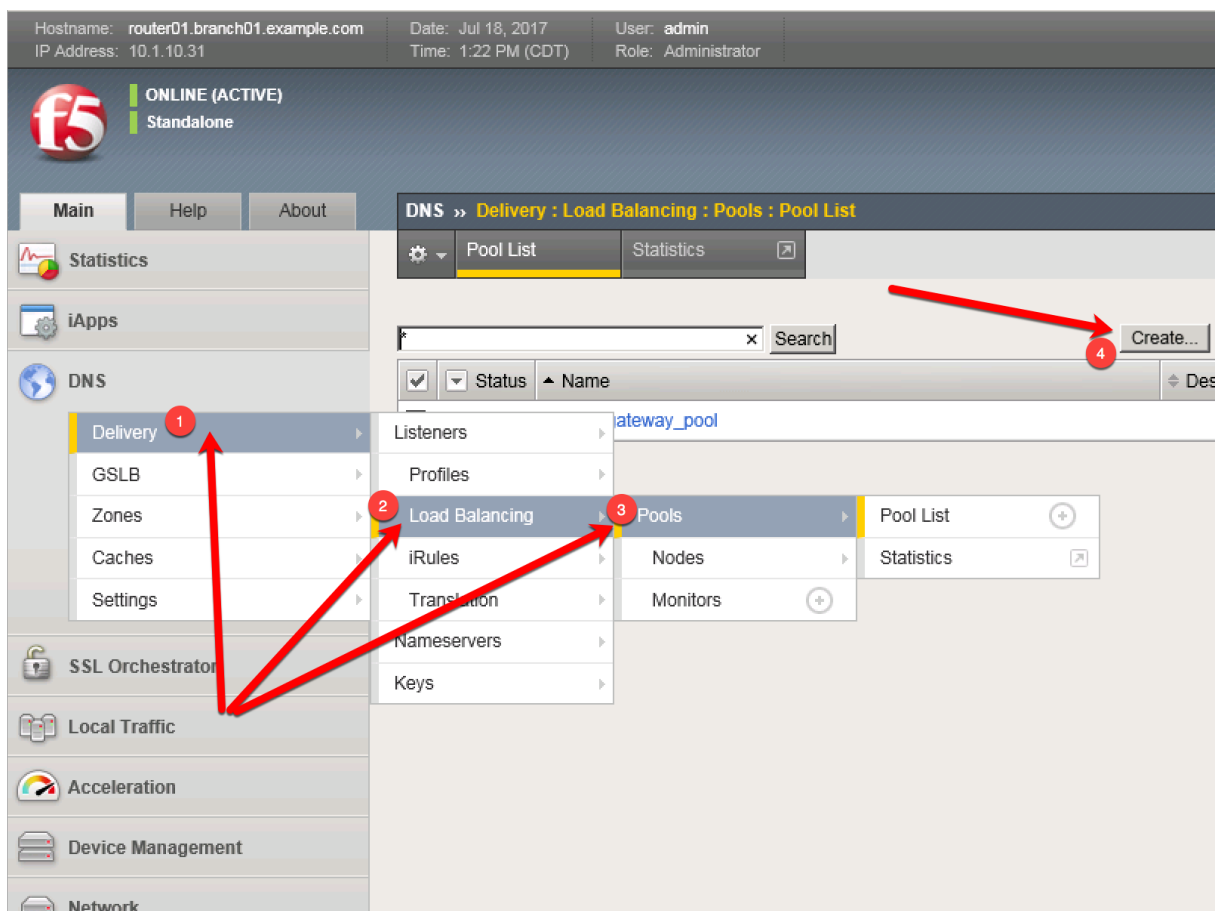
TMSH

```
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

Configuration: Advanced

Name	branch01_dns_pool
Description	
Health Monitors	<div> <div>Active</div> <div>Available</div> <div> <div>/Common</div> <div>example.com_dns_monitor</div> <div><<</div> <div>>></div> </div> <div> <div>/Common</div> <div>gateway_icmp</div> <div>http</div> <div>http_head_f5</div> <div>https</div> <div><</div> <div>></div> </div> </div>
Availability Requirement	All Health Monitor(s)
Allow SNAT	Yes
Allow NAT	Yes
Action On Service Down	None
Slow Ramp Time	10 seconds
IP ToS to Client	Pass Through
IP ToS to Server	Pass Through
Link QoS to Client	Pass Through
Link QoS to Server	Pass Through
Reselect Tries	0
Enable Request Queueing	No
Request Queue Depth	0
Request Queue Timeout	0 ms
IP Encapsulation	None

Resources

Load Balancing Method	Round Robin
Priority Group Activation	Disabled
New Members	<div> <div> <input checked="" type="radio"/> New Node <input type="radio"/> New FQDN Node <input type="radio"/> Node List </div> <div> Node Name: dc02.branch01.example.com_node (Optional) </div> <div> Address: 10.1.70.210 </div> <div> Service Port: 53 Select... </div> <div> Add </div> <div> R:1 P:0 C:0 dc01.branch01.example.com_node 10.1.70.200 :53 R:1 P:0 C:0 dc02.branch01.example.com_node 10.1.70.210 :53 </div> <div> Edit Delete </div> </div>

Create two nodes

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

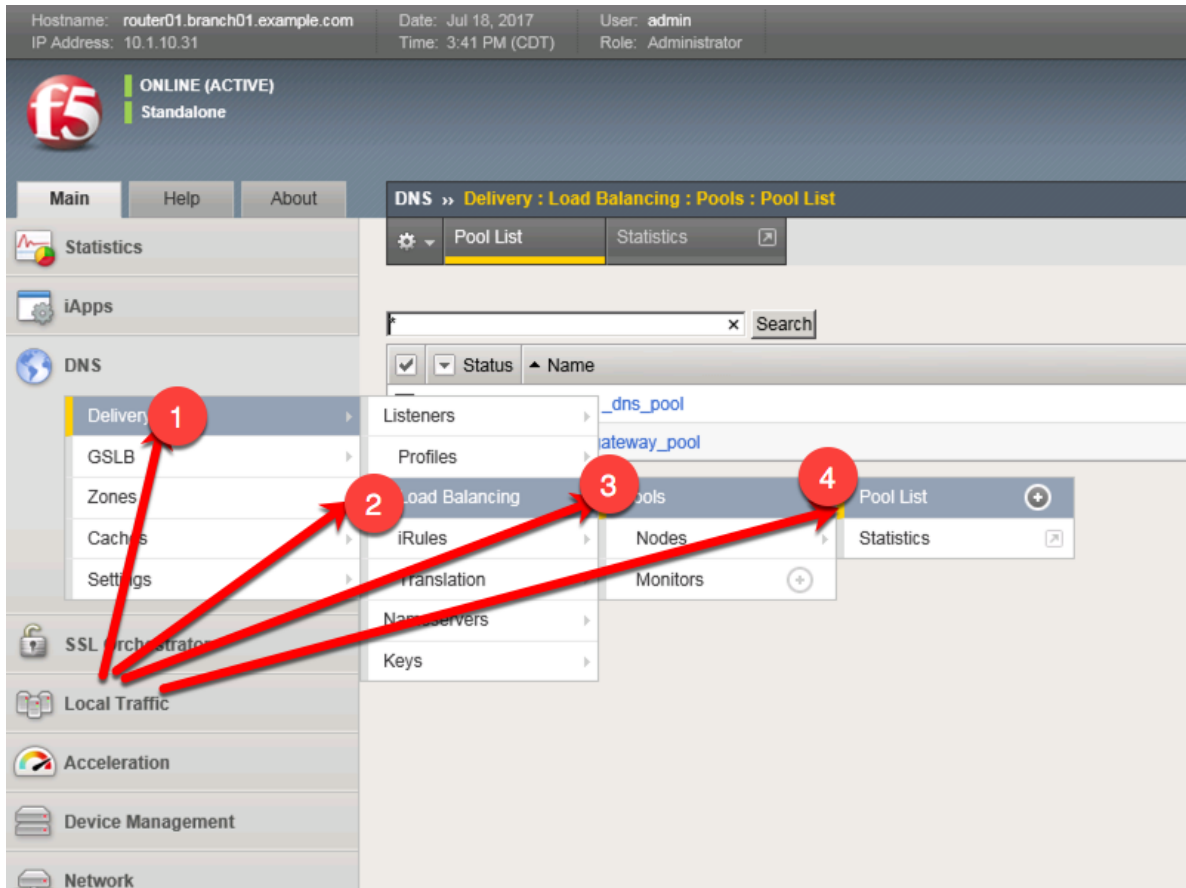
TMSH

```
tmsmsh 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”

Hostname: router01.branch01.example.com Date: Jul 18, 2017 User: admin
IP Address: 10.1.10.31 Time: 3:47 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About

DNS » Delivery : Load Balancing : Pools : Pool List » Properties : branch01_dns_pool

Statistics iApps DNS Delivery GSLB Zones Caches Settings

SSL Orchestrator Local Traffic Acceleration Device Management Network

General Properties

Name	branch01_dns_pool
Partition / Path	Common
Description	
Availability	Available (Enabled) - The pool is available

Health Monitors

Active	Available
/Common example.com_dns_monitor	/Common gateway_icmp http http_head_f5 https

Availability Requirement: All Health Monitor(s)

Allow SNAT: Yes

Allow NAT: Yes

Action On Service Down: None

Click "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.

Hostname: router01.branch01.example.com Date: Jul 18, 2017 User: admin
IP Address: 10.1.10.31 Time: 4:54 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About **DNS » Delivery : Load Balancing : Pools : Pool List » Members : branch01_dns_pool**

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

Load Balancing
Load Balancing Method: Round Robin
Priority Group Activation: Disabled
Update

Notice that health monitors marked one server down

Current Members

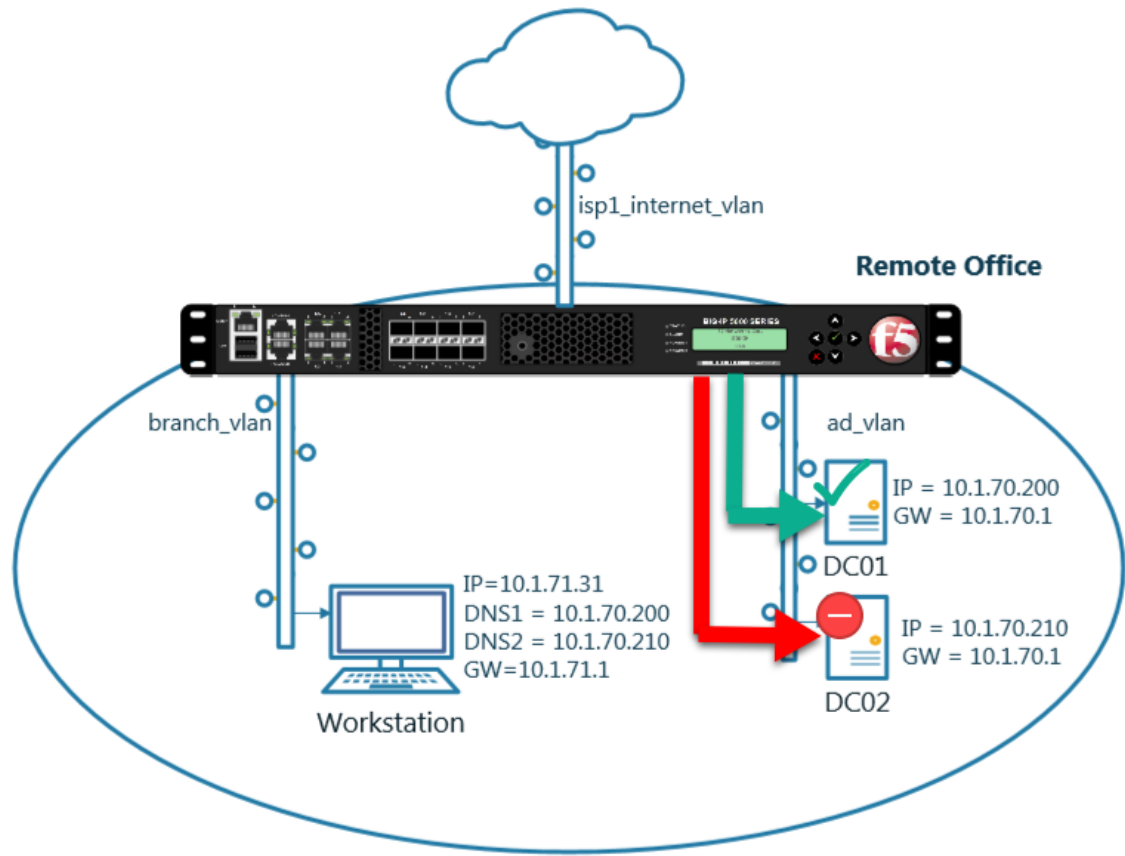
<input checked="" type="checkbox"/>	Status	Member	Address	Service Port	FQDN
<input type="checkbox"/>		dc01.branch01.example.com_node:53	10.1.70.200	53	Nc
<input type="checkbox"/>		dc02.branch01.example.com_node:53	10.1.70.210	53	Nc

Enable Disable Force Offline Remove

Maybe that's why users are complaining. It seems that a local DNS server is failing.

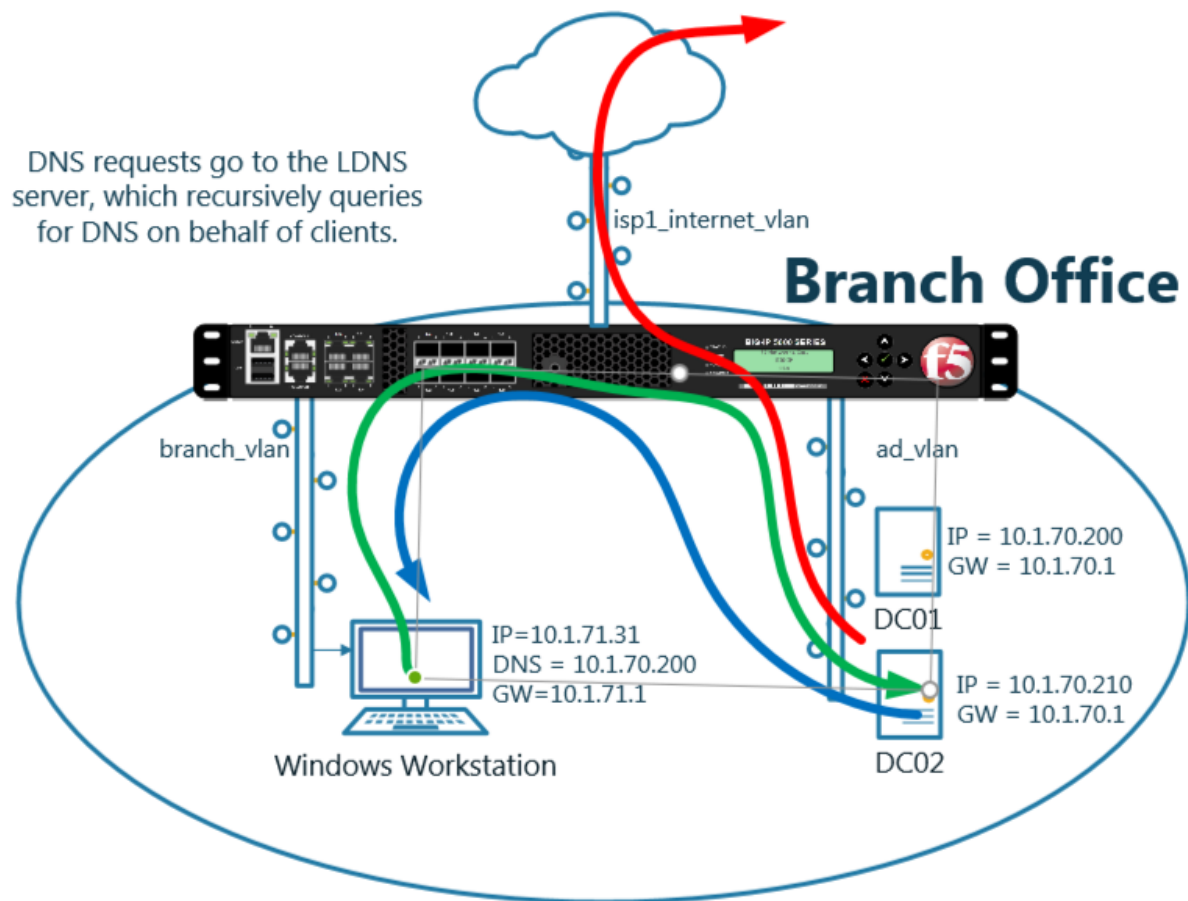
TMSH

tmsh show ltm pool branch01_dns_pool detail

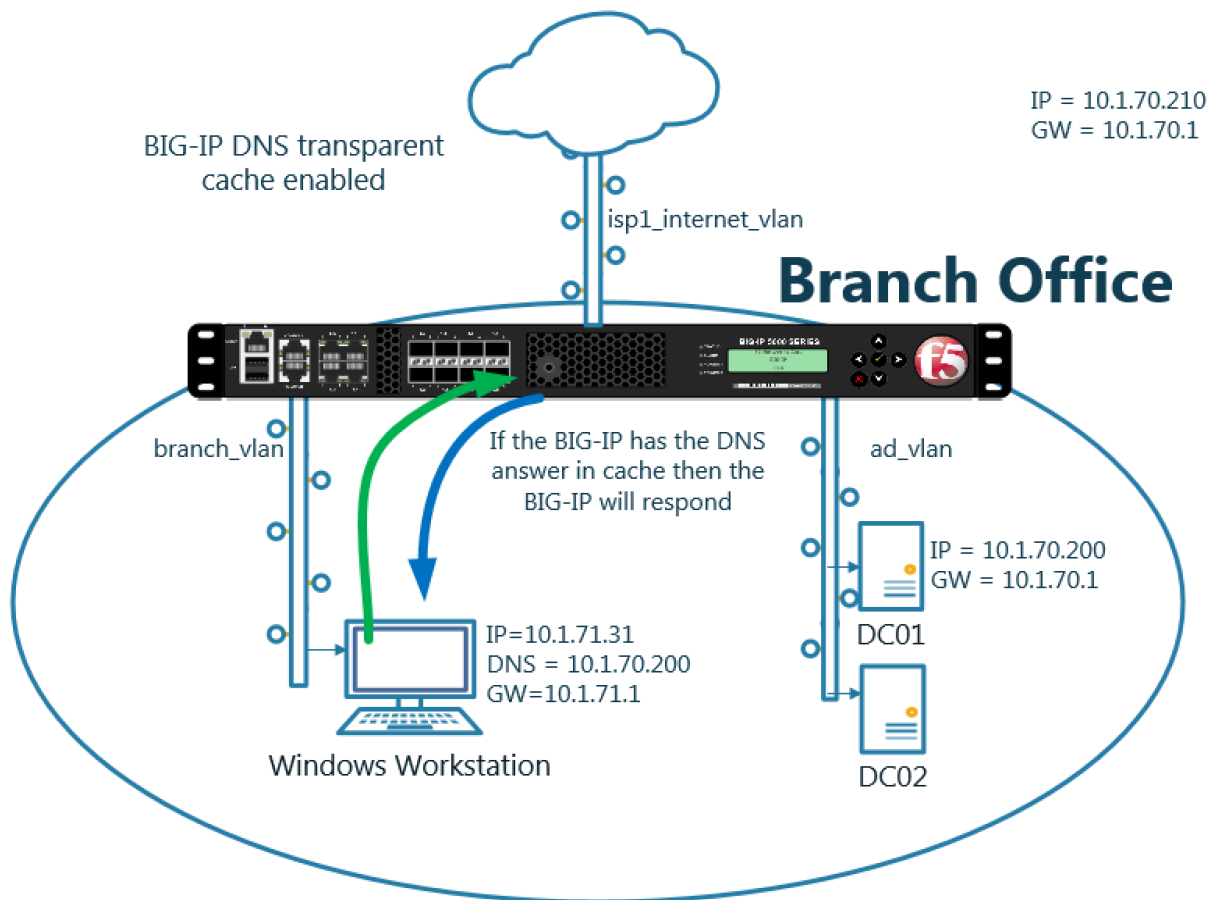


In this module we will prepare the objects required to build a transparent cache.

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.

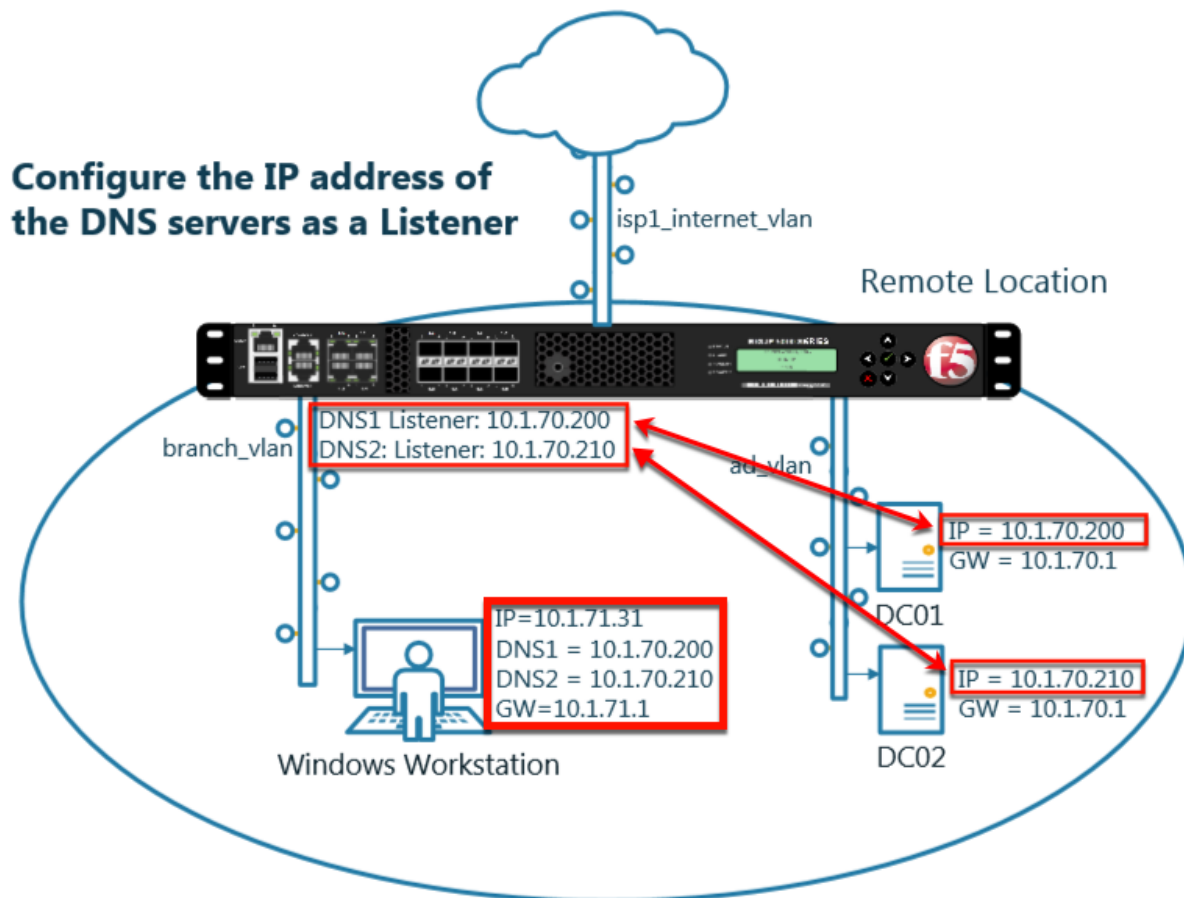


Log into the gateway device router01.brancho1 in the **branch office**

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

Create a transparent cache

Setting	Value
Name	transparent_cache
Resolver Type	Transparent

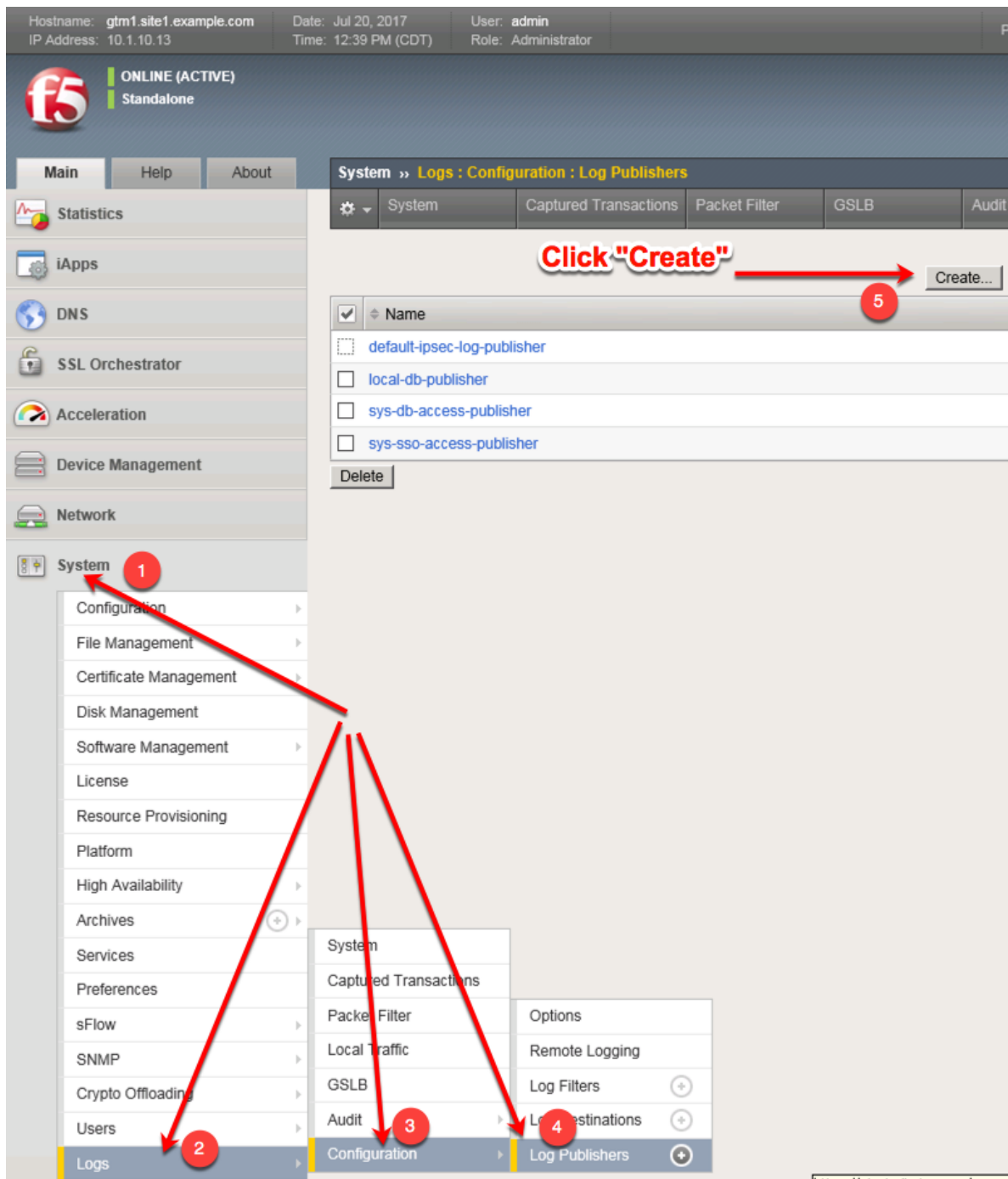


3.2.1 Log Profile

Configure DNS query and response logging.

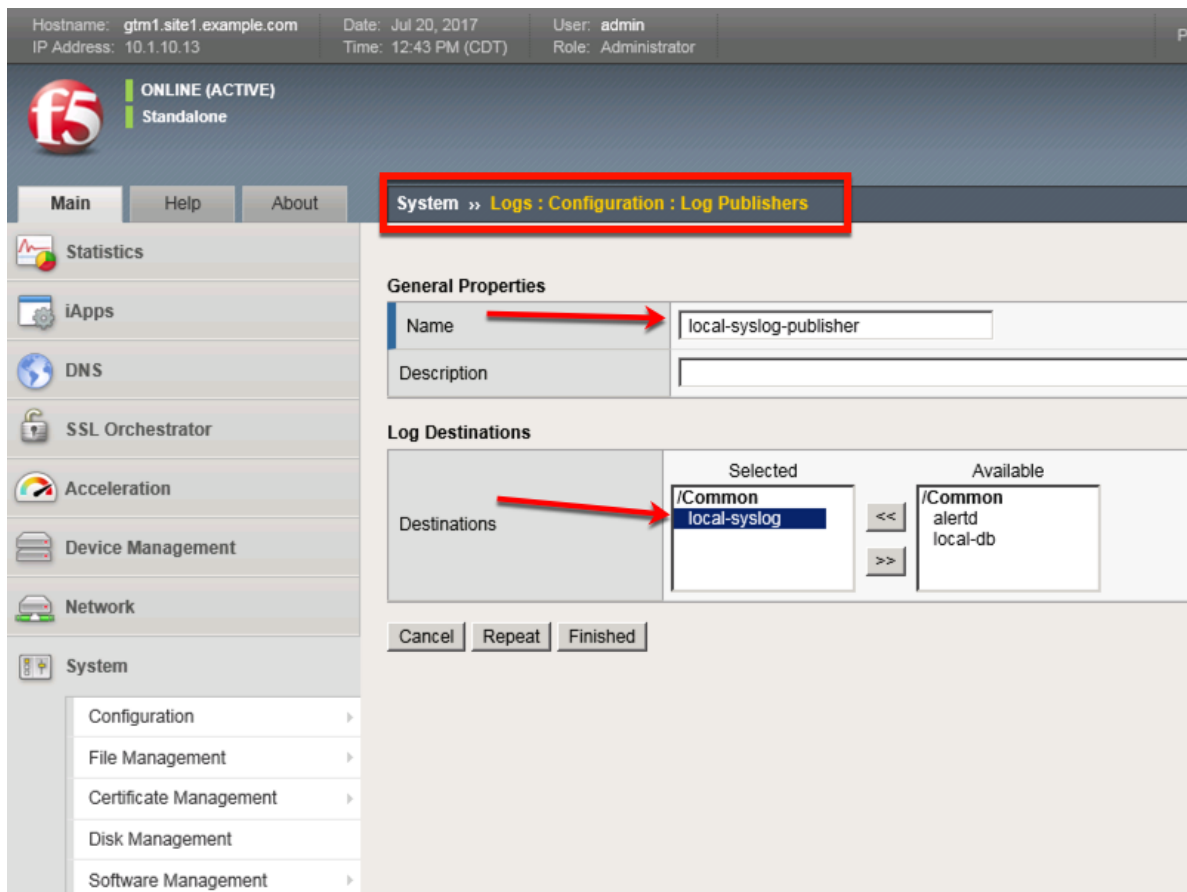
1. Create a "Log Publisher" for local syslog.

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



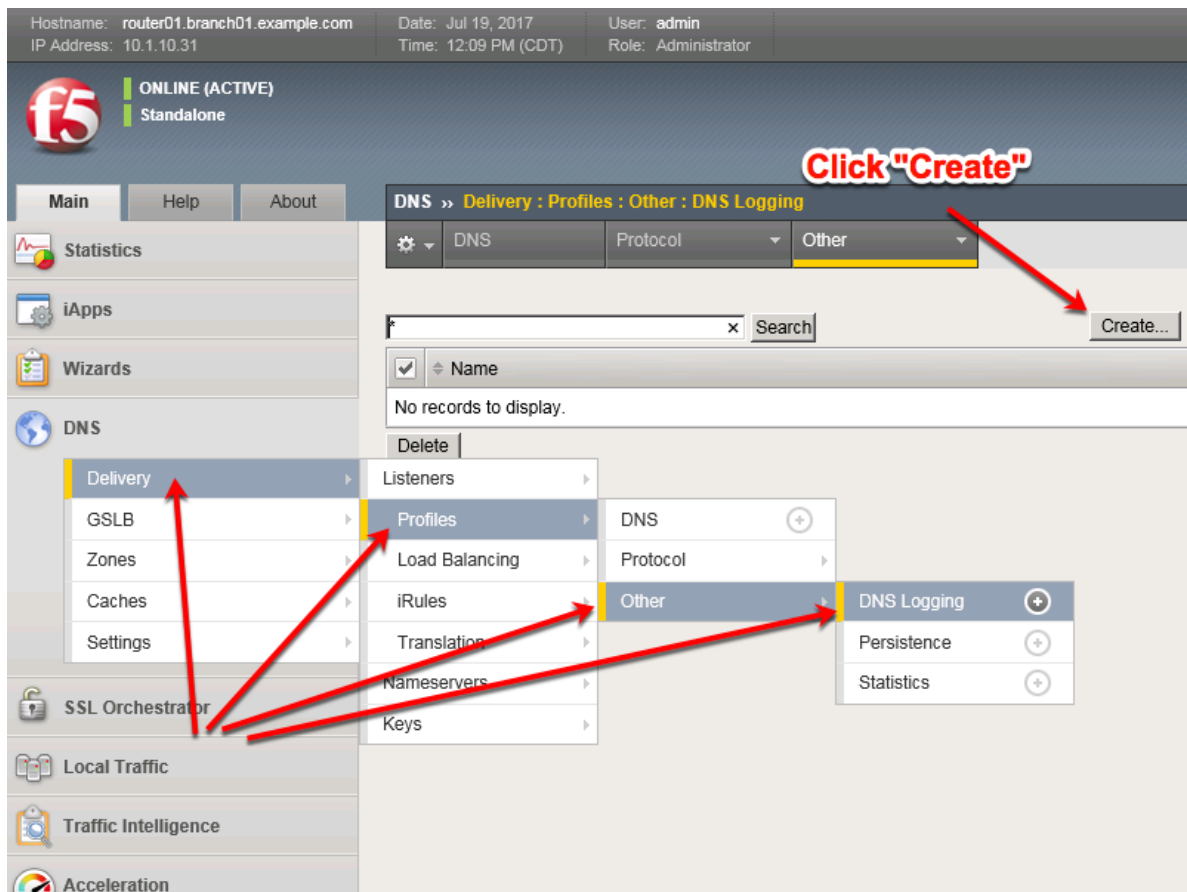
https://router01.branch01.example.com/tmui/Control/jspmap/tmui/system/log/create_publisher.jsp

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

Hostname: router01.branch01.example.com Date: Jul 19, 2017 User: admin
 IP Address: 10.1.10.31 Time: 12:14 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About **DNS » Delivery : Profiles : Other : DNS Logging » New...**

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

General Properties

Name
 Description

Configuration

Log Publisher
 Log Queries ☒ Enabled
 Log Responses ☒ Enabled

Log Fields

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

Cancel Repeat Finished

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

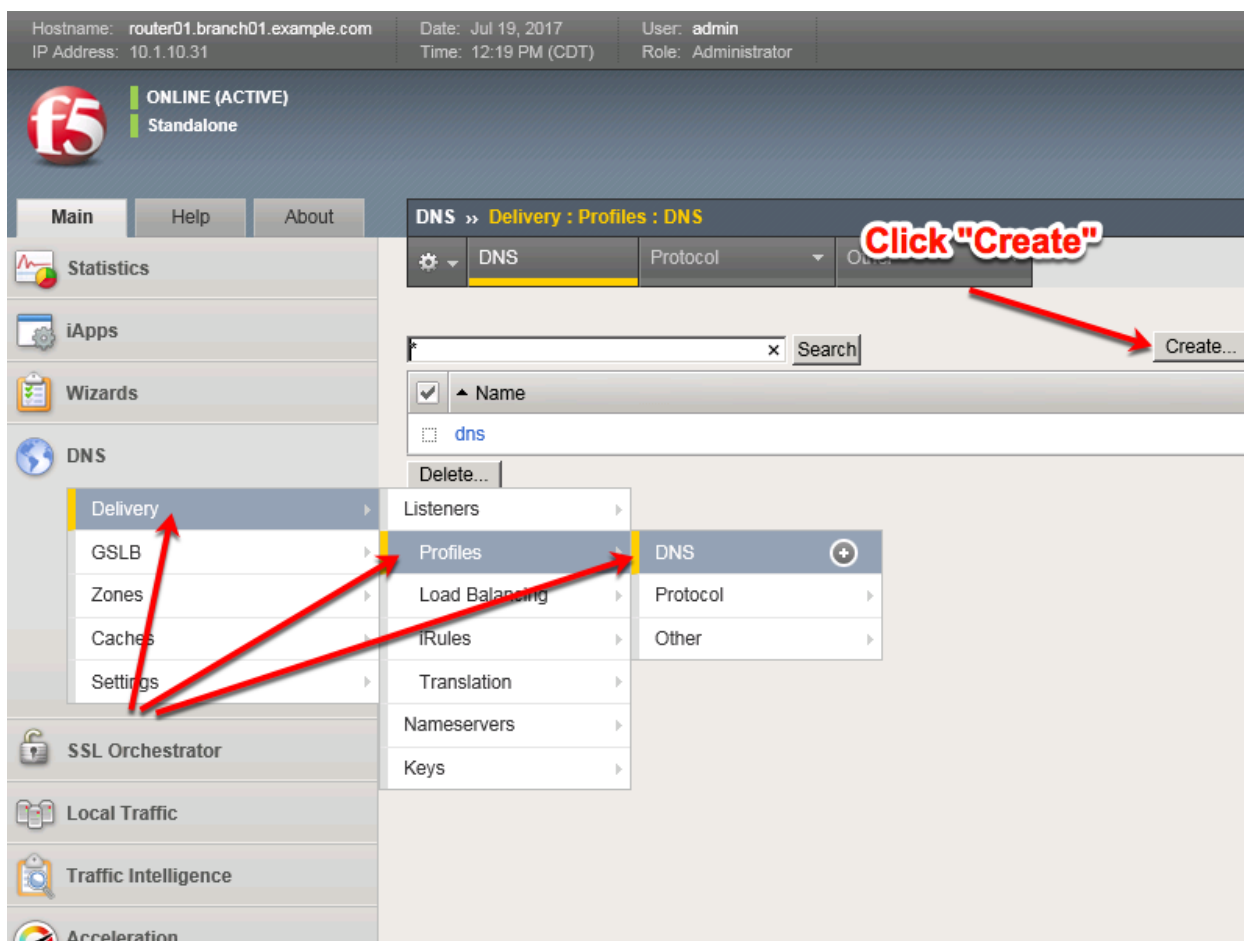
TMSH

```
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>

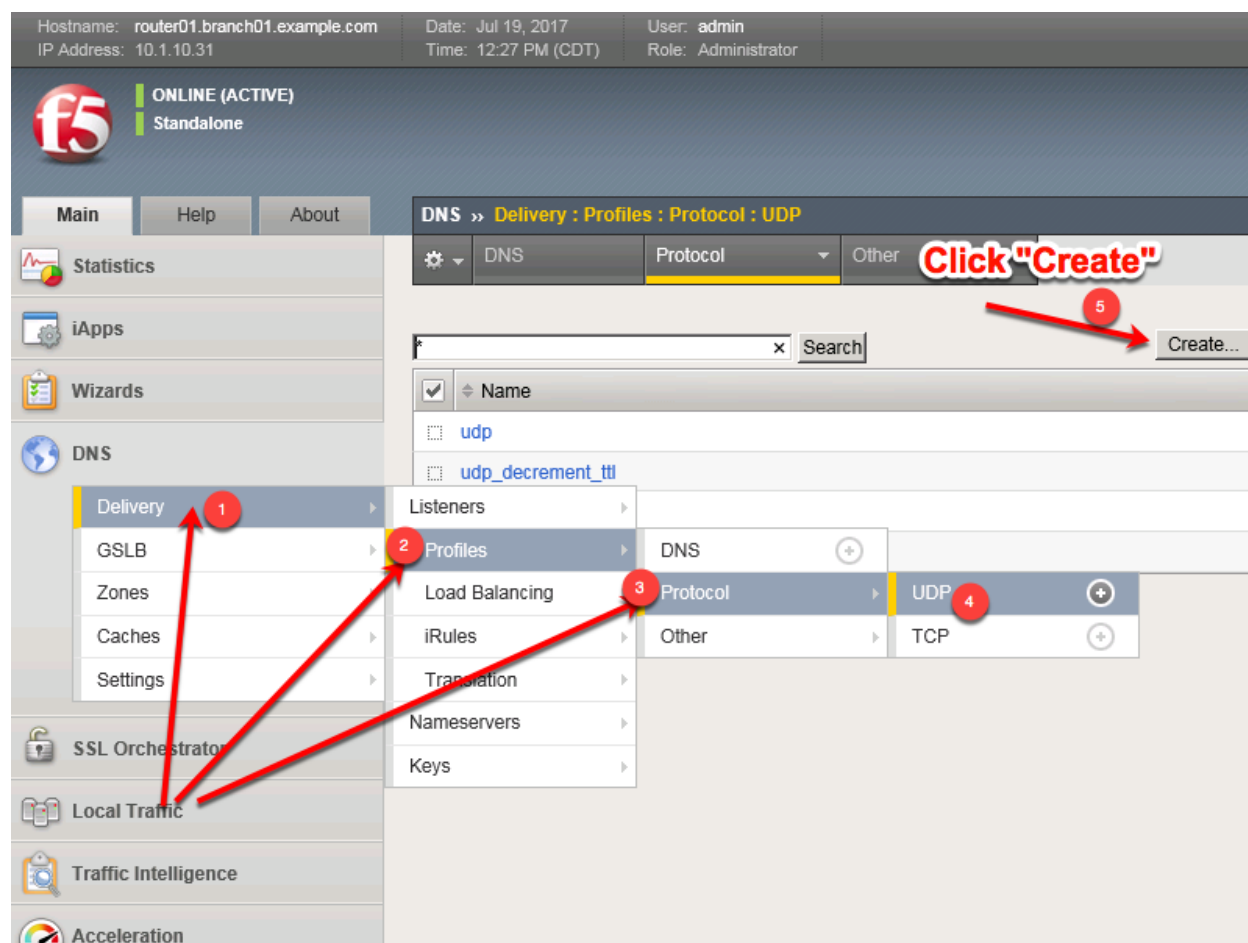
TMSH

```
tmsl 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

Hostname: router01.branch01.example.com Date: Jul 19, 2017 User: admin
IP Address: 10.1.10.31 Time: 12:32 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

Name example.com_udp-
Parent Profile udp_gtm_dns

Settings

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

Cancel Repeat Finished

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

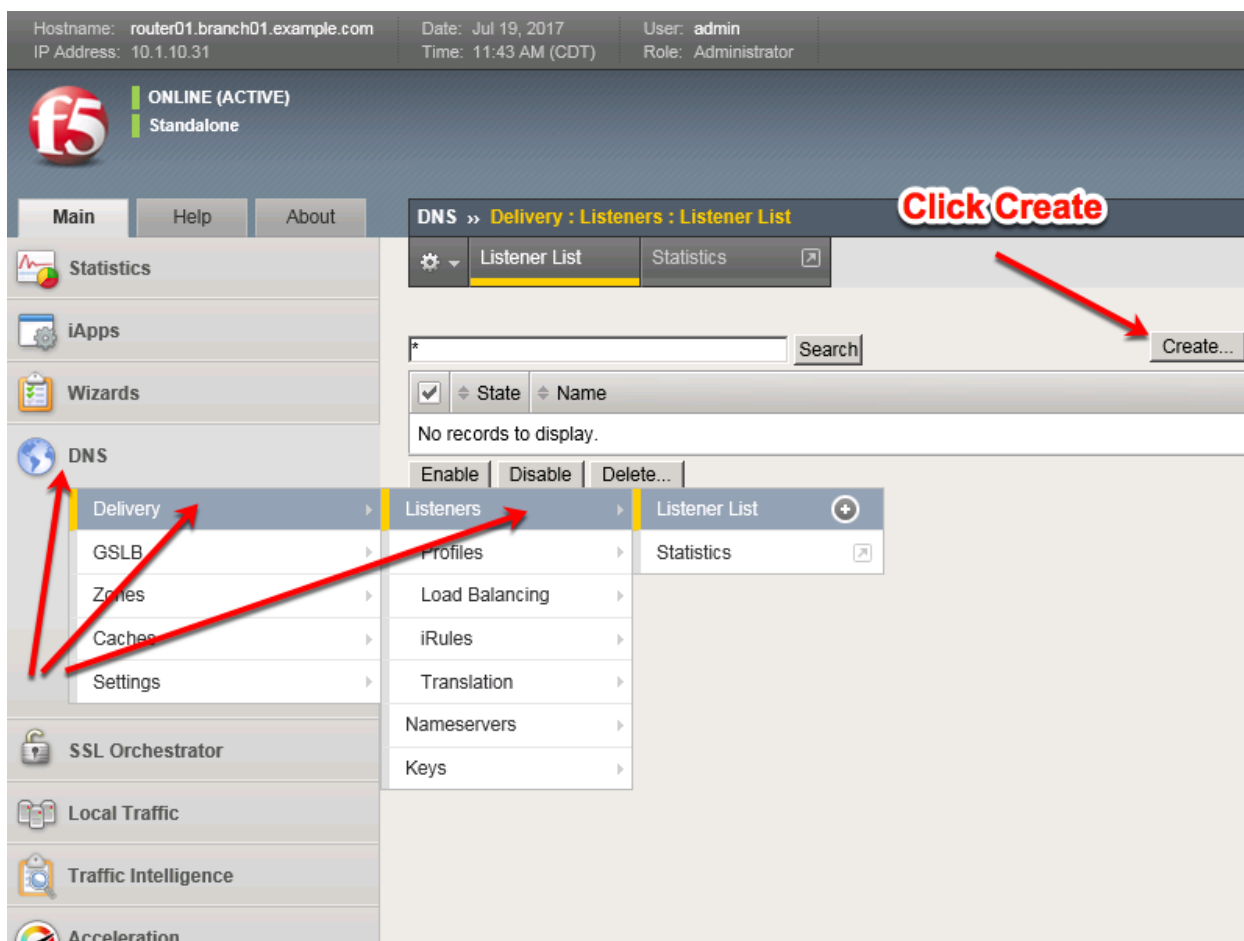
TMSH

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/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/local1b/virtual_server/create.jsp


```
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
```

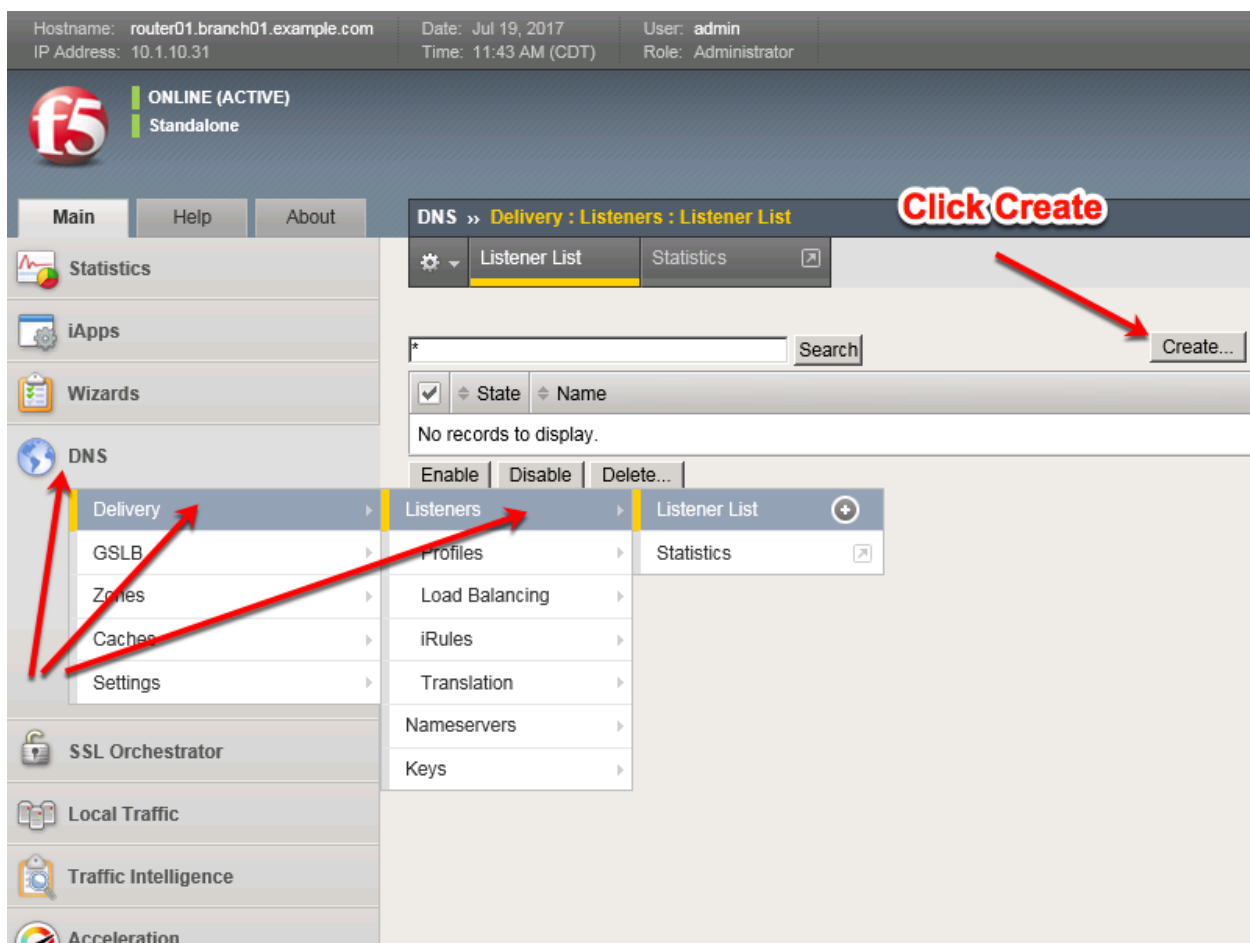
TMSH

```
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

Hostname: router01.branch01.example.com

Date: Jul 19, 2017

User: admin

IP Address: 10.1.10.31

Time: 12:46 PM (CDT)

Role: Administrator

f5

ONLINE (ACTIVE)
Standalone

MainHelpAbout

DNS » Delivery : Listeners : Listener List » New...

Statistics

iApps

Wizards

DNS

- Delivery
- GSLB
- Zones
- Caches
- Settings

SSL Orchestrator

Local Traffic

Traffic Intelligence

Acceleration

Access

Device Management

Network

System

General

NameDC01_tcp_53_virtual

Description

StateEnabled

Listener:Advanced

DestinationType: Host Network
Address: 10.1.70.200

Service PortDNS53

VLAN TrafficEnabled on...

VLANs and Tunnels

Selected
/Common
branch01_vlan

Available
/Common
AD_vlan
external_vlan
http-tunnel
isp1_site1_vlan

Source Address TranslationNone

Address Translation☐ Enabled

Port Translation☐ Enabled

Route Advertisement☐ Enabled

Auto Last HopDefault

Last Hop PoolNone

Service:Advanced

ProtocolTCP

Protocol Profile (Client)example.com_tcp-dns_profile

Protocol Profile (Server)(Use Client Profile)

DNS Profileexample.com_dns_profile

Load Balancing

Default Poolbranch01_dns_pool

Default Persistence ProfileNone

Fallback Persistence ProfileNone

```
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**

Hostname: router01.branch01.example.com Date: Jun 27, 2017 User: admin
IP Address: 10.1.10.31 Time: 12:48 PM (CDT) Role: Administrator

ONLINE (ACTIVE)
Standalone

Main Help About **DNS » Caches : Cache List » Properties : transparent_cache**

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

Properties Local Zones Response Policy Zones **Statistics**

General Properties

Name	transparent_cache
Resolver Type	Transparent (None)

DNS Cache

Message Cache Size	1048576 x bytes
Resource Record Cache Size	10485760 bytes
Answer Default Zones	<input checked="" type="checkbox"/> Enabled
RRSet Rotate	none

Update Delete...

Click Statistics

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**

Hostname: router01.branch01.example.com Date: Jun 27, 2017 User: admin
IP Address: 10.1.10.31 Time: 12:50 PM (CDT) Role: Administrator Partition: Common

ONLINE (ACTIVE)
Standalone

Main Help About **Statistics » Module Statistics : DNS : Caches » Caches**

Statistics
Dashboard
Module Statistics
Analytics
Performance
iApps
DNS
SSL Orchestrator
Local Traffic
Acceleration
Device Management
Network
System

Traffic Summary DNS Local Traffic Network Memory System

Display Options

Statistics Type	Caches
Data Format	Normalized
Auto Refresh	Disabled Refresh

/Common/transparent_cache Search Reset Search

	Name	Partition / Path	Details	Queries	Responses	Sync	Async	Resolve	Connect
<input type="checkbox"/>	transparent_cache	Common	View...	7	4	4	0	0	0

Reset Clear Cache

Click View

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

Hostname: router01.branch01.example.com Date: Jun 27, 2017 User: admin
IP Address: 10.1.10.31 Time: 12:52 PM (CDT) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Statistics » Module Statistics : DNS : Caches » Caches : transparent_cache

Statistics
Dashboard
Module Statistics
Analytics
Performance

iApps
DNS
SSL Orchestrator
Local Traffic
Acceleration
Device Management
Network
System

Display Options
Data Format: Normalized
Auto Refresh: Disabled Refresh
<< Back Clear Statistics

Query Details

Queries	7
Responses	4
Synchronous Responses	4
Asynchronous Responses	0

Failure Details

Resolve	0
Connection	0
Server	0
Send	0

Cache Details

	Hits	Misses	Inserts	Updates	Evictions
DNS Message Cache	4	3	0	0	0
Resource Record Cache	0	15	0	0	0

Forwarder Activity

Queries	0
Responses	0

Response Policy

Rewrites	0
----------	---

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 #
```

TMSH

show ltm dns cache transparent transparent_cache

3. Clearing Entire Cache

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

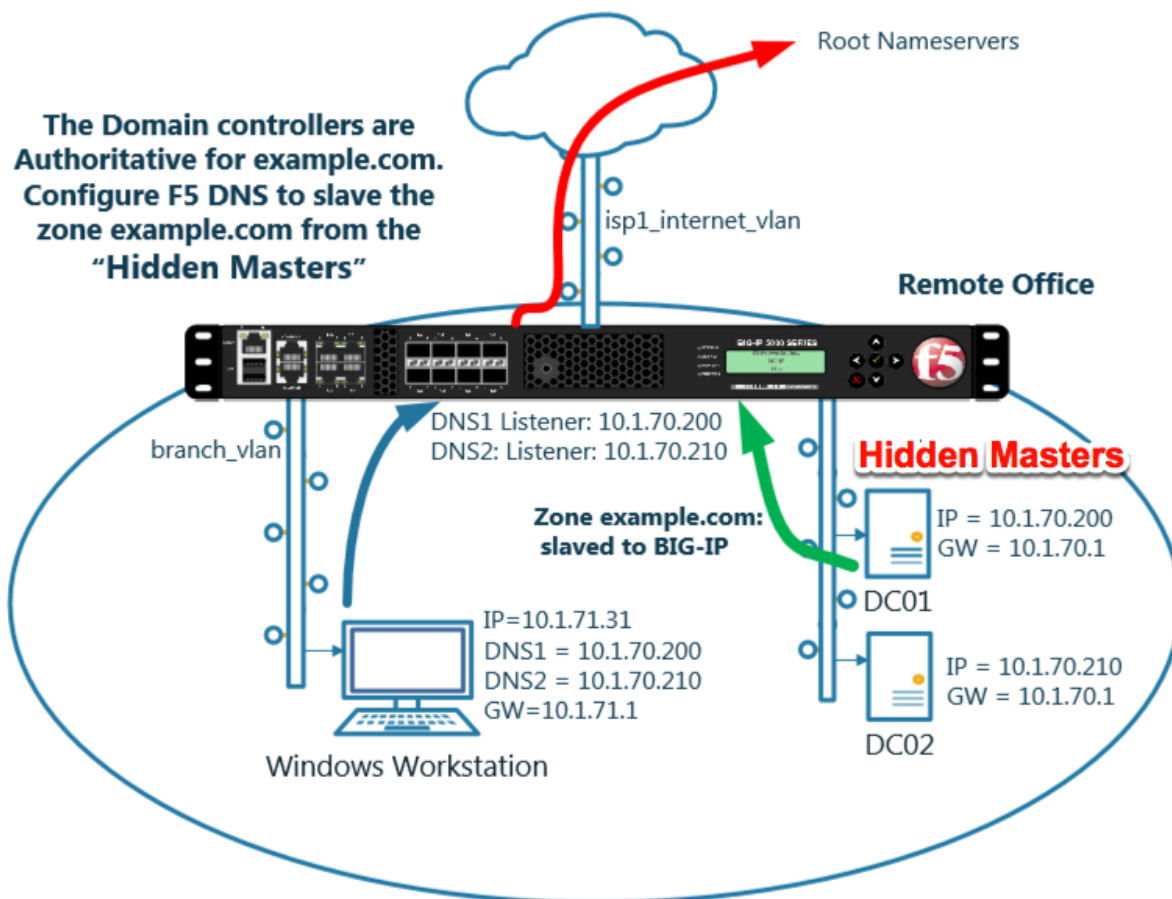
Set “Statistics Type” to “Caches”.

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

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.

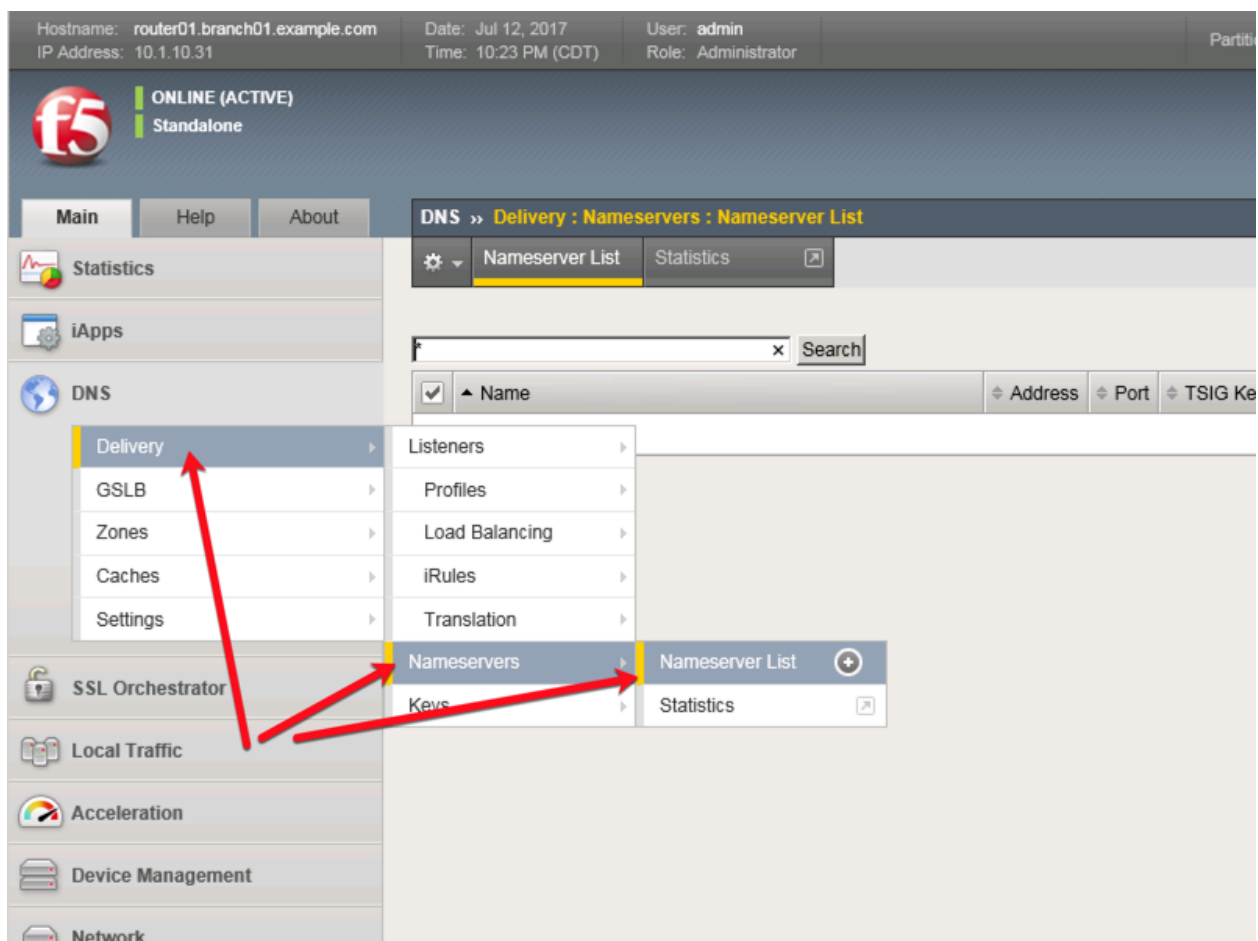


https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/dns-services-implementations-11-6-0/2.html#unique_1658664851

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

Hostname: gtm1.site1.example.com Date: Jul 21, 2017 User: admin
IP Address: 10.1.10.13 Time: 1:47 AM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About

DNS » Delivery : Nameservers : Nameserver List » **New Nameserver...**

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

General Properties

Name dc01.example.com
Address 10.1.70.200
Service Port 53 Other: ▾

Configuration

Route Domain 0 ▾
TSIG Key None ▾

Cancel Repeat Finished

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

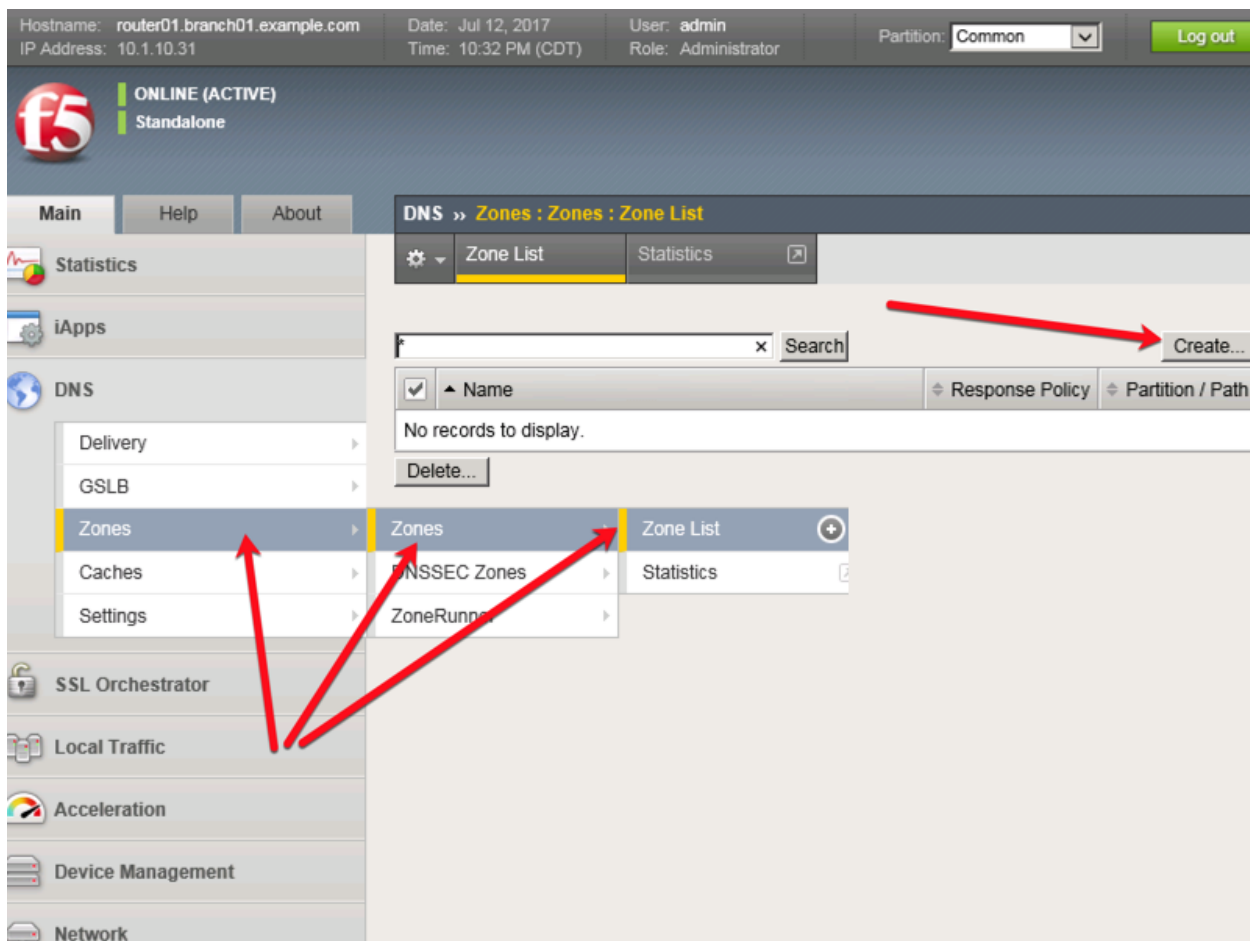
TMSH

```
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

Hostname: gtm1.site1.example.com Date: Jul 21, 2017 User: admin
IP Address: 10.1.10.13 Time: 1:55 AM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About DNS » Zones : Zones : Zone List » **New Zone...**

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

General Properties

Name **example.com**

DNS Express

Server **dc01.example.com**

Availability ☐ Unknown

State **Enabled**

Notify Action **Consume**

Address: **Add**

Allow NOTIFY From

Delete

Verify Notify TSIG ☐

Response Policy ☐

Zone Transfer Clients

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

TMSH

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

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

3.3.3 Results

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

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

DNS Express

Server **dc01.example.com**

Availability **Available (Enabled) - Successful AXFR**

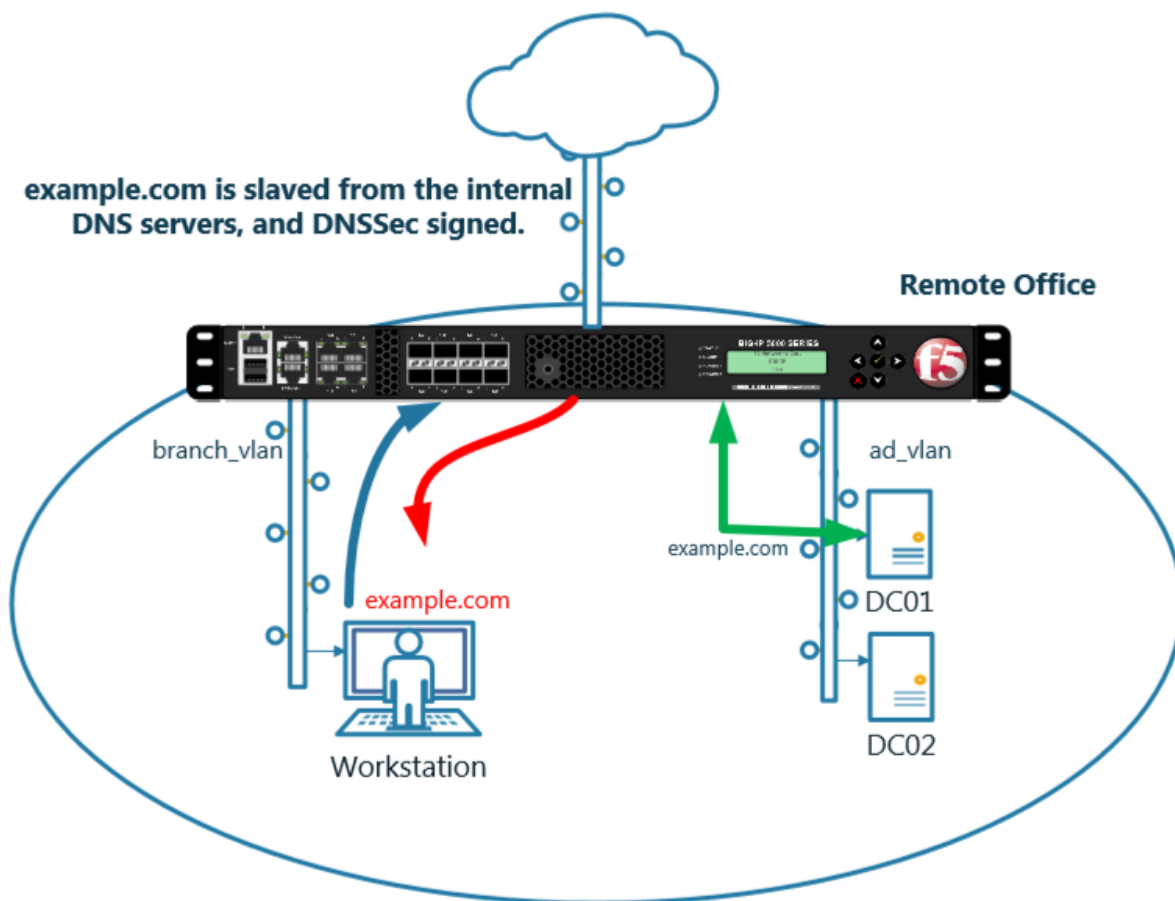
- Run the following command to see the contents of the DNS Express database:

```
dnsxdump | less
```

Examine the results

[illegible]

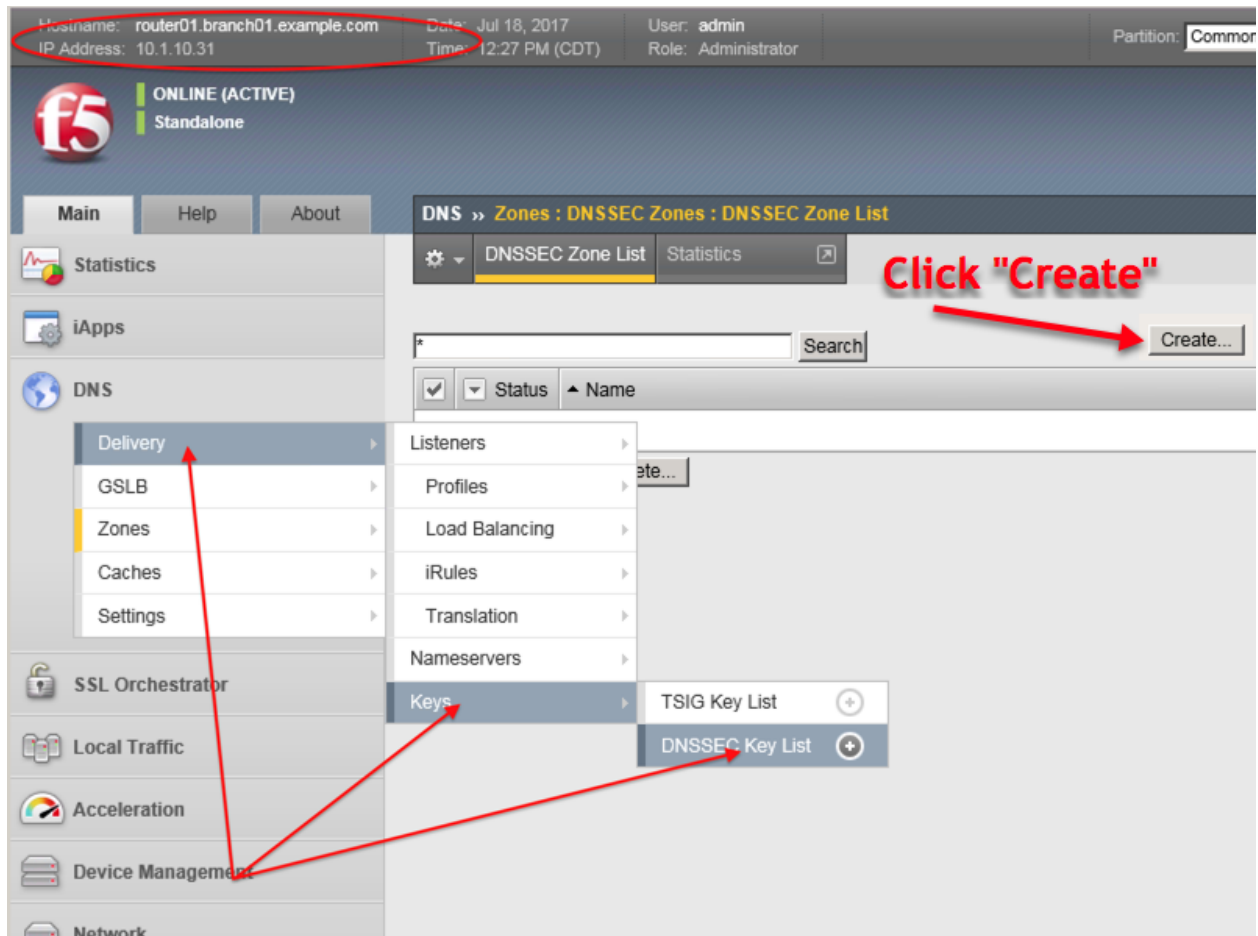
3.4 DNSSec



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

Hostname: **router01.branch01.example.com** Date: Jul 18, 2017 User: admin
 IP Address: 10.1.10.31 Time: 1:40 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
 Standalone

Main Help About **DNS » Delivery : Keys : DNSSEC Key List » New DNSSEC Key...**

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

General Properties

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

Key Settings

Certificate	default.crt	←
Private Key	default.key	←

Cancel Repeat Finished

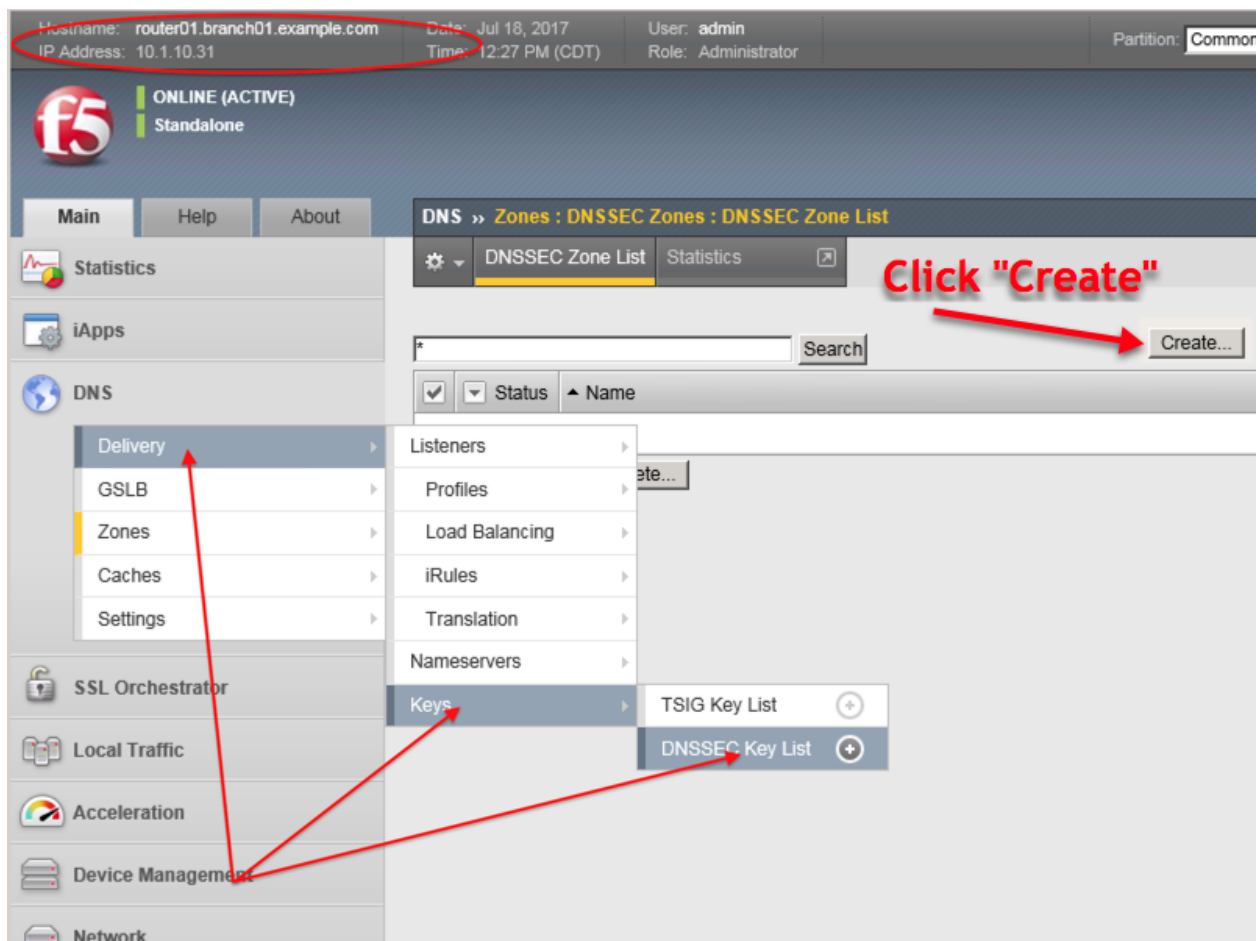
https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/dnssec_key/create.jsp

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

Hostname: router01.branch01.example.com Date: Jul 26, 2017 User: admin
IP Address: 10.1.10.31 Time: 12:30 AM (CDT) Role: Administrator Partition:

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

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

General Properties

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

Key Settings

Certificate	default.crt
Private Key	default.key

Cancel Repeat Finished

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

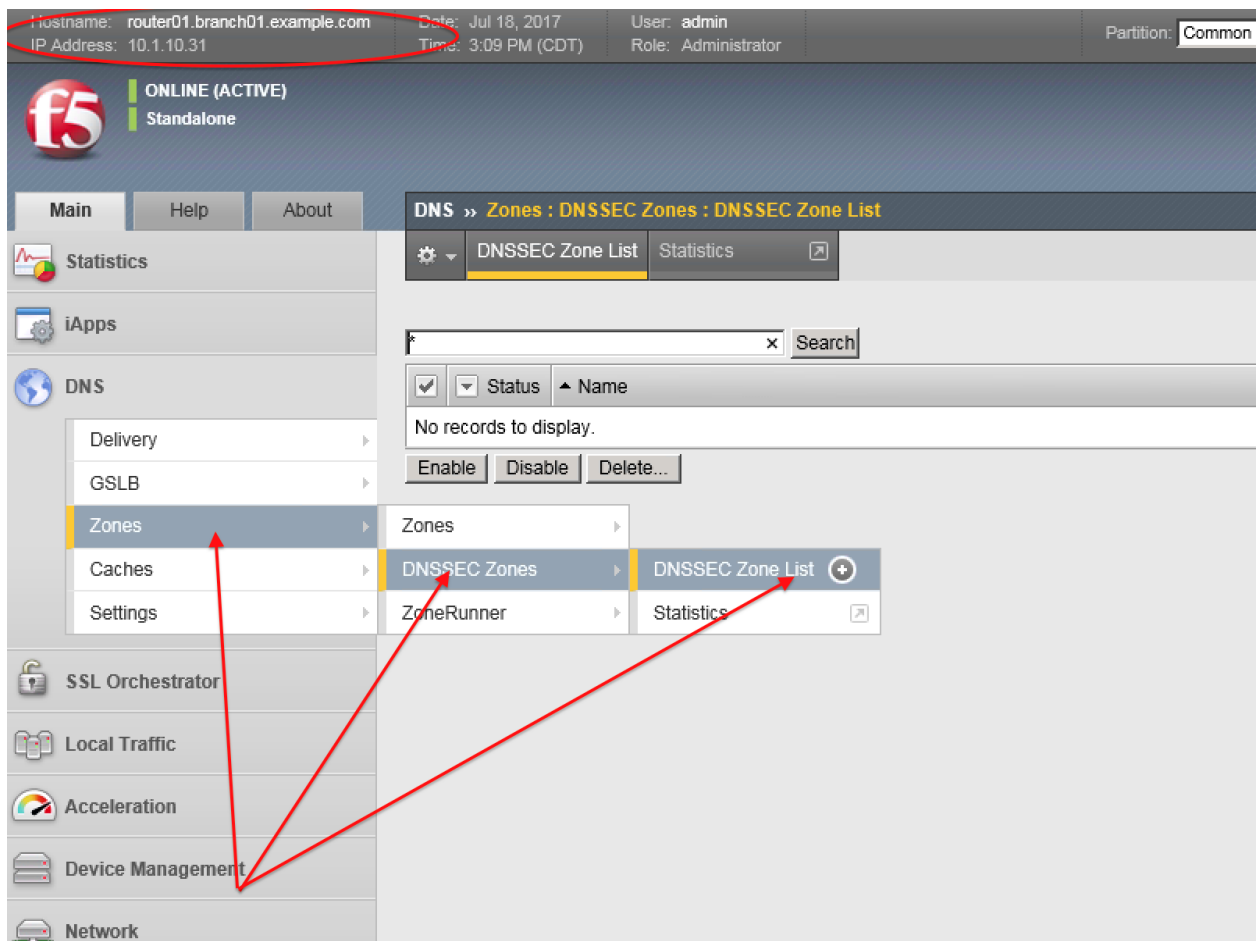
TMSH commands for Key Signing key creation:

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

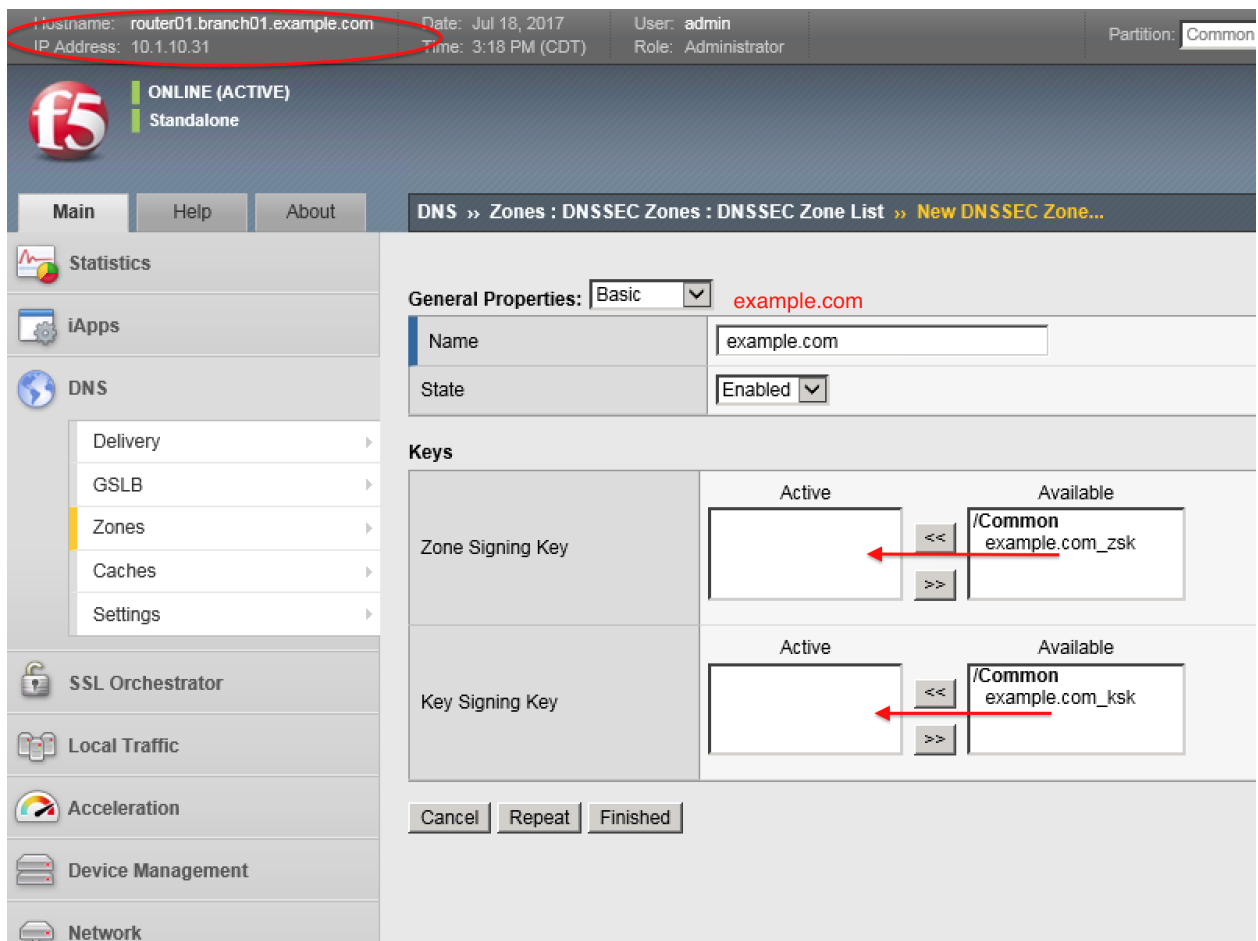
Navigate to: **DNS » Zones : DNSSEC Zones : DNSSEC Zone List**



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:

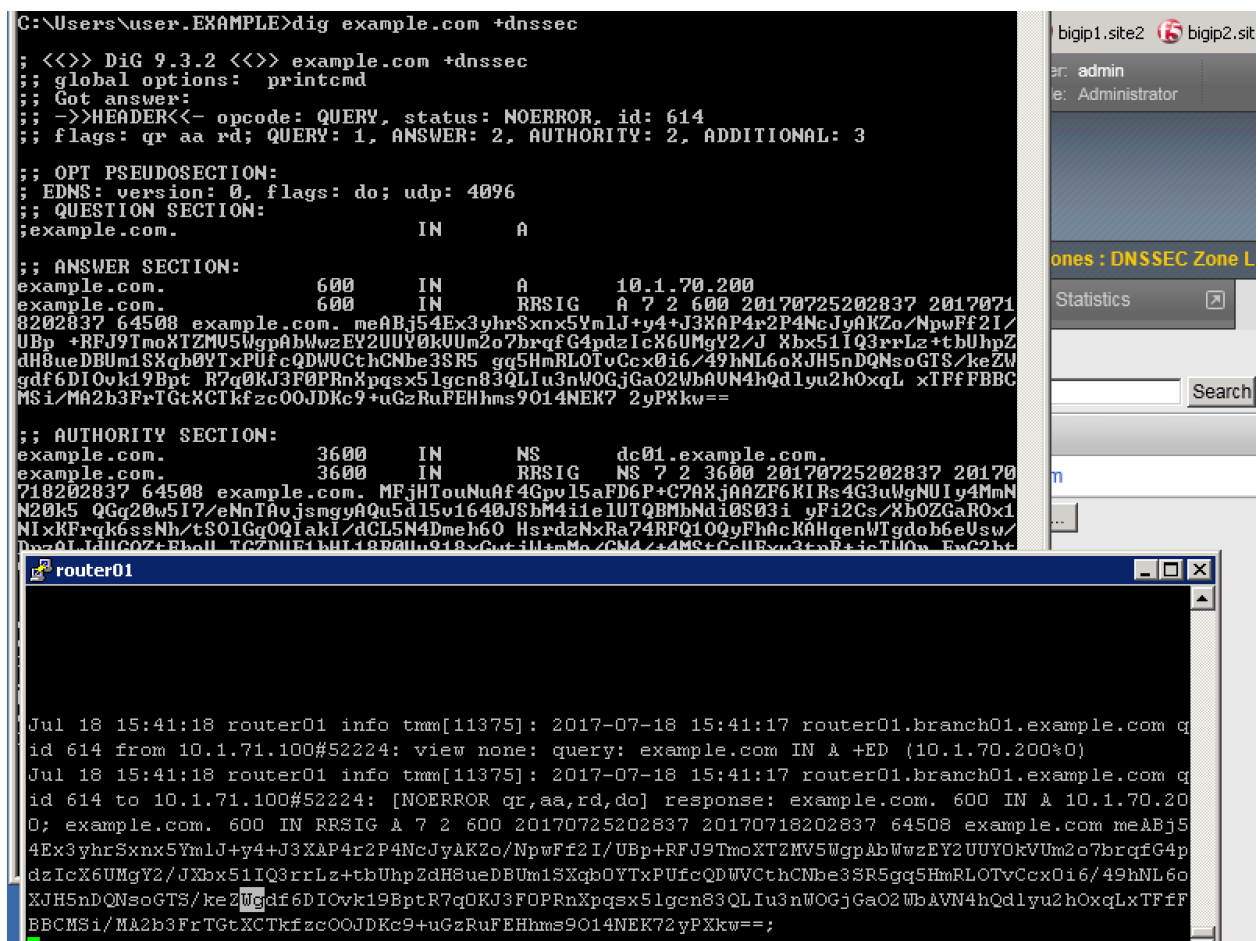
TMSH

```
tmsl 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

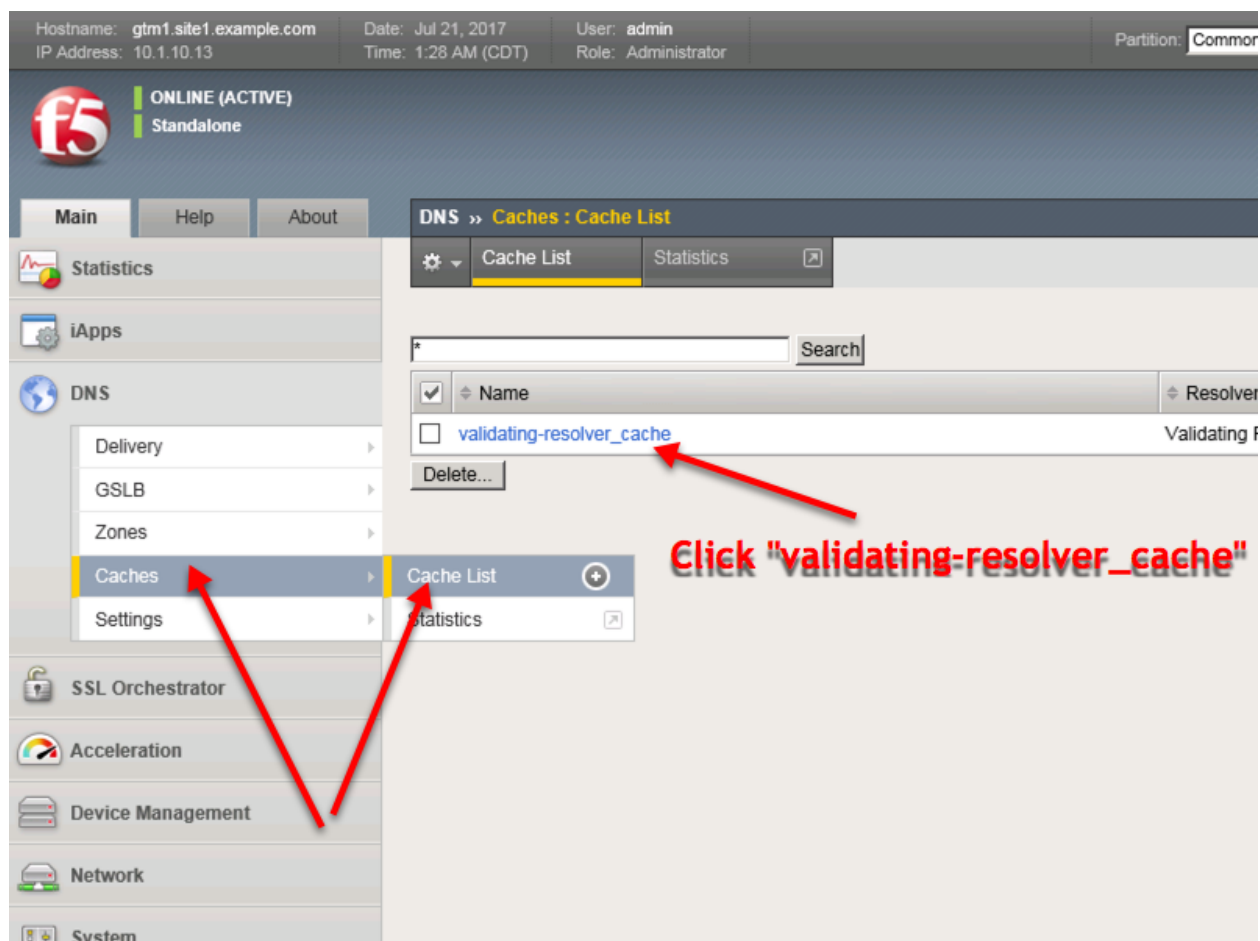
```
dig dnskey . | grep 257 > /root/dnskey.txt
```

```
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 #
[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 #
```

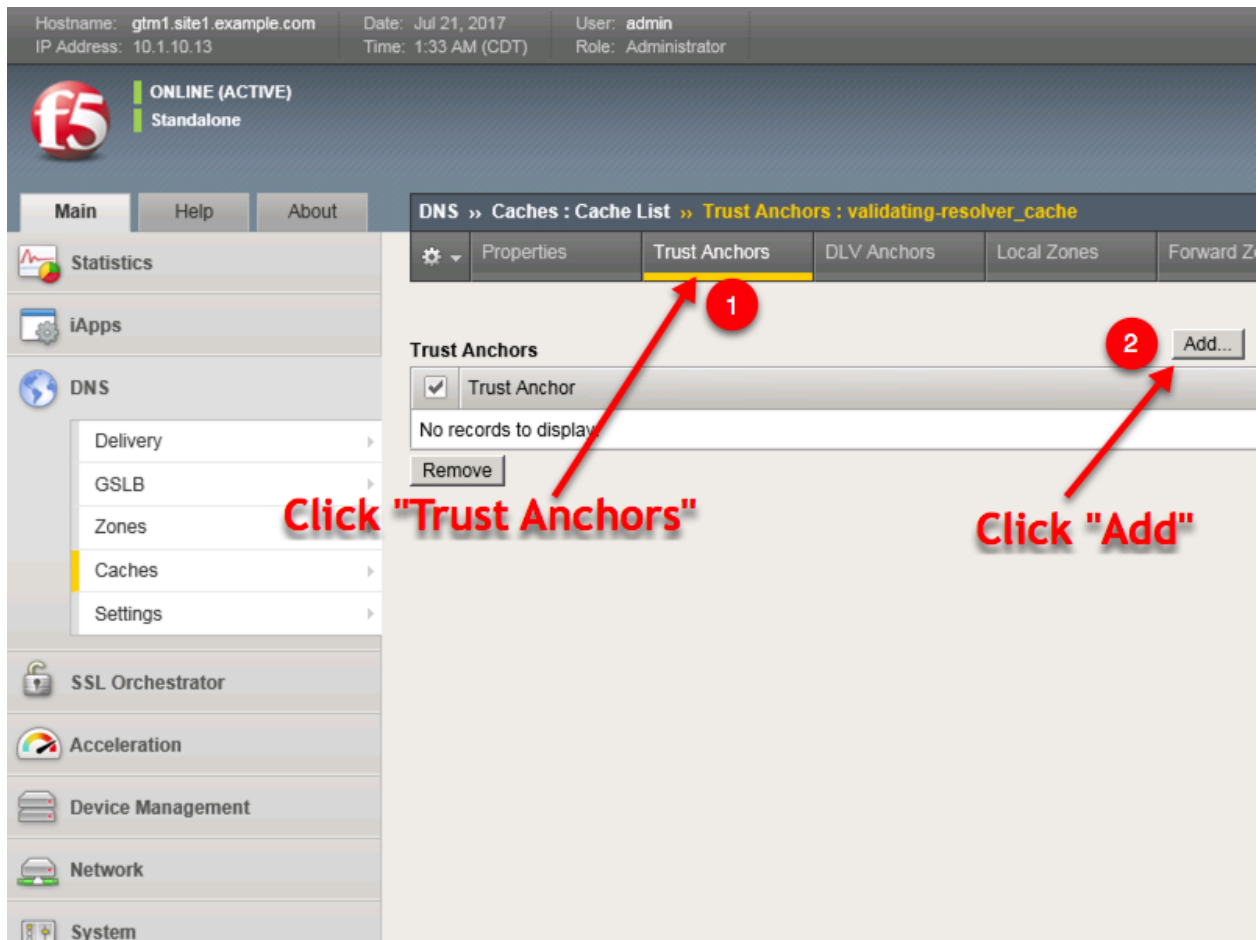
Navigate to: **DNS » Caches : Cache List » validating-resolver_cache : Trust Anchors**

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"

DNS » Caches : Cache List

Add Trust Anchor

Trust Anchor

. IN DS 19036 8 1 B256BD09DC8DD59F0E0F0D8541B8328DD986DF6E

Cancel

Repeat

Finished

```

router01
[root@router01:Eval:Active:Standalone] config #
[root@router01:Eval:Active:Standalone] config #
[root@router01:Eval:Active:Standalone] config # tmsh create ltm virtual DC02_tcp_53_virt
210:domain ip-protocol tcp mask 255.255.255.255 profiles add { example.com_dns_profile {
rofile { } } translate-address disabled vlans add { branch01_vlan } vlans-enabled pool b
[root@router01:Eval:Active:Standalone] config #
[root@router01:Eval:Active:Standalone] config #
[root@router01:Eval:Active:Standalone] config # tmsh create ltm dns cache validating-res
r_cache answer-default-zones yes
[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.t
[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 # c

```

DNS » Caches : Cache List » Trust Anchors : validating-resolver_cache



Properties

Trust Anchors

DLV Anchors

Local Zones

Forward Zones

Response Policy Zones

Statistics

Trust Anchors

Add...

<input checked="" type="checkbox"/>	Trust Anchor
<input checked="" type="checkbox"/>	. IN DS 19036 8 1 B256BD09DC8DD59F0E0F0D8541B8328DD986DF6E
<input type="checkbox"/>	. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
<input type="checkbox"/>	. IN DS 20326 8 1 AE1EA5B974D4C858B740BD03E3CED7EBFCBD1724
<input type="checkbox"/>	. IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D

Remove

```

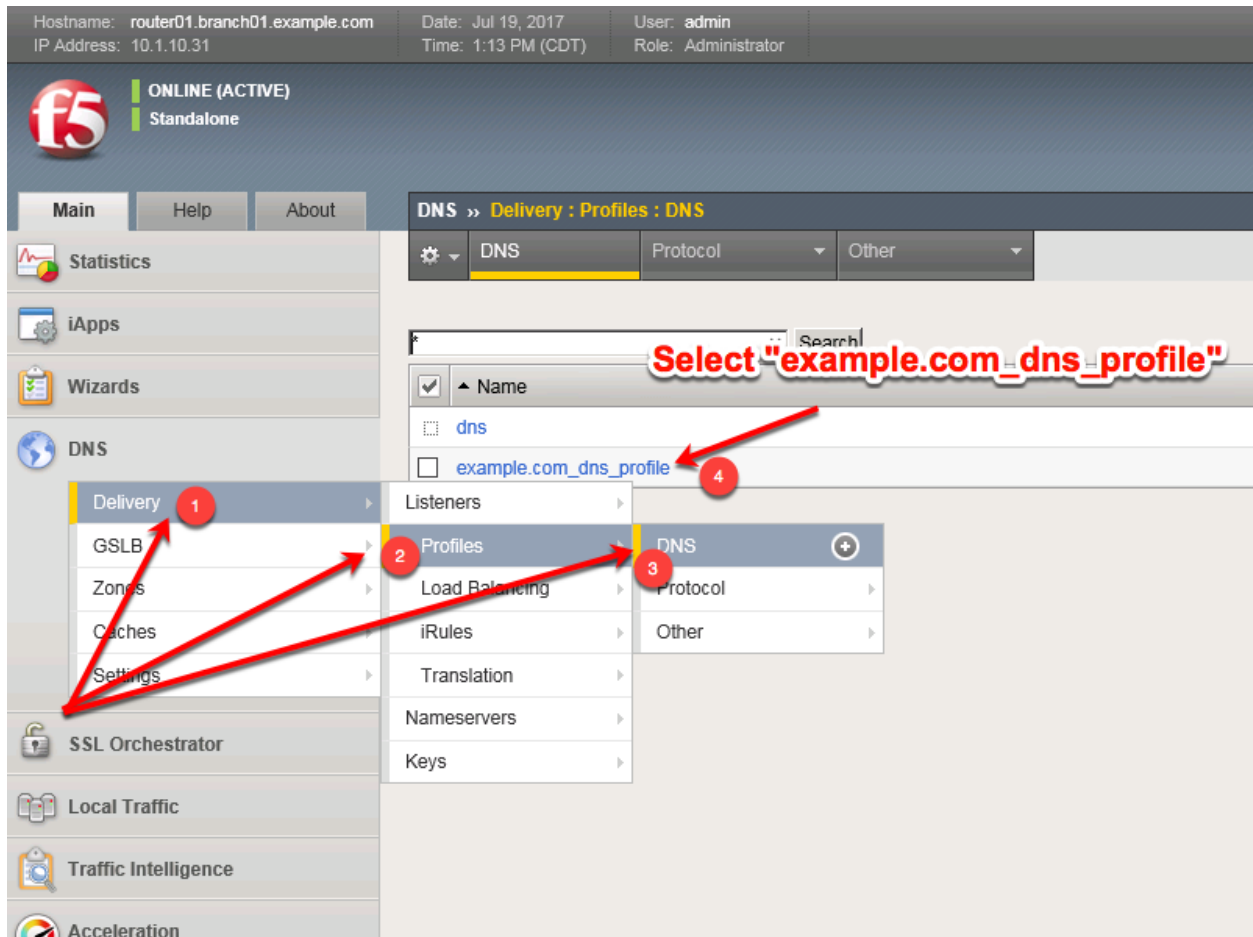
tmsh modify ltm dns cache validating-resolver validating-resolver_cache trust-anchors
→replace-all-with { ". IN DS 19036 8 1 B256BD09DC8DD59F0E0F0D8541B8328DD986DF6E" ".
→IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5" ".
→IN DS 20326 8 1 AE1EA5B974D4C858B740BD03E3CED7EBFCBD1724"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

```

3.5.2 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

MainHelpAbout

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	<div>dns</div>

Denial of Service Protection

Rapid Response Mode	<div>Disabled</div>
Rapid Response Last Action	<div>Drop</div>

Hardware Acceleration

Protocol Validation	<div>Disabled</div>
Response Cache	<div>Disabled</div>

DNS Features

DNSSEC	<div>Enabled</div>
GSLB	<div>Enabled</div>
DNS Express	<div>Enabled</div>
DNS Cache	<div>Enabled</div>
DNS Cache Name	<div>validating-resolver_cache</div>
DNS IPv6 to IPv4	<div>Disabled</div>
Unhandled Query Actions	<div>Allow</div>
Use BIND Server on BIG-IP	<div>Disabled</div>

DNS Traffic

Zone Transfer	<div>Disabled</div>
DNS Security	<div>Disabled</div>
DNS Security Profile Name	<div>Select...</div>
Process Recursion Desired	<div>Enabled</div>

Logging and Reporting

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

Select the "validating-resolver_cache"

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

TMSH

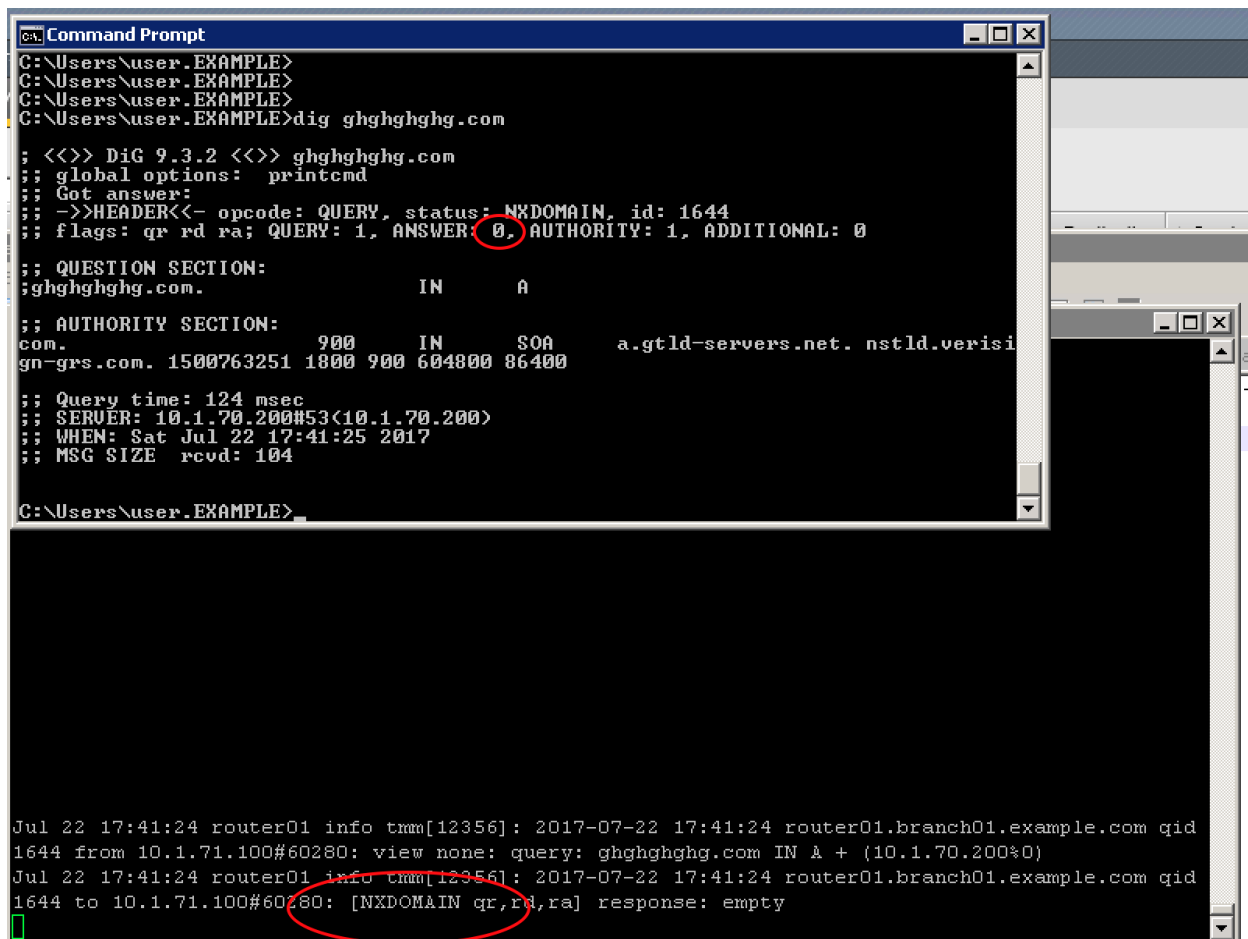
tms modify ltm profile dns example.com_dns_profile cache validating-resolver_cache

3.5.3 Results

From the CLI on the router01.branch01 BIGIP run

tail -f /var/log/ltm

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



```
Command Prompt
C:\Users\user.EXAMPLE>
C:\Users\user.EXAMPLE>
C:\Users\user.EXAMPLE>
C:\Users\user.EXAMPLE>dig ghghghghg.com
; <<>> DiG 9.3.2 <<>> ghghghghg.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 1644
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;ghghghghg.com.                IN      A
;; AUTHORITY SECTION:
com.                900      IN      SOA      a.gtld-servers.net. nstld.verisi
gn-grs.com. 1500763251 1800 900 604800 86400
;; Query time: 124 msec
;; SERVER: 10.1.70.200#53(10.1.70.200)
;; WHEN: Sat Jul 22 17:41:25 2017
;; MSG SIZE rcvd: 104

C:\Users\user.EXAMPLE>

Jul 22 17:41:24 router01 info tmm[12356]: 2017-07-22 17:41:24 router01.branch01.example.com qid
1644 from 10.1.71.100#60280: view none: query: ghghghghg.com IN A + (10.1.70.200%0)
Jul 22 17:41:24 router01 info tmm[12356]: 2017-07-22 17:41:24 router01.branch01.example.com qid
1644 to 10.1.71.100#60280: [NXDOMAIN qr,rd,ra] response: empty
```

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

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

; <<>> DiG 9.3.2 <<>> google.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 448
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                 300     IN      A      216.58.218.238

;; Query time: 77 msec
;; SERVER: 10.1.70.200#53(10.1.70.200)
;; WHEN: Sat Jul 22 17:39:11 2017
;; MSG SIZE rcvd: 44

C:\Users\user.EXAMPLE>

Jul 22 17:39:10 router01 info tmm[12356]: 2017-07-22 17:39:09 router01.branch01.example.com qid
0.1.71.100#49573: view none: query: google.com IN A + (10.1.70.200%0)
Jul 22 17:39:10 router01 info tmm[12356]: 2017-07-22 17:39:10 router01.branch01.example.com qid
1.71.100#49573: [NOERROR qr,rd,ra] response: google.com. 300 IN A 216.58.218.238;
```

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

```
Command Prompt
C:\Users\user.EXAMPLE>dig dnssec-deployment.org +dnssec

; <<>> DiG 9.3.2 <<>> dnssec-deployment.org +dnssec
;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 1568
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 1

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

;; ANSWER SECTION:
dnssec-deployment.org.  294     IN      A      46.43.37.10
dnssec-deployment.org.  294     IN      RRSIG   A 5 2 300 20170801204001 20170718204001 36518 dnssec-deployment.org. fceSC4irvKmA0c+39rYtx+tWzp9cPb6I/MRveG9gvnwNKKGNFXuJwU1+eBsy6NRNW184maIW7vY0bmWJkqsET2okUCcEP00/BzY/RFPHmzBsG5N Bxhg+0LeiMUYp/gHiDX0tGQVMvMgn6Z3oeqD4Vt6FJECLuyGED0cRYNB yBc=

;; AUTHORITY SECTION:
dnssec-deployment.org.  294     IN      NS      ns1.sea1.afiliast.net.
dnssec-deployment.org.  294     IN      NS      ns1.mia1.afiliast.net.
dnssec-deployment.org.  294     IN      NS      ns1.yyz1.afiliast.net.
dnssec-deployment.org.  294     IN      NS      ns1.hkg1.afiliast.net.
dnssec-deployment.org.  294     IN      NS      ns1.ams1.afiliast.net.
dnssec-deployment.org.  294     IN      RRSIG   NS 5 2 300 20170801204001 20170718204001 36518 dnssec-deployment.org. Jr13JdhS8T+Sckm+ZRpweEMywc1h0LM6T/5032dwp5

Jul 19 13:07:46 router01 info tmm[12513]: 2017-07-19 13:07:45 router01.branch01.example.com qid 1568 from 10.1.71.100#65485: view none: query: dnssec-deployment.org IN A + (10.1.70.200%0)
Jul 19 13:07:46 router01 info tmm[12513]: 2017-07-19 13:07:45 router01.branch01.example.com qid 1568 to 10.1.71.100#65485: [NOERROR qr,rd,ra] response: dnssec-deployment.org. 300 IN A 46.43.37.10;
Jul 19 13:07:52 router01 info tmm[12513]: 2017-07-19 13:07:52 router01.branch01.example.com qid 1568 from 10.1.71.100#65486: view none: query: dnssec-deployment.org IN A +ED (10.1.70.200%0)
Jul 19 13:07:52 router01 info tmm[12513]: 2017-07-19 13:07:52 router01.branch01.example.com qid 1568 to 10.1.71.100#65486: [NOERROR qr,rd,ra,ad] response: dnssec-deployment.org. 294 IN A 46.43.37.10; dnssec-deployment.org. 294 IN RRSIG A 5 2 300 20170801204001 20170718204001 36518 dnssec-deployment.org fceSC4irvKmA0c+39rYtx+tWzp9cPb6I/MRveG9gvnwNKKGNFXuJwU1+eBsy6NRNW184maIW7vY0bmWJkqsET2okUCcEP00/BzY/RFPHmzBsG5NBxhg+0LeiMUYp/gHiDX0tGQVMvMgn6Z3oeqD4Vt6FJECLuyGED0cRYNB yBc=;
```

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

```
C:\Users\user.EXAMPLE>dig dnssec-failed.org +dnssec
; <<>> DiG 9.3.2 <<>> dnssec-failed.org +dnssec
;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: SERVFAIL, id: 635
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;dnssec-failed.org.          IN      A

;; Query time: 15 msec
;; SERVER: 10.1.70.200#53(10.1.70.200)
;; WHEN: Thu Jul 20 11:49:38 2017
;; MSG SIZE rcvd: 35

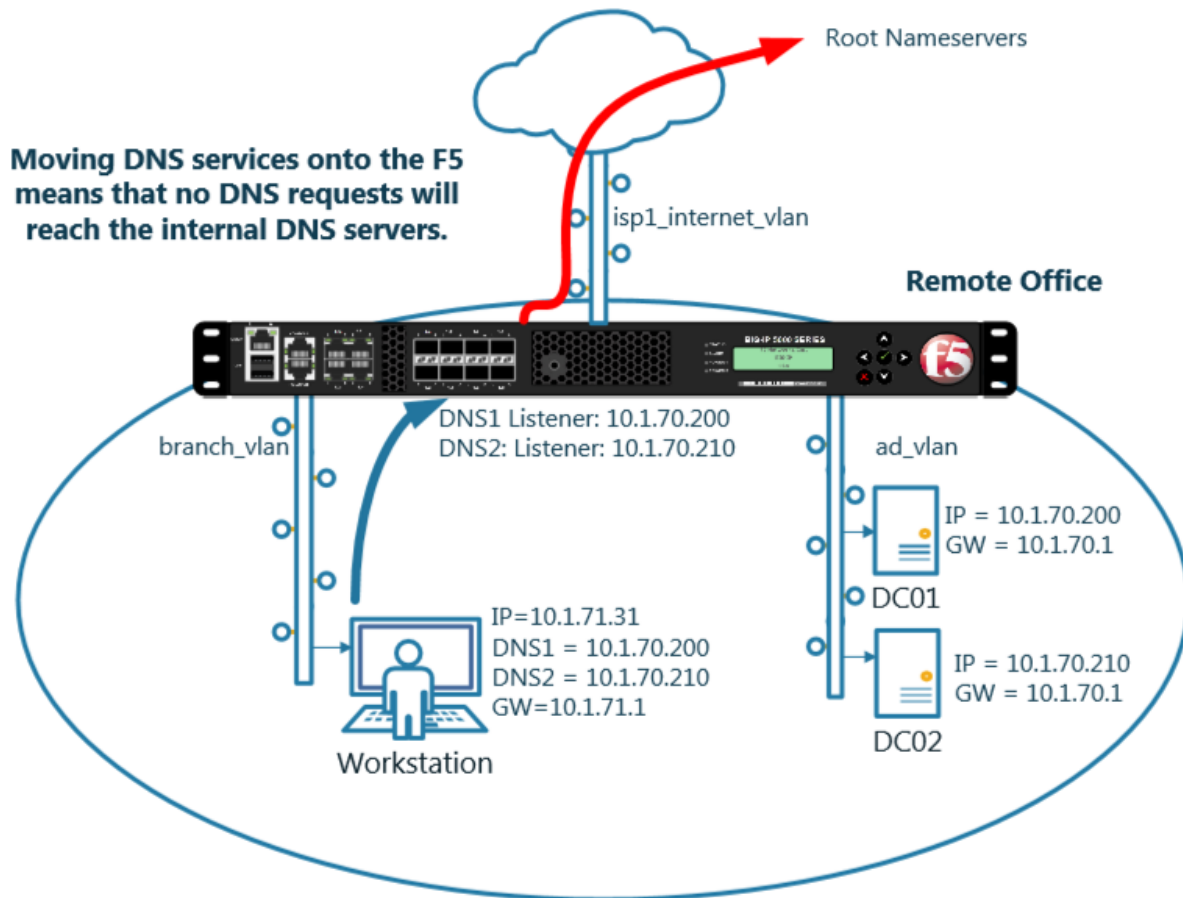
C:\Users\user.EXAMPLE>

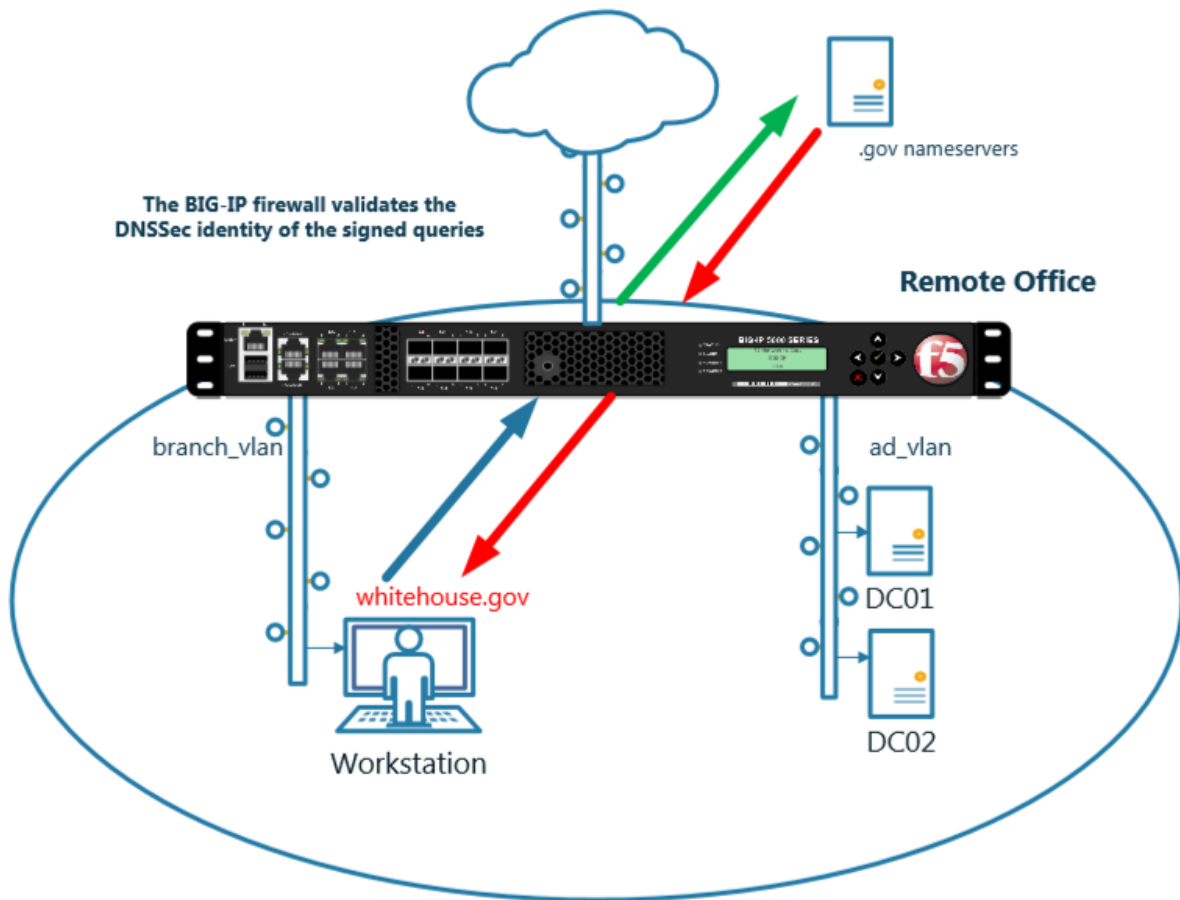
Jul 20 11:49:38 router01 info tmm[12352]: 2017-07-20 11:49:38 router01.branch01.example.com qid 63
5 from 10.1.71.100#61266: view none: query: dnssec-failed.org IN A +ED (10.1.70.200%0)
Jul 20 11:49:38 router01 info tmm[12352]: 2017-07-20 11:49:38 router01.branch01.example.com qid 63
5 to 10.1.71.100#61266: [SERVFAIL qr,rd,ra] response: empty
```

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

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

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





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

General Properties

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

DNS Cache

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

DNS Resolver

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

140

DNSSEC Validator

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

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

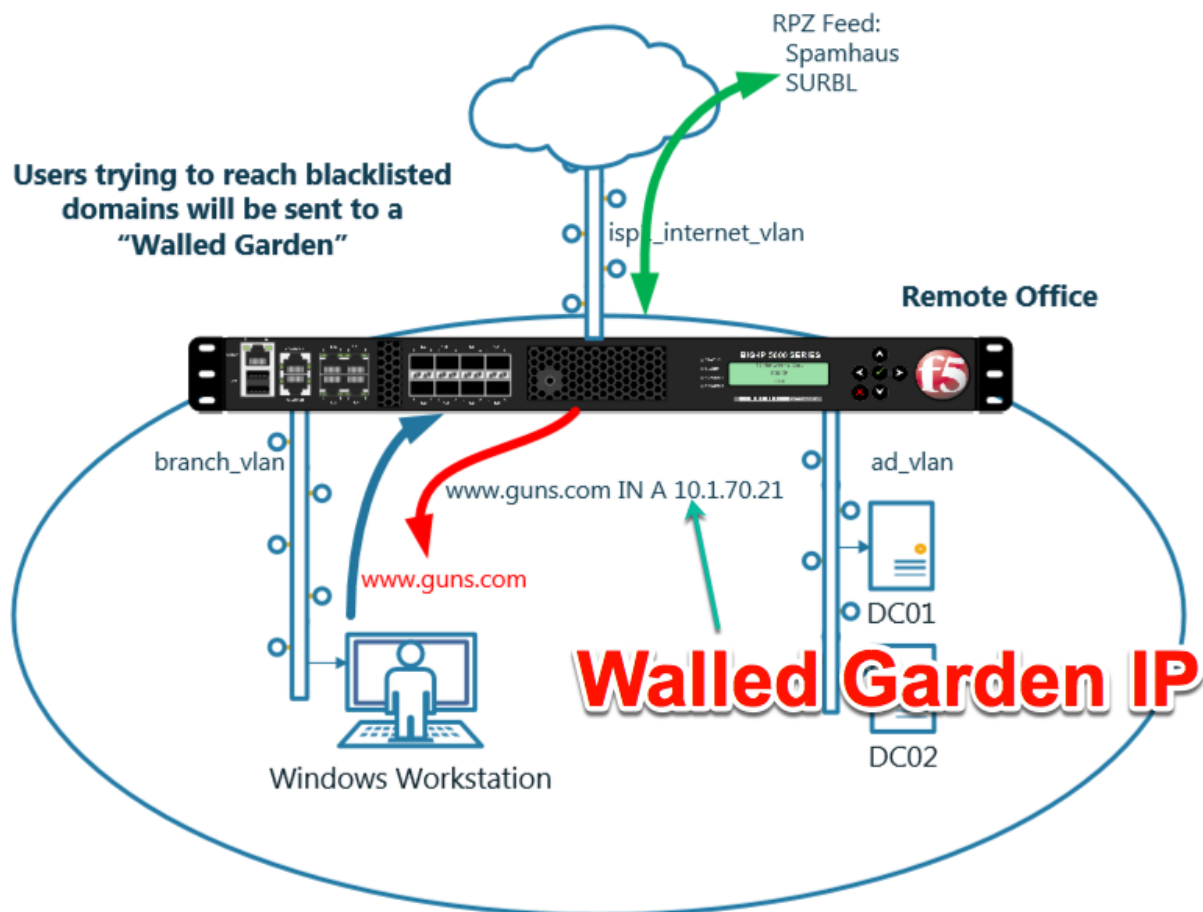
TMSH

```
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>

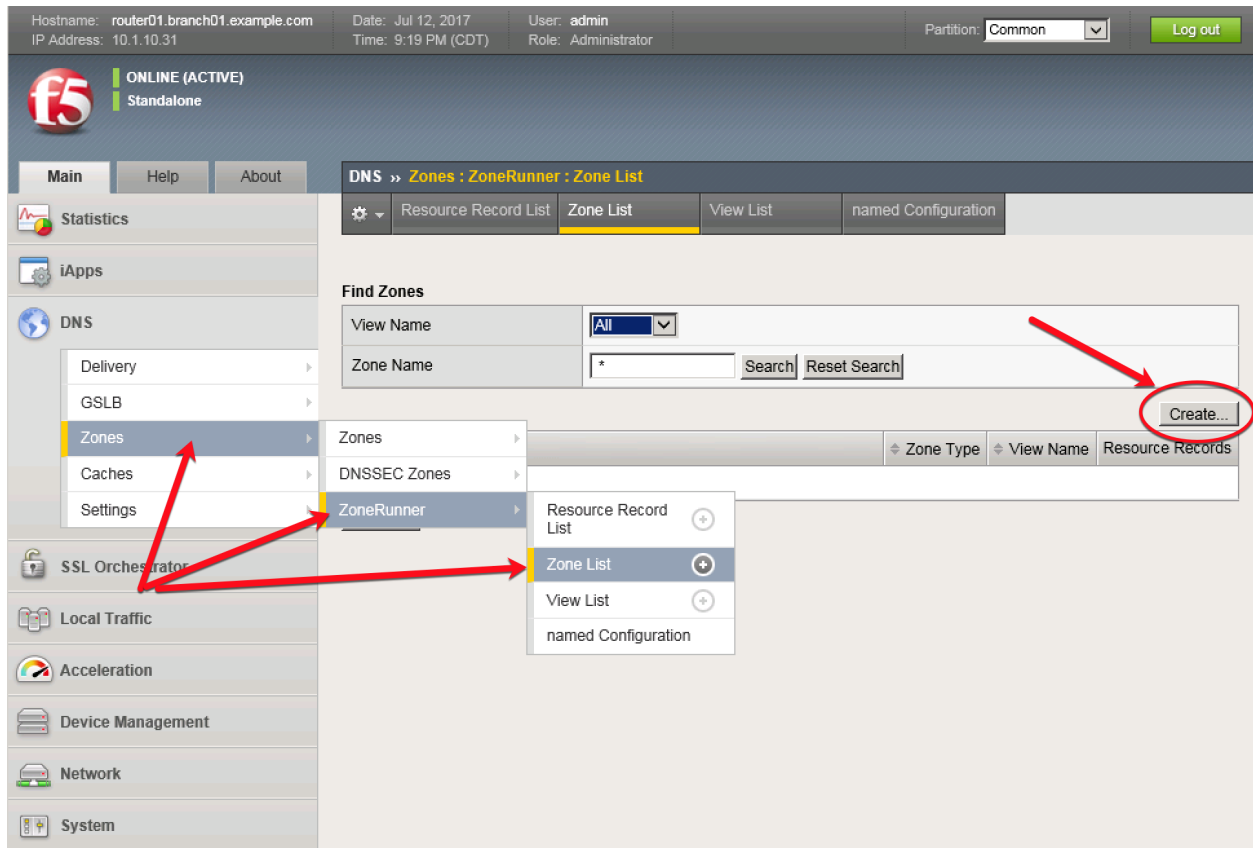
3.6.1 Zone Runner

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

General Properties

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

Configuration

Records Creation Method	Manual
Zone File Name	db.external.rpz.example.com
Options	<pre>allow-update { localhost; }; also-notify { ::1 port 5353; };</pre>
Create Reverse Zone	<input type="checkbox"/> Enable

Records Creation

SOA Record	TTL	300
	Master Server	router01.branch01.example.com.
	Email Contact	hostmaster.example.com.
	Serial Number	2017071801
	Refresh Interval	10800 Seconds
	Retry Interval	3600 Seconds
	Expire	604800 Seconds
	Negative TTL	86400 Seconds
NS Record	TTL	300
	Nameserver	router01.branch01.example.com.
Create A Record	<input checked="" type="checkbox"/> Enable	
A Record	IP Address	10.1.71.1

No dot at the end

Dots at the end

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

<https://router01.branch01.example.com/tmui/Control/jspmap/tmui/globalb/zfd/record/create.jsp>

Record Configuration

View Name	external ▾
Zone Name	rpz.example.com. ▾
Name	*.guns.com.rpz.example.com.
TTL	300
Type	CNAME ▾ ←
CNAME	. ← Period

Hostname: router01.branch01.example.com Date: Jul 18, 2017 User: admin
IP Address: 10.1.10.31 Time: 11:29 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About

DNS » Zones : ZoneRunner : Resource Record List

⚙️ Resource Record List Zone List View List named Configuration

Find Records

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

Search Reset Search Create

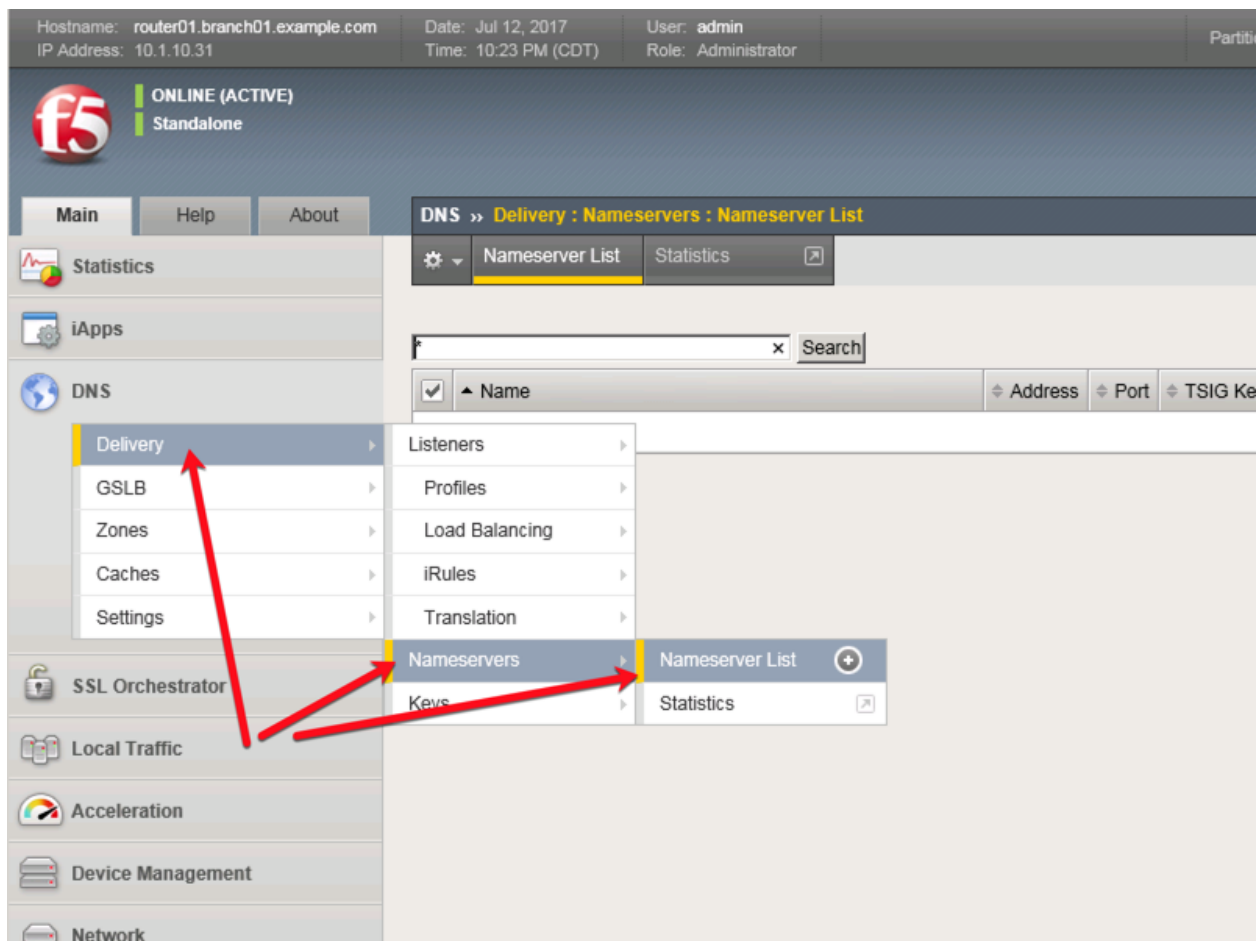
Click "Search"

<input checked="" type="checkbox"/>	Name	View Name	Zone Name	
<input type="checkbox"/>	*.guns.com.rpz.example.com.	external	rpz.example.com.	30
<input type="checkbox"/>	rpz.example.com.	external	rpz.example.com.	30
<input type="checkbox"/>	rpz.example.com.	external	rpz.example.com.	30

Delete...

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

Hostname: router01.branch01.example.com Date: Jul 18, 2017 User: admin
 IP Address: 10.1.10.31 Time: 11:33 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About **DNS » Delivery : Nameservers : Nameserver List » New Nameserver...**

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

General Properties

Name	localhost	
Address	127.0.0.1	
Service Port	53	Other: <input type="text"/>

Configuration

Route Domain	0
TSIG Key	None

Cancel Repeat Finished

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

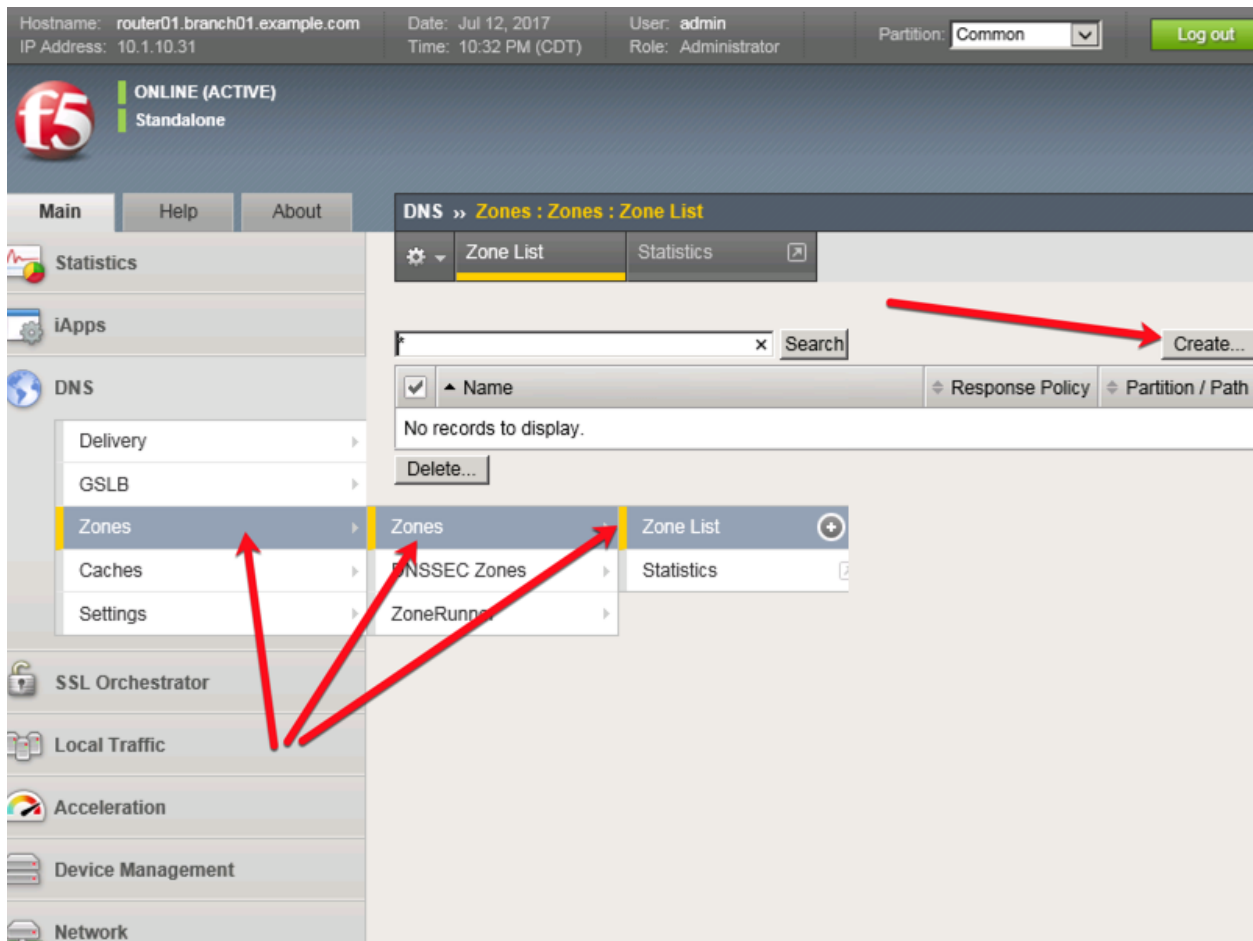
TMSH

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

3.6.3 DNS Express

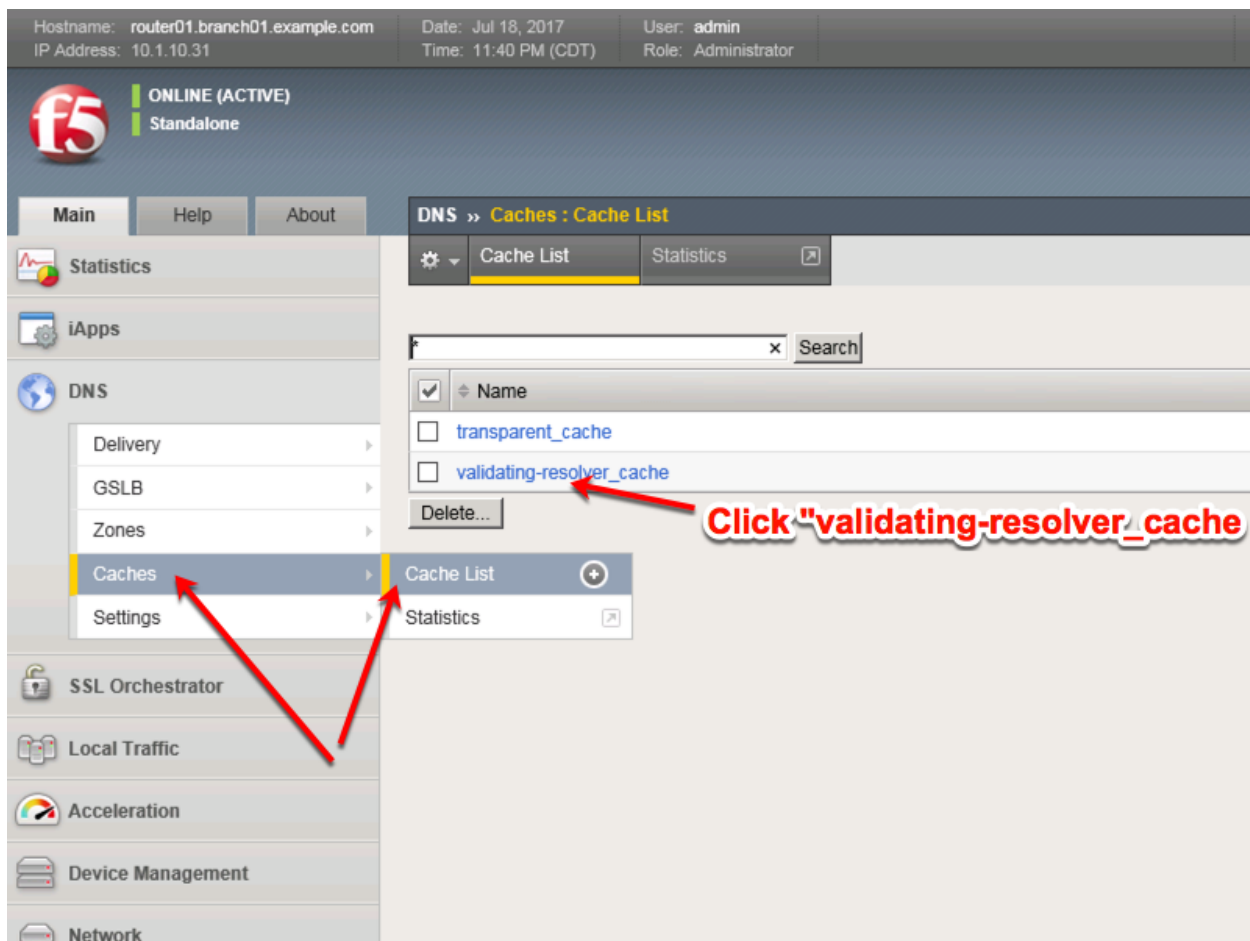
Navigate to **DNS » Zones : Zones : Zone List**

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



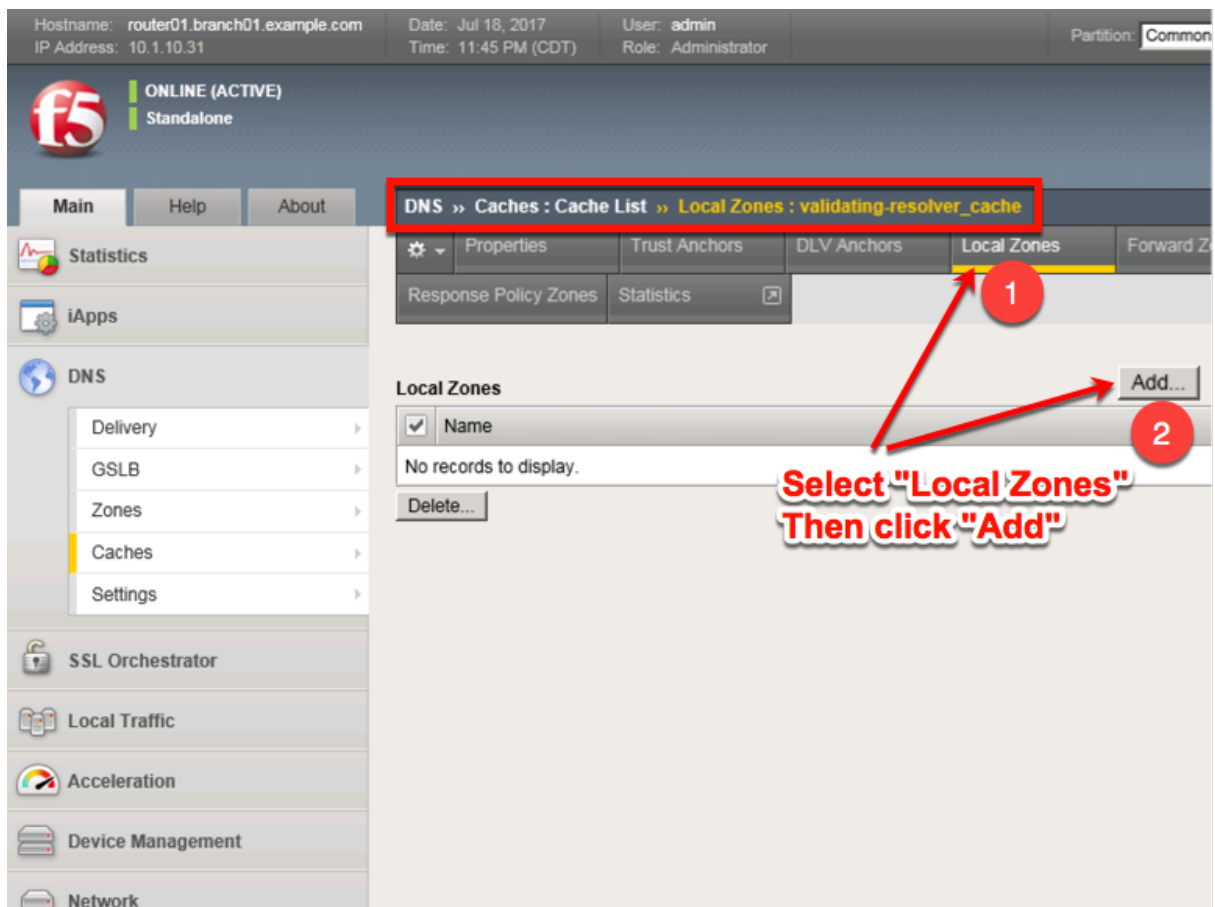
Create a DNS Express zone according to the following table:

Setting	Value
Name	rpz.example.com
Server	localhost
Allow NOTIFY From	127.0.0.1
Response Policy	checked



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

Local Zone

Name **No "dot" at the end !!**

Type

Records **There is a "dot" at the end !!**

TMSH commands for router01.branch01:

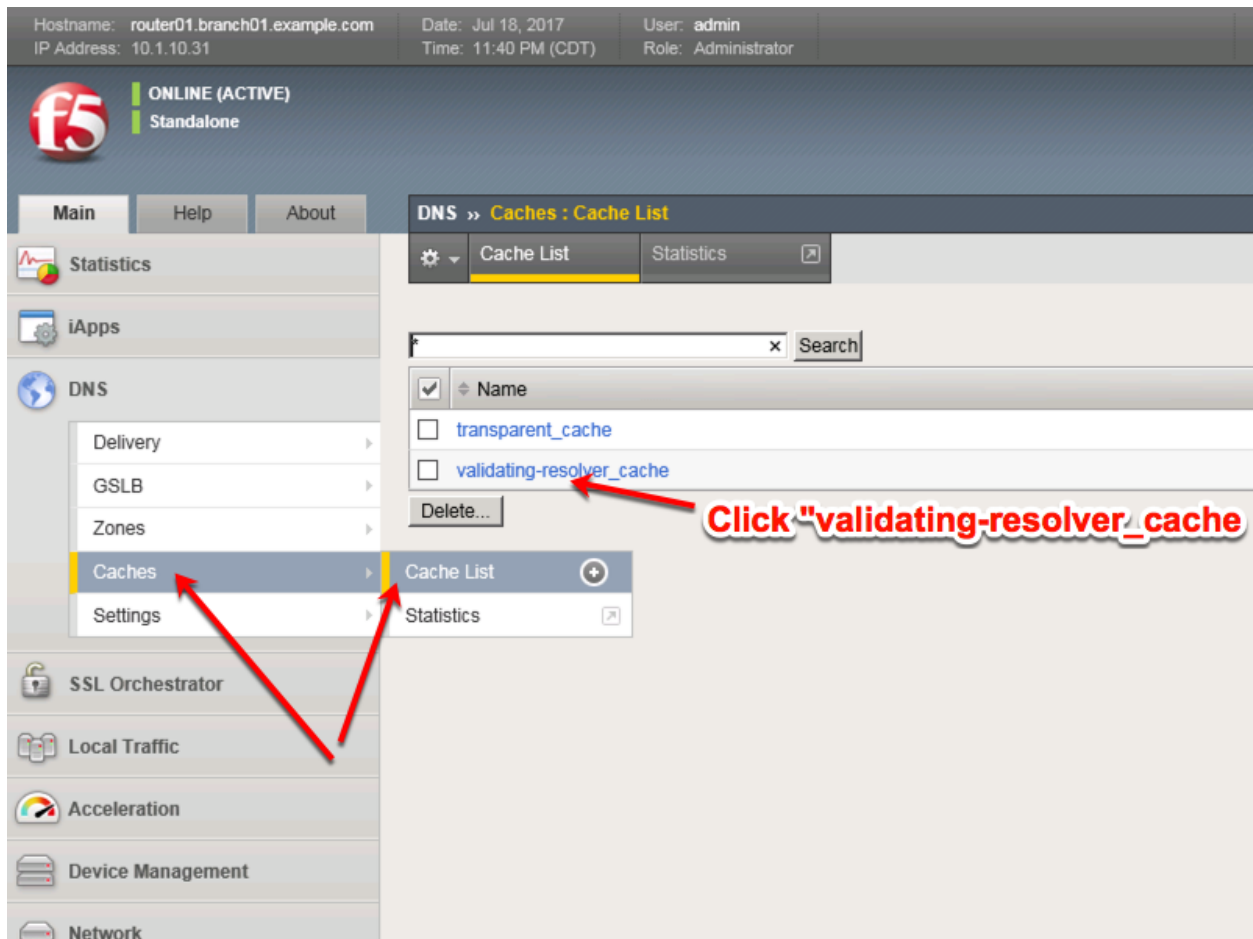
```
tmsl modify ltm dns cache validating-resolver validating-resolver_cache local-zones {
  { name sorry.example.com records add { "sorry.example.com. IN A 10.1.71.21" } type
  static } }
```

3.6.5 Walled Garden

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

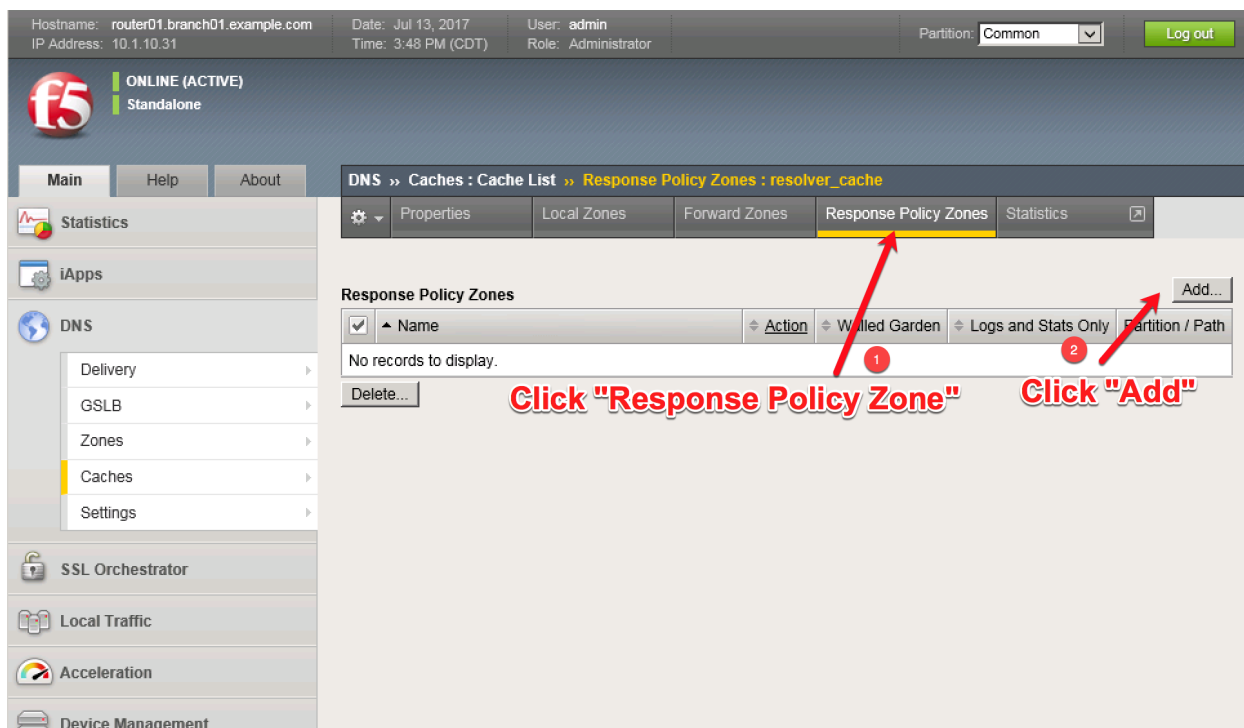
<https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/list.jsp>

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

Response Policy Zone

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

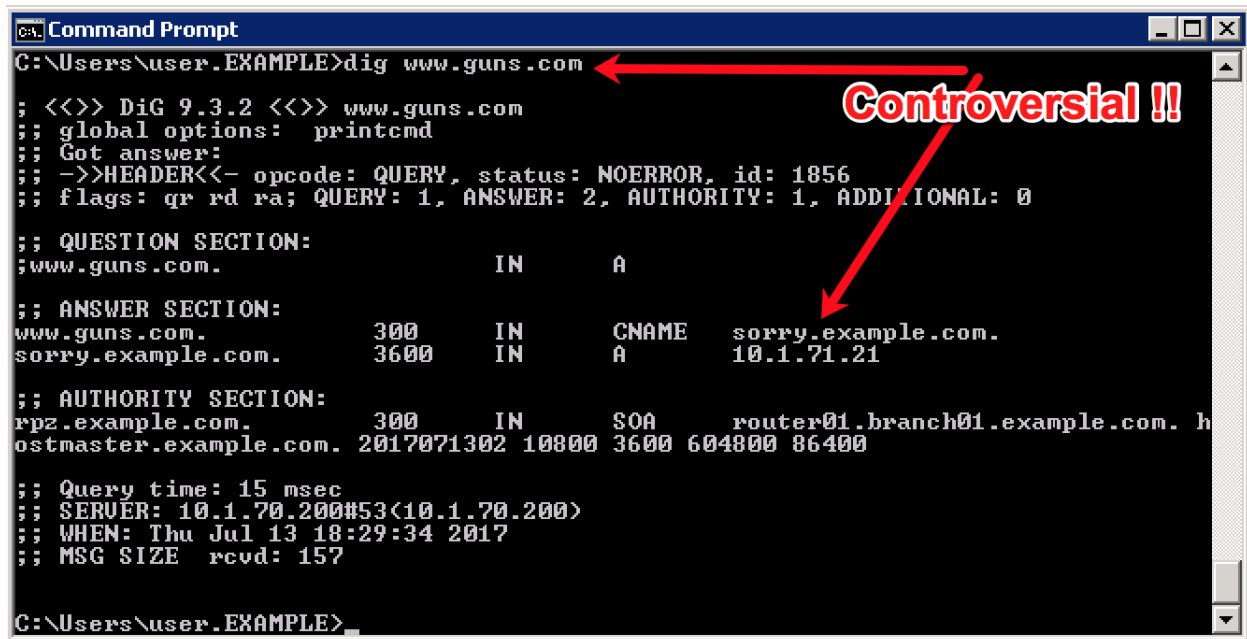
TMSH commands for router01.branch01:

TMSH

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

3.6.6 Results

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



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

;; <<>> DiG 9.3.2 <<>> www.guns.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1856
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.guns.com.                 300     IN      CNAME   sorry.example.com.
sorry.example.com.           3600    IN      A       10.1.71.21

;; AUTHORITY SECTION:
rpz.example.com.             300     IN      SOA     router01.branch01.example.com. h
ostmaster.example.com. 2017071302 10800 3600 604800 86400

;; Query time: 15 msec
;; SERVER: 10.1.70.200#53(10.1.70.200)
;; WHEN: Thu Jul 13 18:29:34 2017
;; MSG SIZE rcvd: 157

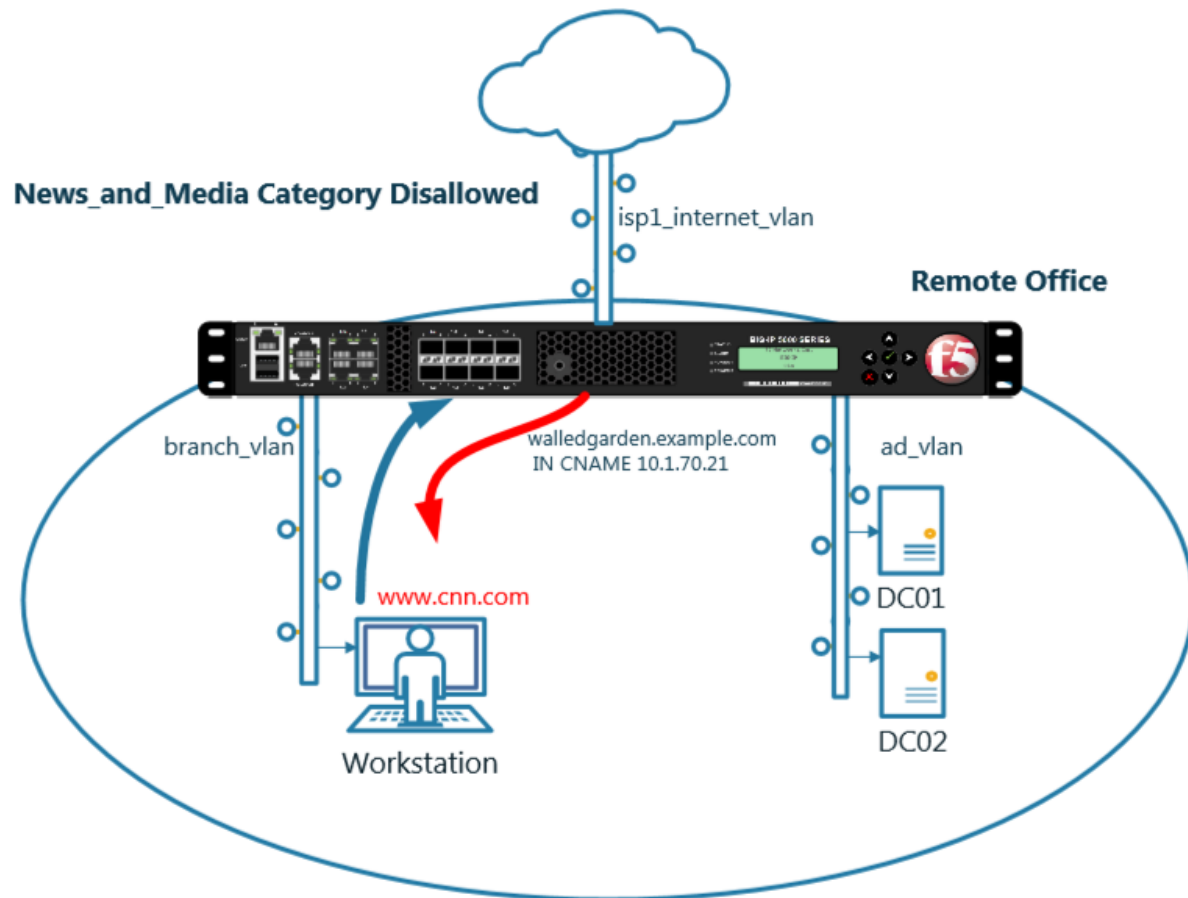
C:\Users\user.EXAMPLE>
```

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**


```

# 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

Repeat the following steps for all 4 DNS listeners.

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

DNS » Delivery : Listeners : Listener List » Properties : DC01_udp_virtual

General

Name	DC01_udp_virtual
Partition	Common
Description	
State	Enabled

Listener:

Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.1.70.200
Service Port	DNS <input type="button" value="53"/>
VLAN Traffic	Enabled on... <input type="button"/>
VLANs and Tunnels	<div> <div>Selected</div> <div>Available</div> </div> <div> <div>/Common branch01_vlan</div> <div><< >></div> <div>/Common AD_vlan external_vlan http-tunnel isp1_site1_vlan</div> </div>
Source Address Translation	None
Address Translation	<input type="checkbox"/> Enabled
Port Translation	<input type="checkbox"/> Enabled
Route Advertisement	<input type="checkbox"/> Enabled

Navigate to Manage

DNS » Delivery : Listeners : Listener List » iRules : DC01_udp_virtual

Statistics

Statistics Profile: None

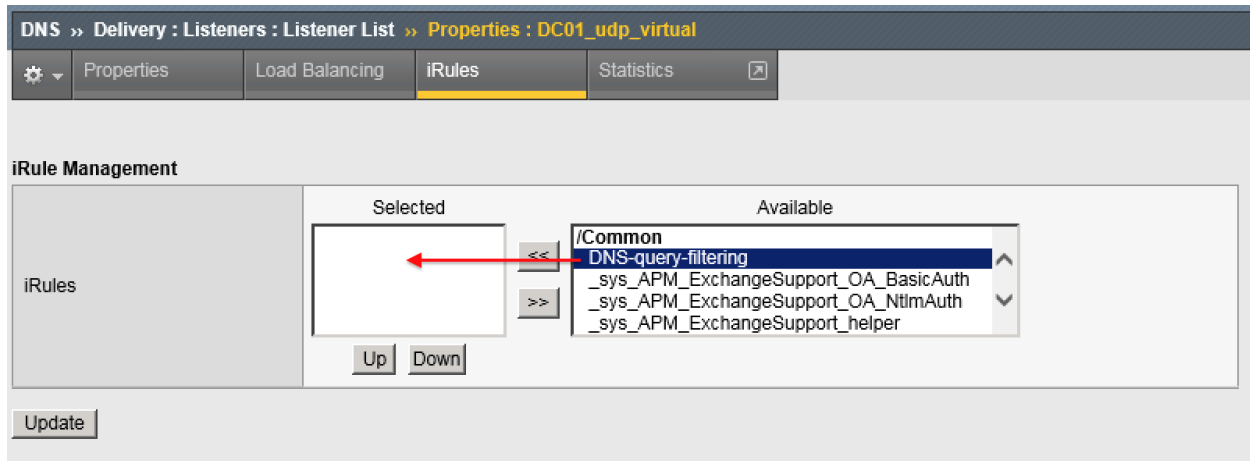
iRules

Name

No records to display.

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

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



TMSH commands for router01.branch01

TMSH

```
tmsh modify gtm listener all 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

```
Command Prompt
; <<>> DiG 9.3.2 <<>> example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 116
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; QUESTION SECTION:
;example.com.                IN      A
;; ANSWER SECTION:
example.com.                600     IN      A      10.1.70.200
;; AUTHORITY SECTION:
example.com.                3600    IN      NS      dc01.example.com.
;; ADDITIONAL SECTION:
dc01.example.com.          3600    IN      A      10.1.70.200
;; Query time: 31 msec
;; SERVER: 10.1.70.200#53(10.1.70.200)
;; WHEN: Tue Jul 18 22:06:35 2017
;; MSG SIZE rcvd: 80
C:\Users\user.EXAMPLE>

Jul 18 22:06:35 router01 info tmm[11519]: 2017-07-18 22:06:34 router01.branch01.example.com
qid 116 from 10.1.71.100#49954: view none: query: example.com IN A + (10.1.70.200%0)
Jul 18 22:06:35 router01 info tmm3[11519]: Rule /Common/DNS-querv-filtering <DNS_REQUEST>: C
ategory /Common/Information_Technology matching example.com is not filtered
Jul 18 22:06:35 router01 info tmm[11519]: 2017-07-18 22:06:34 router01.branch01.example.com
qid 116 to 10.1.71.100#49954: [NOERROR qr,aa,rd] response: example.com. 600 IN A 10.1.70.200
;
[ ]

[Update] [Delete]
```

From the Workstation command prompt run “dig porno.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 porno.com

; <<>> DiG 9.3.2 <<>> porno.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2037
;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;porno.com.                IN      A

;; ANSWER SECTION:
porno.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 22:09:13 2017
;; MSG SIZE rcvd: 43

C:\Users\user.EXAMPLE>

Jul 18 22:09:12 router01 info tmm[11519]: 2017-07-18 22:09:12 router01.branch01.example.com
qid 2037 from 10.1.71.100#49955: view none: query: porno.com IN A + (10.1.70.200%)
Jul 18 22:09:12 router01 info tmm2[11519]: Rule /Common/DNS-query-filtering <DNS_REQUEST>: B
LOCKED Category /Common/Sex matching porno.com is filtered.
Jul 18 22:09:12 router01 info tmm[11519]: 2017-07-18 22:09:12 router01.branch01.example.com
qid 2037 to 10.1.71.100#49955: [NOERROR qr,rd] response: porno.com. 111 IN A 10.1.71.21;
```

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

Hostname: router01.branch01.example.com Date: Jul 19, 2017 User: admin
 IP Address: 10.1.10.31 Time: 8:30 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
 Standalone

Main Help About

Statistics

iApps

DNS

Delivery

GSLB

Zones

Caches

Settings

SSL Orchestrator

Local Traffic

Acceleration

Device Management

Network

DNS » Delivery : iRules : iRule List

iRule List Data Group List iFile List Statistics

Search

Name	Verification
Listeners	None
Profiles	
Load Balancing	
iRules	
Translation	
Nameservers	
Keys	
Support_OA_BasicAuth	F5 Verified
Support_OA_NtlmAuth	F5 Verified
Support_helios	F5 Verified
	F5 Verified
Data Group List	F5 Verified
iFile List	F5 Verified
Statistics	F5 Verified
_sys_auth_ldap	F5 Verified
_sys_auth_radius	F5 Verified
_sys_auth_ssl_cc_ldap	F5 Verified
_sys_auth_ssl_crlap	F5 Verified
_sys_auth_ssl_ocsp	F5 Verified

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

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

DNS » Delivery : iRules : iRule List » Properties : DNS-query-filtering

⚙️ Properties 📊 Statistics

Properties

Name	DNS-query-filtering
Partition / Path	Common
Definition	<pre> 1 when RULE_INIT { 2 # Set categories to block for DNS hosts 3 set static::blocked_categories { 4 /Common/Bot_Networks 5 /Common/Spyware 6 /Common/Malicious_Web_Sites 7 /Common/Adult_Content 8 /Common/Sex 9 /Common/News_and_Media 10 } 11 12 13 # CONFIGURATION 14 # Check all requests by default 15 set static::request_check 1 16 # If the category returns as blocked, return NXDOMAIN (1) 17 # Otherwise if (0), return a statically defined IP address 18 set static::request_return_nxdomain 0 19 set static::request_redirect_to "10.1.71.21" 20 # Toggle for debug logs 21 set static::request_debug 1 22 } 23 24 25 when DNS_REQUEST { 26 if { \$static::request_check } { </pre>

☐ Wrap Text
☐ Show Print Margin

☐ Ignore Signature/Checksum

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%)
Jul 18 22:15:27 router01 info tmm[11519]: Rule /Common/DNS-query-filtering <DNS_REQUEST>: B
LOCKED: 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;
```


- Agility 2017:

Bill Wester

Boris Gekhtman

Brendan Gladney

Brian Buback

Emilio Torres

Dave Doucette

Josh Anderson

Robin Mordasiewicz

- Advisors:

Hitesh Patel

Joe Hermes

Jonathan Dehaan

Pat Chang

Pat Fiorino

Brian Van Lieu

WE MAKE APPS  FASTER.
SMARTER.
SAFER.

F5 Networks, Inc. | f5.com



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