
Reference Architecture Documentation

F5 Networks, Inc.

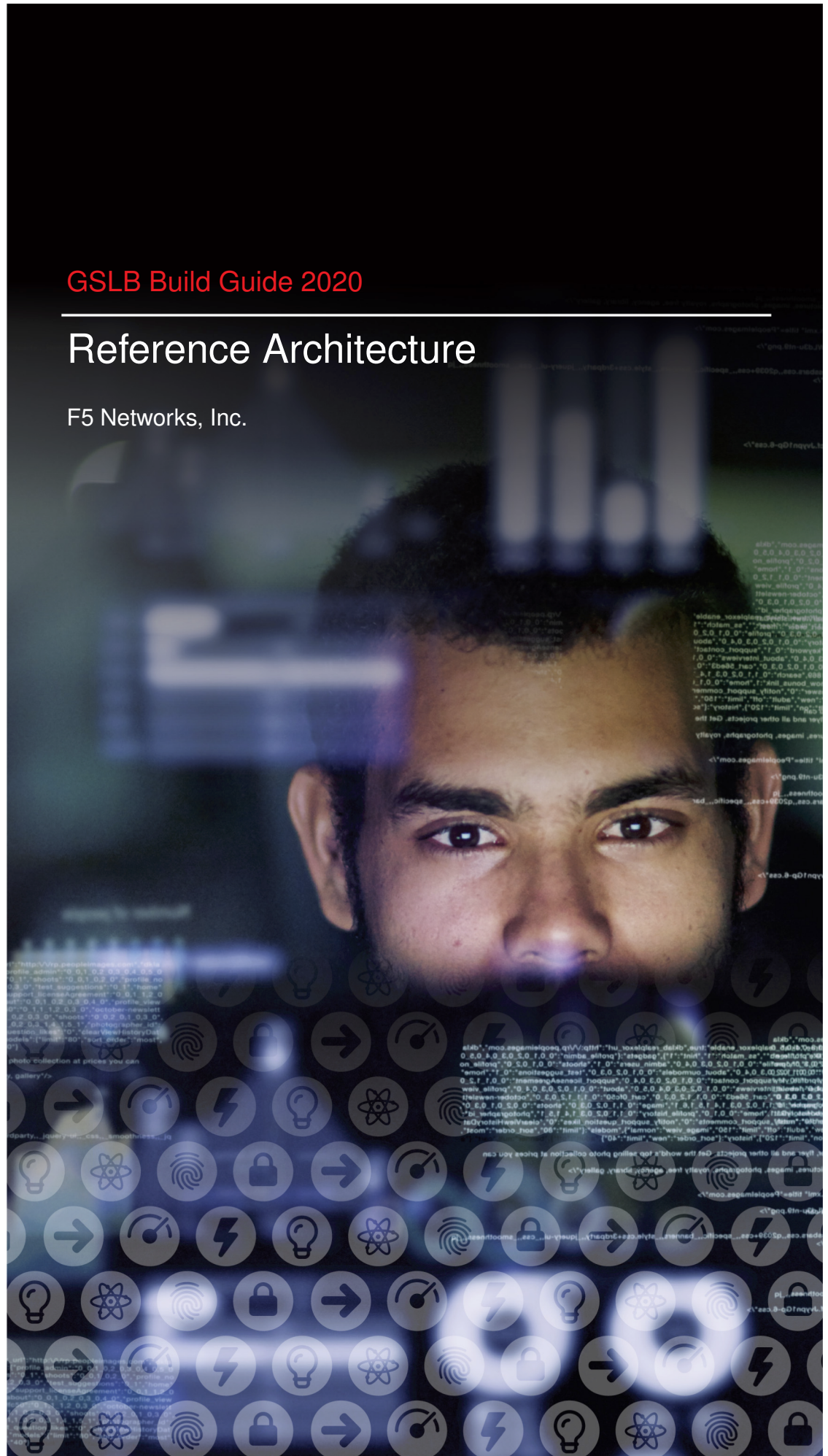
Mar 26, 2020



GSLB Build Guide 2020

Reference Architecture

F5 Networks, Inc.



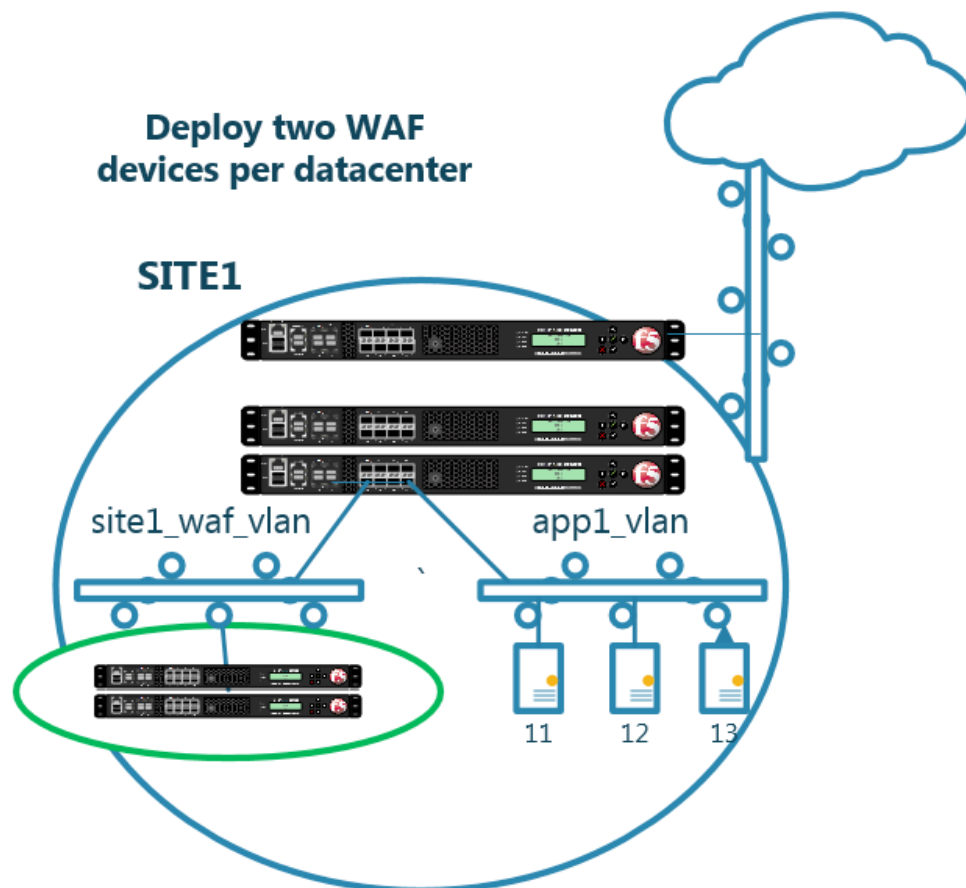
Contents

1	WAF	7
1.1	Onboarding	7
1.1.1	Networking	8
1.1.1.1	VLAN's	8
1.1.1.2	SELFIP's	12
1.1.1.3	Default Route	14
1.1.1.4	Results	17
1.1.2	Cluster	18
1.1.2.1	ConfigSync IP	19
1.1.2.2	Trust Members	21
1.1.2.3	Changes Pending	23
1.1.2.4	Device Groups	25
1.1.2.5	Sync... Again	27
1.1.3	Shared Objects	29
1.1.3.1	Sync Folder	29
1.1.3.2	HTTP Profile	31
1.1.3.3	TCP Profile	33
1.1.3.4	Health Monitor	35
1.1.3.5	Pools	37
1.1.4	Virtuals	40
1.1.5	Security Policy	43
1.1.5.1	Sync	43
1.1.5.2	Parent Child	44
1.1.5.3	Associate Policy	46
1.1.6	Cut-Over	48
1.2	Policy Tuning	51
1.3	Hack and Defend	51
2	DNS	53
2.1	Availability	53
2.1.1	Network Map	53
2.1.2	System	58
2.1.3	Settings	62
2.1.4	Listeners	63
2.1.4.1	DNS Profile	64

2.1.4.2	UDP Profile	66
2.1.4.3	TCP Profile	68
2.1.4.4	UDP IP Address	70
2.1.4.5	TCP IP Address	74
2.1.5	Data Centers	77
2.1.5.1	Servers	77
2.1.5.1.1	gtm1.SITE1	77
2.1.5.1.2	gtm1.SITE2	79
2.1.5.1.3	site1_ha-pair	84
2.1.5.1.4	site2_ha-pair	90
2.1.5.2	Device Trust	97
2.1.5.3	Sync Group	101
2.1.6	Pools	104
2.1.7	FQDN	106
2.1.8	Delegation	113
2.1.8.1	A Records	114
2.1.8.2	Sub Domain	118
2.1.8.3	CNAME	125
2.1.8.4	Results	128
2.1.9	Failure Condition	133
2.1.10	Rest API	137
2.1.10.1	Authenticate	137
2.1.10.2	POST	139
2.1.10.3	Results	139
2.1.10.4	Active/Standby	140
2.1.10.5	API Extras (Optional)	140
2.1.11	Congratulations	141
2.2	Security	142
2.2.1	Transparent Cache	143
2.2.1.1	Monitors	143
2.2.1.2	Load Balancing	146
2.2.1.3	Results	149
2.2.2	Listeners	155
2.2.2.1	Log Profile	156
2.2.2.2	DNS Profile	160
2.2.2.3	UDP Profile	163
2.2.2.4	TCP Profile	164
2.2.2.5	DNS Servers	166
2.2.2.6	UDP Listener	170
2.2.2.7	TCP Listeners	173
2.2.2.8	Results	176
2.2.3	Hidden Master	179
2.2.3.1	Name Server	179
2.2.3.2	DNS Express	181
2.2.3.3	Results	183
2.2.4	DNSSEC	185
2.2.4.1	Zone Signing Key	185
2.2.4.2	Key Signing Key	187
2.2.4.3	Signed Zone	189
2.2.4.4	Results	191
2.2.5	Validating Resolver	192
2.2.5.1	Trust Anchors	192
2.2.5.2	Modify DNS Profile	196
2.2.5.3	Results	198

2.2.6	RPZ	206
2.2.6.1	Zone Runner	206
2.2.6.2	Name Server	210
2.2.6.3	DNS Express	212
2.2.6.4	Local Zone	214
2.2.6.5	Walled Garden	217
2.2.6.6	Results	219
2.2.7	URL Categorization	219
2.2.7.1	Create an iRule	220
2.2.7.2	iRule assignment	222
2.2.7.3	Results	225
2.2.8	Title	230

1.1 Onboarding



Four dedicated WAF instances are deployed across two datacenters.

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

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

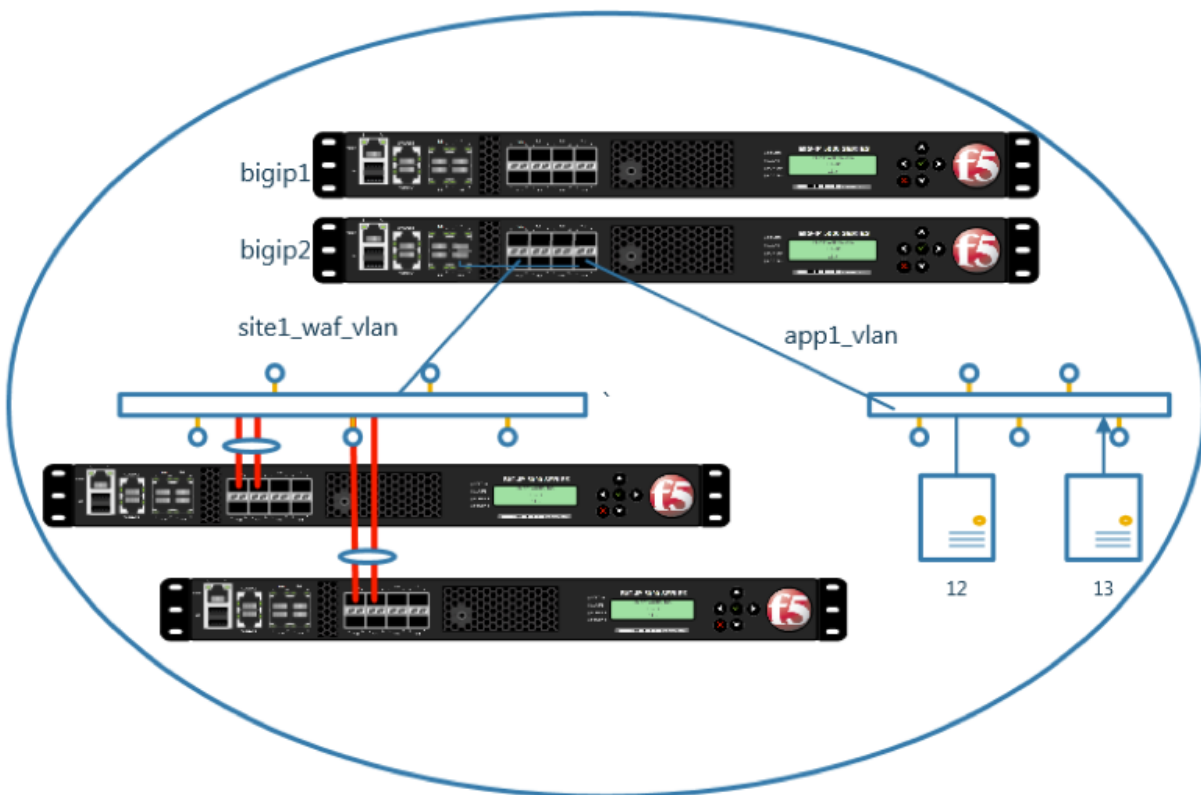
1.1.1 Networking



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

1.1.1.1 VLAN's

Create New Vlans

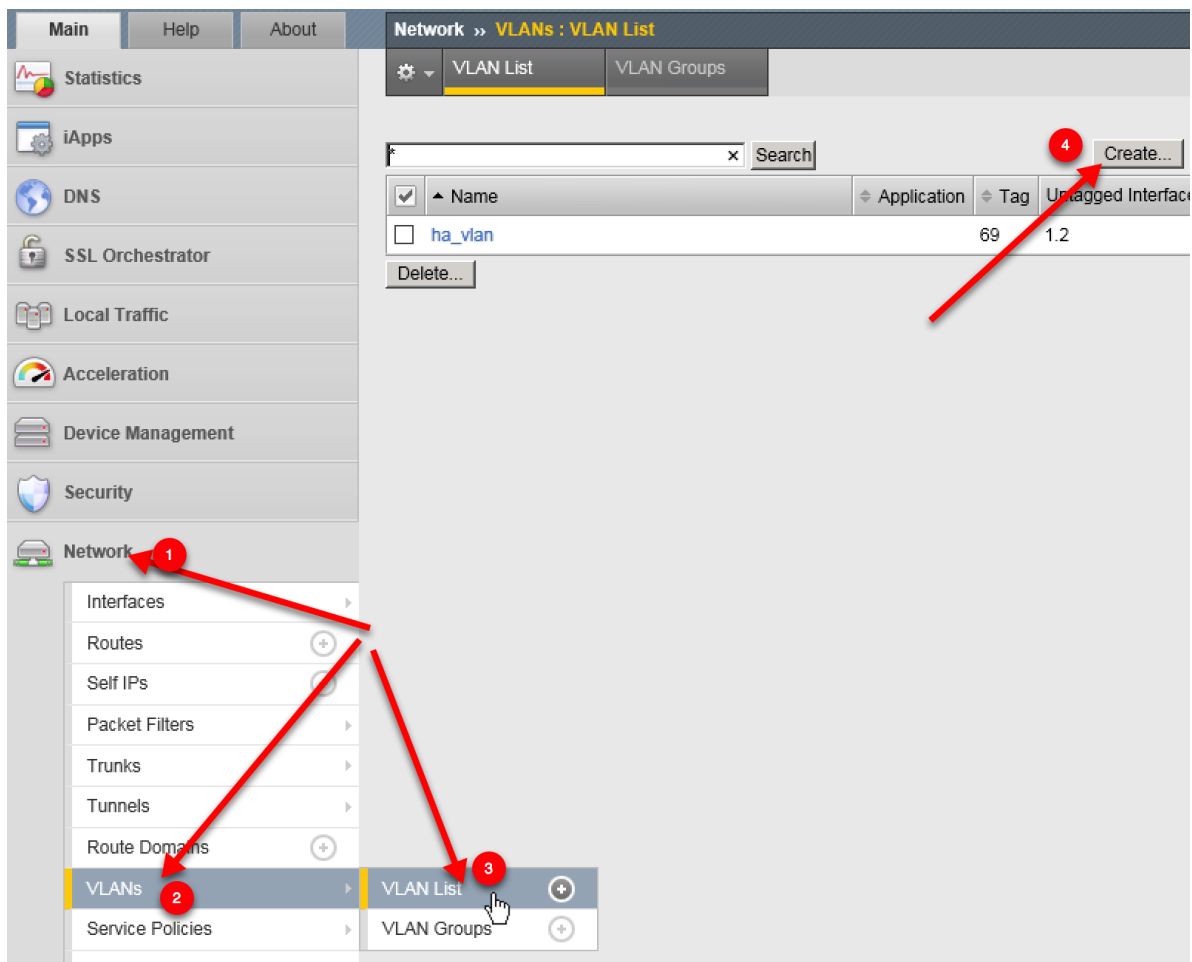


Create a vlan on each WAF

1.

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

Navigate to: **Network » VLANs : VLAN List**



Create a new vlan according to the following table.

Setting	Value
Name	site1_waf_vlan
Tag	50
Interface	1.1 - Untagged

Hostname: asm1.site1.example.com Date: Sep 13, 2017 User: admin
IP Address: 10.1.10.14 Time: 11:03 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About **Network » VLANs : VLAN List » New VLAN...**

Statistics
iApps
DNS
SSL Orchestrator
Local Traffic
Acceleration
Device Management
Security
Network

General Properties

Name **site1_waf_vlan**
Description
Tag **50**

Resources

Interfaces **1.2**
Tagging: **Untagged**
Add
1.1 (untagged)
Edit Delete

Configuration: **Advanced**

Source Check ☐
MTU **1500**

<https://asm1.site1.example.com/tmui/Control/jspmap/tmui/local/network/vlan/create.jsp>

<https://asm2.site1.example.com/tmui/Control/jspmap/tmui/local/network/vlan/create.jsp>

TMSH command for both asm1.site1 and asm2.site1:

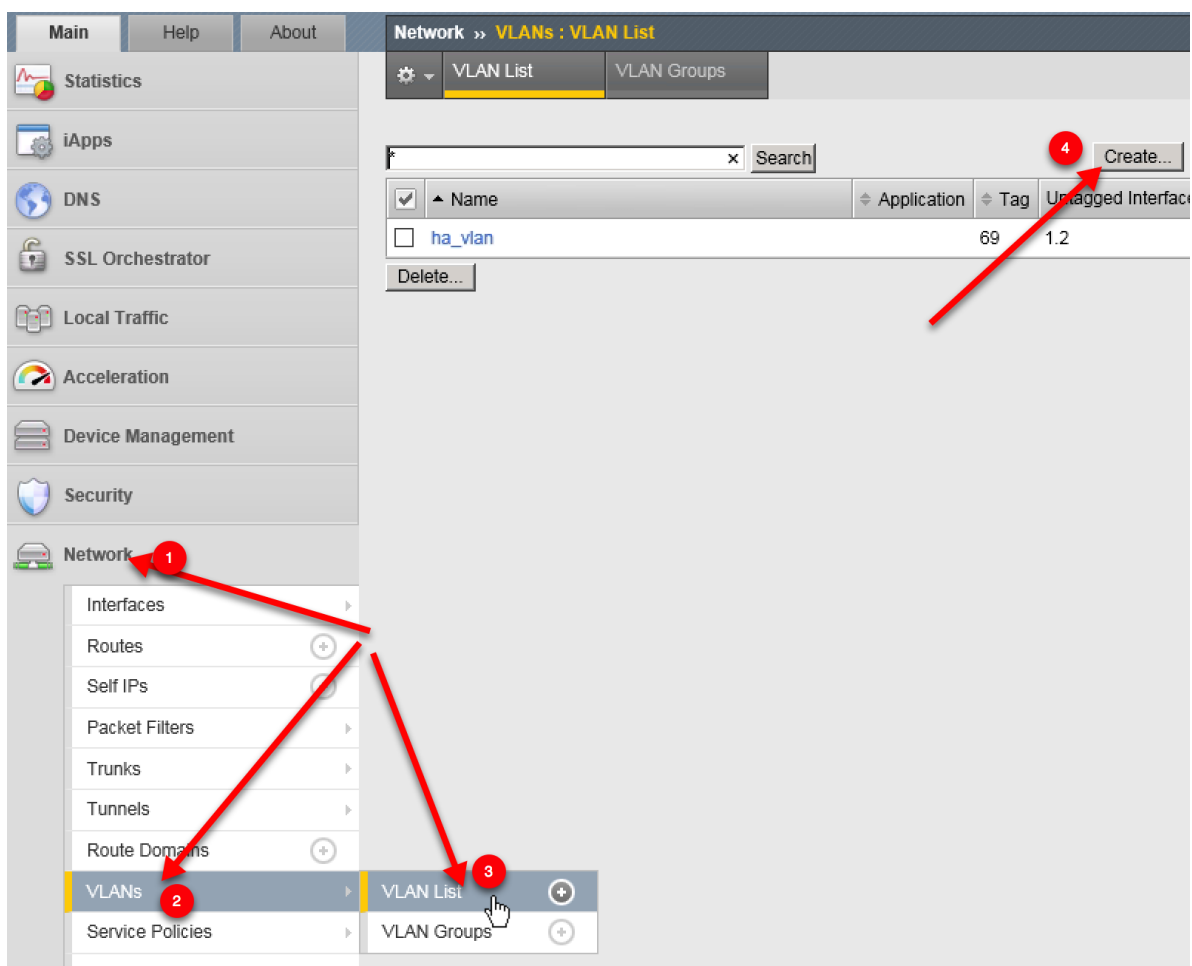
TMSH

```
tmsh create net vlan site1_waf_vlan { interfaces add { 1.1 { } } tag 50 }
```

2.

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

Navigate to: **Network » VLANs : VLAN List**



Create a new vlan according to the following table.

Setting	Value
Name	site2_waf_vlan
Tag	60
Interface	1.1 - Untagged

<https://asm1.site2.example.com/tmui/Control/jspmap/tmui/localb/network/vlan/create.jsp>

<https://asm2.site2.example.com/tmui/Control/jspmap/tmui/localb/network/vlan/create.jsp>

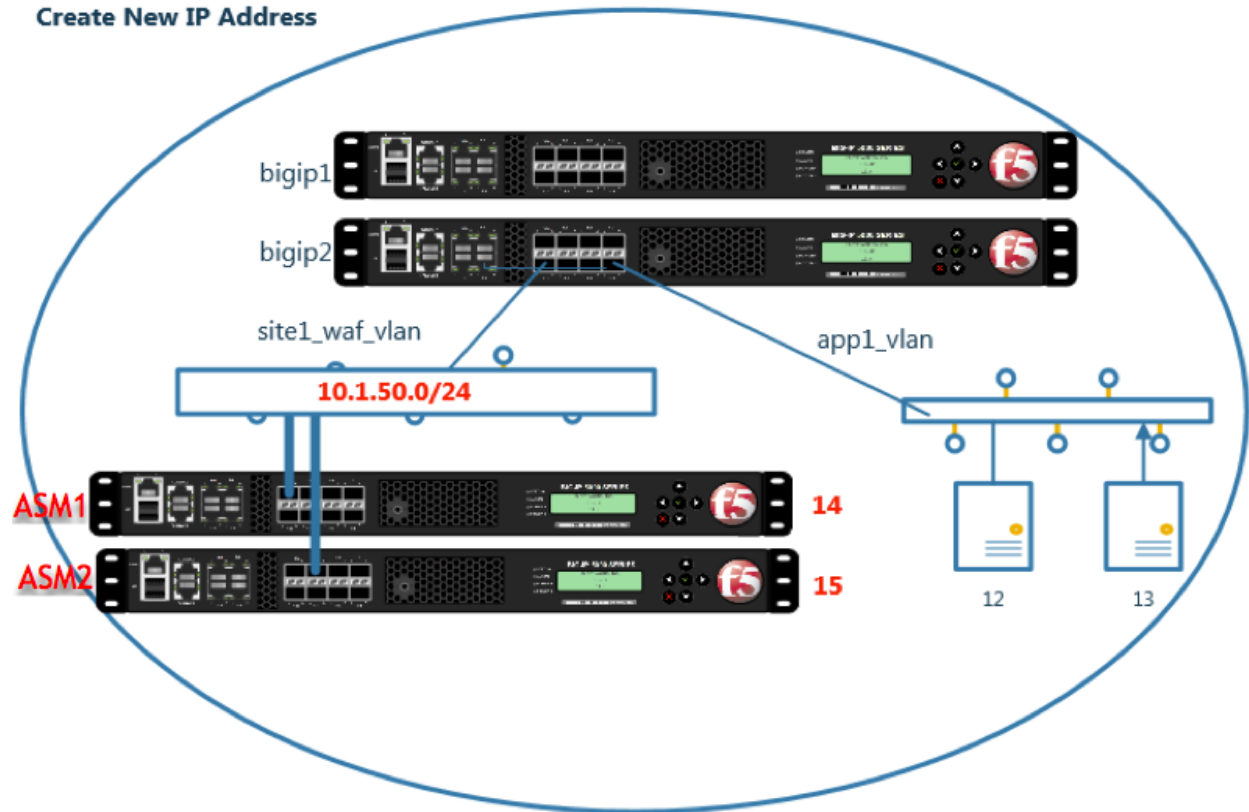
TMSH command for both asm1.site2 and asm2.site2:

TMSH

```
tms create net vlan site2_waf_vlan { interfaces add { 1.1 { } } tag 60 }
```

1.1.1.2 SELFIP's

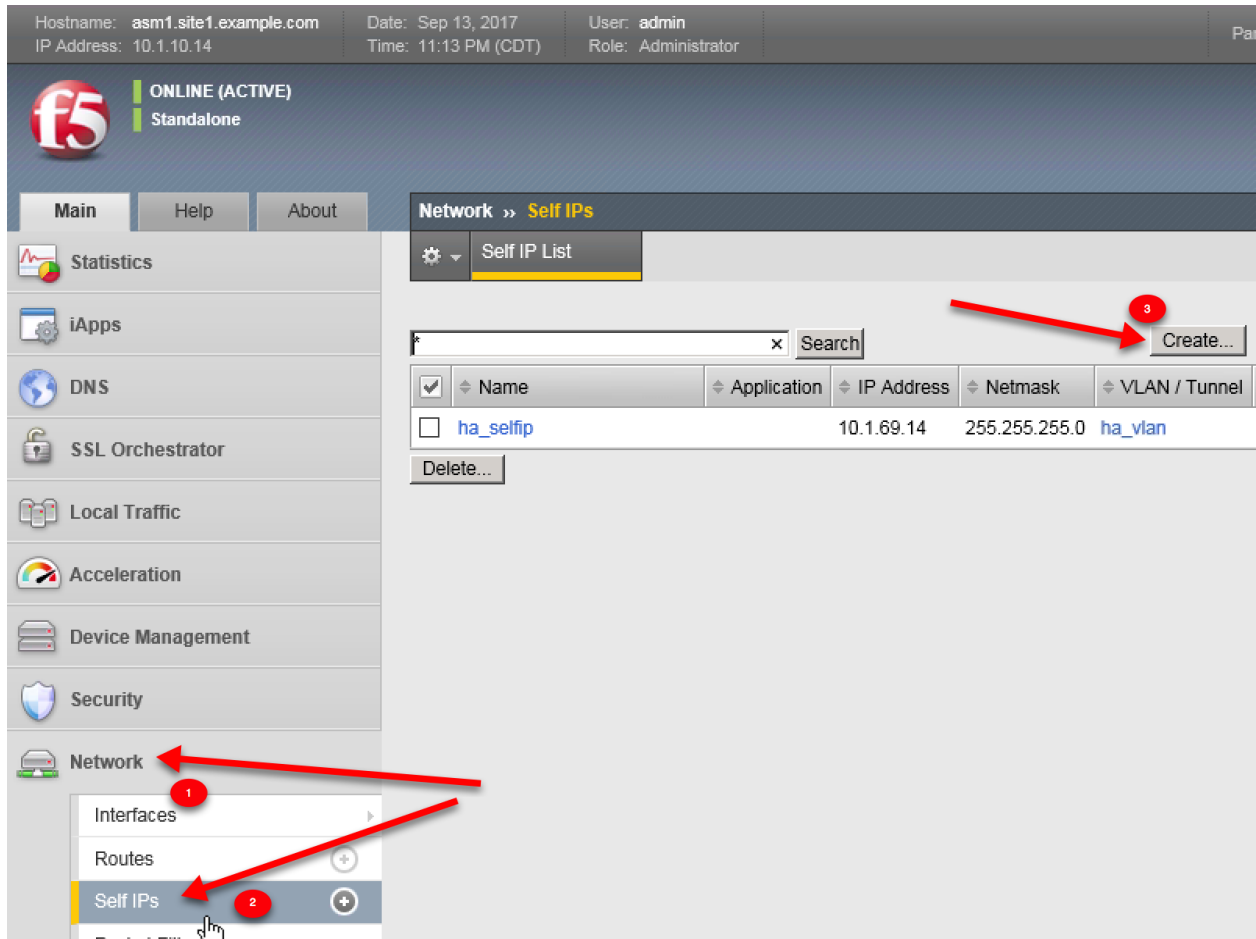
Create New IP Address



Create an IP address on each WAF instance

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

Navigate to: **Network » Self IPs**



1. asm1.site1

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

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

https://asm1.site1.example.com/tmui/Control/jspmap/tmui/local/b/network/self_ip/create.jsp

TMSH command for **asm1.site1**:

TMSH

```
tmsh create net self site1_waf_selfip { address 10.1.50.14/24 vlan site1_waf_vlan }
```

2. asm2.site1

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

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

https://asm2.site1.example.com/tmui/Control/jspmap/tmui/locallb/network/self_ip/create.jsp

TMSH command for **asm2.site1**:

TMSH

```
tmsh create net self site1_waf_selfip { address 10.1.50.15/24 vlan site1_waf_vlan }
```

3. asm1.site2

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

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

https://asm1.site2.example.com/tmui/Control/jspmap/tmui/locallb/network/self_ip/create.jsp

TMSH

```
tmsh create net self site2_waf_selfip { address 10.1.60.24/24 vlan site2_waf_vlan }
```

4. asm2.site2

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

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

https://asm2.site2.example.com/tmui/Control/jspmap/tmui/locallb/network/self_ip/create.jsp

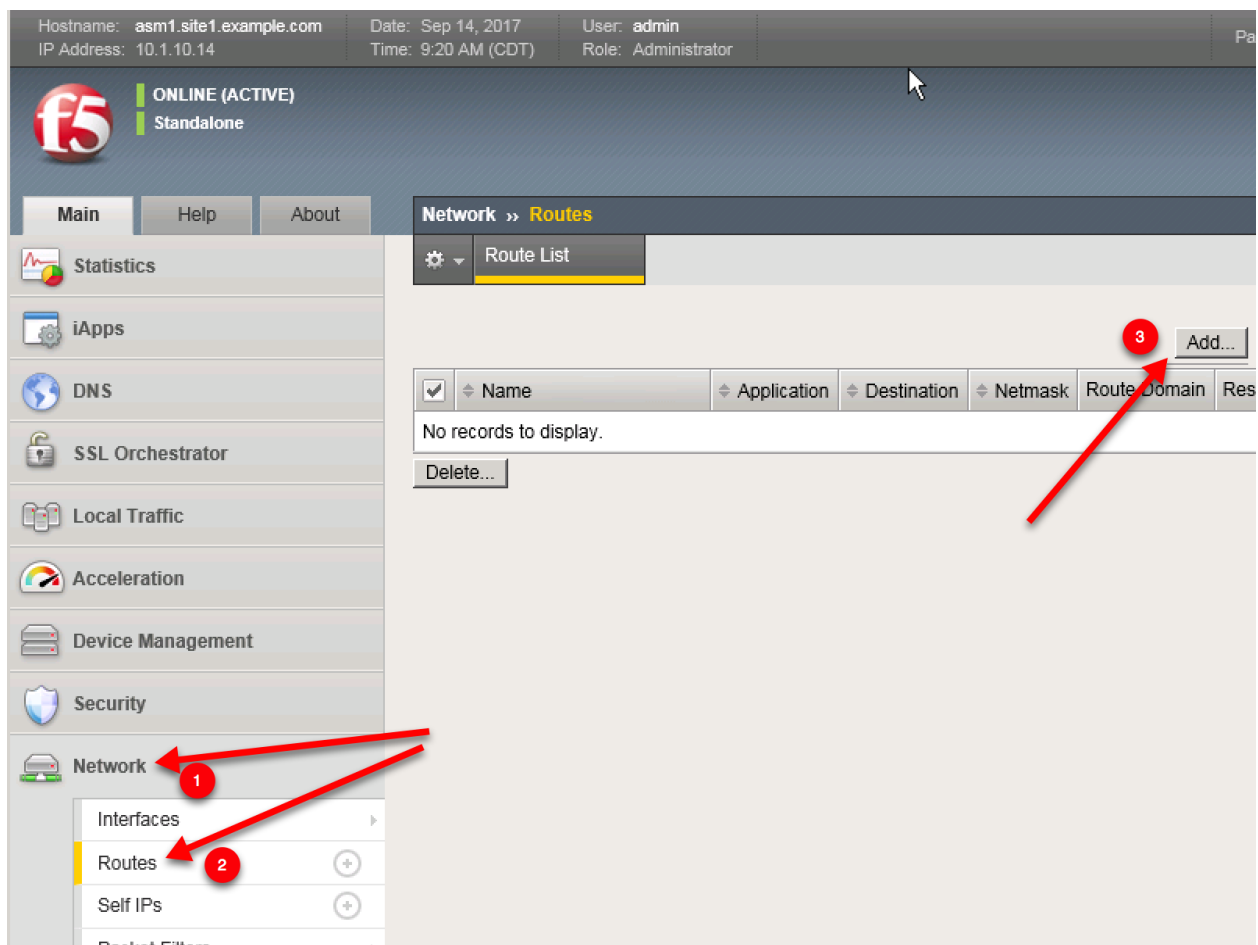
TMSH

```
tmsh create net self site2_waf_selfip { address 10.1.60.25/24 vlan site2_waf_vlan }
```

1.1.1.3 Default Route

Create a default gateway on each WAF

Navigate to: **Network** » **Routes**



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

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

Setting	Value
Name	default_route
Destination	0.0.0.0
Netmask	0.0.0.0
Gateway Address	10.1.50.1

Hostname: asm1.site1.example.com Date: Sep 14, 2017 User: admin
IP Address: 10.1.10.14 Time: 9:24 AM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About Network » Routes » New Route...

Statistics
iApps
DNS
SSL Orchestrator
Local Traffic
Acceleration
Device Management
Security
Network

Interfaces
Routes
Self IPs
Packet Filters

Properties

Name

Description

Destination

Netmask

Resource

Gateway Address

MTU

Cancel Repeat Finished

<https://asm1.site1.example.com/tmui/Control/jspmap/tmui/localb/network/route/create.jsp>

<https://asm2.site1.example.com/tmui/Control/jspmap/tmui/localb/network/route/create.jsp>

TMSH command for asm1.site1 and asm2.site1:

TMSH

```
tmsh create net route default_route { gw 10.1.50.1 network default }
```

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

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

Setting	Value
Name	default_route
Destination	0.0.0.0
Netmask	0.0.0.0
Gateway Address	10.1.60.1

<https://asm1.site2.example.com/tmui/Control/jspmap/tmui/localb/network/route/create.jsp>

<https://asm2.site2.example.com/tmui/Control/jspmap/tmui/localb/network/route/create.jsp>

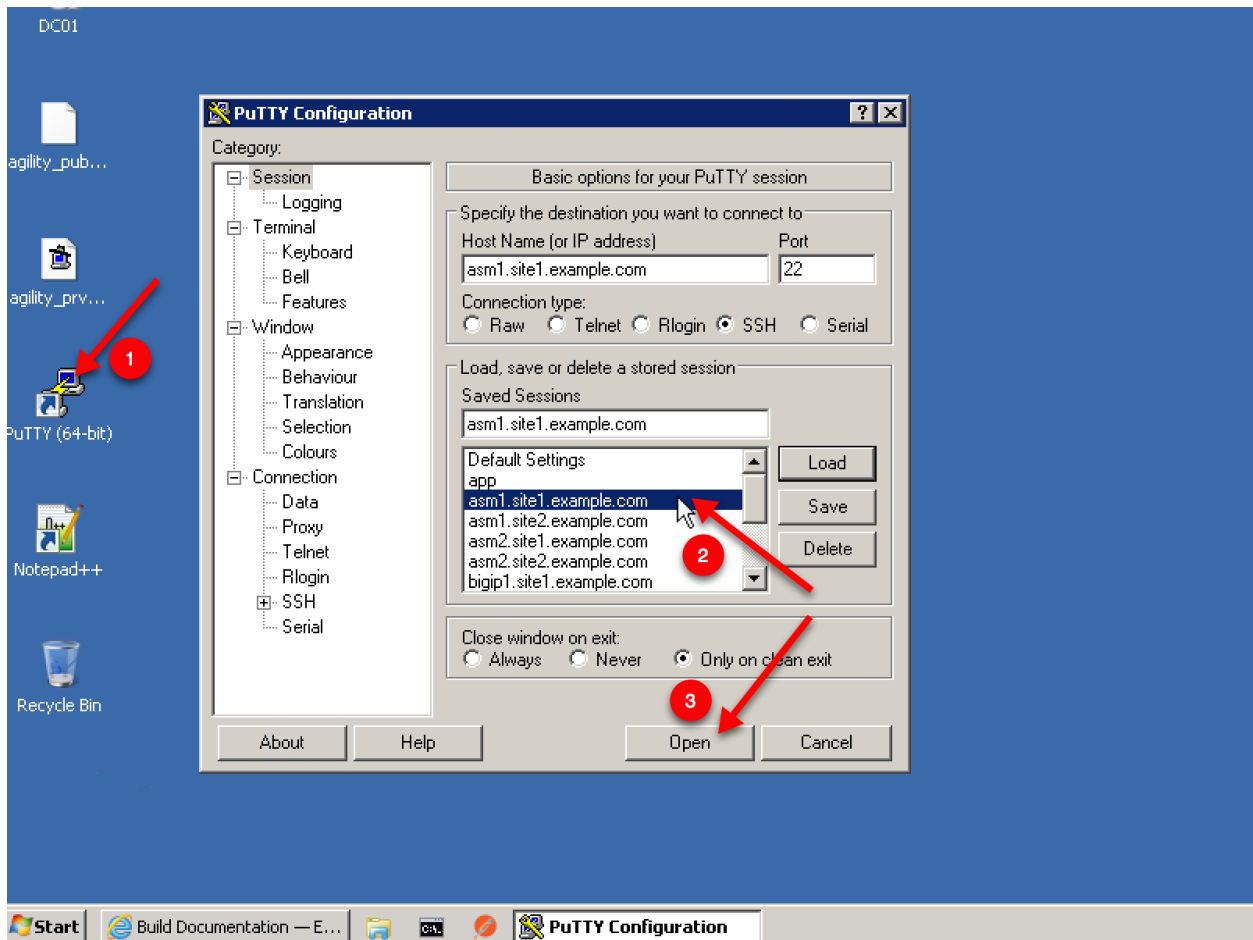
TMSH command for asm1.site2 and asm2.site2:

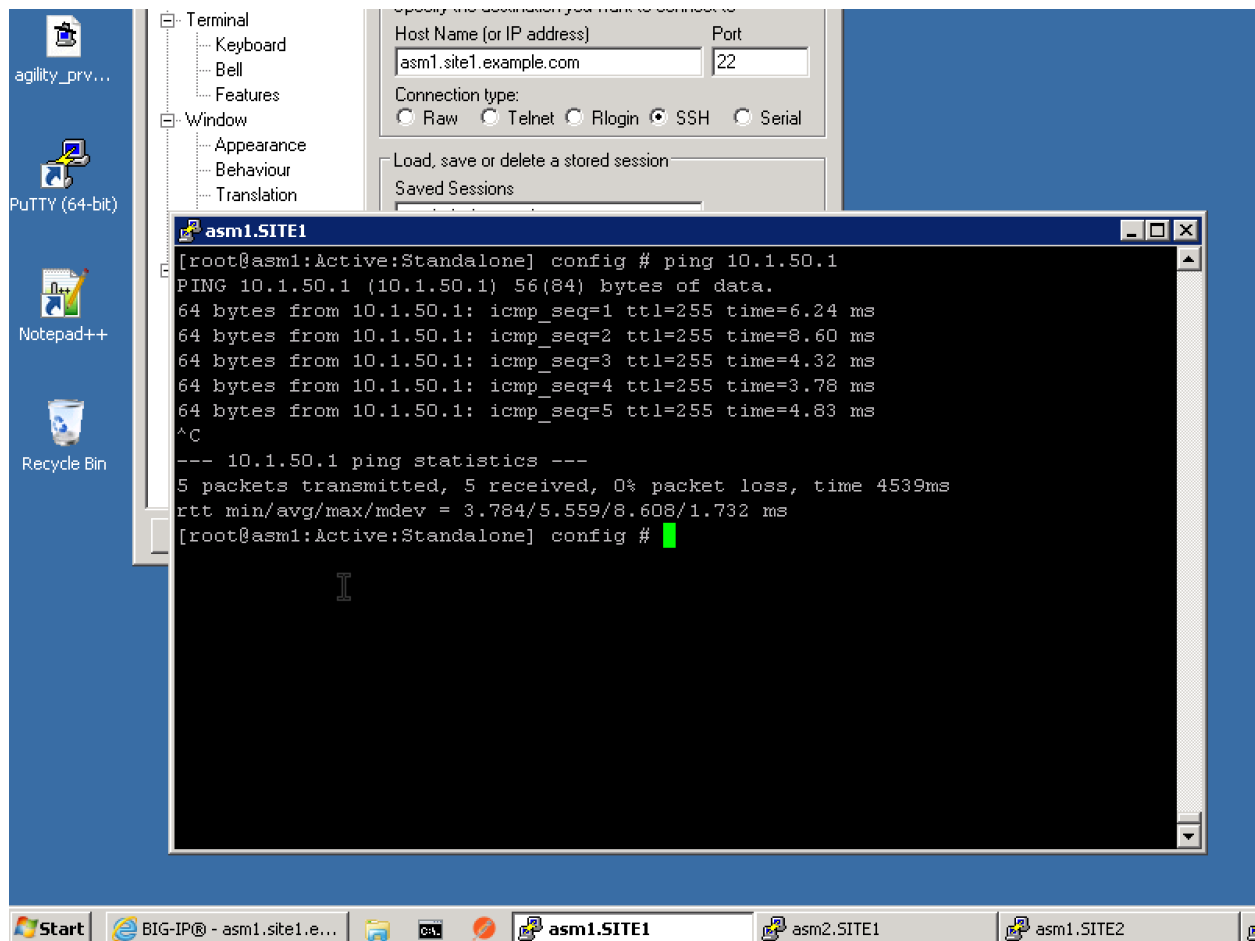
TMSH

```
tmsh create net route default_route { gw 10.1.60.1 network default }
```

1.1.1.4 Results

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

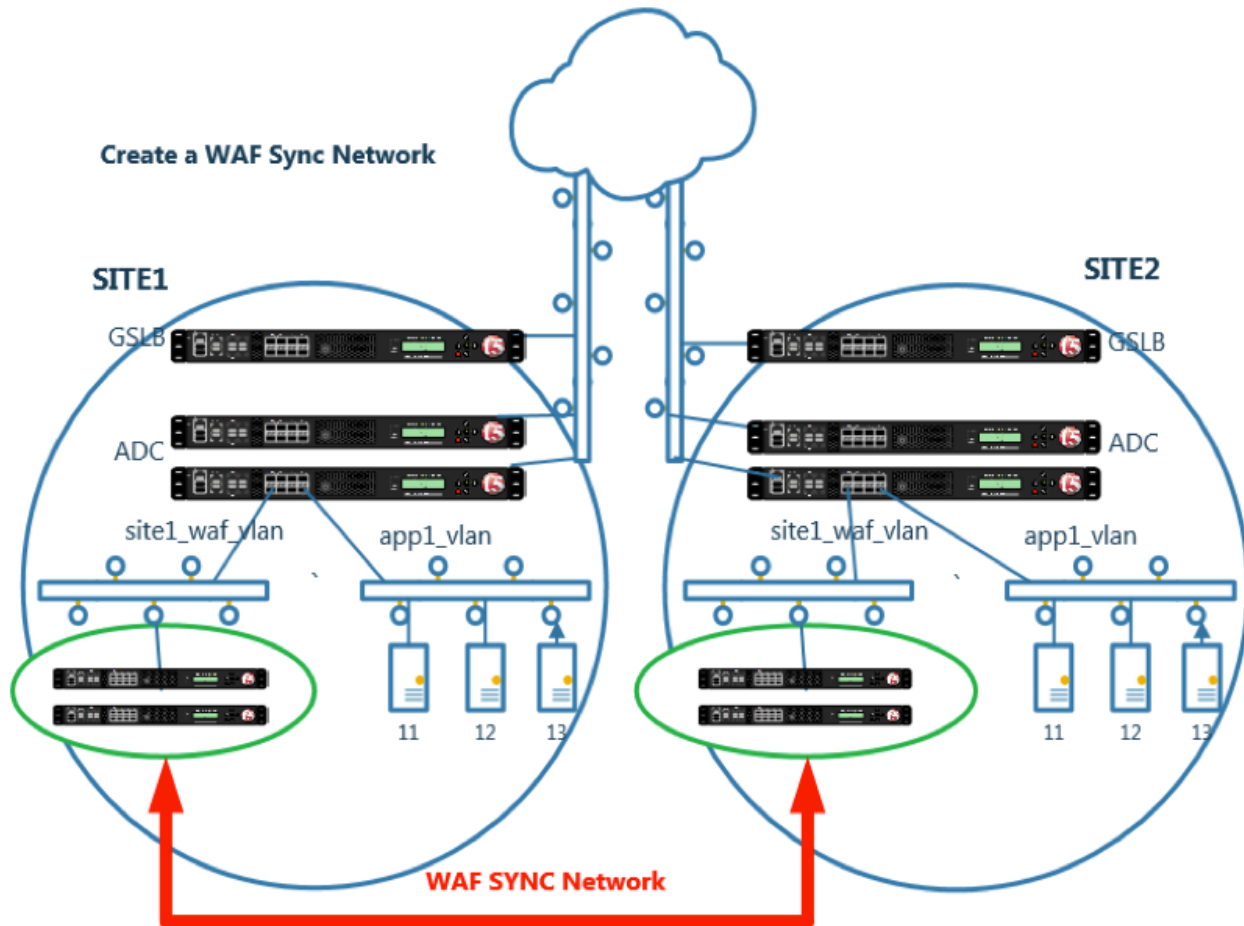




1. From asm1.site1 ping the gateway
 - ping 10.1.50.1
2. From asm1.site1 ping bigip1.site1 and bigip2.site1
 - ping 10.1.50.2
 - ping 10.1.50.3
3. From **asm1.site2** ping the gateway
 - ping 10.1.60.1
4. From asm1.site2 ping bigip1.site2 and bigip2.site2
 - ping 10.1.60.2
 - ping 10.1.60.3

1.1.2 Cluster

Create a trust relationship across all WAF devices

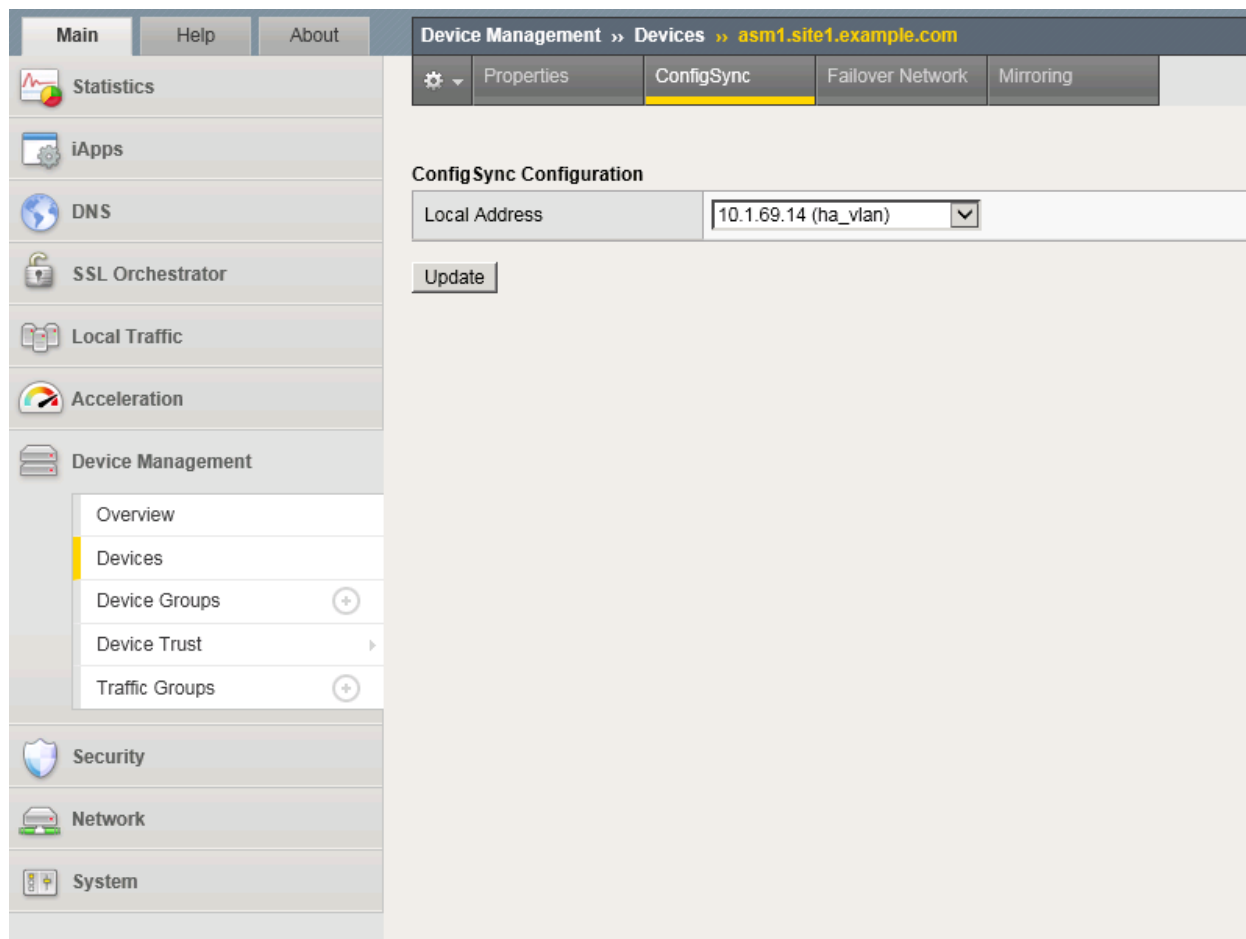


1.1.2.1 ConfigSync IP

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

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

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

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

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

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

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

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

TMSH command for asm1.site1:

TMSH

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

TMSH command for asm2.site1:

TMSH

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

TMSH command for asm1.site2:

TMSH

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

TMSH command for asm2.site2:

TMSH

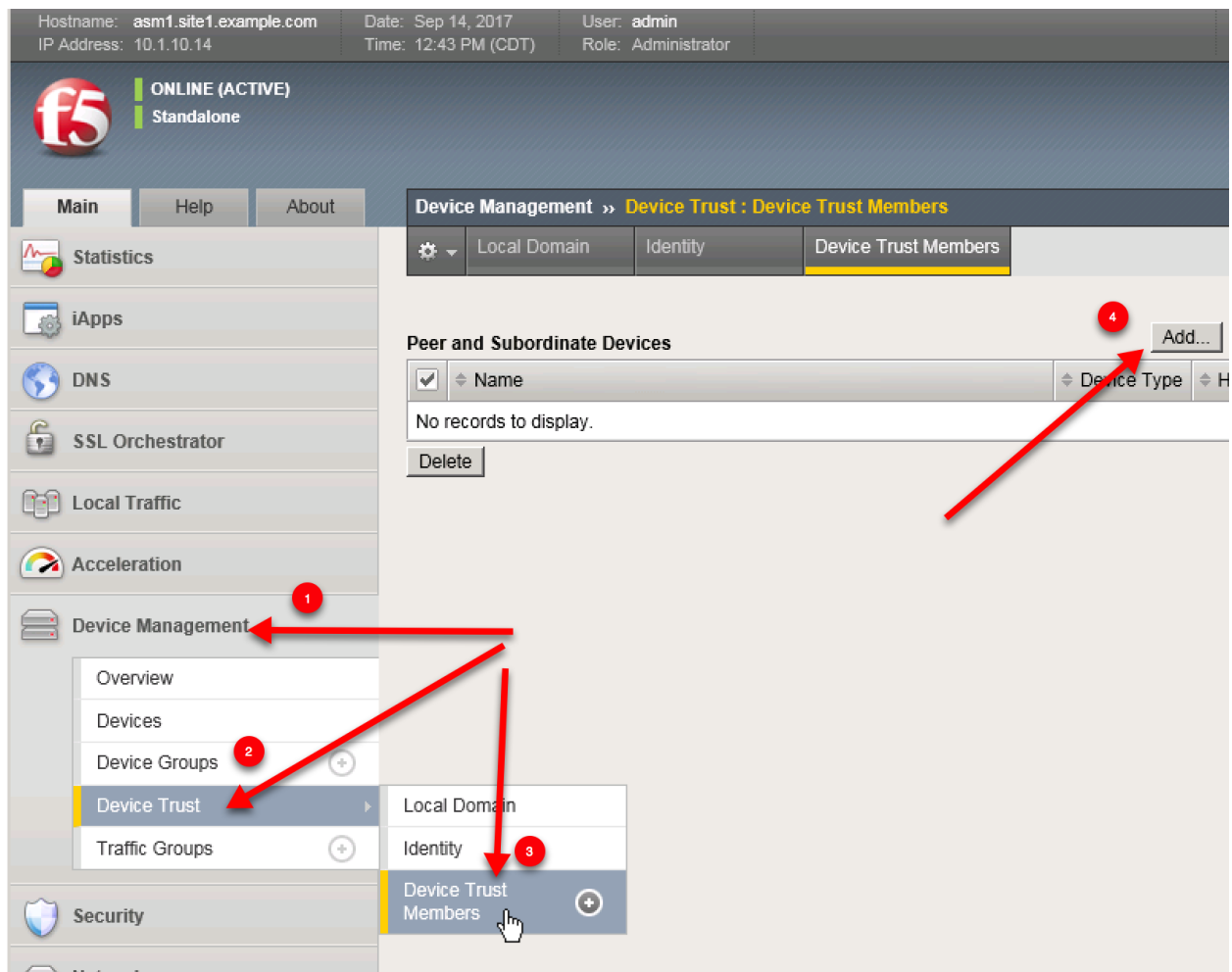
```
tmsl modify cm device asm2.site2.example.com configsync-ip 10.1.69.25
```

1.1.2.2 Trust Members

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

Navigate to: **Device Management » Device Trust : Device Trust Members**

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



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

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

Main
Help
About
Device Management » Device Trust

Statistics
iApps
DNS
SSL Orchestrator
Local Traffic
Acceleration
Device Management
Overview
Devices
Device Groups
Device Trust
Traffic Groups
Security
Network
System

Retrieve Device Credentials (Step 1 of 3)

Device Type	Peer
Device IP Address	10.1.10.15
Administrator Username	admin
Administrator Password	•••••

Verify Device Certificate (Step 2 of 3)

Subject	/C=US/ST=WA/L=Seattle/O=F5 Networks/OU=IT/CN=asm2.site1.example.com/emailAddress=roo
Management IP Address	10.1.10.15
Expiration	Sun Aug 27 14:30:28 CST 2027
Serial Number	0e67cf04
Signed	Yes
SHA-1	736c1726ae1ce4da7f312a38b4be9807c317f003
MD5	f9665ba229ac3a87704f683bba59ec40

Add Device (Step 3 of 3)

Name	asm2.site1.example.com
------	------------------------

Cancel
Add Device

Device Management » Device Trust : Device Trust Members

Peer and Subordinate Devices

<input checked="" type="checkbox"/>	Name	Device Type	Hostname	Serial Number	MAC Address
<input type="checkbox"/>	asm1.site2.example.com	Peer	asm1.site2.example.com	564dadcc-a795-99fc-24afead600c3	2c:c2:60:53:92:4f
<input type="checkbox"/>	asm2.site1.example.com	Peer	asm2.site1.example.com	564dadcc-a795-99fc-24afead600c3	2c:c2:60:1f:ef:92
<input type="checkbox"/>	asm2.site2.example.com	Peer	asm2.site2.example.com	564dadcc-a795-99fc-24afead600c3	2c:c2:60:55:ca:b3

Delete

1.1.2.3 Changes Pending

1. From asm1.site1 click the “Changes Pending” link:

Hostname: asm1.site1.example.com Date: Sep 7, 2017 User: admin
IP Address: 10.1.10.14 Time: 11:33 AM (CDT) Role: Administrator Partition: Common

f5 ONLINE (ACTIVE)
Changes Pending

Click

Main Help About

Statistics
iApps
DNS
SSL Orchestrator
Local Traffic
Acceleration
Device Management
Security

Device Management » Device Trust : Device Trust Members

Local Domain Identity Device Trust Members

Peer and Subordinate Devices

<input checked="" type="checkbox"/>	Name	Device Type	Hostname	Serial Number
<input type="checkbox"/>	asm1.site2.example.com	Peer	asm1.site2.example.com	564dadcc-a795-99fc-24a
<input type="checkbox"/>	asm2.site1.example.com	Peer	asm2.site1.example.com	564dadcc-a795-99fc-24a
<input type="checkbox"/>	asm2.site2.example.com	Peer	asm2.site2.example.com	564dadcc-a795-99fc-24a

Delete

2. Click “Sync”

Sync Issues :

▼ datasync-global-dg Changes Pending 4 Devices Sync-Only Group Manu

Changes Pending
 4 devices with 4 different configurations
 asm2.site1.example.com made last configuration change on Tue Aug 29 10:35:52 2017
 asm1.site2.example.com made last configuration change on Tue Aug 29 10:36:02 2017
 This device made last configuration change on Tue Aug 29 10:36:09 2017
 asm2.site2.example.com made last configuration change on Tue Aug 29 10:44:19 2017
 Recommended action: Synchronize asm2.site2.example.com to group datasync-global-dg

Devices:

HA Status	Name	Sync Status
<input checked="" type="radio"/>	asm2.site2.example.com	In Sync
<input type="radio"/>	asm1.site1.example.com (Self)	Does not have the last synced configuration
<input type="radio"/>	asm1.site2.example.com	Does not have the last synced configuration
<input type="radio"/>	asm2.site1.example.com	Does not have the last synced configuration

Sync Options:
☒ Push the selected device configuration to the group
☐ Pull the most recent configuration to the selected device

Click "Sync"

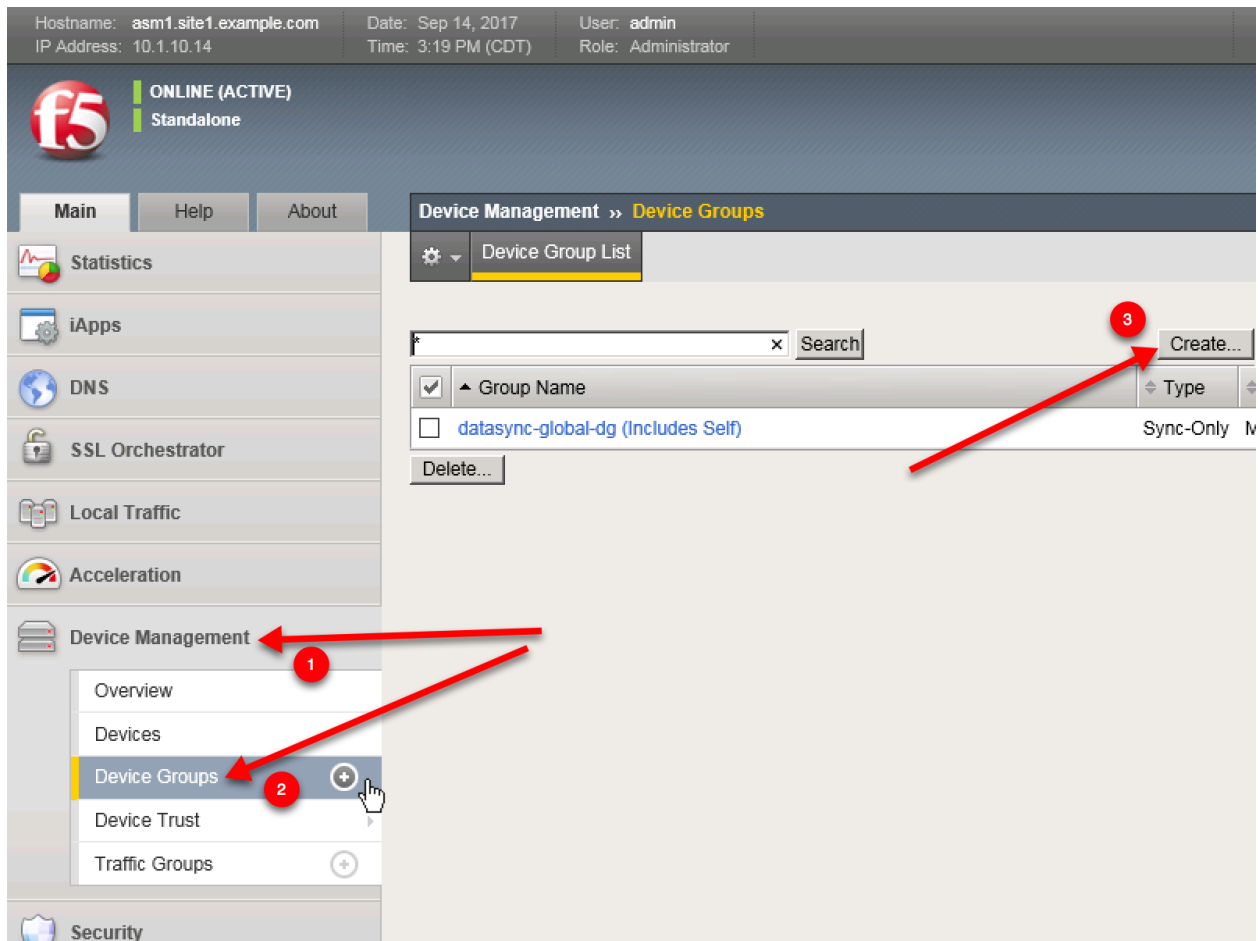
After initial synchronization devices will go “OFFLINE” for a few minutes.

1.1.2.4 Device Groups

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

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

Navigate to: **Device Management » Device Groups**



Create the device group according to the following table:

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

Hostname: asm1.site1.example.com Date: Sep 7, 2017 User: admin
IP Address: 10.1.10.14 Time: 11:45 AM (CDT) Role: Administrator Partition

f5 ONLINE (ACTIVE)
In Sync

Main Help About **Device Management » Device Groups » New Device Group...**

Statistics
iApps
DNS
SSL Orchestrator
Local Traffic
Acceleration
Device Management
Overview
Devices
Device Groups
Device Trust
Traffic Groups
Security

General Properties

Name: example.com_waf_sync-group x

Group Type: Sync-Only

Description:

Configuration: Advanced

Members:

Includes:

Available:

Sync Type: Automatic with Full Sync

Save on Automatic Sync: ☒ Save the configuration to file on the remote devices after an au

Cancel Repeat Finished

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

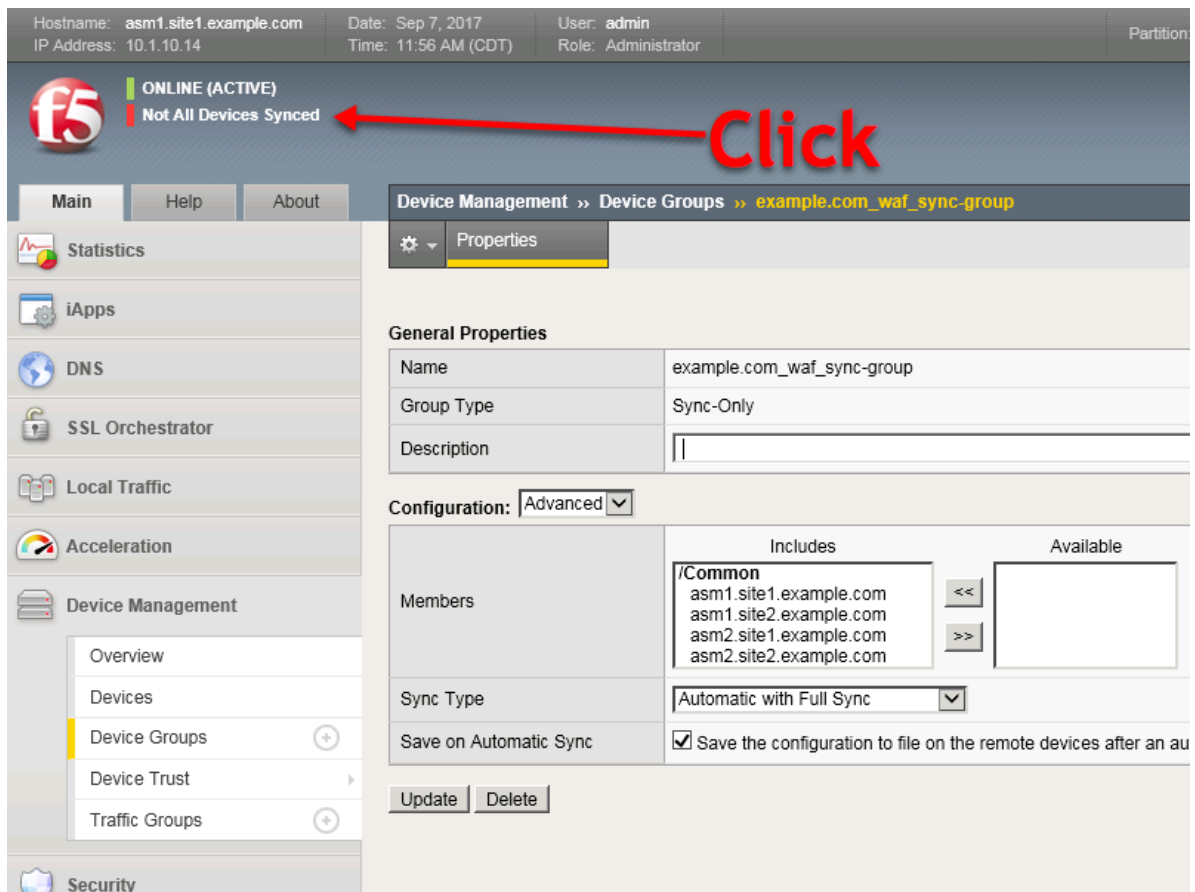
TMSH command for asm1.site1:

TMSH

```
tmsl create cm device-group example.com_waf_sync-group { auto-sync enabled devices
add { asm1.site1.example.com { } asm1.site2.example.com { } asm2.site1.example.com { }
asm2.site2.example.com { } } full-load-on-sync true save-on-auto-sync true }
```

1.1.2.5 Sync... Again

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



2. Click "Sync"

The label may show "Awaiting Initial Sync"

TMSH command for asm1.site1:

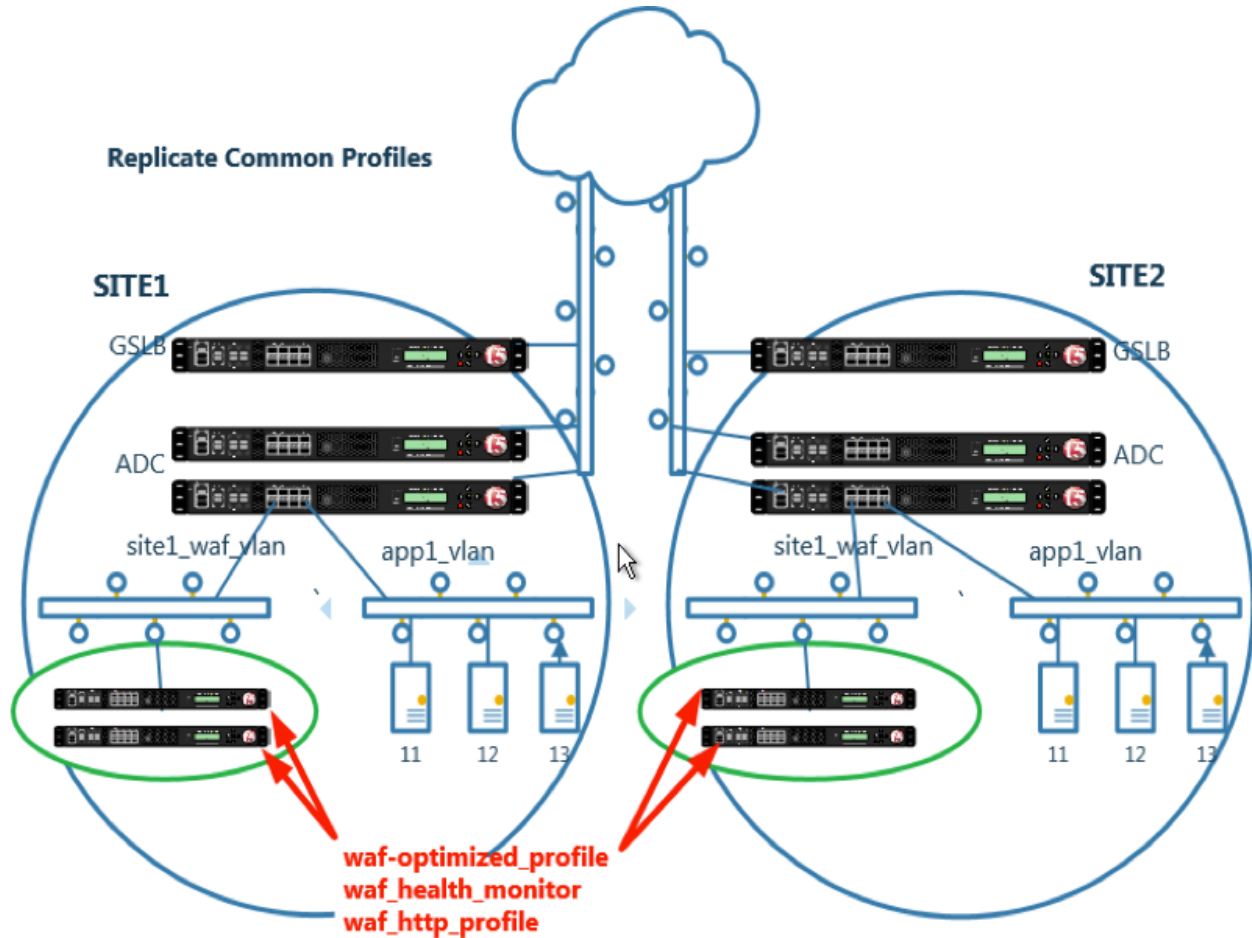
TMSH

```
tmsh run /cm config-sync force-full-load-push to-group example.com_waf_sync-group
```

Be Patient. Sometimes initial sync takes a minute.

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

1.1.3 Shared Objects



Some configuration objects are common across all devices.

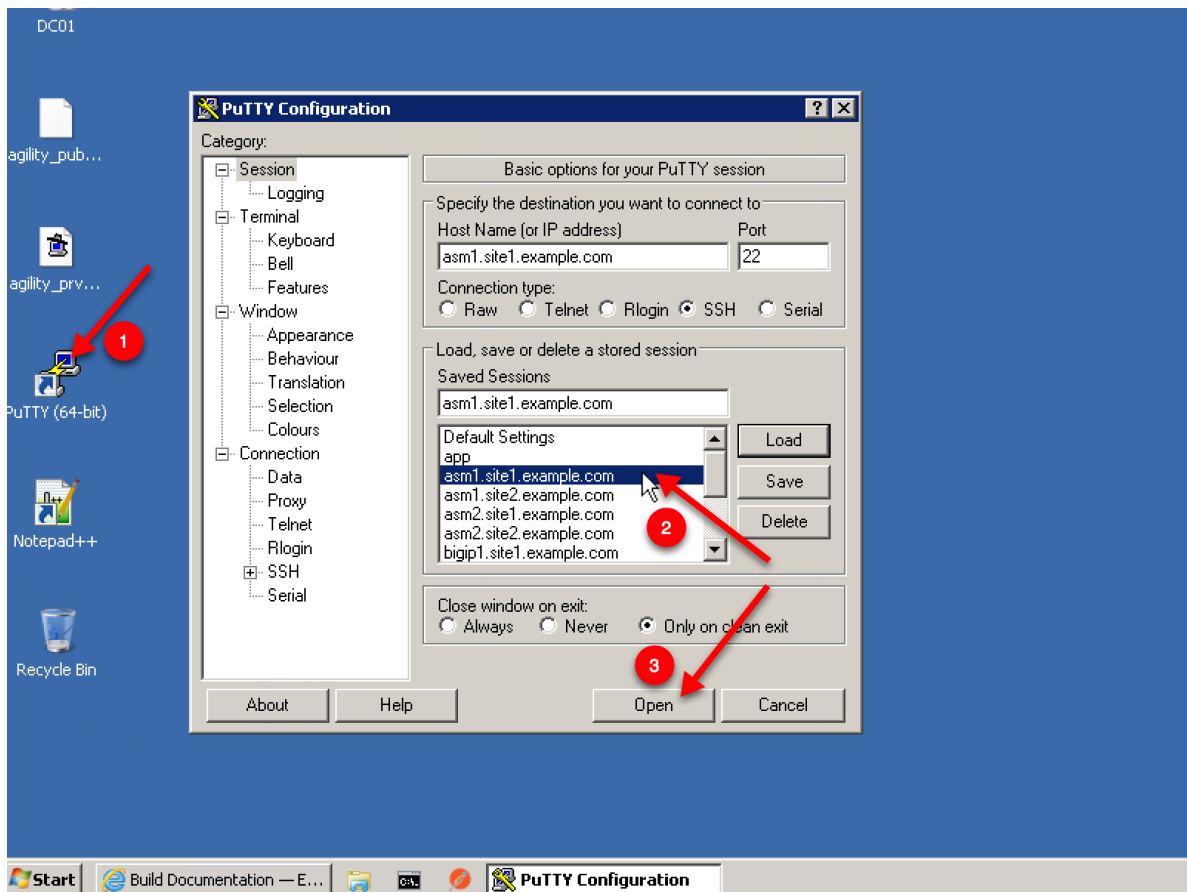
Common objects will replicate across the cluster.

1.1.3.1 Sync Folder

Create the sync folder.

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

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

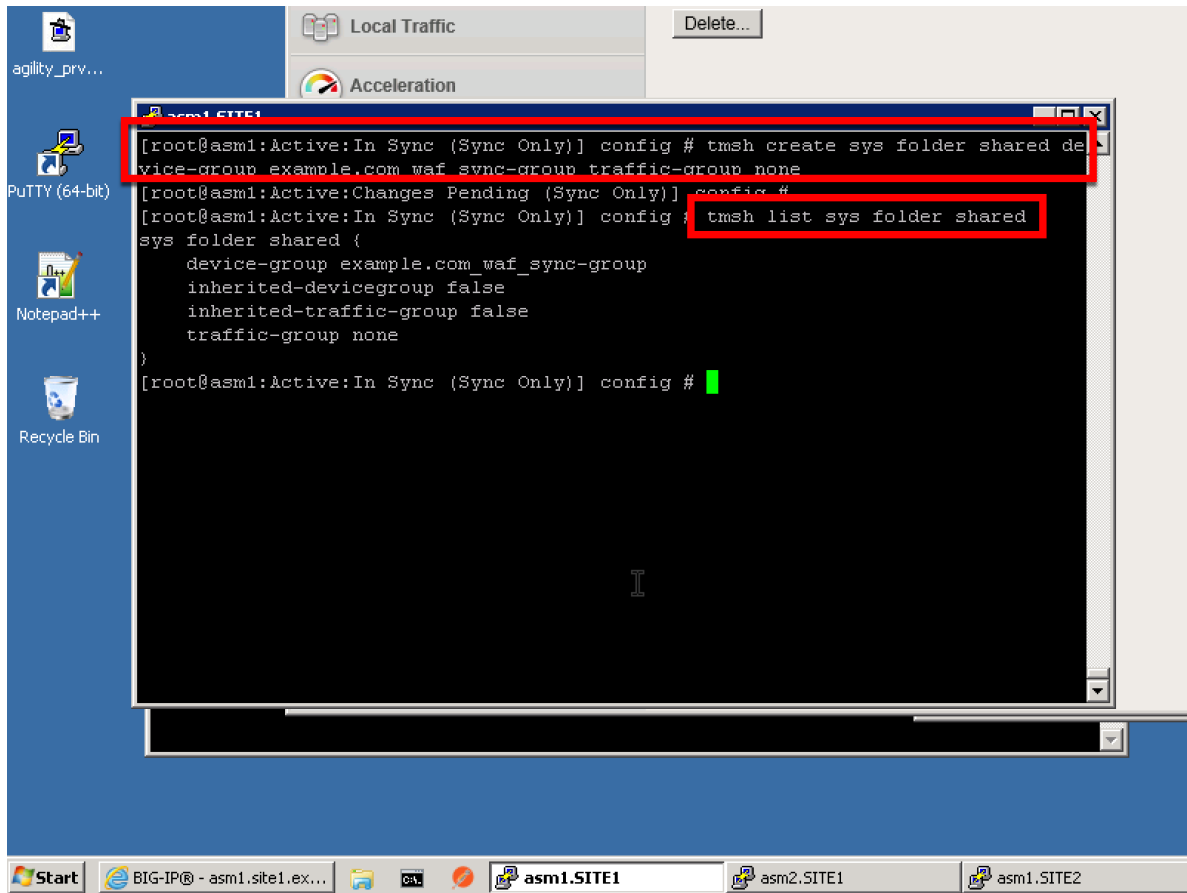


2. Run the following command.

TMSH command for asm1.site1:

TMSH

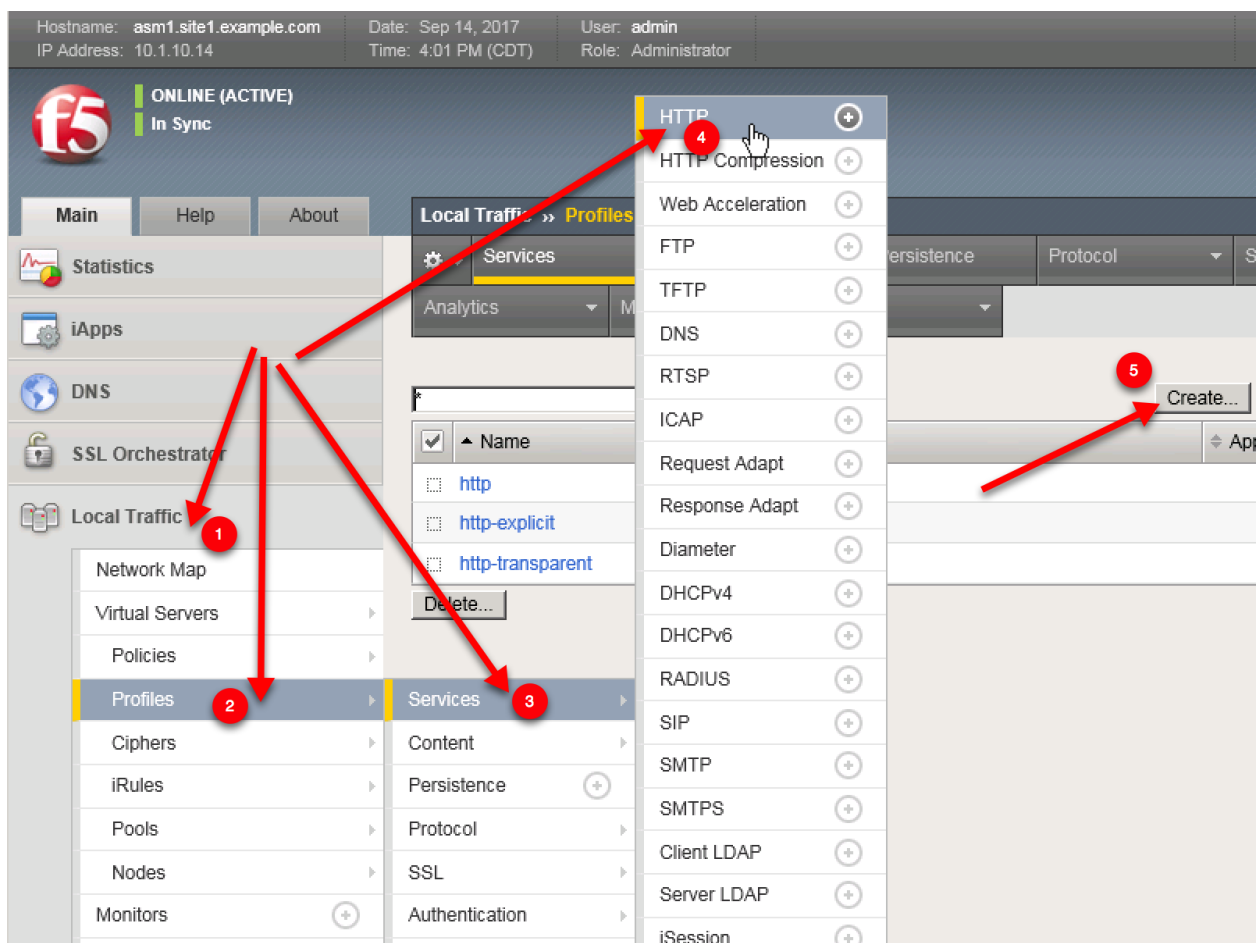
```
tmsh create sys folder shared device-group example.com_waf_sync-group traffic-group none
```



1.1.3.2 HTTP Profile

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

Navigate to: **Local Traffic » Profiles : Services : HTTP**



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

Create an HTTP profile according to the table below.

Setting	Value
Name	shared/example.com_http_profile

The screenshot shows the TMSH configuration interface. The left sidebar contains a tree view with categories: Main, Help, About, Local Traffic, Profiles, Services, HTTP, and New HTTP Profile... The 'Local Traffic' category is expanded, showing sub-items: Network Map, Virtual Servers, Policies, Profiles, Ciphers, iRules, Pools, Nodes, Monitors, Traffic Class, and Address Translation. The 'Profiles' sub-item is selected. The main panel displays the 'General Properties' and 'Settings' for the 'New HTTP Profile...' configuration. The 'Name' field is highlighted with a red arrow and contains the text 'shared/example.cc'. The 'Proxy Mode' is set to 'Reverse' and the 'Parent Profile' is set to 'http'. The 'Settings' section includes various options like 'Basic Auth Realm', 'Fallback Host', 'Request Header Erase', 'Request Header Insert', 'Response Headers Allowed', 'Request Chunking', 'Response Chunking', 'OneConnect Transformations', 'Redirect Rewrite', 'Encrypt Cookies', 'Cookie Encryption Passphrase', and 'Confirm Cookie Encrvotion'.

TMSH command for asm1.site1:

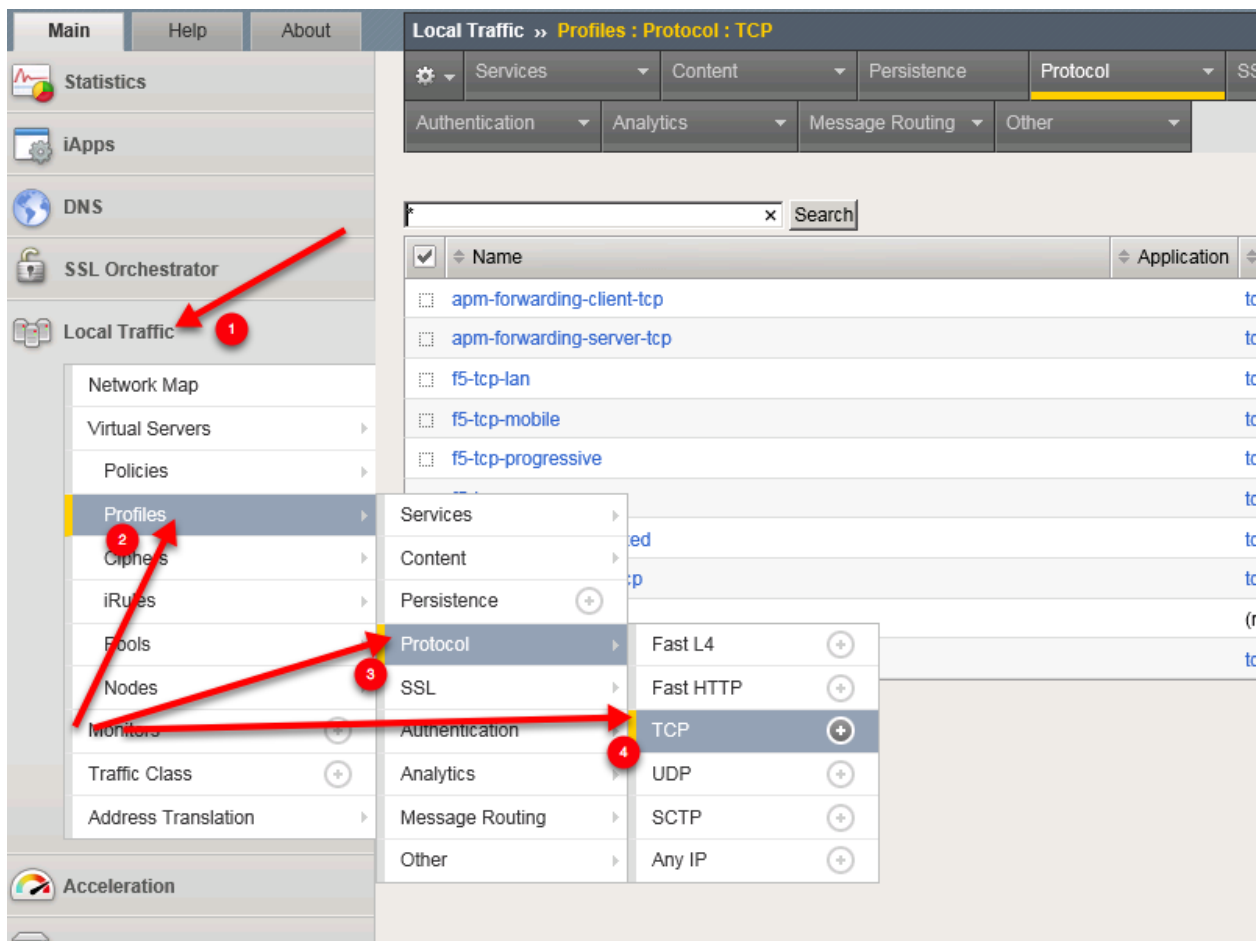
TMSH

```
tmsh create ltm profile http shared/example.com_http_profile
```

1.1.3.3 TCP Profile

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

Navigate to: **Local Traffic » Profiles : Protocol : TCP**



Create a TCP profile according to the table below.

Setting	Value
Name	shared/example.com_tcp_profile

Main | **Help** | **About** | **Local Traffic >> Profiles : Protocol : TCP >> New TCP Profile...**

General Properties

Name	shared/example x
Parent Profile	tcp

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	1000 milliseconds
Reset On Timeout	<input checked="" type="checkbox"/> Enabled
Time Wait	Specify... 2000 milliseconds
Time Wait Recycle	<input checked="" type="checkbox"/> Enabled
Zero Window Timeout	Specify... 20000 milliseconds

Memory Management

Auto Proxy Buffer	<input type="checkbox"/>
Auto Receive Window	<input type="checkbox"/>
Auto Send Buffer	<input type="checkbox"/>

TMSH command for asm1.site1:

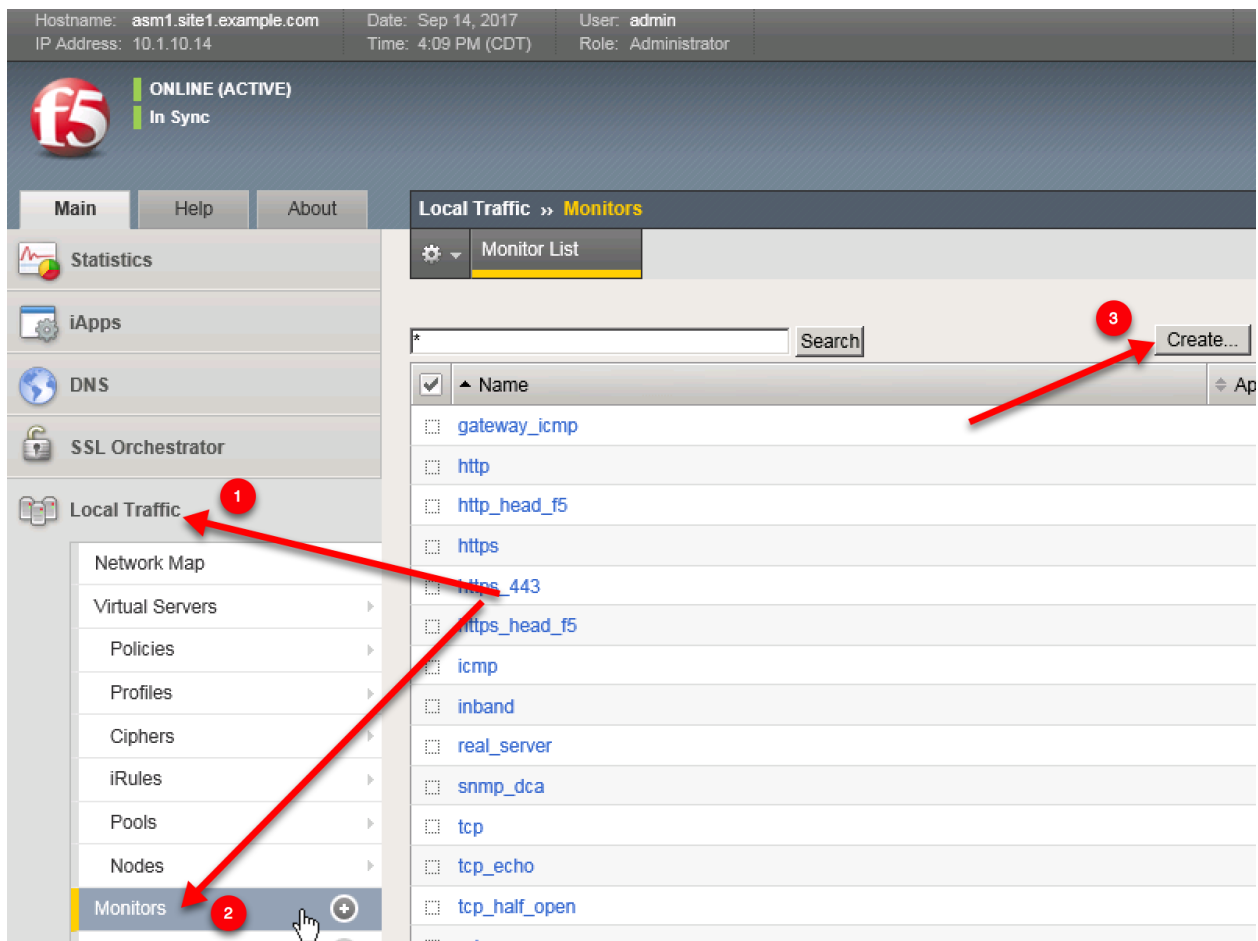
TMSH

```
tmsh create ltm profile tcp shared/example.com_tcp_profile defaults-from f5-tcp-lan
```

1.1.3.4 Health Monitor

Create a common health monitor

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



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

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

Hostname: asm1.site1.example.com Date: Sep 14, 2017 User: admin
IP Address: 10.1.10.14 Time: 4:14 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
In Sync

Main Help About Local Traffic » Monitors » New Monitor...

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

General Properties

Name shared/example.com_https_monitor
Description
Type HTTPS
Parent Monitor https

Configuration: Advanced

Interval 5 seconds
Up Interval Disabled
Time Until Up 0 seconds
Timeout 16 seconds
Manual Resume Yes No
Send String GET /login.php\r\n

TMSH command for asm1.site1:

```
tmsm create ltm monitor https shared/example.com_https_monitor send "GET /login.php\r\n"
```

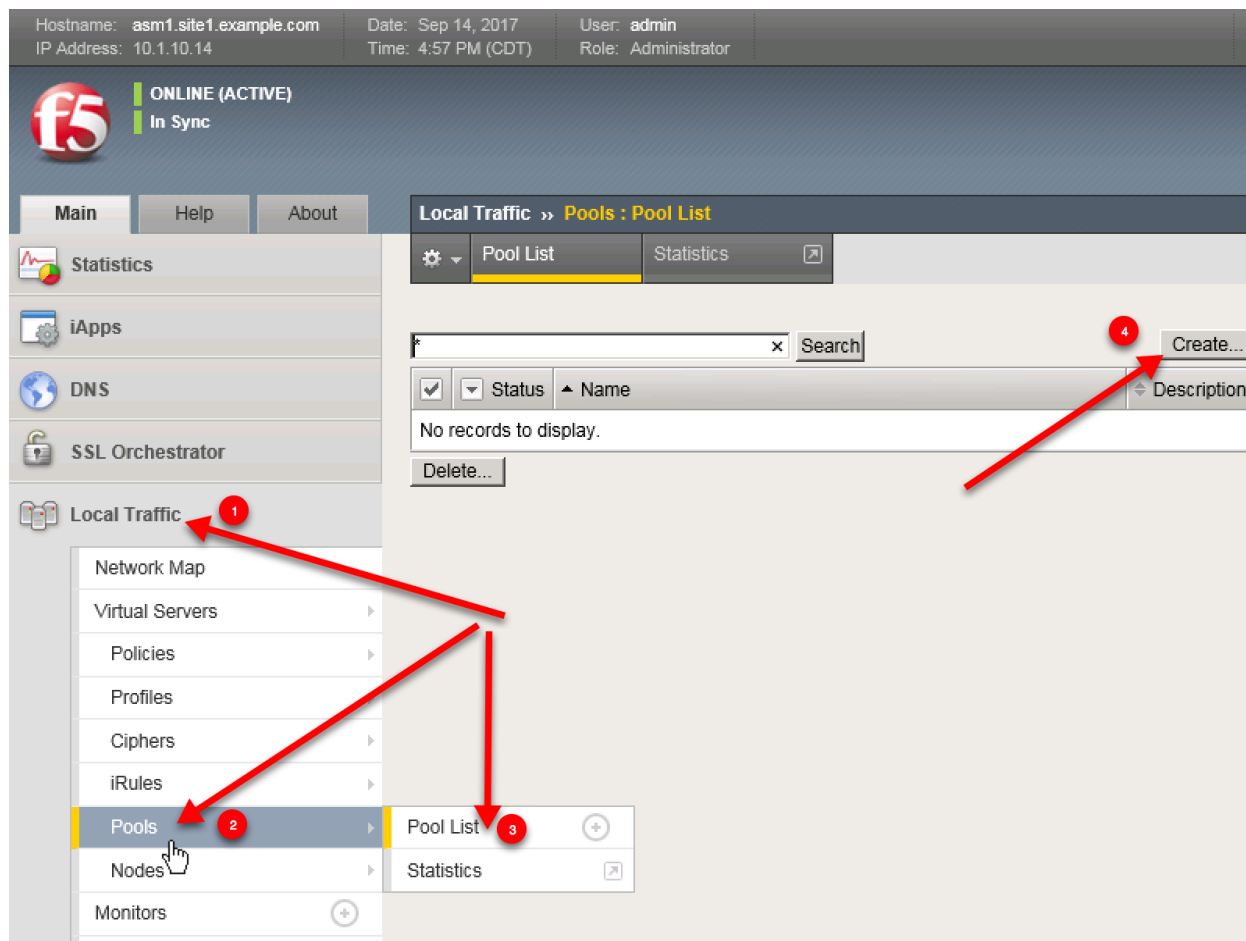
<https://support.f5.com/csp/article/K13397>

1.1.3.5 Pools

Create a pool with a single member

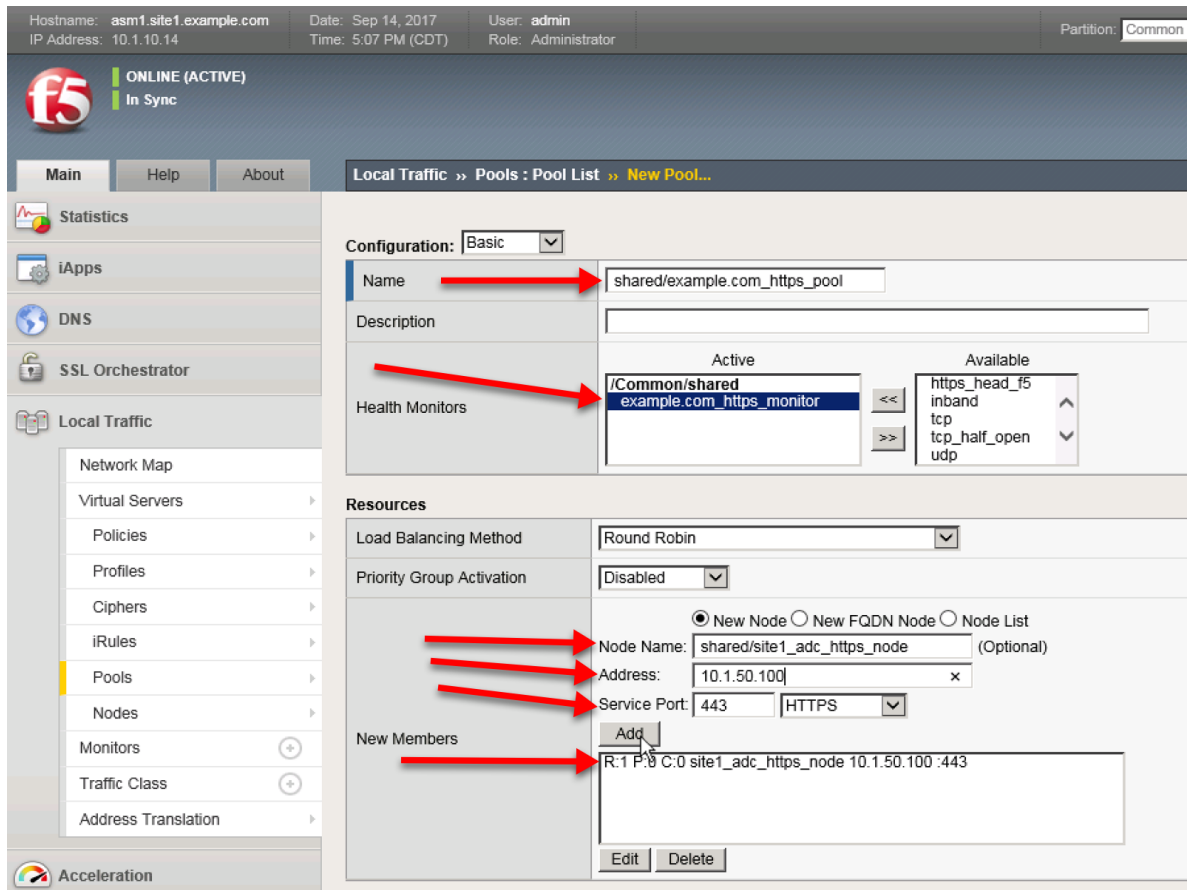
Navigate to: **Local Traffic » Pools : Pool List**

<https://asm1.site1.example.com/tmui/Control/jspmap/tmui/local/pool/create.jsp>



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

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



TMSH command for asm1.site1

TMSH

```
tmsh create ltm pool shared/site1_adc_https_pool monitor shared/example.com_https_monitor members add { shared/site1_adc_https_node:443 { address 10.1.50.100 } }
```

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

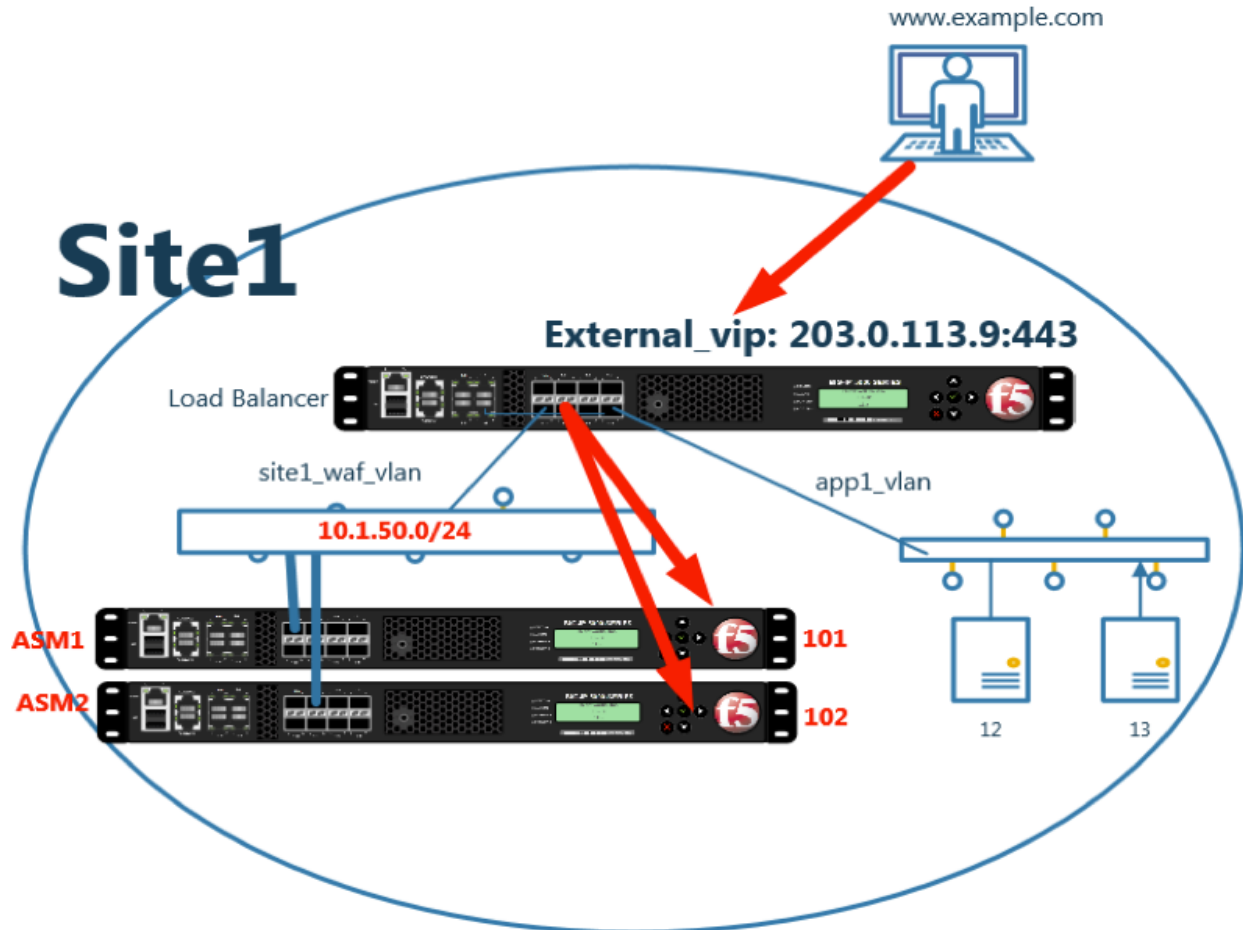
Setting	Value
Name	shared/site2_adc_https_pool
Health Monitors	shared/example.com_https_monitor
New Members	Node Name: shared/site2_adc_https_node
New Members	Address: 10.1.60.100
Service Port	443

TMSH command for asm1.site1

TMSH

```
tmsh create ltm pool shared/site2_adc_https_pool monitor shared/example.com_https_monitor members add { shared/site2_adc_https_node:443 { address 10.1.60.100 } }
```

1.1.4 Virtuals



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

Navigate to: **Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server**

Main | **Help** | **About** | **Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...**

General Properties

Name	waf1_virtual
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.1.50.101
Service Port	443 HTTPS
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

Configuration: Advanced

Protocol	TCP
Protocol Profile (Client)	example.com_tcp_profile
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	example.com_http_profile
HTTP Proxy Connect Profile	None
Traffic Acceleration Profile	None
FTP Profile	None
RTSP Profile	None
SOCKS Profile	None
Stream Profile	None
XML Profile	None
MQTT	<input type="checkbox"/>

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

1. asm1.site1

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

TMSH command for asm1.site1:

```
tmsh create ltm virtual site1_waf1_virtual { destination 10.1.50.101:https ip-
↪protocol tcp profiles add { clientssl { context clientside } serverssl {
↪context serverside } shared/example.com_http_profile { } shared/example.com_tcp_
↪profile { } } source-address-translation { type automap } security-log-profiles_
↪add { "Log all requests" } pool shared/site1_adc_https_pool }
```

2. asm2.site1

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

TMSH command for asm2.site1:

```
tmsh create ltm virtual site1_waf2_virtual { destination 10.1.50.102:https ip-
↪protocol tcp profiles add { clientssl { context clientside } serverssl {
↪context serverside } shared/example.com_http_profile { } shared/example.com_tcp_
↪profile { } } source-address-translation { type automap } security-log-profiles_
↪add { "Log all requests" } pool shared/site1_adc_https_pool }
```

3. asm1.site2

Setting	Value
Name	site2_waf1_virtual
Destination Address/Mask	10.1.60.101
Service Port	443
Protocol Profile (Client)	shared/example.com_tcp_profile
HTTP Profile	shared/example.com_http_profile
SSL Profile (Client)	clientssl
SSL Profile (Server)	serverssl
Source Address Translation	Auto Map
Default Pool	pool shared/site2_adc_https_pool

TMSH command for asm1.site2:

```
tmsh create ltm virtual site2_waf1_virtual { destination 10.1.60.101:https ip-
↪protocol tcp profiles add { clientssl { context clientside } serverssl {
↪context serverside } shared/example.com_http_profile { } shared/example.com_tcp_
↪profile { } } source-address-translation { type automap } security-log-profiles_
↪add { "Log all requests" } pool shared/site2_adc_https_pool }
```

4. asm2.site2

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

TMSH command for asm2.site2:

```
tmsm create ltm virtual site2_waf2_virtual { destination 10.1.60.102:https ip-
→protocol tcp profiles add { clientssl { context clientside } serverssl {
→context serverside } shared/example.com_http_profile { } shared/example.com_tcp_
→profile { } } source-address-translation { type automap } security-log-profiles_
→add { "Log all requests" } pool shared/site2_adc_https_pool }
```

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

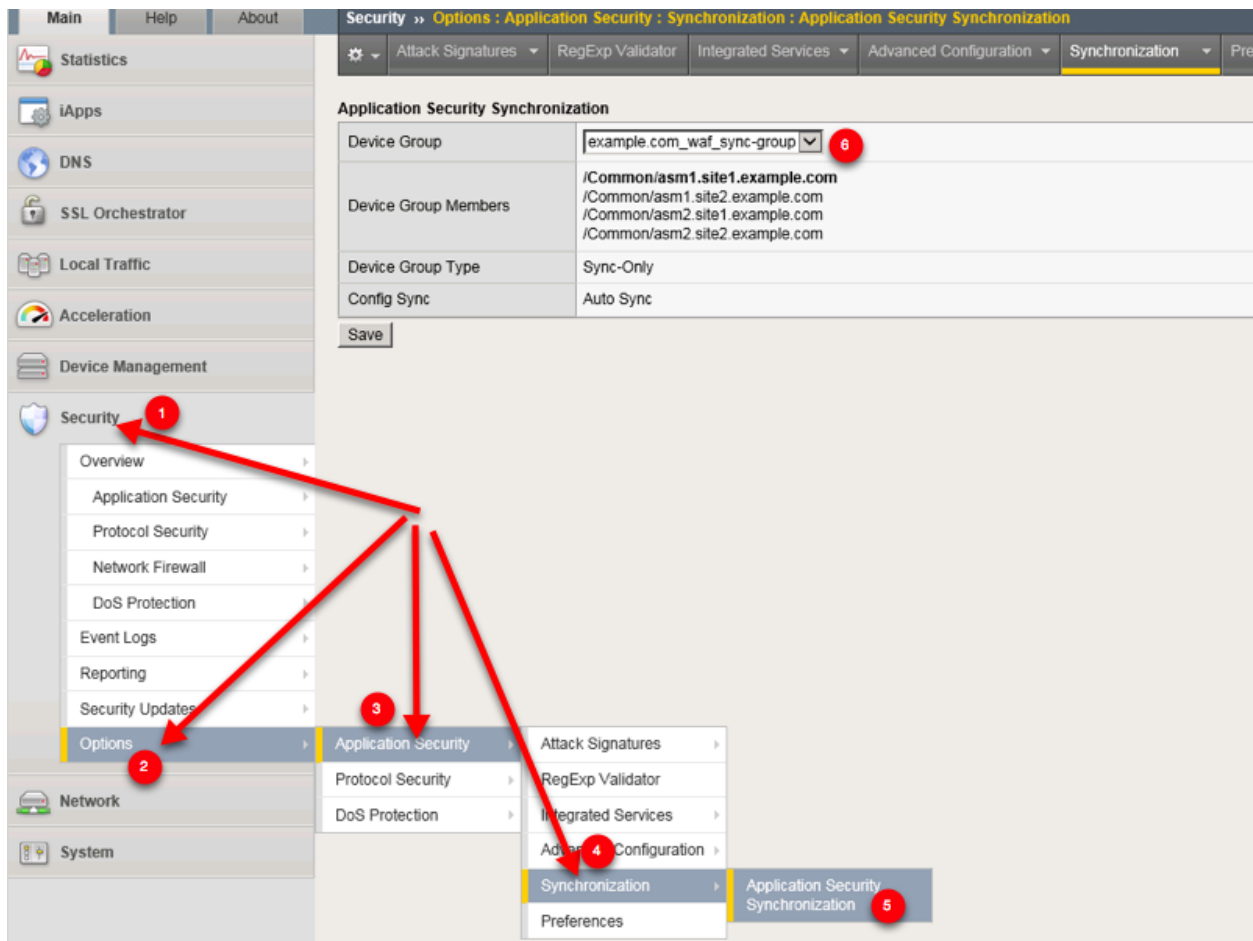
1.1.5 Security Policy

1.1.5.1 Sync

Configure global policy synchronization on asam1..site1 only

Navigate to: **Security » Options : Application Security : Synchronization : Application Security Synchronization**

Modify “Device Group” to enable “example.com_waf_sync-group”



1.1.5.2 Parent Child

Finally... Let's create a policy.

Navigate to: **Security » Application Security : Security Policies : Policies List**

Create a parent policy according to the following table

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

Main | **Help** | **About** | **Security >> Application Security : Security Policies : Policies List**

Statistics | **iApps** | **DNS** | **SSL Orchestrator** | **Local Traffic** | **Acceleration** | **Device Management** | **Security**

Policy Name Partition: Common

Description

Policy Type

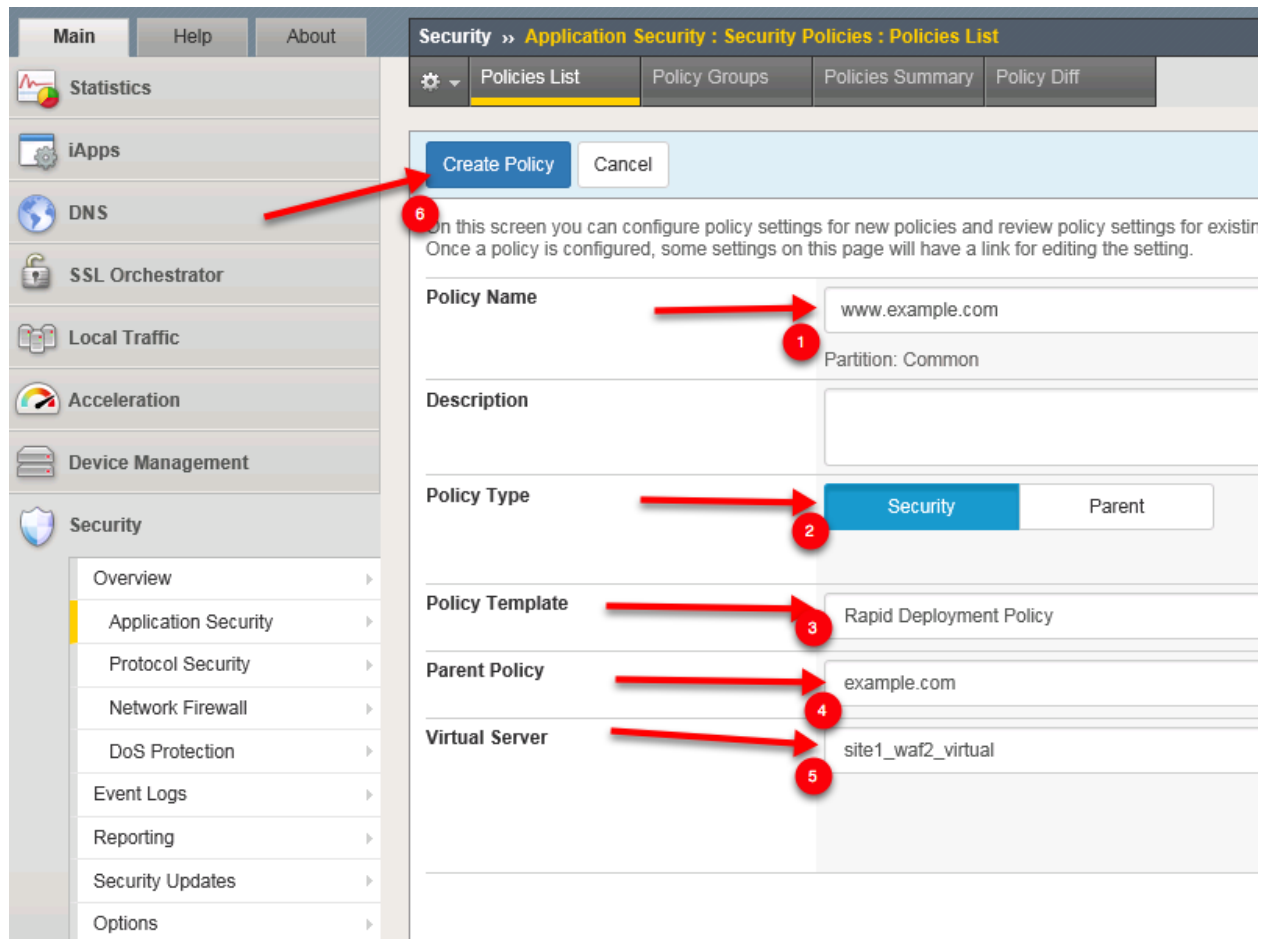
Policy Template

On this screen you can configure policy settings for new policies and review policy settings for existing policies. Once a policy is configured, some settings on this page will have a link for editing the setting.

https://asm1.site1.example.com/dms/policy/policies_ng.php?create_policy=1

Create a child policy according to the following table

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



1.1.5.3 Associate Policy

Log into asm2.site1 asm1.site2 and asm2.site2 and associate the security policy to the VIPS.

Navigate to: **Local Traffic >> Virtual Servers : Virtual Server List >> site1_waf2_virtual**

Click Security and set "Application Security Policy" "Enabled" "www.example.com"

Repeat steps for all ASM devices.

Hostname: asm1.site1.example.com Date: Sep 14, 2017 User: admin
IP Address: 10.1.10.14 Time: 10:10 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
In Sync

Main Help About

Local Traffic » Virtual Servers : Virtual Server List » **site1_waf1_virtual**

Statistics iApps DNS SSL Orchestrator Local Traffic

Network Map Virtual Servers Policies Profiles Ciphers iRules Pools Nodes Monitors

Policy Settings

Destination	10.1.50.101:443
Service	HTTPS
Application Security Policy	Enabled... Policy: www.example.com
Service Policy	None
IP Intelligence	Disabled
DoS Protection Profile	Disabled
Log Profile	<div> <div>Enabled...</div> <div> <div>Selected</div> <div>Available</div> </div> </div> <div> <div>/Common</div> <div>Log all requests</div> </div> <div> <div><<</div> <div>>></div> </div> <div> <div>/Common</div> <div>Log illegal requests</div> <div>global-network</div> <div>local-dos</div> </div>

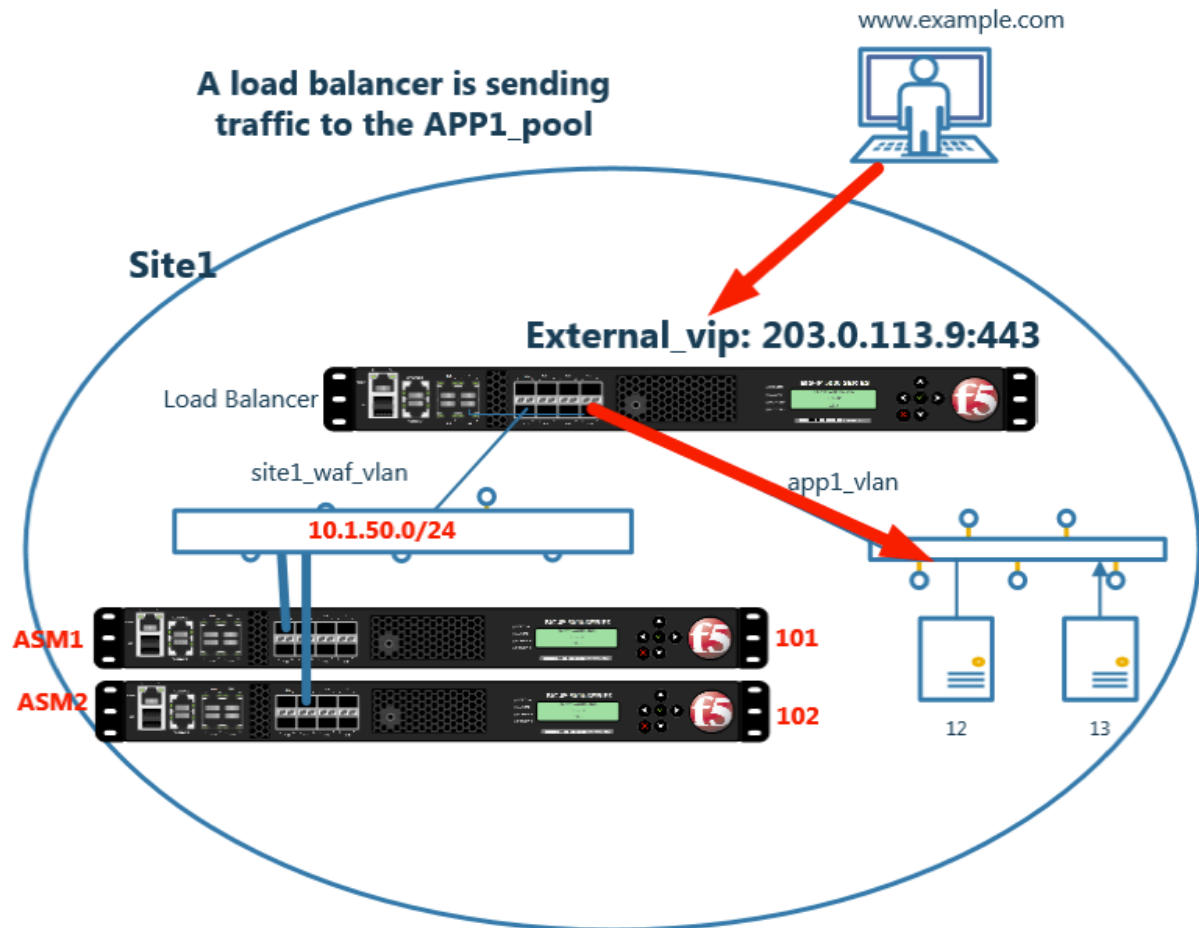
Update

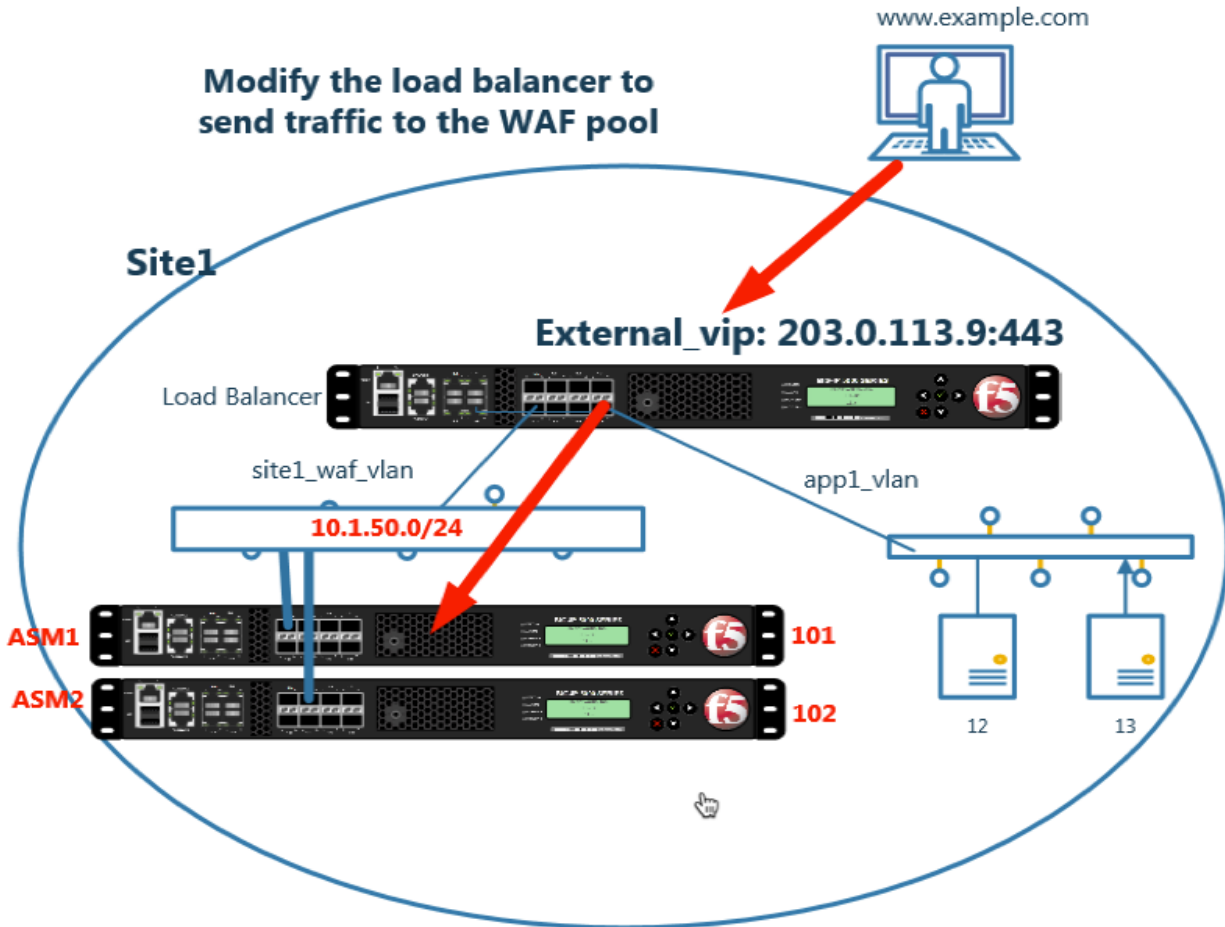
https://asm2.site1.example.com/tmui/Control/jspmap/tmui/local/virtual_server/security.jsp?name=/Common/site1_waf2_virtual

https://asm1.site2.example.com/tmui/Control/jspmap/tmui/local/virtual_server/security.jsp?name=/Common/site2_waf1_virtual

https://asm2.site2.example.com/tmui/Control/jspmap/tmui/local/virtual_server/security.jsp?name=/Common/site2_waf2_virtual

1.1.6 Cut-Over



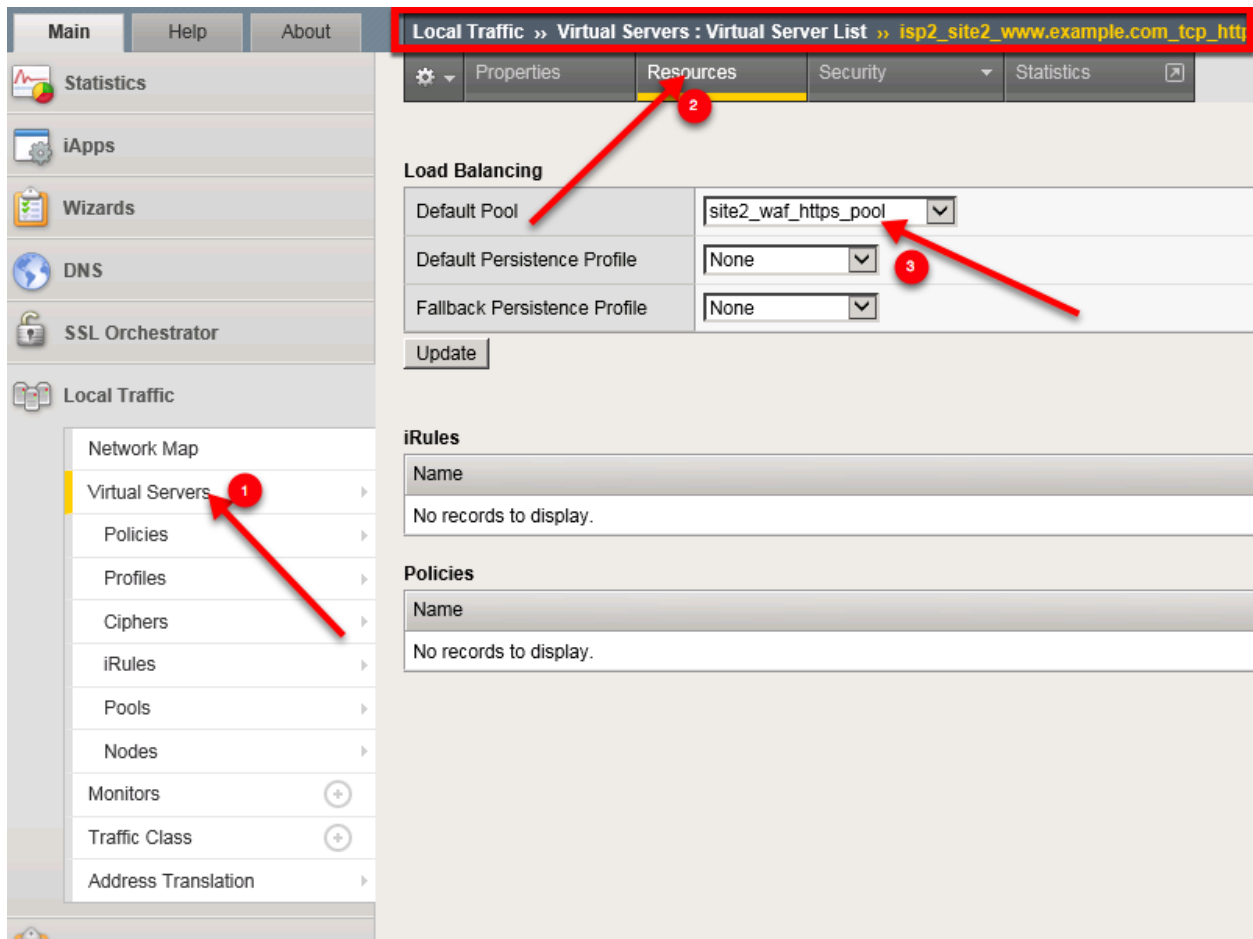


Change the ADC load balancing configuration so that traffic goes through the WAF before the application server.

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

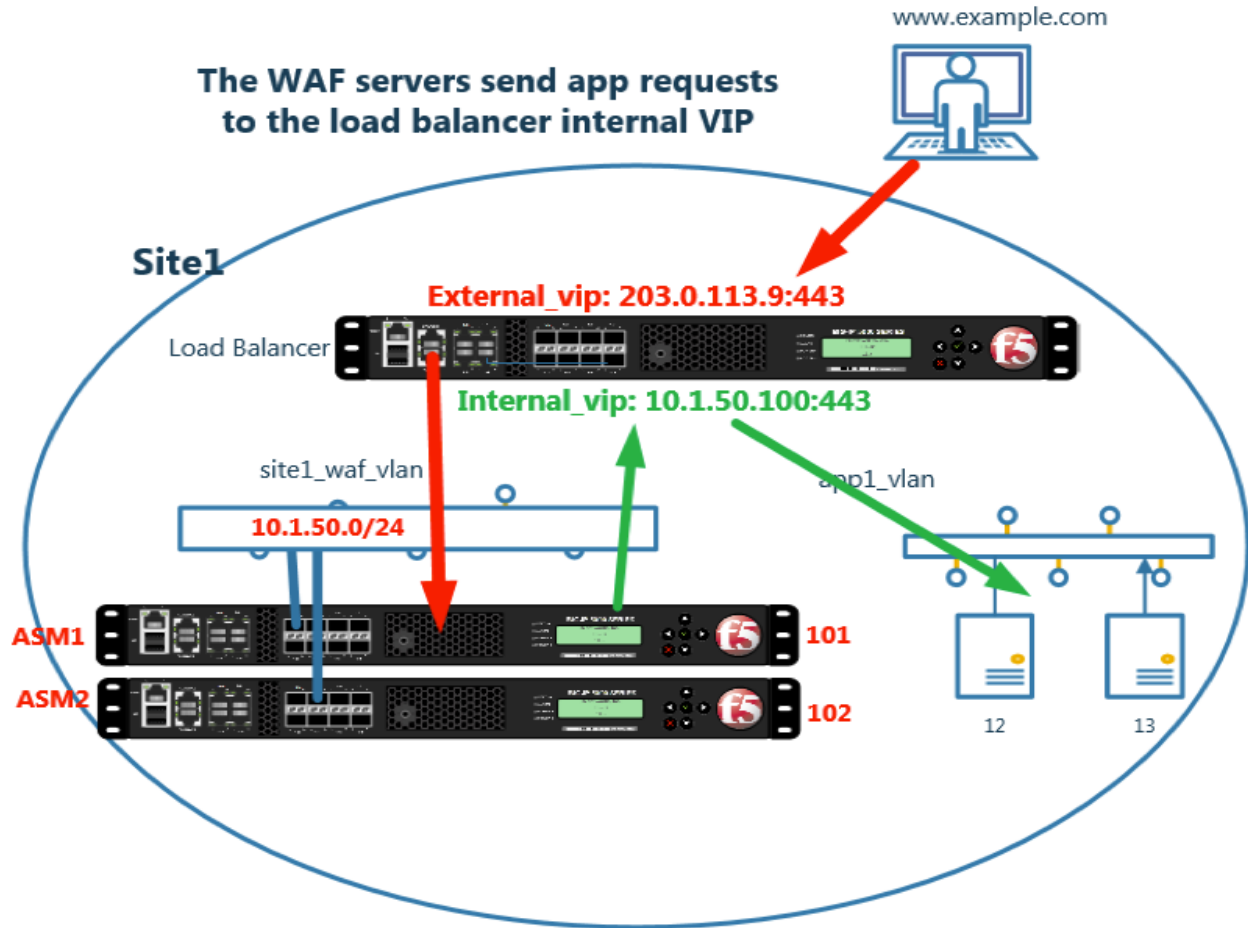
Navigate to: **Local Traffic » Virtual Servers : Virtual Server List » isp2_site2_www.example.com_tcp_https_virtual**

Select "Resources" and associate the "site1_waf_https_pool"



https://bigip1.site1.example.com/tmui/Control/jspmap/tmui/locallb/virtual_server/properties.jsp?name=/Common/isp1_site1_www.example.com_tcp_https_virtual

https://bigip1.site2.example.com/tmui/Control/jspmap/tmui/locallb/virtual_server/properties.jsp?name=/Common/isp2_site2_www.example.com_tcp_https_virtual



1.2 Policy Tuning

WAF policies and

Four dedicated WAF instances are deployed across two datacenters.

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

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

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

1.3 Hack and Defend

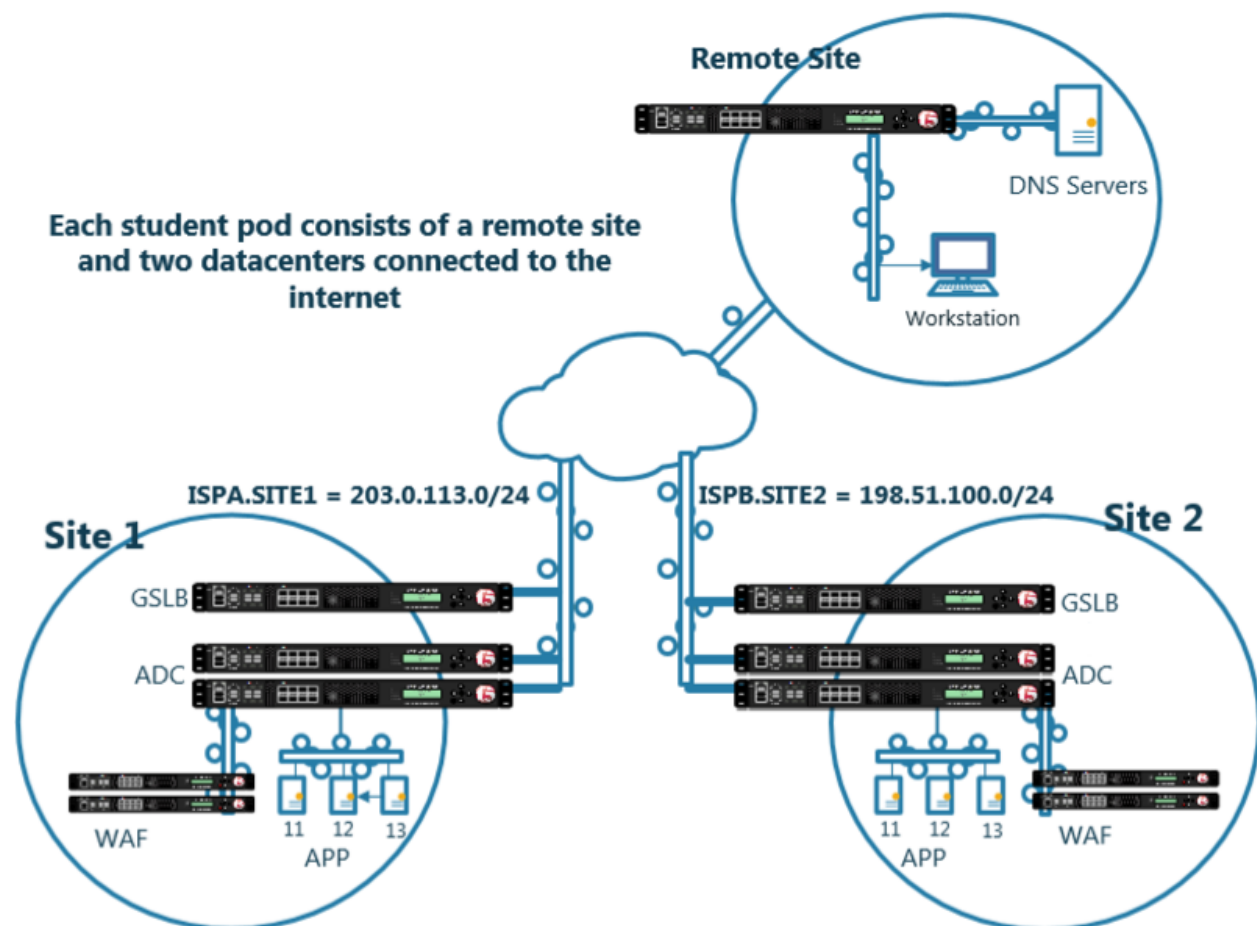
Four dedicated WAF instances are deployed across two datacenters.

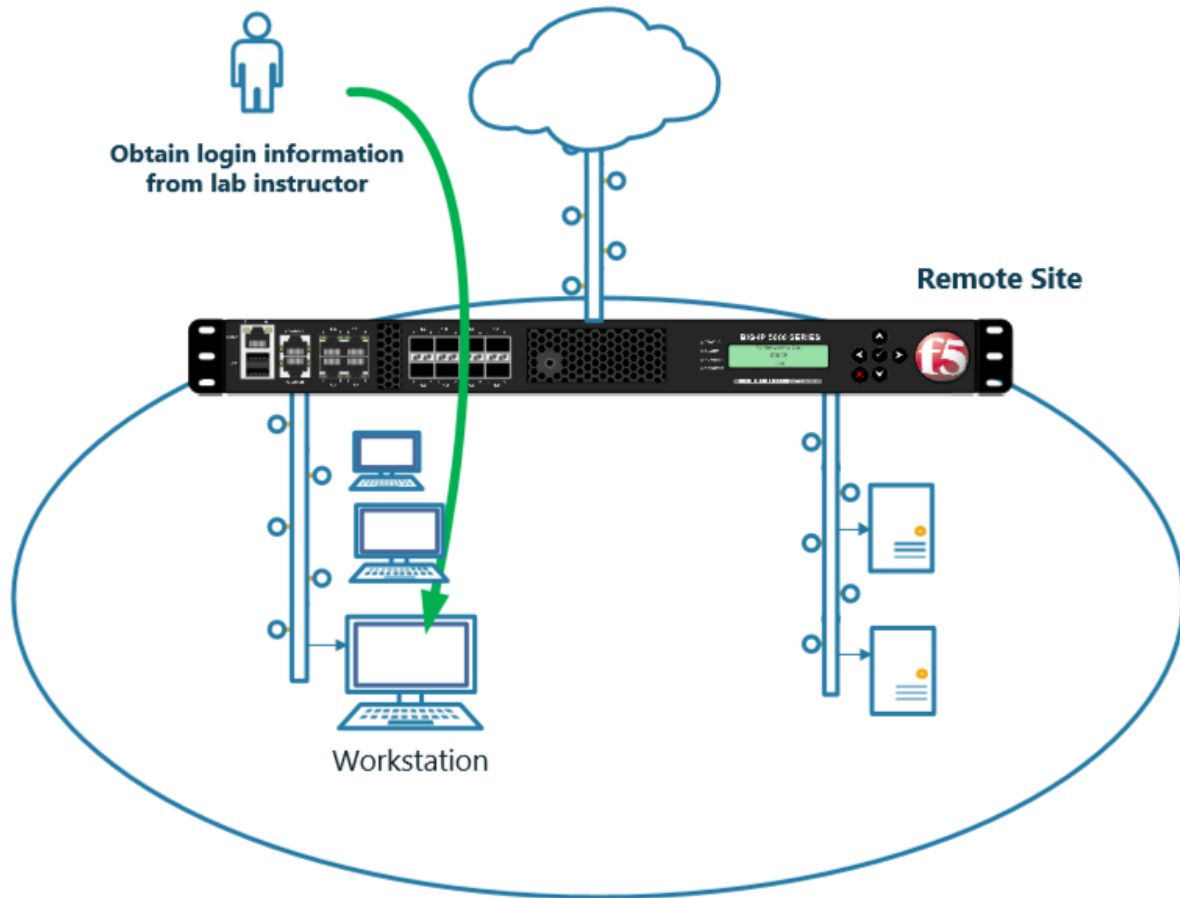
Each WAF device has already been licensed, and a base configuration including hostname, and DNS settings.

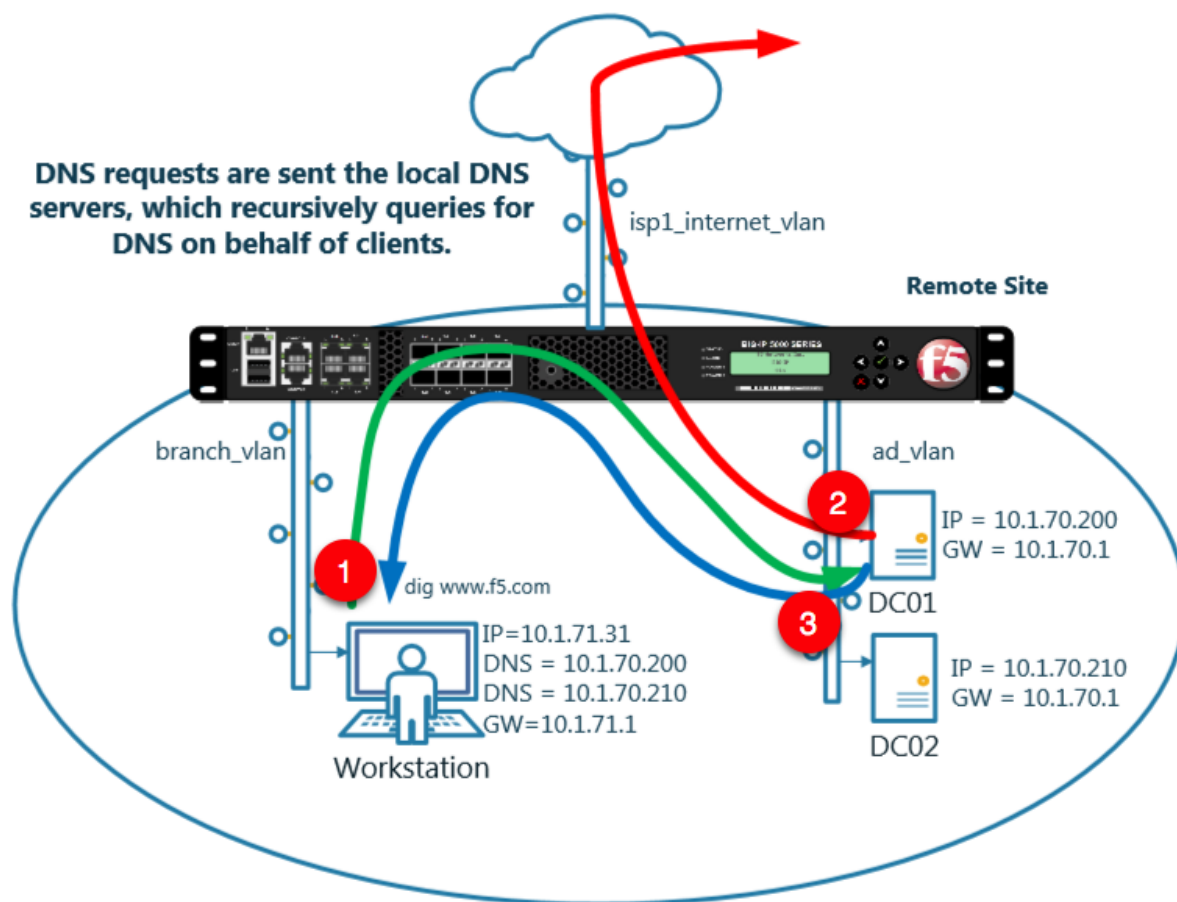
The dedicated WAF instances will be load balanced by the HA pair of F5 LTM's.

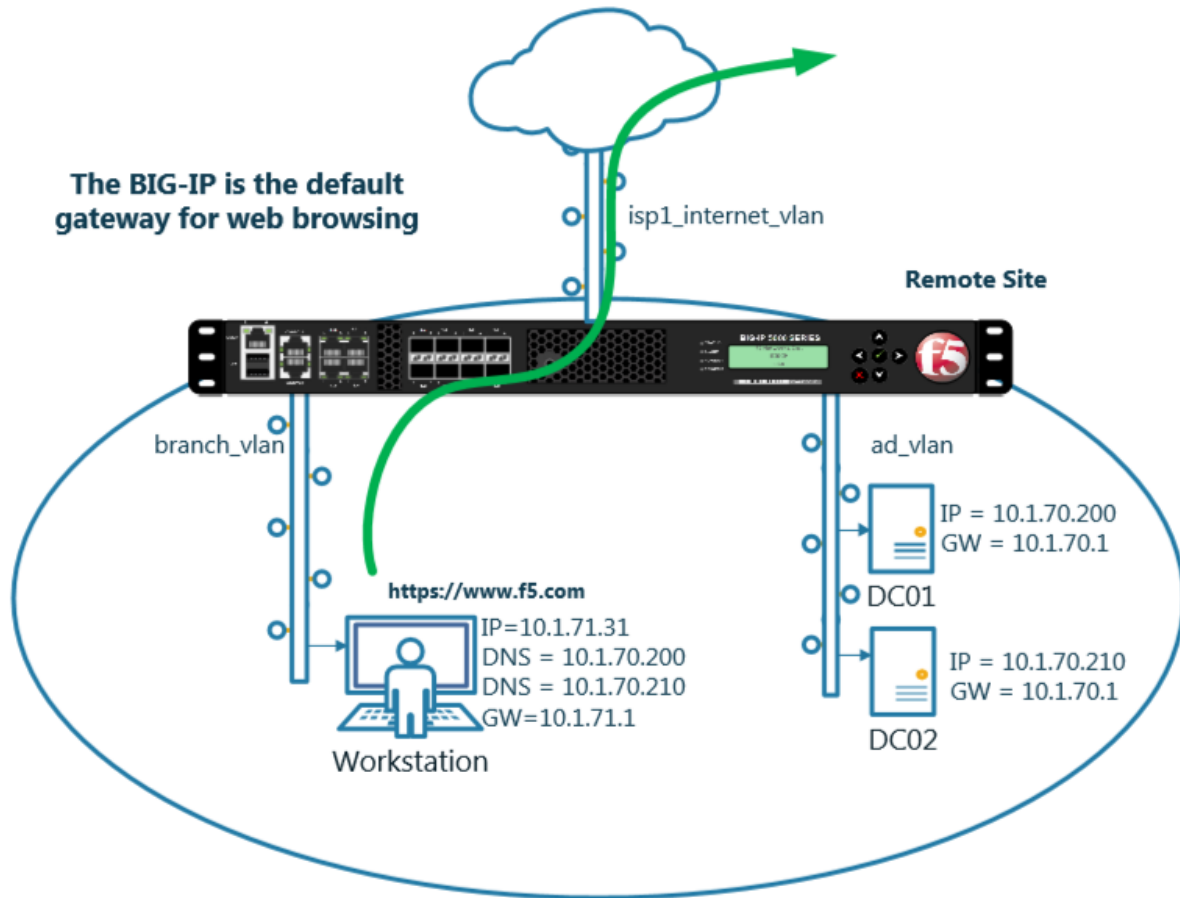
2.1 Availability

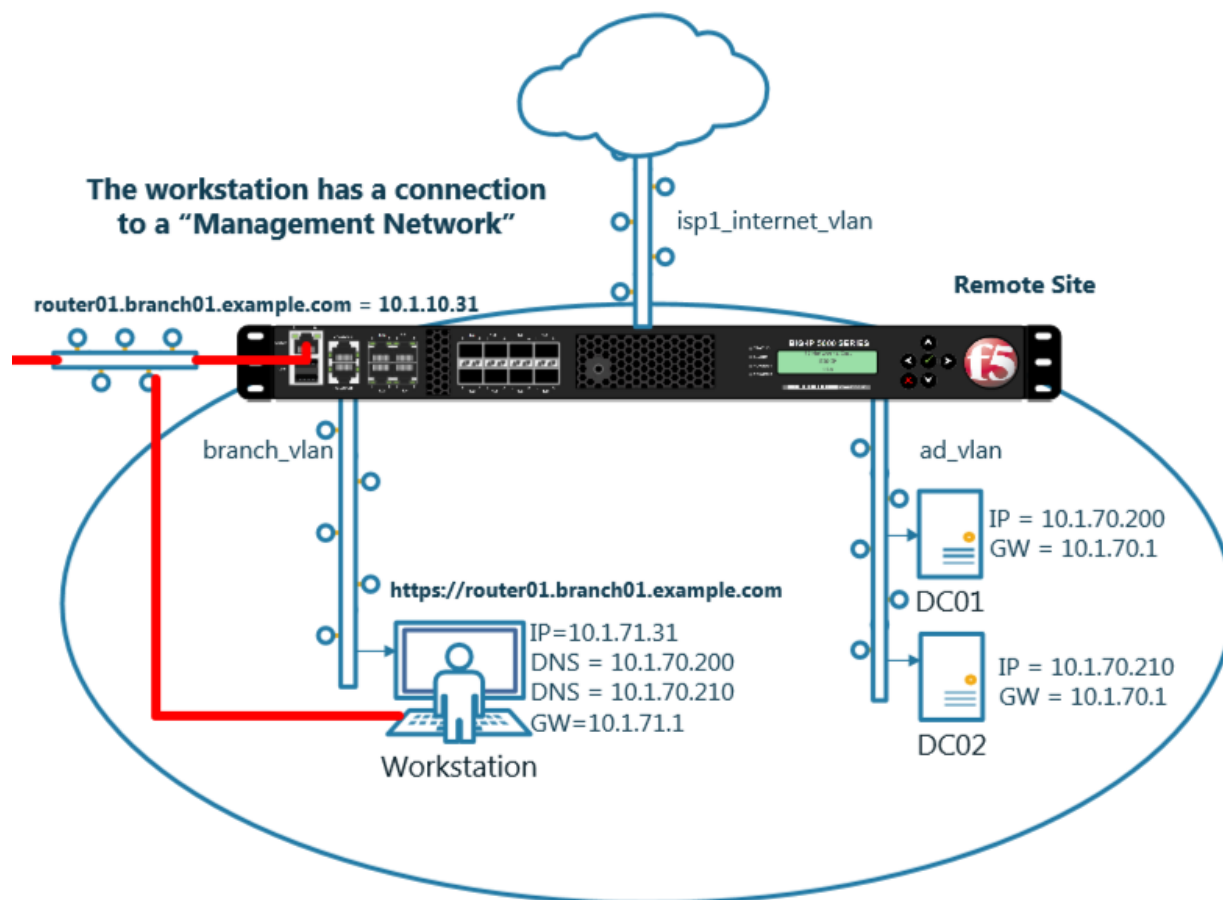
2.1.1 Network Map

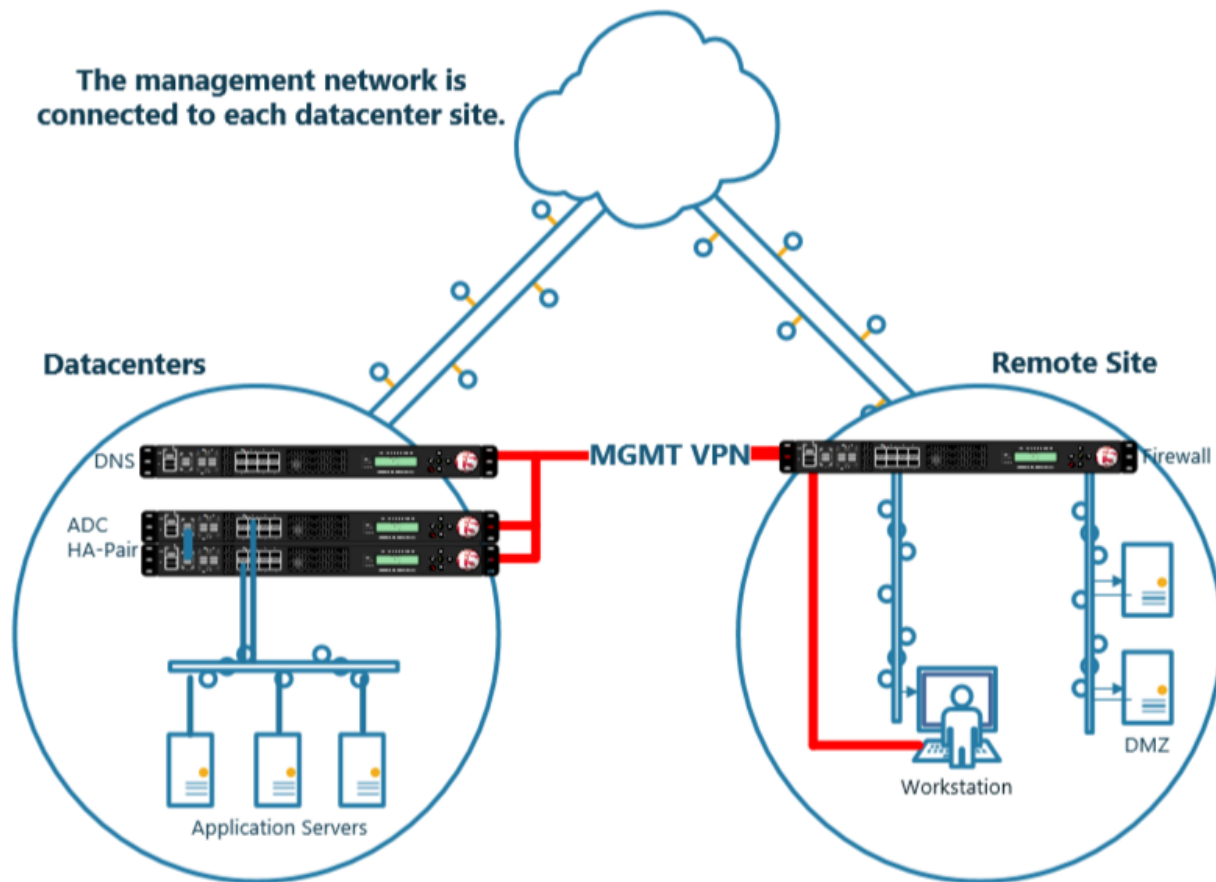










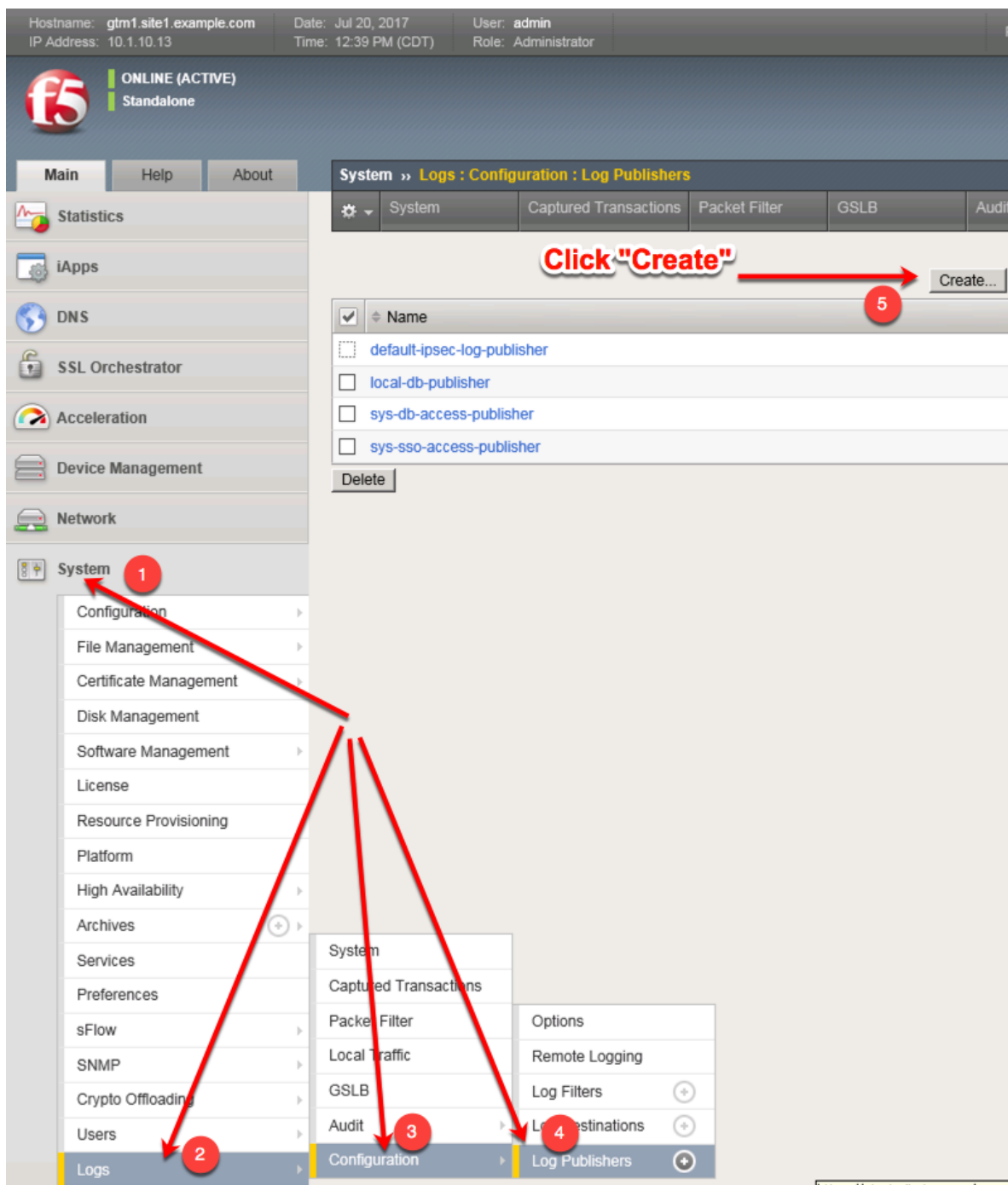


2.1.2 System

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

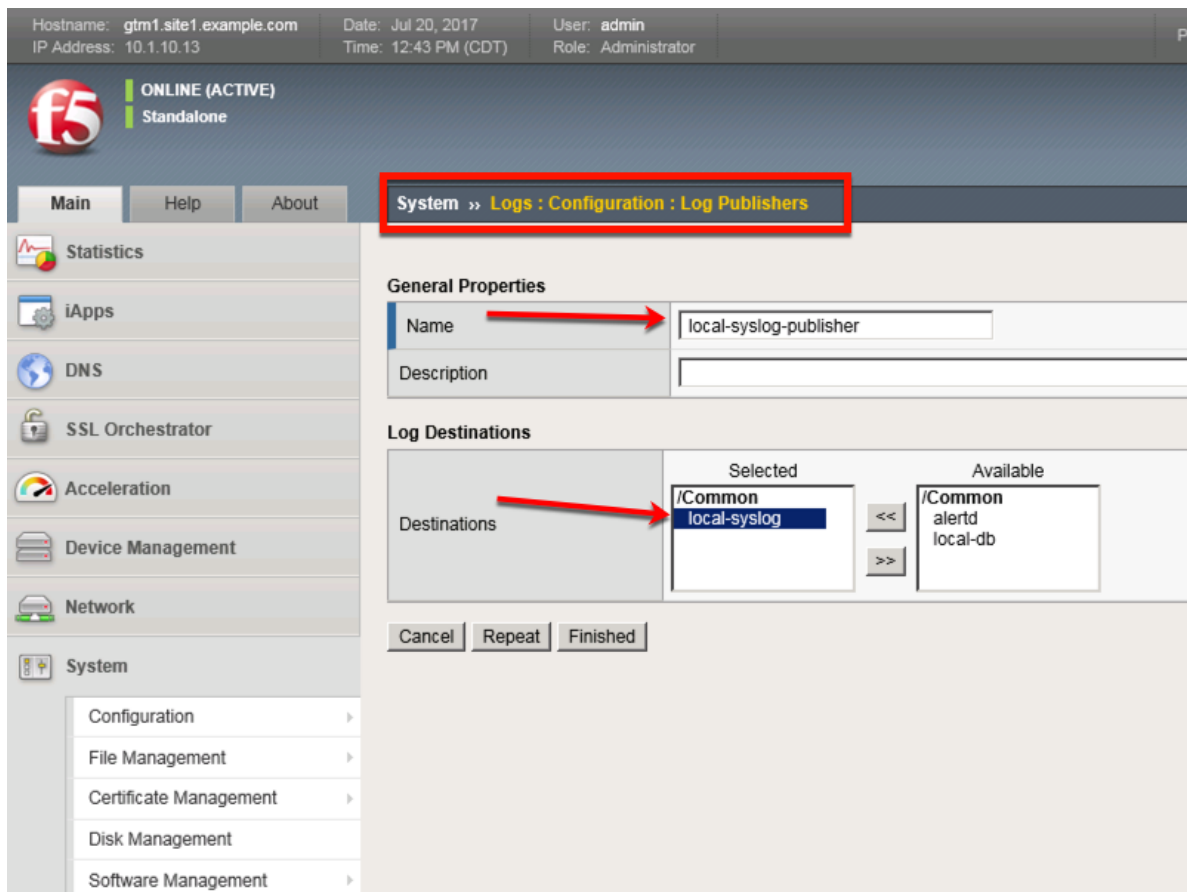
1. Create a “Log Publisher”

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



Create a local syslog publisher according to the table below:

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



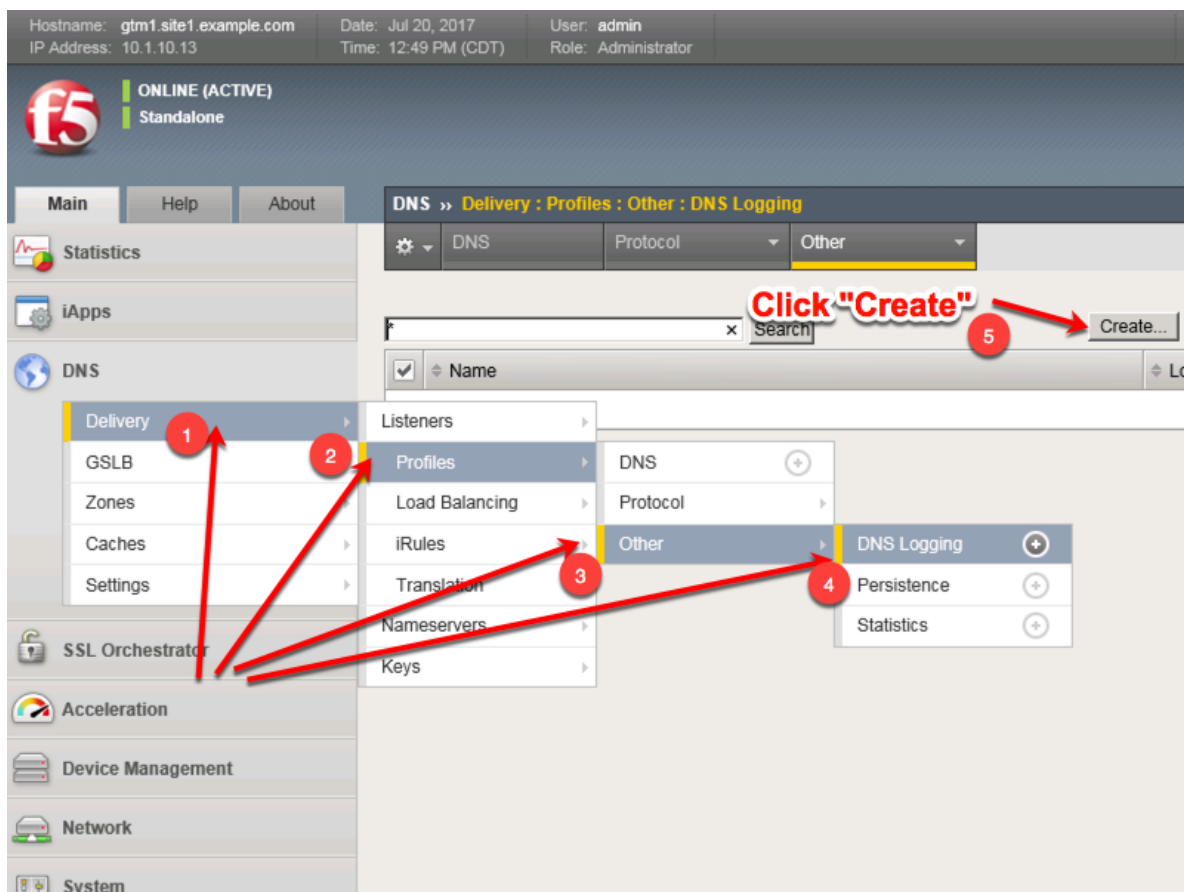
TMSH command for both gtm1.site1 and gtm1.site2:

TMSH

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

2. Create a "Logging Profile"

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



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

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

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

ONLINE (ACTIVE)
Standalone

Main Help About

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

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

General Properties

Name example_dns_logging_profile
Description

Configuration

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

Log Fields

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

Cancel Repeat Finished

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

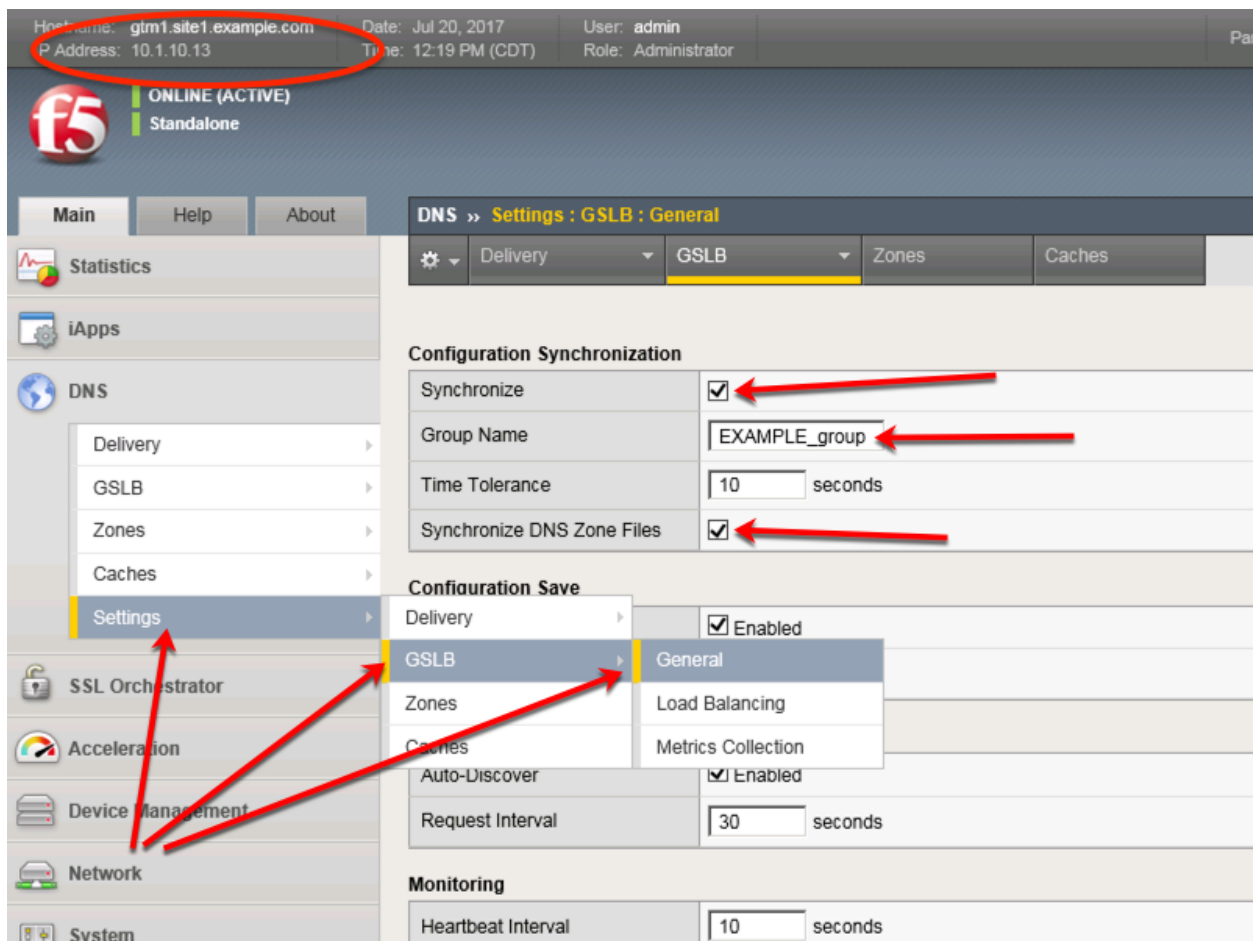
TMSH

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

2.1.3 Settings

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

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



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

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

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

TMSH

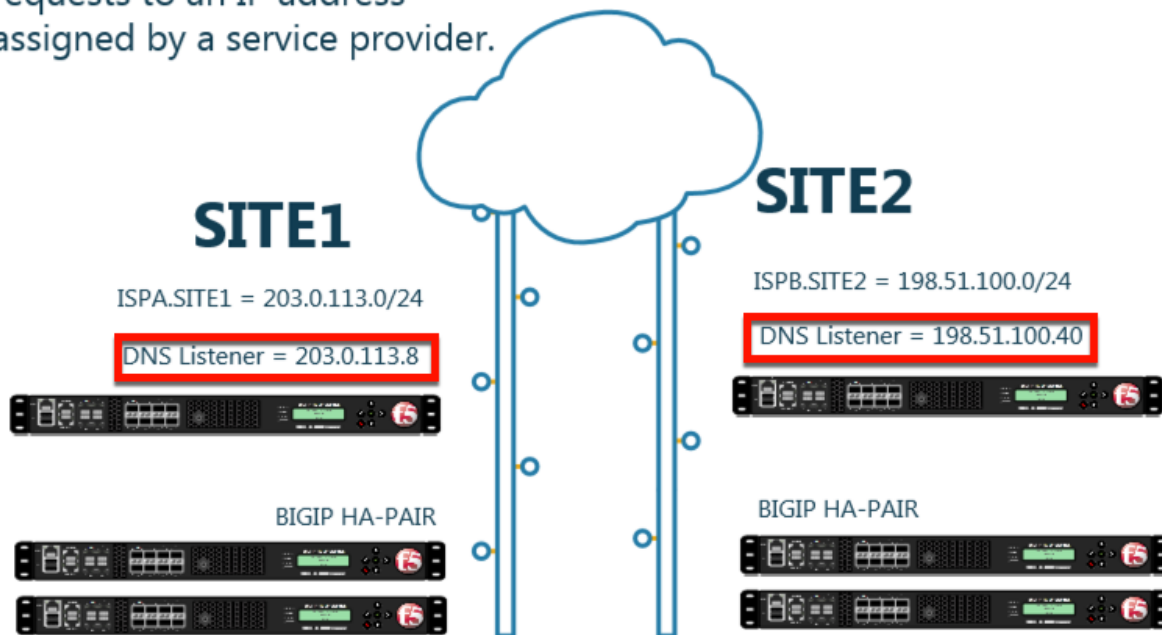
```
tmsh modify gtm global-settings general synchronization yes synchronization-group-name EXAM-
PLE_group synchronize-zone-files yes
```

2.1.4 Listeners

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

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

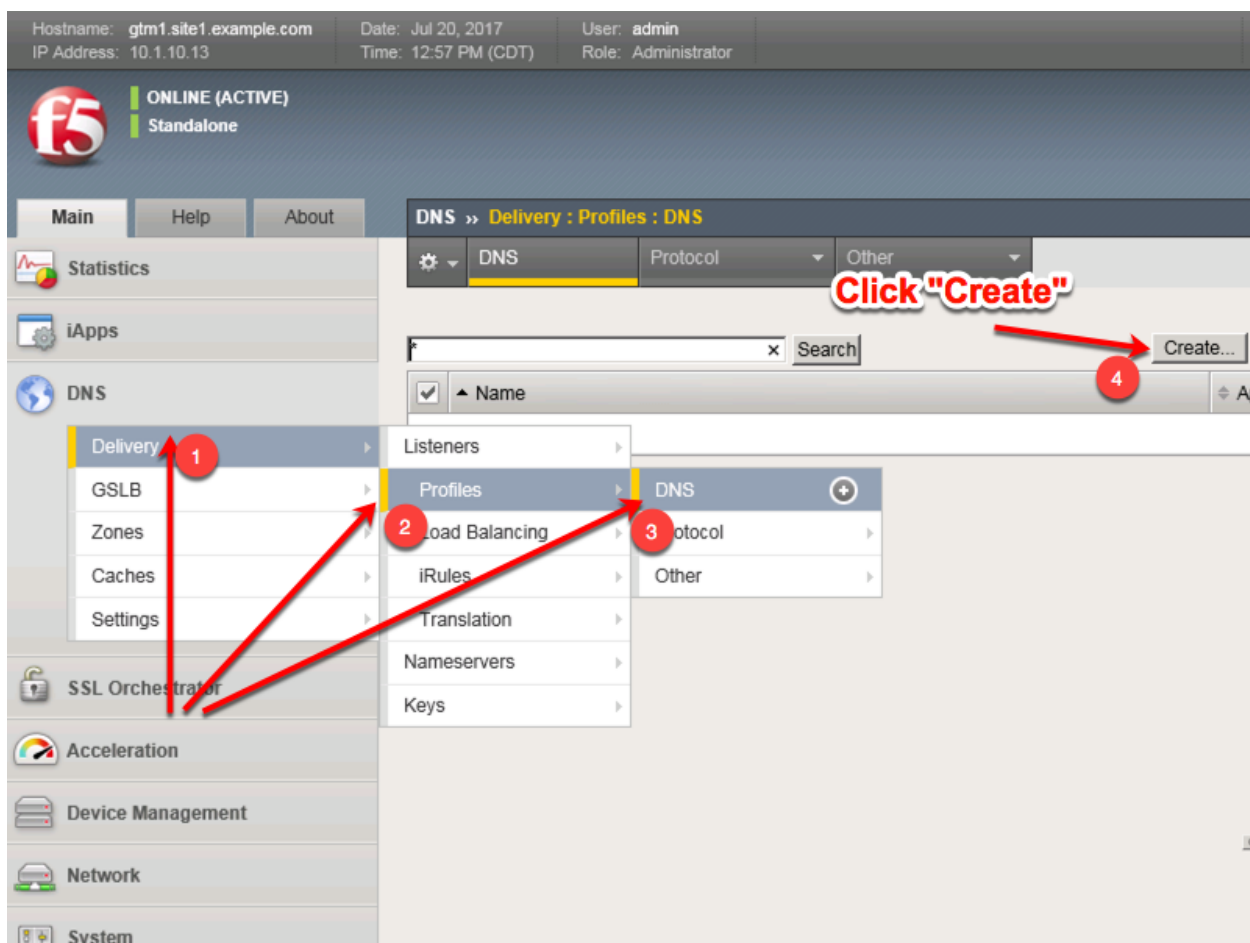
A listener will receive DNS requests to an IP address assigned by a service provider.



2.1.4.1 DNS Profile

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

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



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

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

The screenshot displays the 'Properties' page for a DNS profile named 'example.com_dns_profile'. The left sidebar shows the navigation menu with 'DNS' selected. The main content area is divided into several sections:

- General Properties:** Name is 'example.com_dns_profile' (highlighted with a red box). Partition / Path is 'Common'. Parent Profile is 'dns'.
- Denial of Service Protection:** Custom checkbox is checked. Rapid Response Mode is 'Disabled'. Rapid Response Last Action is 'Drop'.
- Hardware Acceleration:** Protocol Validation is 'Disabled'. Response Cache is 'Disabled'.
- DNS Features:**
 - DNSSEC: 'Disabled' (highlighted with a red box and arrow).
 - GSLB: 'Enabled'.
 - DNS Express: 'Disabled' (highlighted with a red box and arrow).
 - DNS Cache: 'Disabled'.
 - DNS Cache Name: 'Select...'.
 - DNS IPv6 to IPv4: 'Disabled'.
 - Unhandled Query Actions: 'Drop' (highlighted with a red box and arrow).
 - Use BIND Server on BIG-IP: 'Disabled' (highlighted with a red box and arrow).
- DNS Traffic:**
 - Zone Transfer: 'Disabled'.
 - DNS Security: 'Disabled'.
 - DNS Security Profile Name: 'Select...'.
 - Process Recursion Desired: 'Enabled'.
- Logging and Reporting:**
 - Logging: 'Enabled' (highlighted with a red box and arrow).
 - Logging Profile: 'example_dns_logging_profile' (highlighted with a red box).
 - AVR Statistics Sample Rate: 'Enabled 1/ 1 queries sampled' (highlighted with a red box and arrow).

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

TMSH

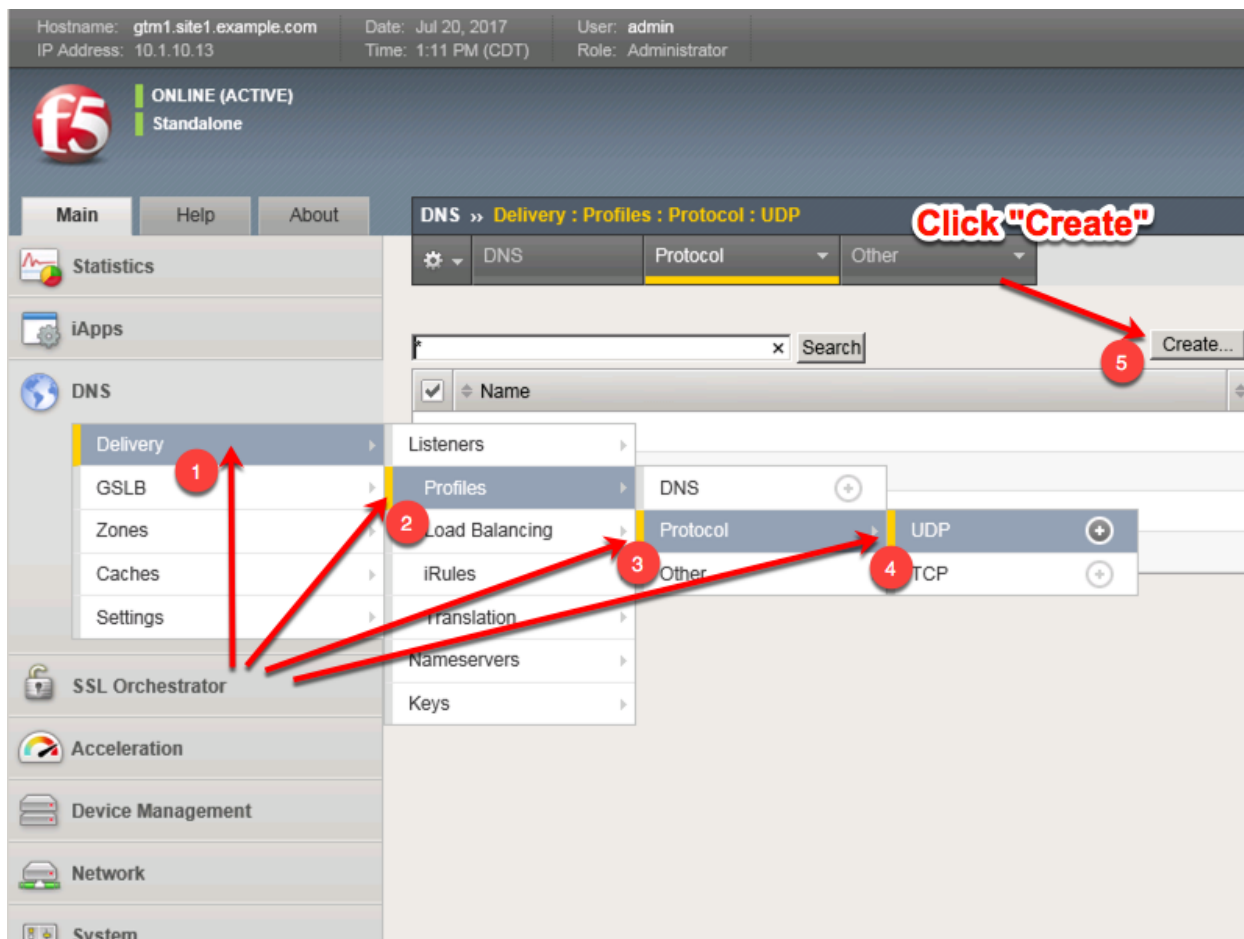
```
tmsl create ltm profile dns example.com_dns_profile use-local-bind no unhandled-query-action drop log-profile example_dns_logging_profile enable-logging yes avr-dnsstat-sample-rate 1 enable-dns-express no enable-dnssec no
```

2.1.4.2 UDP Profile

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

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

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



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

Field	Value
Name	example.com_udp-dns_profile
Parent Profile	udp_gtm_dns

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

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

Name
Parent Profile

Settings Custom ☐

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

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

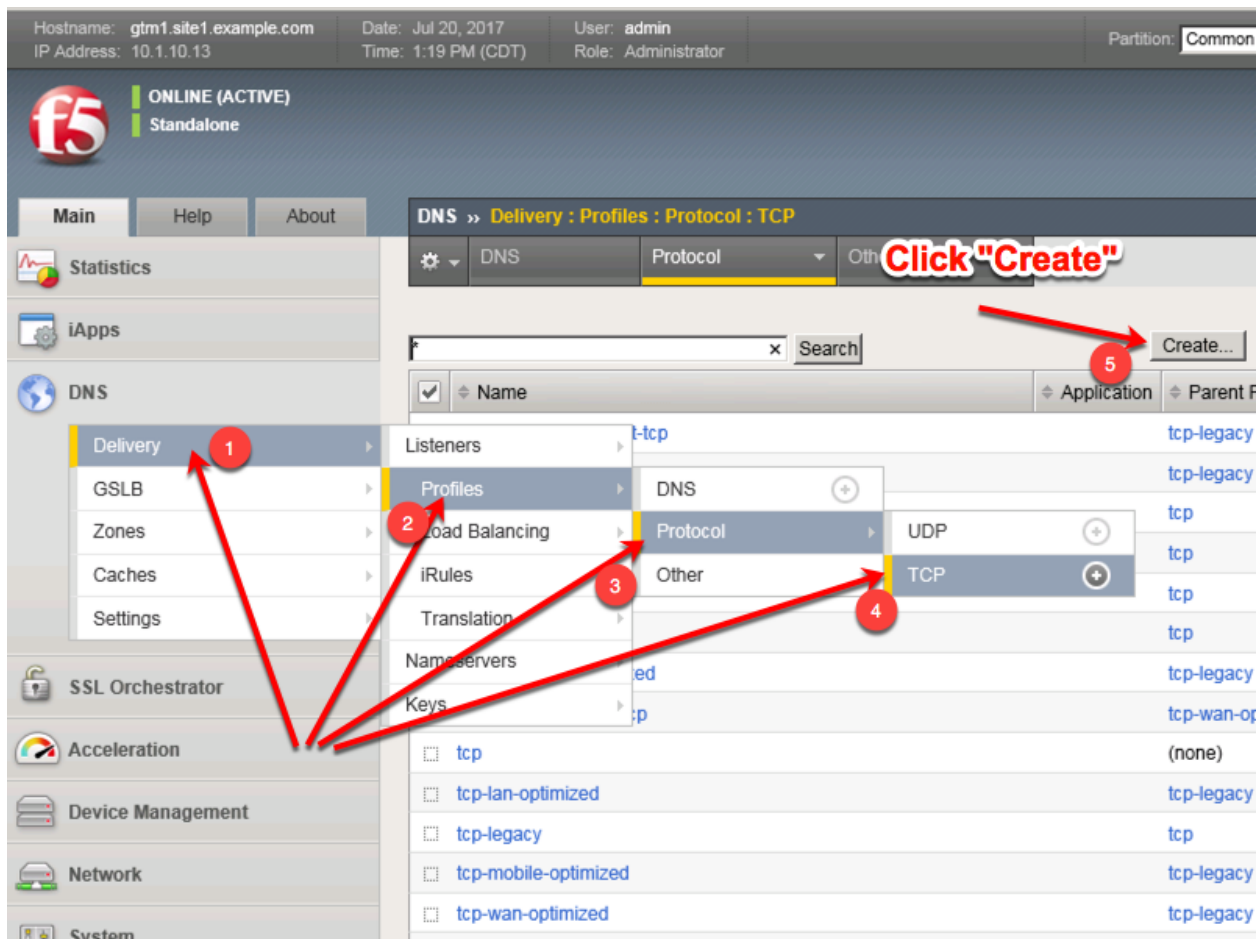
TMSH

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

2.1.4.3 TCP Profile

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

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



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

Field	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-dns_profile**
Parent Profile **f5-tcp-wan**

Timer Management

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

Scroll way down to find the "Finish" button

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

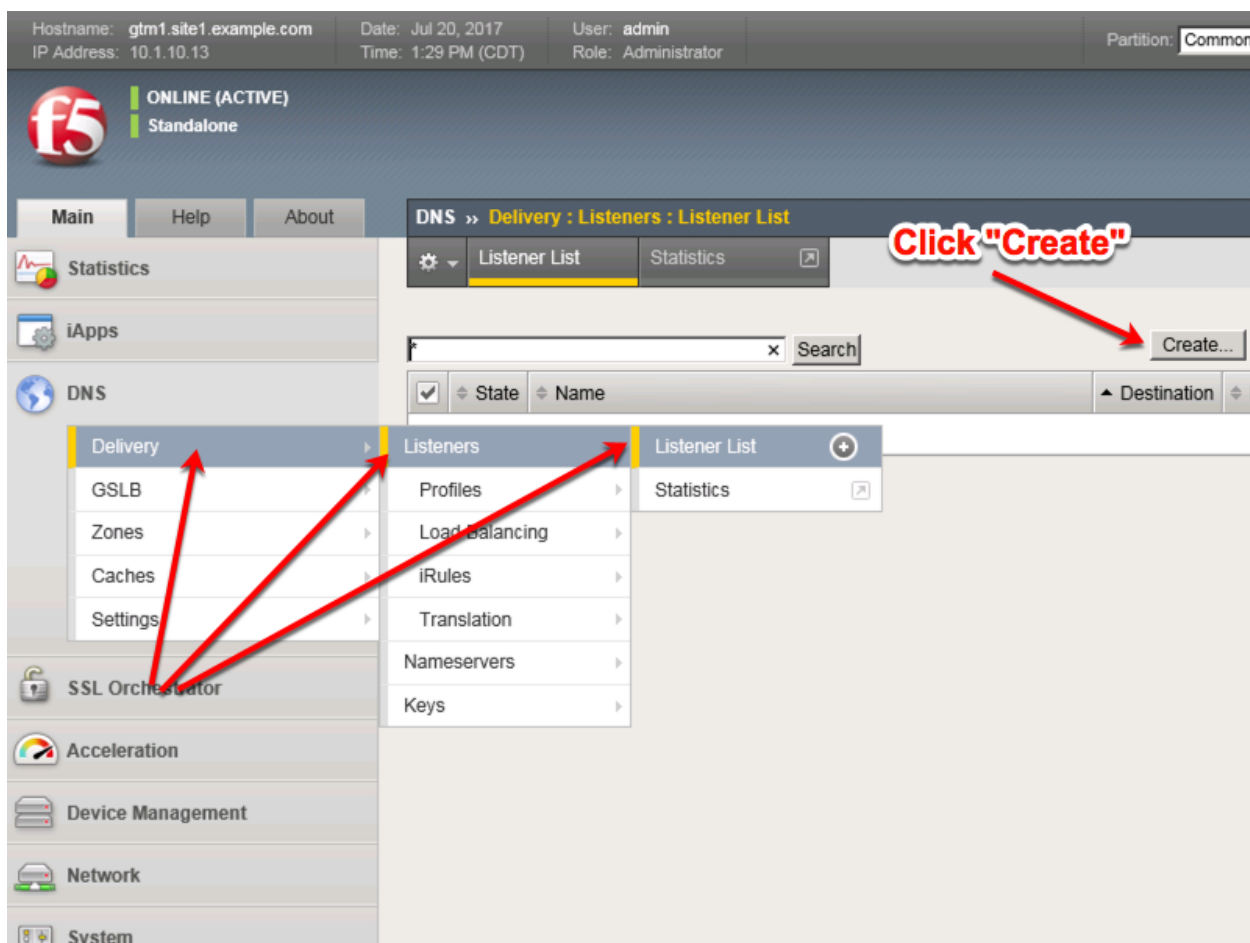
TMSH

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

2.1.4.4 UDP IP Address

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

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



Create a UDP listener according to the following table:

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

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

Be sure to create 203.0.113.8 on gtm1.SITE1

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

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

General

Name: **isp1_site1_ns1.example.com_udp_53_virtual**
Description:
State: Enabled

Listener: Advanced

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

Service: Advanced

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

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

Hostname: **gtm1.site2.example.com** Date: Jul 20, 2017 User: admin
 IP Address: 10.1.10.23 Time: 1:32 PM (CDT) Role: Administrator Partition: Common

Be sure to create 198.51.100.40 on gtm1.SITE2

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

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

General

Name: **isp1_site2_ns2.example.com_udp_53_virtual**
 Description:
 State: Enabled

Listener: Advanced

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

Service: Advanced

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

gtm1.site1 TMSH command:

TMSH

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

gtm1.site2 TMSH command:

TMSH

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

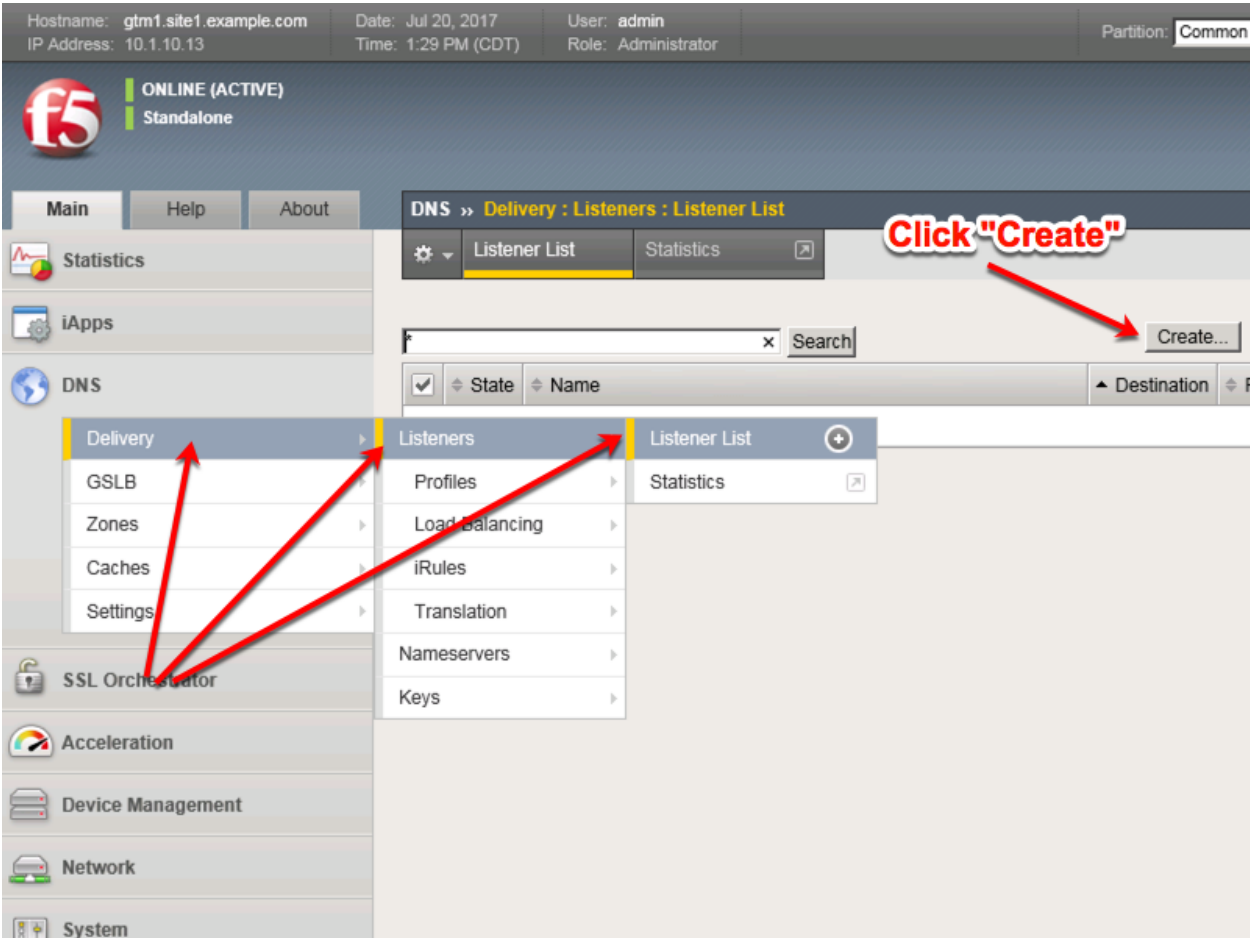
}

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

2.1.4.5 TCP IP Address

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

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



Create a TCP listener.

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

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

f5 ONLINE (ACTIVE) Standalone **Be sure to create 203.0.113.8 on gtm1.SITE1**

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

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

General

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

Listener: Advanced

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

Be sure to select "TCP"

Service: Advanced

Protocol: **TCP**
Protocol Profile (Client): example.com_tcp-dns_profile
Protocol Profile (Server): (Use Client Profile)
DNS Profile: example.com_dns_profile

Load Balancing

Default Pool: None
Default Persistence Profile: None
Fallback Persistence Profile: None

Be sure to create the 198.51.100.40 address on gtm1.site2

Hostname: **gtm1.site2.example.com** Date: Jul 20, 2017 User: admin
 IP Address: 10.1.10.23 Time: 2:18 PM (CDT) Role: Administrator Partition: Common

Be sure to create 198.51.100.40 on gtm1.SITE2

ONLINE (ACTIVE)
Standalone

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

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

General

Name: **isp1_site2_ns2.example.com_udp_53**
 Description:
 State: Enabled

Listener: Advanced

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

Be sure to select "TCP"

Service: Advanced

Protocol: **TCP**
 Protocol Profile (Client): example.com_tcp-dns_profile
 Protocol Profile (Server): (Use Client Profile)
 DNS Profile: example.com_dns_profile

Load Balancing

Default Pool: None
 Default Persistence Profile: None
 Fallback Persistence Profile: None

gtm1.site1 TMSH command:

TMSH

```
tmsl create gtm listener isp1_site1_ns1.example.com_tcp_53_virtual address 203.0.113.8 ip-protocol tcp
mask 255.255.255.255 port 53 profiles add { example.com_dns_profile example.com_tcp-dns_profile }
```

gtm1.site2 TMSH command:

TMSH

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

2.1.5 Data Centers

2.1.5.1 Servers

2.1.5.1.1 gtm1.SITE1

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

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

1. Fill in the Name and Datacenter

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

ONLINE (ACTIVE)
Standalone

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

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

General Properties

Name
Product
Data Center
Prober Preference
Prober Fallback
State

Devices

Click "Add"

Add

Device Name	Address
No data available in table	

Edit Delete

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
Add 3
203.0.113.7
Delete

Click "Add"

OK Cancel 4

Click "OK"

Big-IP System Devices

No data available in table

Edit Delete

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

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

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

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

Devices

Device Name	Address
gtm1.site1.example.com	203.0.113.7

Add Edit Delete

Configuration: Advanced

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

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
```

2.1.5.1.2 gtm1.SITE2

Continue the same configuration for gtm1.site2.

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

ONLINE (ACTIVE)
Standalone

Main Help About

DNS >> GSLB : Servers : Server List

Server List Trusted Server Certificates Statistics

Search Create...

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

Enable Disable Delete...

Click "Create" to define gtm1.site2

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

1. Fill in the Name and Datacenter

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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

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

General Properties

Name

Product

Data Center

Prober Preference

Prober Fallback

State

Devices

Click "Add"

Device Name	Address
No data available in table	

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

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

ONLINE (ACTIVE)
Standalone

Main Help About

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

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

Add BIG-IP System Device

General Properties

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

Prober Preference Add
Prober Fallback 198.51.100.39
State

Devices

Add
Delete

OK Cancel

Click "Add"

Click "OK"

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

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

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

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

Devices

Device Name	Address
gtm1.site2.example.com	198.51.100.39

Add Edit Delete

Configuration: Advanced

Health Monitors

Selected	Available
/Common bigip	/Common gateway_icmp gtp http http_head_f5

Availability Requirements: All Health Monitors

Limit Settings

Bits: Disabled
Packets: Disabled
Current Connections: Disabled

iQuery Options

Service Check ☒
Path ☒
SNMP ☒

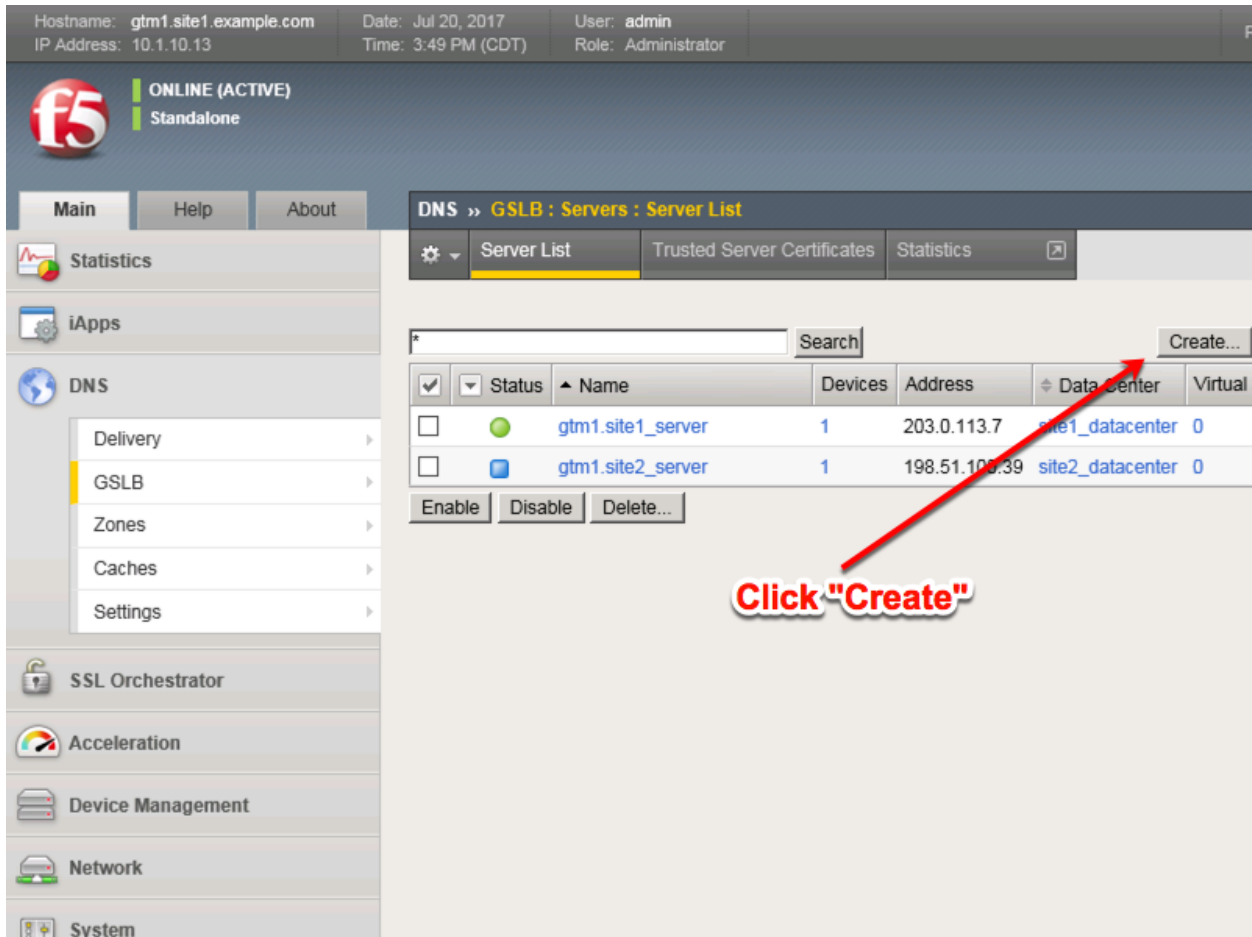
TMSH

```
tmsh create gtm server gtm1.site2_server datacenter site2_datacenter devices add {
gtm1.site2.example.com { addresses add { 198.51.100.39 } } } monitor bigip product bigip
```

2.1.5.1.3 site1_ha-pair

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

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



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

1. Fill in the Name and Datacenter

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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

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

General Properties

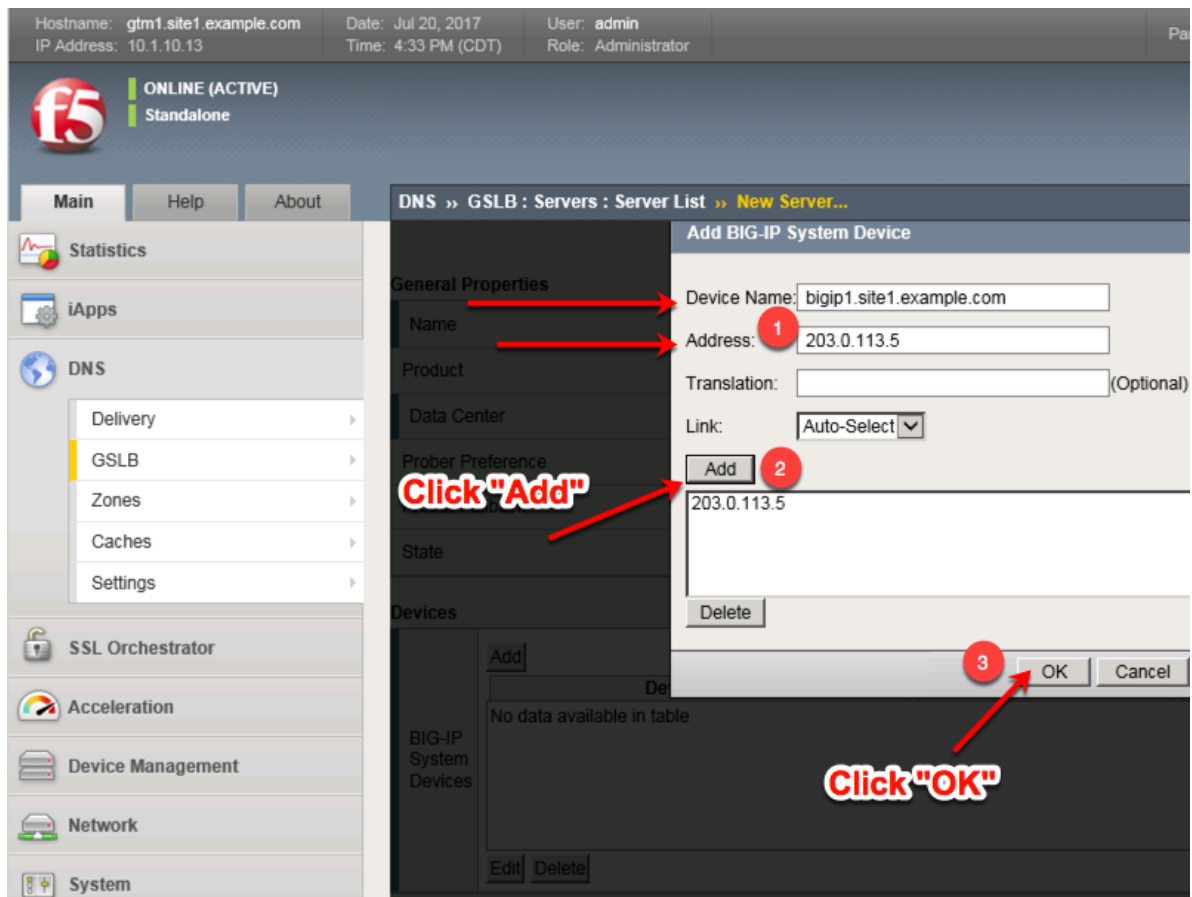
Name
Product
Data Center
Prober Preference
Prober Fallback
State

Devices

Click "Add"

Device Name	Address
No data available in table	

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



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

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

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

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

Devices

Add

Device Name	Address
bigip1.site1.example.com	203.0.113.5

Edit Delete

Click "Add"again

- 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

Configuration: Advanced

Health Monitors

Selected: /Common bigip
Available: /Common gateway_icmp, gtp, http, http_head_f5

Availability Requirements: All Health Monitors

Add the "bigip" Health Monitor

Two devices belong to this HA-Pair

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

Resources

Virtual Server Discovery	Enabled
Link Discovery	Enabled

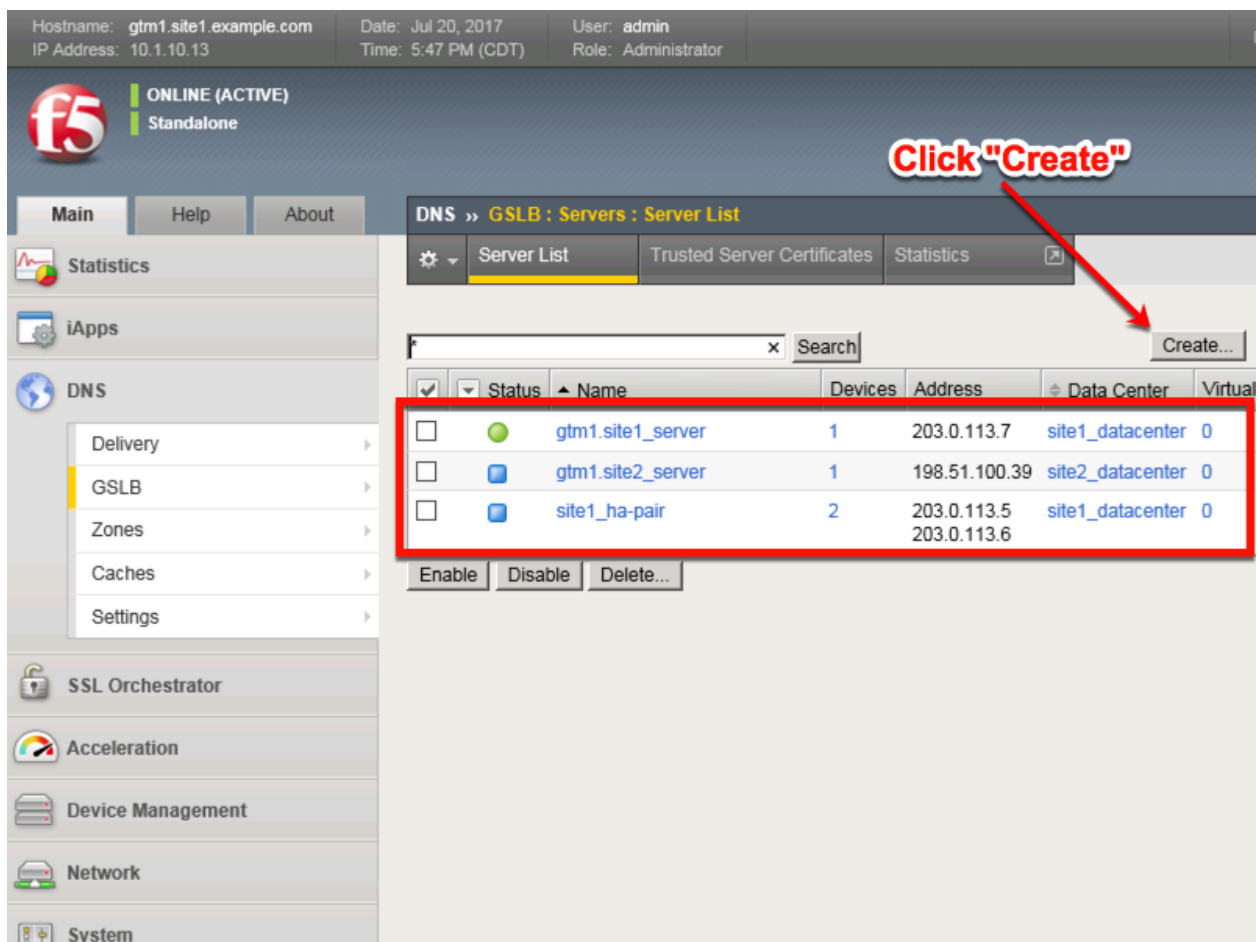
Cancel Repeat Finished

TMSH

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

2.1.5.1.4 site2_ha-pair

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



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

1. Fill in the Name and Datacenter

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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

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

General Properties

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

Devices

Click "Add"

Add

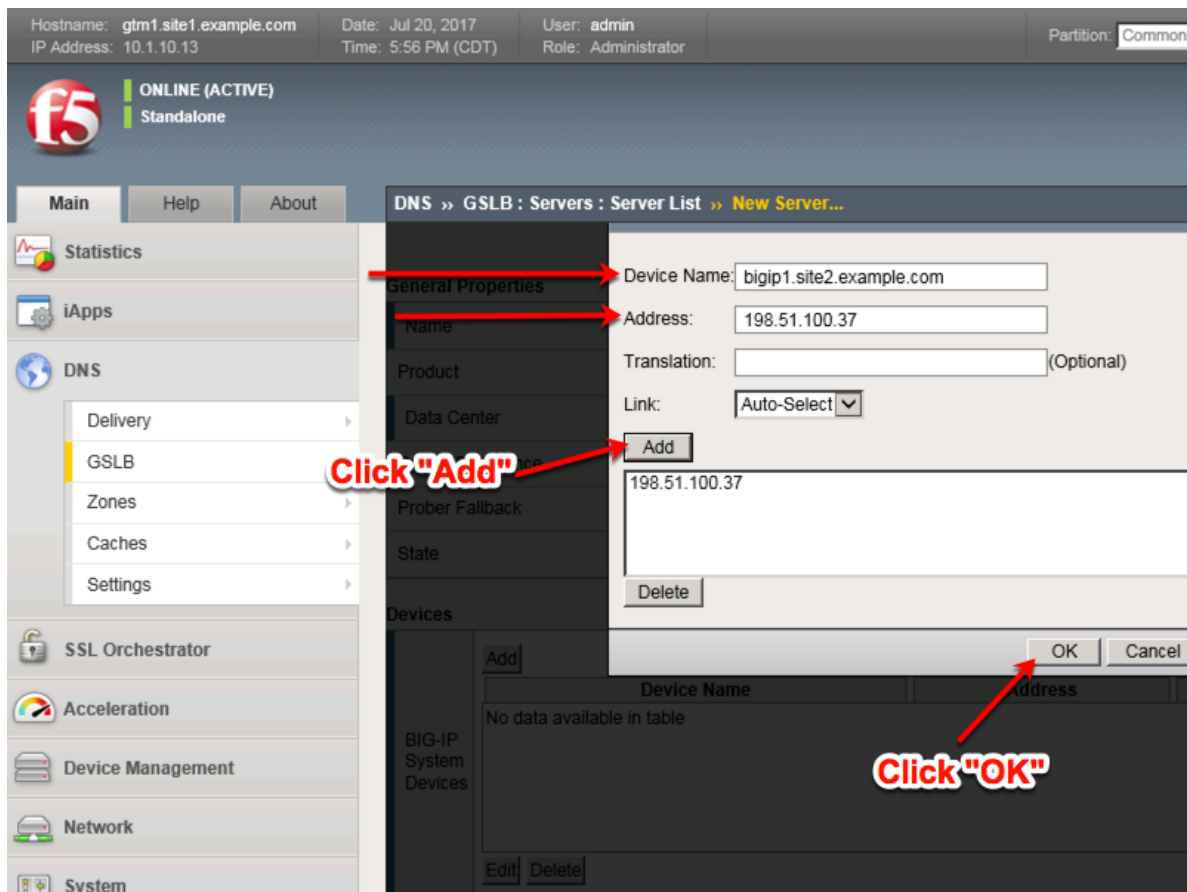
Device Name

No data available in table

BIG-IP System Devices

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: 6:13 PM (CDT) Role: Administrator Partition: Common

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

Name
Product
Data Center
Prober Preference
Prober Fallback
State

Devices

Click "Add"

Device Name	Address
bigip1.site2.example.com	198.51.100.37

Edit Delete

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

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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

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

General Properties

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

Click "Add"

Devices

Device Name	Address
bigip1.site2.example.com	198.51.100.37

Click "OK"

OK Cancel

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

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

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties

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

Devices

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

Add Edit Delete

Configuration: Advanced

Health Monitors

Selected: /Common bigip

Available: /Common gateway_icmp gtp http http_head_f5

Availability Requirements: All Health Monitors

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

Resources

Virtual Server Discovery	Enabled
Link Discovery	Enabled

Cancel Repeat Finished

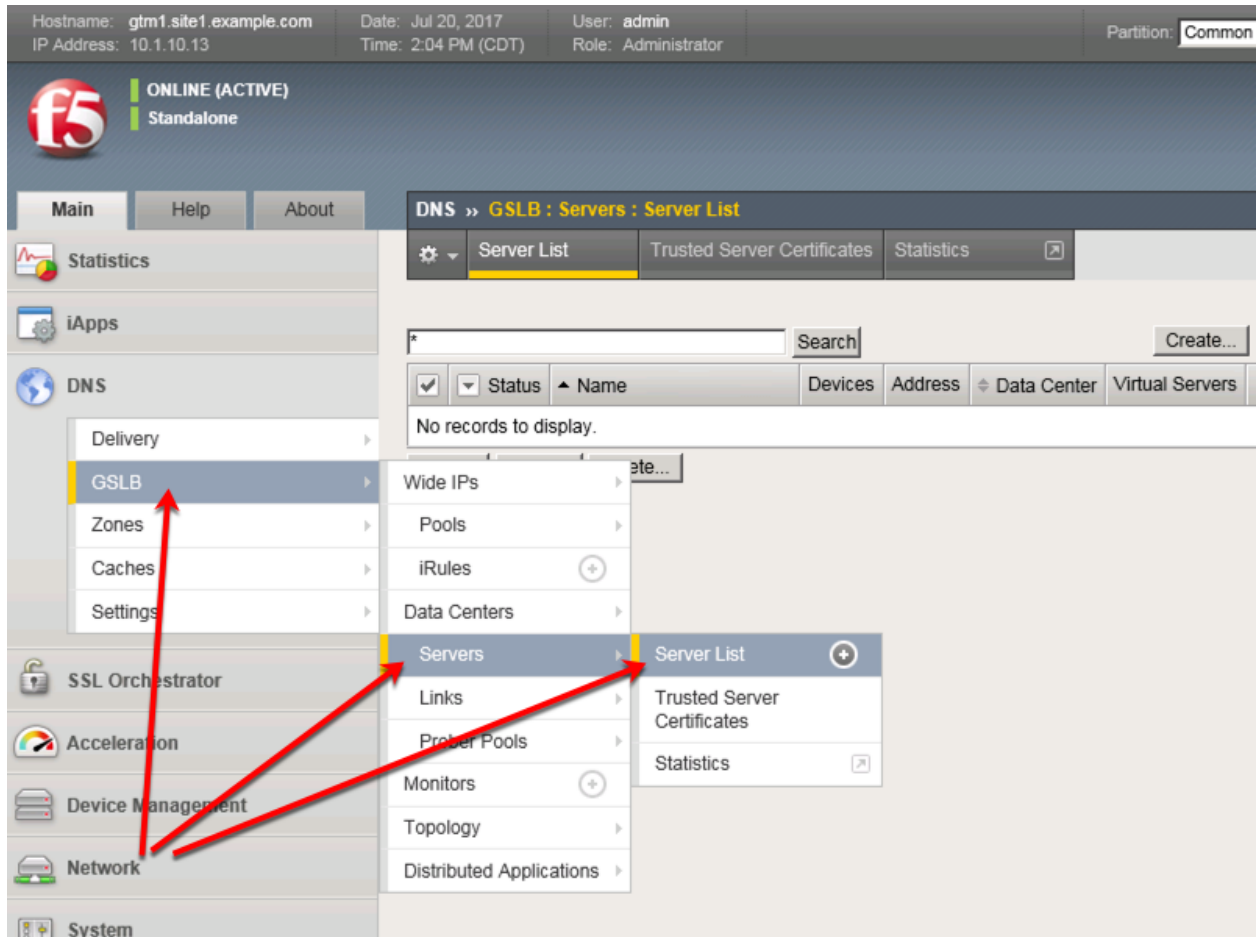
TMSH

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

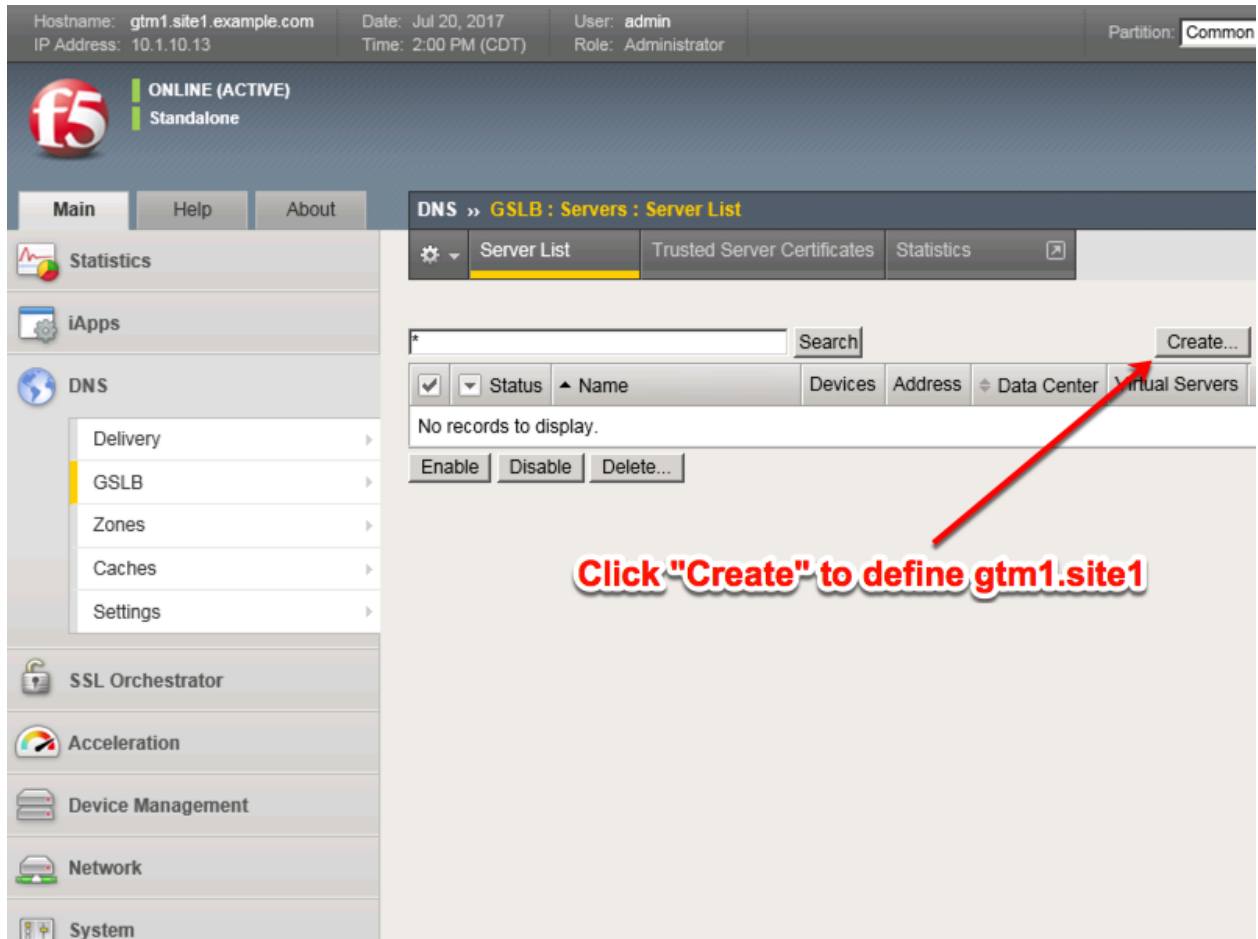
Server objects represent a system such as an application delivery controller which host a service. A server can be a BIG-IP system, a third party ADC or a third-party host server such as a web or database server.

In this task we will create a server on gtm1.site1 referencing gtm1.site2, which is required for config synchronization.

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



Click the create button and continue to define objects



2.1.5.2 Device Trust

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

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

f5 ONLINE (ACTIVE) Standalone

Main Help About

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

DNS » GSLB : Servers : Server List

Server List Trusted Server Certificates Statistics

* Search

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

Enable Disable Delete...

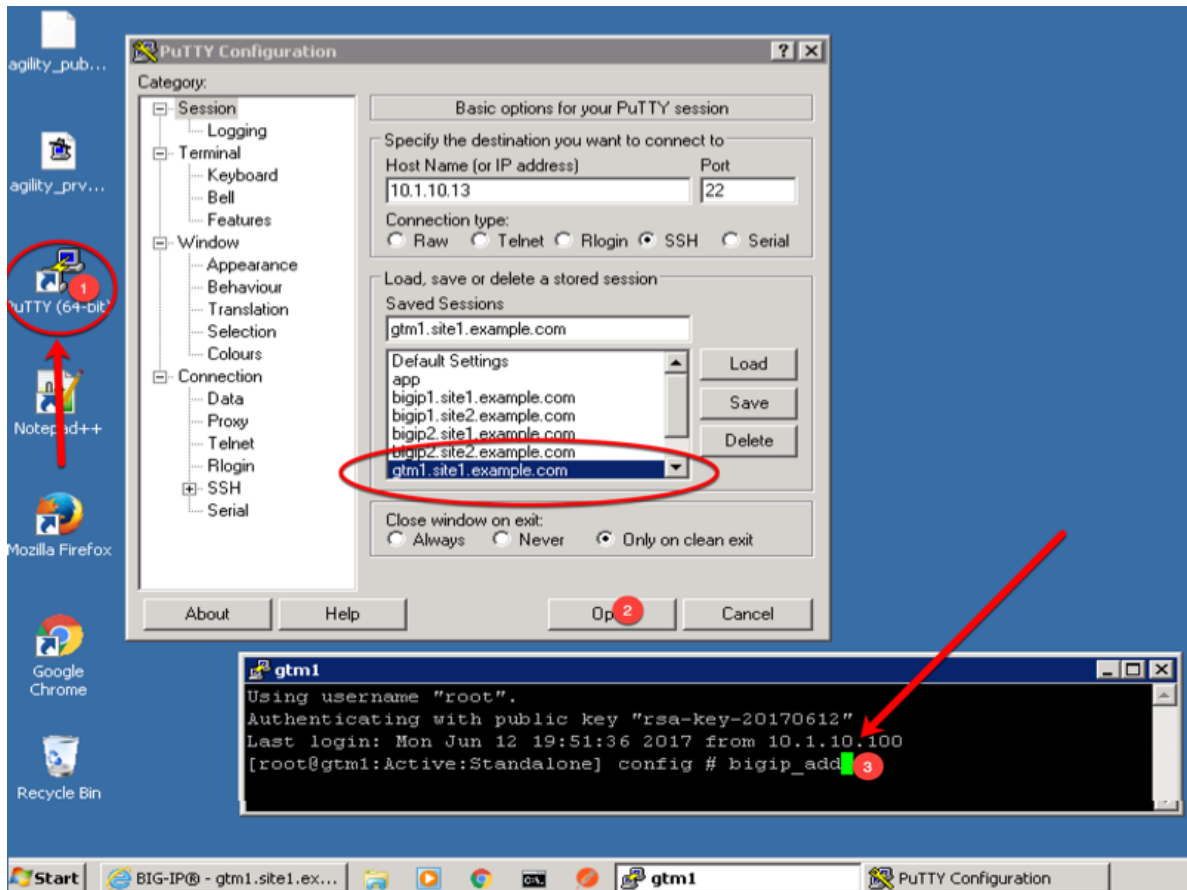
Three other servers need to "establish trust"

1. Launch Putty and login to gtm1.SITE1

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

TMSH

bigip_add



2. Observe the exchanged certificates

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

ONLINE (ACTIVE)
Standalone

Main Help About

Statistics
iApps
DNS
SSL Orchestrator
Acceleration
Device Management

DNS » GSLB : Servers : Trusted Server Certificates

Server List Trusted Server Certificates Statistics

General Properties

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

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

234963207
Common Name: gtm1.site2.example.com

3. Observe the server status

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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

DNS » GSLB : Servers : Server List

Server List Trusted Server Certificates Statistics

Search

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

Enable Disable Delete...

Green Green Green !!

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

2.1.5.3 Sync Group

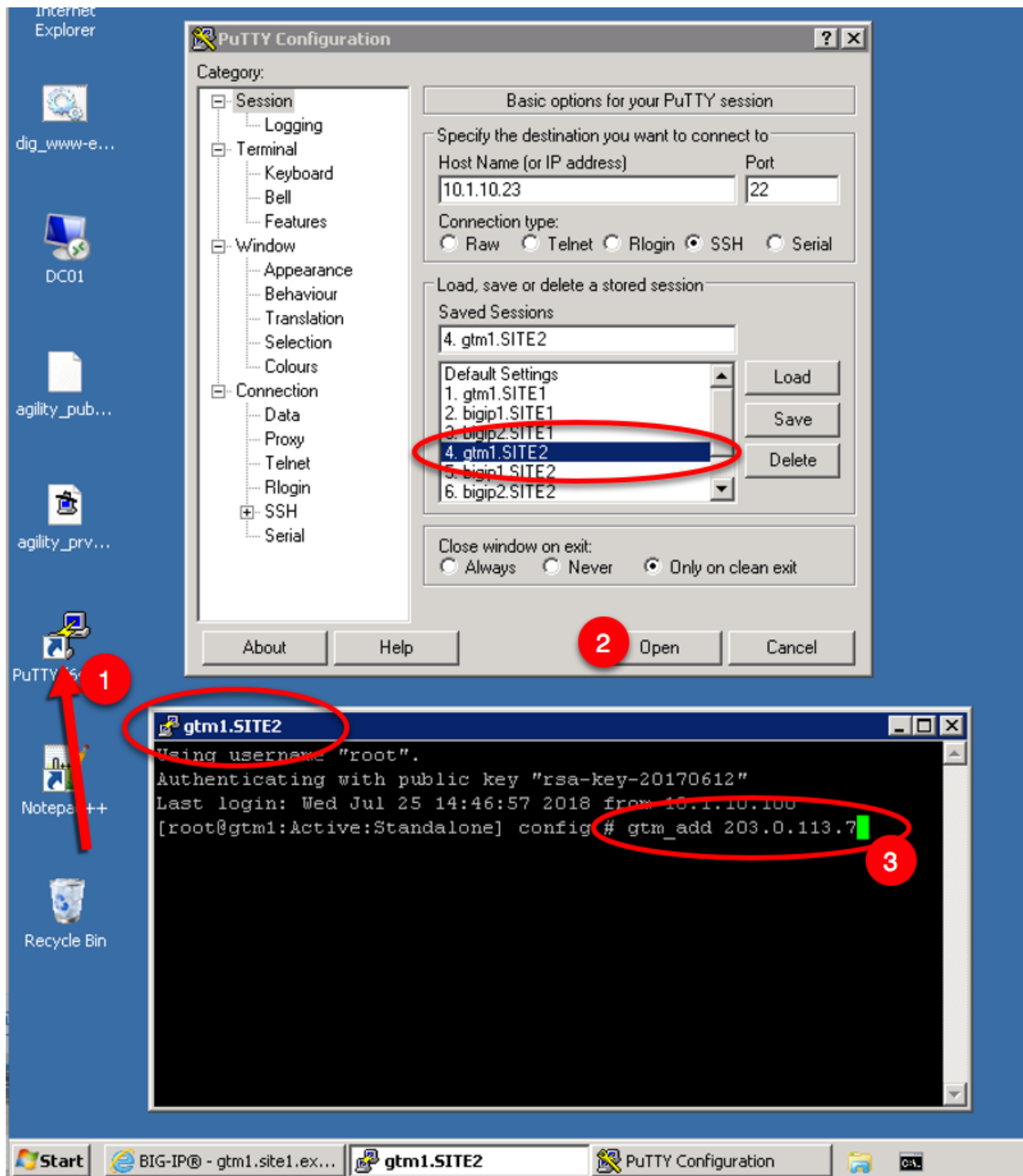
After the BIG-IP DNS server in the site 2 data center is joined to the sync group, an administrator may make changes on any of the F5 DNS servers, and changes will be automatically replicated across all F5 DNS servers.

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

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

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

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



TMSH

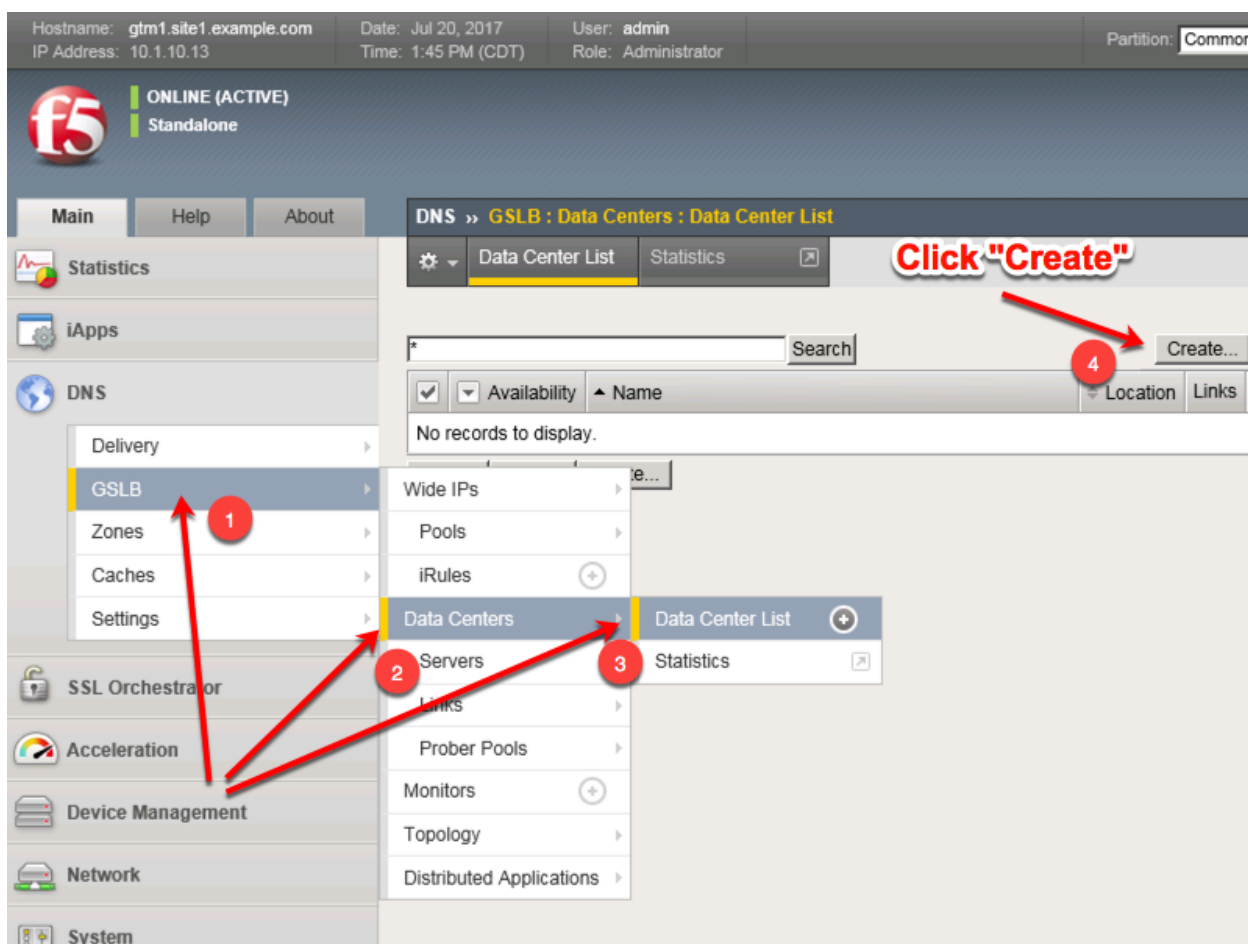
gtm_add 203.0.113.7

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

please refer to the link below.

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

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



Create two data centers according to the table below:

Field	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"

TMSH command for only site1.gtm1:

TMSH

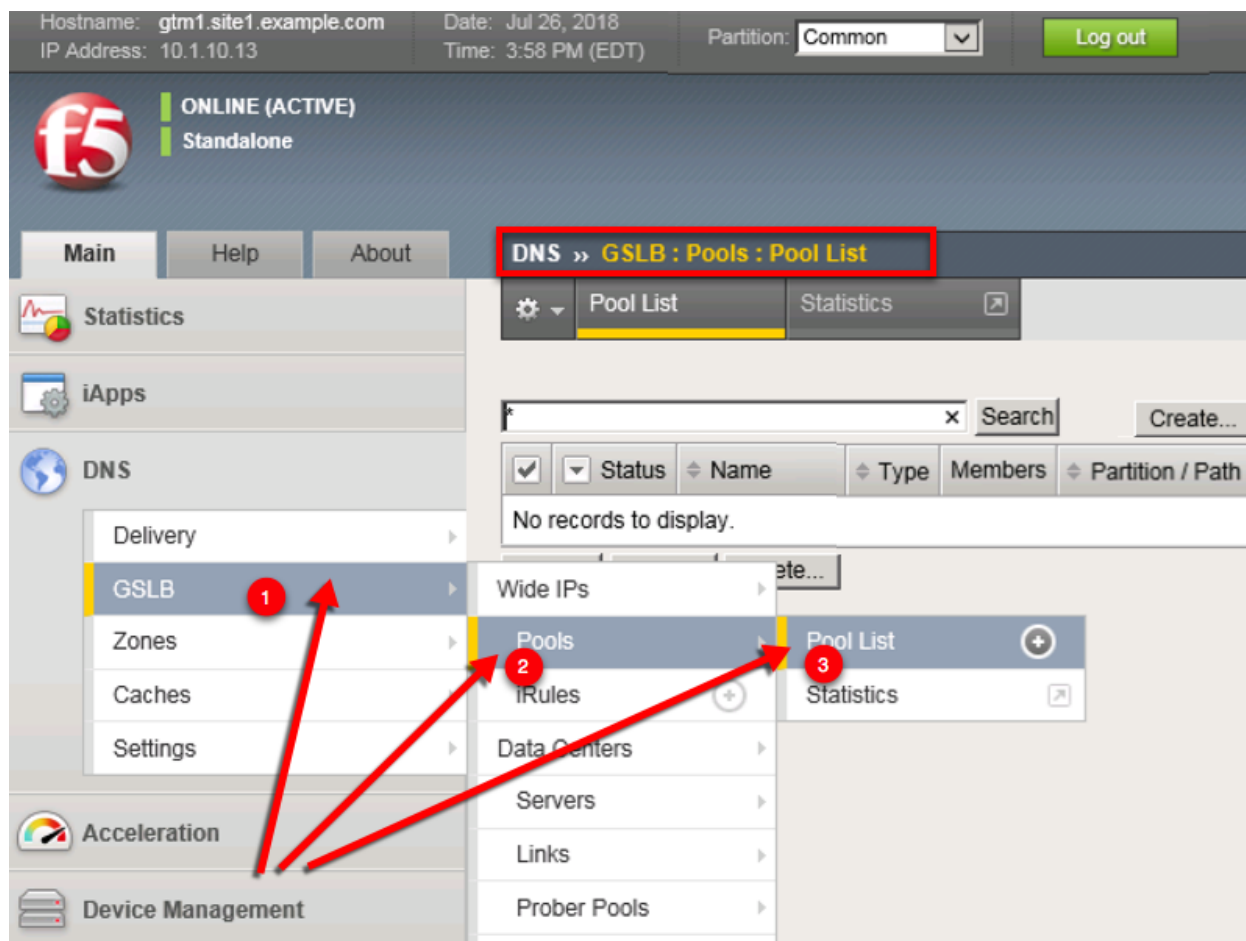
```
tmsh create gtm datacenter site1_datacenter
```

TMSH

```
tmsh create gtm datacenter site2_datacenter
```

2.1.6 Pools

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



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

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

ONLINE (ACTIVE)
Standalone

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

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

General Properties

Name: www.example.com_pool
Type: A
State: Enabled

Configuration

Health Monitors: Selected (empty), Available: /Common/gateway_icmp, gtp, http, http_head_f5
Availability Requirements: All Health Monitors
Limit Settings: Bits: Disabled, Packets: Disabled, Current Connections: Disabled
Manual Resume: ☐
TTL: 30
Dynamic Ratio: ☐
Maximum Answers Returned: 1
Verify Member Availability: ☒

Members

Load Balancing Method: Preferred: Round Robin, Alternate: Round Robin, Fallback: Return to DNS
Fallback IP: 0.0.0.0
Virtual Server: Select...
Ratio: 1
Add
Member List: /Common/isp1_site1_www.example.com_tcp_https_virtual (/Common/site1_ha-pair) - 203.0.113.9:443, Ratio(1)
/Common/isp2_site2_www.example.com_tcp_https_virtual (/Common/site2_ha-pair) - 198.51.100.41:443, Ratio(1)
Delete Up Down

Select two LTM VIP's and click "Add"

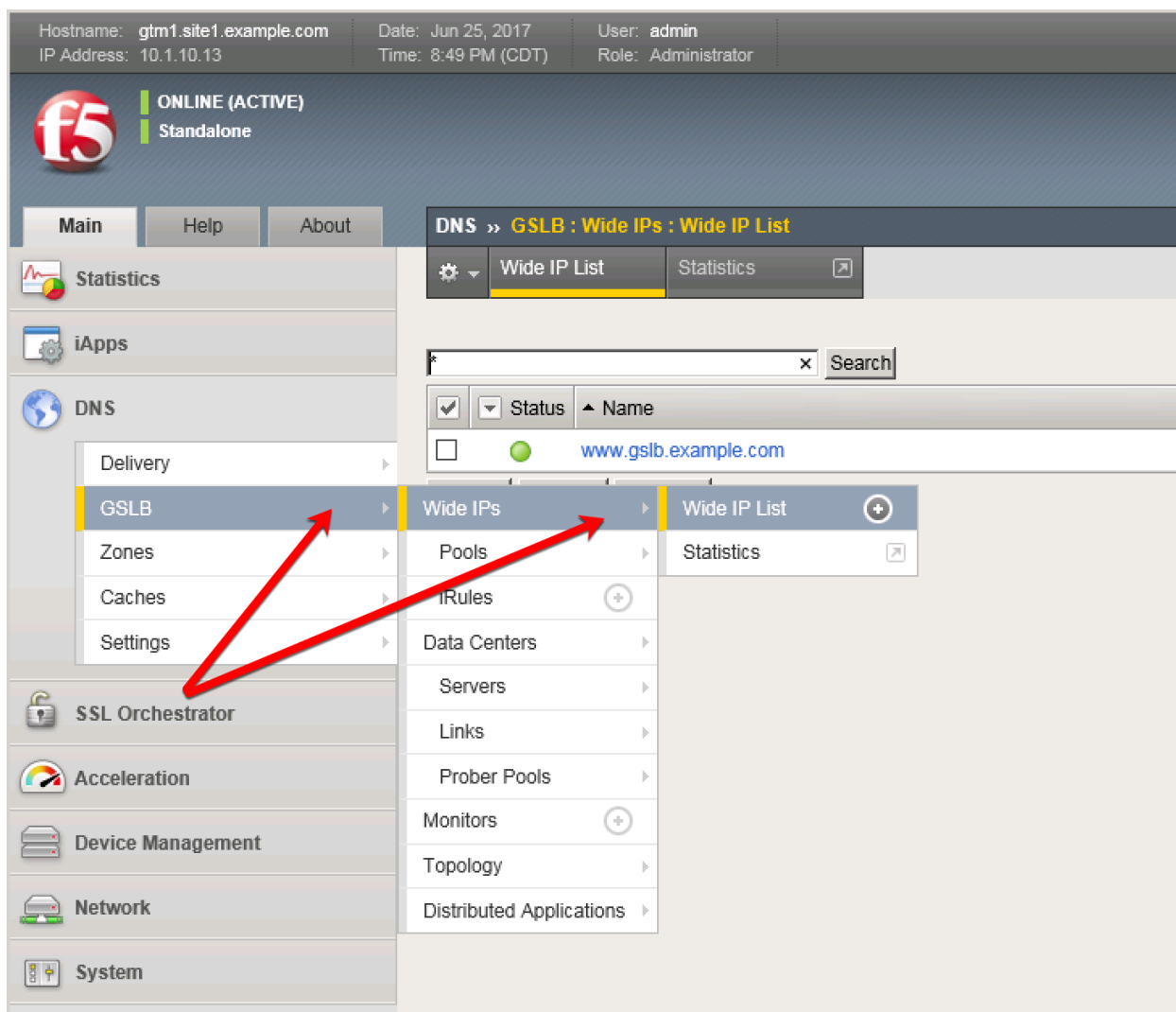
TMSH command to run on only gtm1.site1:

TMSH

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

2.1.7 FQDN

F5 refers to an FQDN as a “wide-ip”, or “wip”. The Wide IP maps a FQDN (fully qualified domain name) to one or more pools of virtual servers. For more information on Wide IPs, please refer to the link below.



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

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

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

f5 ONLINE (ACTIVE)
Standalone

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

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

General Properties: Advanced

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

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

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

For troubleshooting purposes enable verbose logging

Chapter 2. DNS

TMSH command to run on only gtm1.site1:

TMSH

```
tmsl create gtm wideip a www.example.com { pools add { www.example.com_pool } aliases add { www.gslb.example.com } load-balancing-decision-log-verbosity { pool-member-selection pool-member-traversal pool-selection pool-traversal } }
```

Results

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

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

Note: Your result may differ from below

```
C:\Users\user.EXAMPLE>dig @203.0.113.8 www.example.com
; <<>> DiG 9.3.2 <<>> @203.0.113.8 www.example.com
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 389
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;www.example.com.                IN      A
;; ANSWER SECTION:
www.example.com.                 30      IN      A      198.51.100.41
;; Query time: 15 msec
;; SERVER: 203.0.113.8#53(203.0.113.8)
;; WHEN: Sun Jul 29 16:42:09 2018
;; MSG SIZE rcvd: 49

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

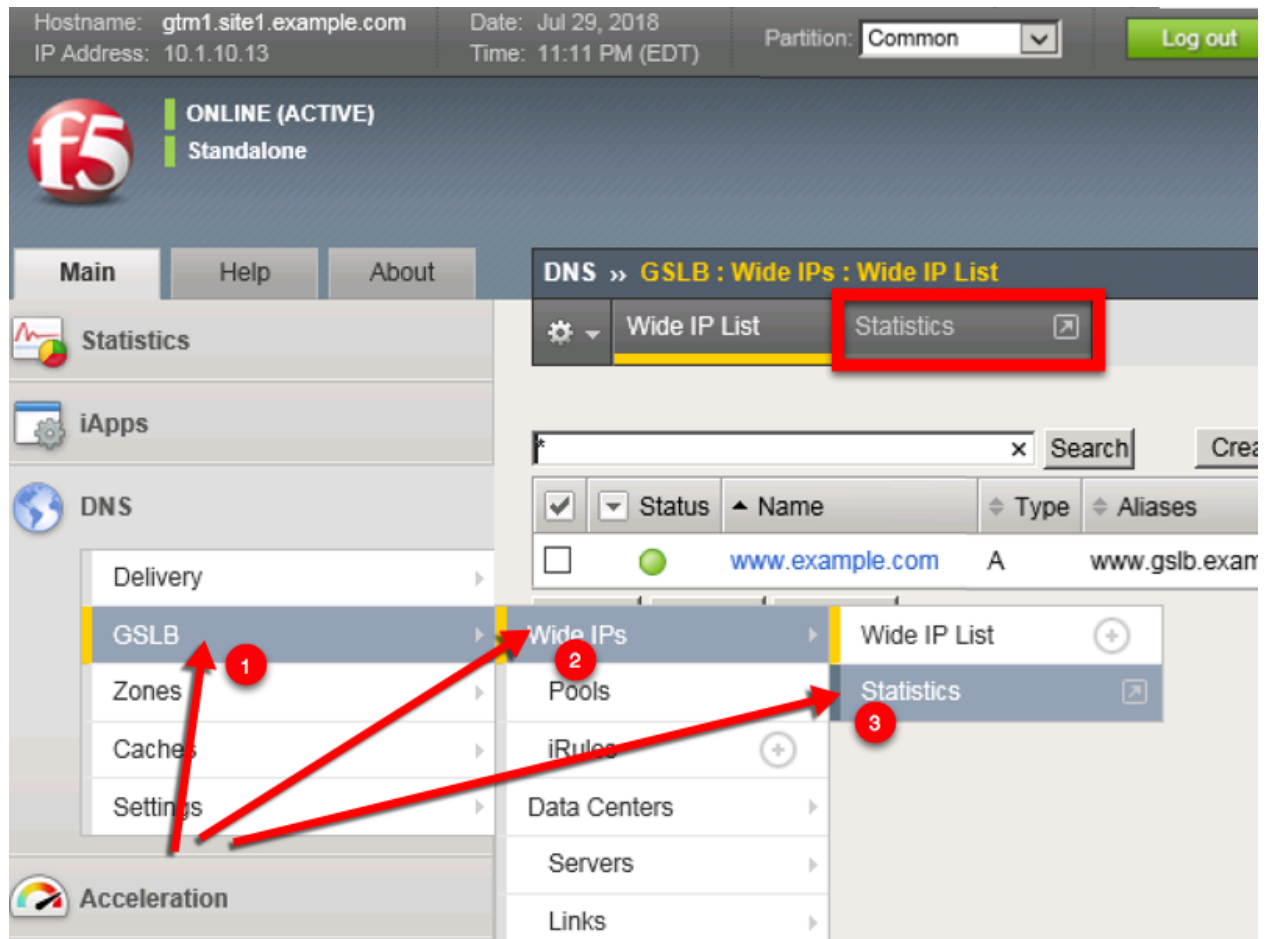
C:\Users\user.EXAMPLE>dig +short @203.0.113.8 www.example.com
198.51.100.41

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

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

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

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



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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

Traffic Summary DNS Subscriber Management Network

Statistics

- Dashboard
- Module Statistics
- Analytics
- Performance

iApps

DNS

Acceleration

Device Management

Network

System

Display Options

Statistics Type: Wide IPs

Data Format: Normalized

Auto Refresh: Disabled Refresh

* Search

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

Reset

For more details click

TMSH

tmsh show gtm wideip A www.example.com detail

```

gtm1.SITE1
[root@gtm1:Active:Standalone] config # tmsh show gtm wideip A www.example.com detail

Gtm::WideIp::A www.example.com
-----
Status
  Availability : available
  State       : enabled
  Reason      : Available

Requests
  Total       44
  Persisted   0
  Resolved    44
  Dropped     0

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

-----
| Gtm::Pool::A www.example.com_pool
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Available
|
| Load Balancing
|   Preferred   44
|   Alternate   0
|   Fallback    0
|   Returned from DNS 0
|   Returned to DNS 0
|   Dropped     0
|
-----
| Gtm::Pool Member: www.example.com_pool:A isp1_site1_www.example.com_tcp_https_virtual:site1_ha-pair
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Available
|
| Load Balancing
|   Preferred   35
|   Alternate   0
|   Fallback    0
|
-----
| Gtm::Virtual Server: isp1_site1_www.example.com_tcp_https_virtual
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Monitor /Common/bigip from 203.0.113.5 : UP
|   Destination : 203.0.113.9:443
|   Up Time     : 10:18
|
| Link Name      203.0.113.1
|
| Global
|   Picks        35
|   Connections  0
|   Virtual Server Score 1
|
| Throughput
|   In  Out
|   Bits/sec  0  0
|   Packets/sec 0  0
|
-----
| Gtm::Pool Member: www.example.com_pool:A isp2_site2_www.example.com_tcp_https_virtual:site2_ha-pair
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Available

```

TMSH

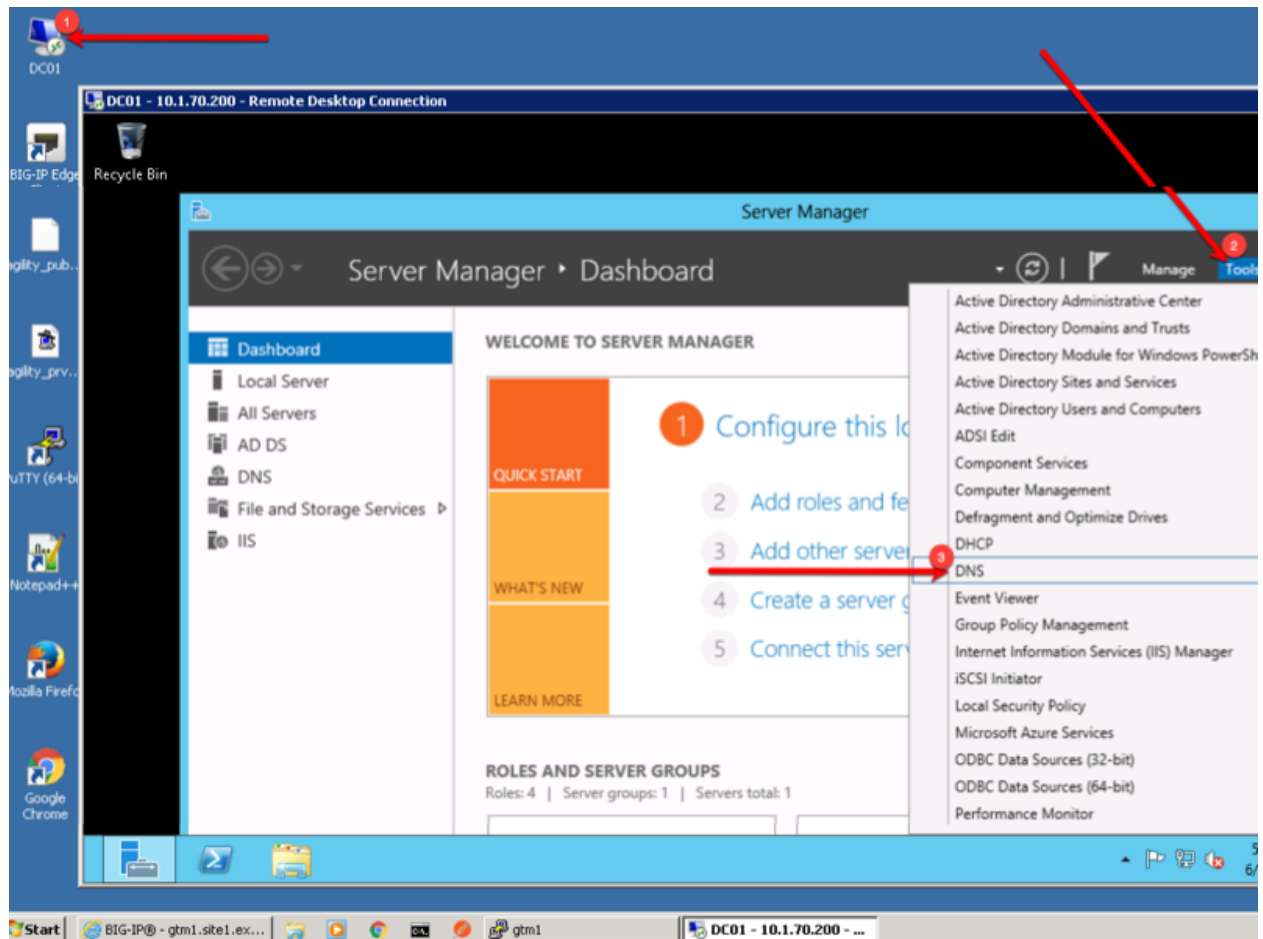
```
tail -f /var/log/ltm
```

```
gtm1.SITE1
[root@gtm1:Active:Standalone] config # tail -f -n 12 /var/log/ltm
Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com qid 991 from 198.51.100.68#64119: view none: query: www.gslb.example.com IN A + (203.0.113.8%0)
Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com qid 991 from 198.51.100.68#64119 [www.gslb.example.com A] [round robin selected pool (www.example.com_pool)] [pool member check succeeded (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9) - pool member state is available (green)] [round robin selected pool member (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9)]
Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com qid 991 to 198.51.100.68#64119: [NOERROR qr,aa,rd] response: www.gslb.example.com. 30 IN A 203.0.113.9;
Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 from 198.51.100.68#64120: view none: query: www.gslb.example.com IN A + (203.0.113.8%0)
Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 from 198.51.100.68#64120 [www.gslb.example.com A] [round robin selected pool (www.example.com_pool)] [pool member check succeeded (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9) - pool member state is available (green)] [round robin selected pool member (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9)]
Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 to 198.51.100.68#64120: [NOERROR qr,aa,rd] response: www.gslb.example.com. 30 IN A 203.0.113.9;
Jul 30 00:23:44 gtm1 info tmm[11966]: 2018-07-30 00:23:43 gtm1.site1.example.com qid 261 from 203.0.113.68#64121: view none: query: www.example.com IN A + (203.0.113.8%0)
Jul 30 00:23:44 gtm1 info tmm[11966]: 2018-07-30 00:23:43 gtm1.site1.example.com qid 261 from 203.0.113.68#64121 [www.example.com A] [round robin selected pool (www.example.com_pool)] [pool member check succeeded (isp2_site2_www.example.com_tcp_https_virtual:198.51.100.41) - pool member state is available (green)] [round robin selected pool member (isp2_site2_www.example.com_tcp_https_virtual:198.51.100.41)]
Jul 30 00:23:44 gtm1 info tmm[11966]: 2018-07-30 00:23:43 gtm1.site1.example.com qid 261 to 203.0.113.68#64121: [NOERROR qr,aa,rd] response: www.example.com. 30 IN A 198.51.100.41;
Jul 30 00:23:50 gtm1 info tmm[11966]: 2018-07-30 00:23:50 gtm1.site1.example.com qid 97 from 203.0.113.68#64122: view none: query: www.example.com IN A + (203.0.113.8%0)
Jul 30 00:23:50 gtm1 info tmm[11966]: 2018-07-30 00:23:50 gtm1.site1.example.com qid 97 from 203.0.113.68#64122 [www.example.com A] [round robin selected pool (www.example.com_pool)] [pool member check succeeded (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9) - pool member state is available (green)] [round robin selected pool member (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9)]
Jul 30 00:23:50 gtm1 info tmm[11966]: 2018-07-30 00:23:50 gtm1.site1.example.com qid 97 to 203.0.113.68#64122: [NOERROR qr,aa,rd] response: www.example.com. 30 IN A 203.0.113.9;
```

2.1.8 Delegation

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

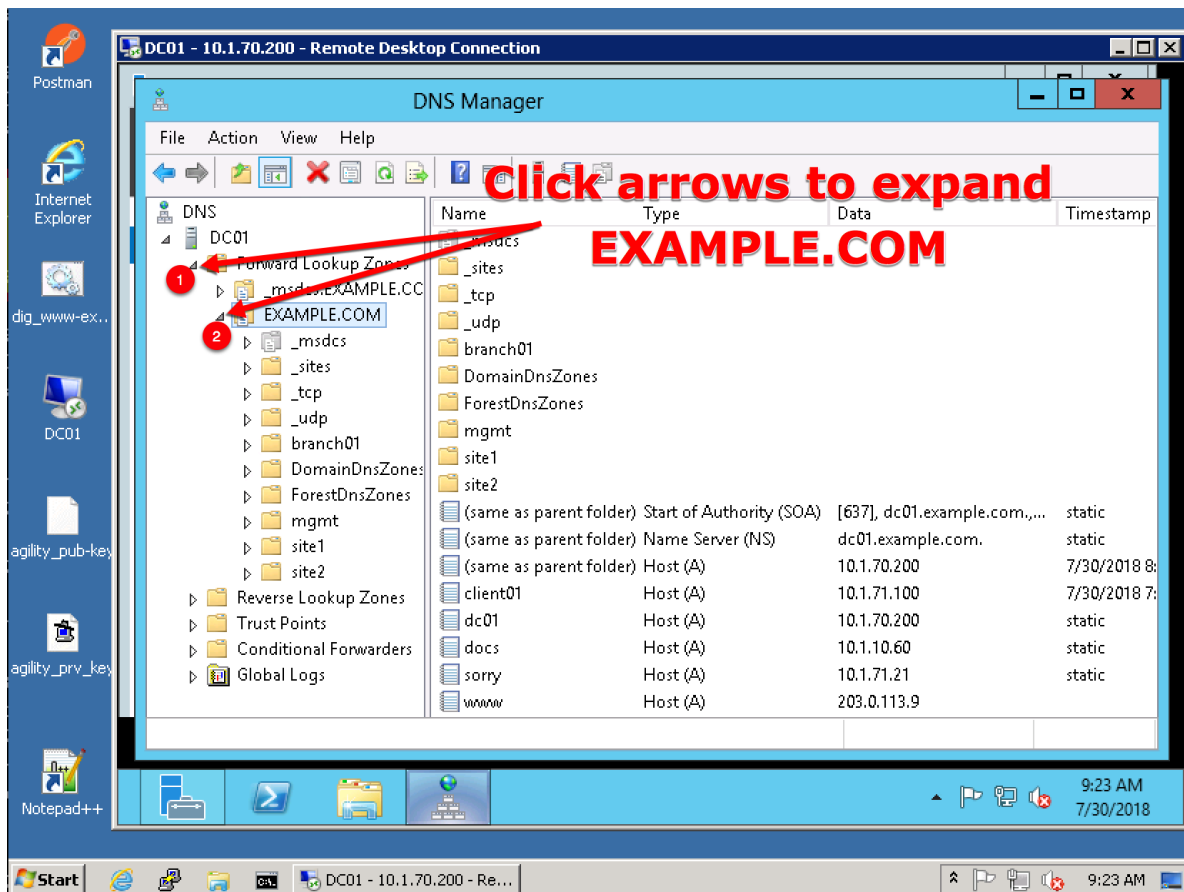
Login to the local DNS server (this should already be open) from the jumpbox, and open the DNS management UI:



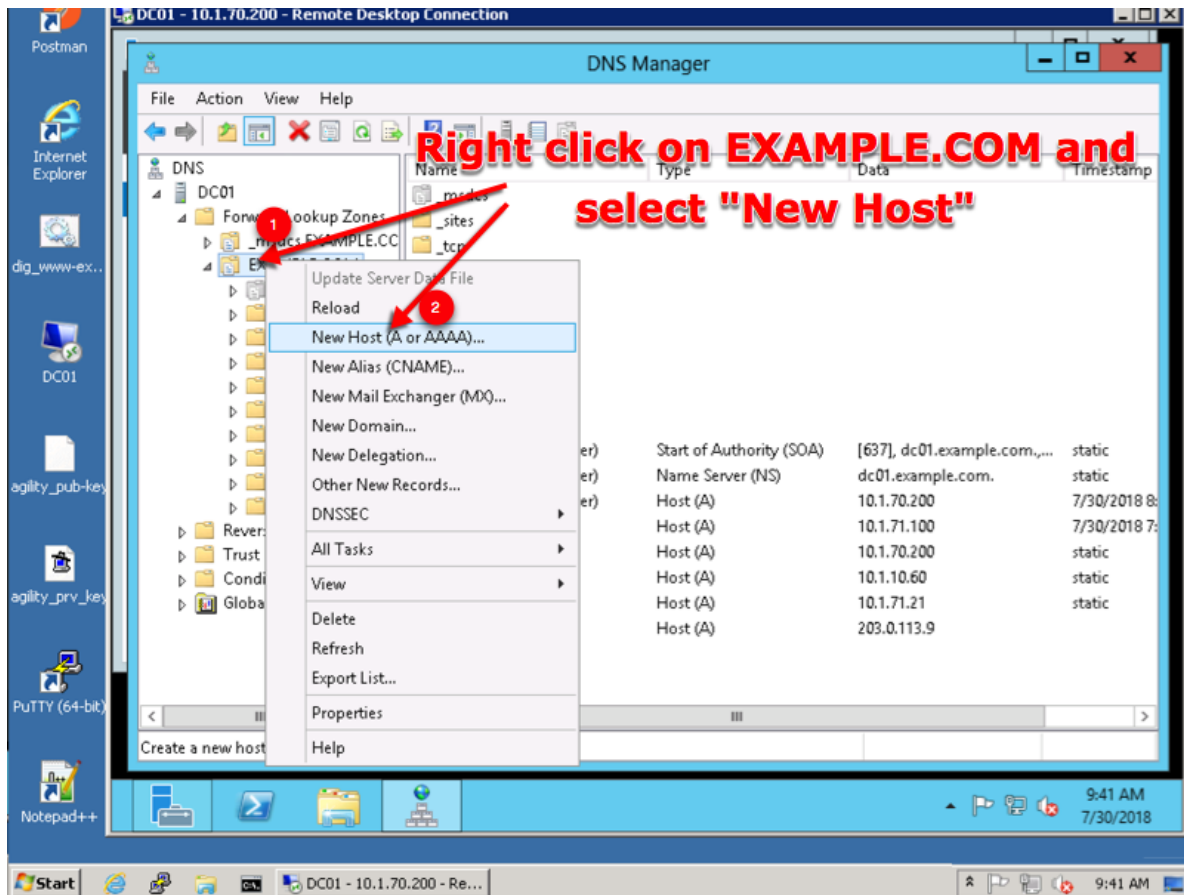
2.1.8.1 A Records

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

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

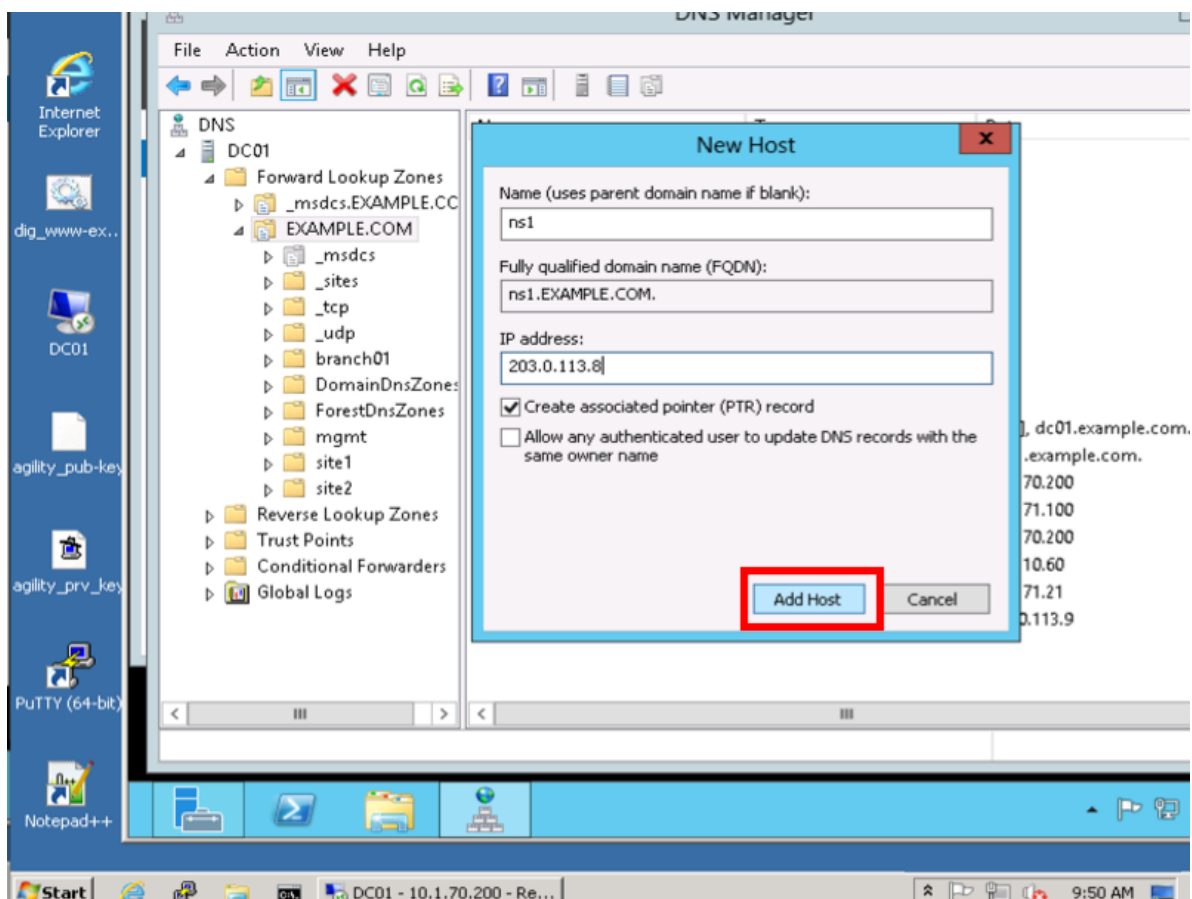


2. Right click on EXAMPLE.COM and select "New Host (A or AAAA)"

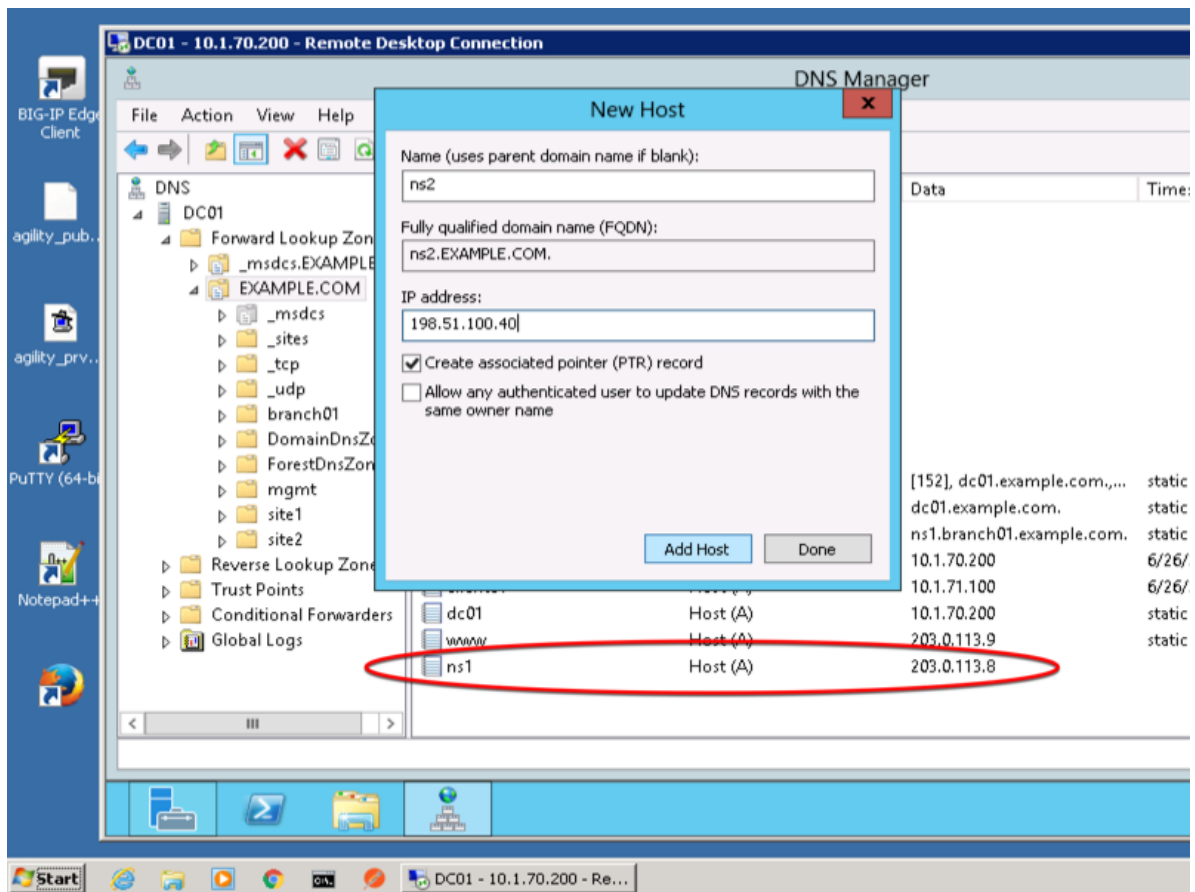


3. Create two new A records for the new BIGP-IP nameservers.

Field	Value
ns1	203.0.113.8
ns2	198.51.100.40



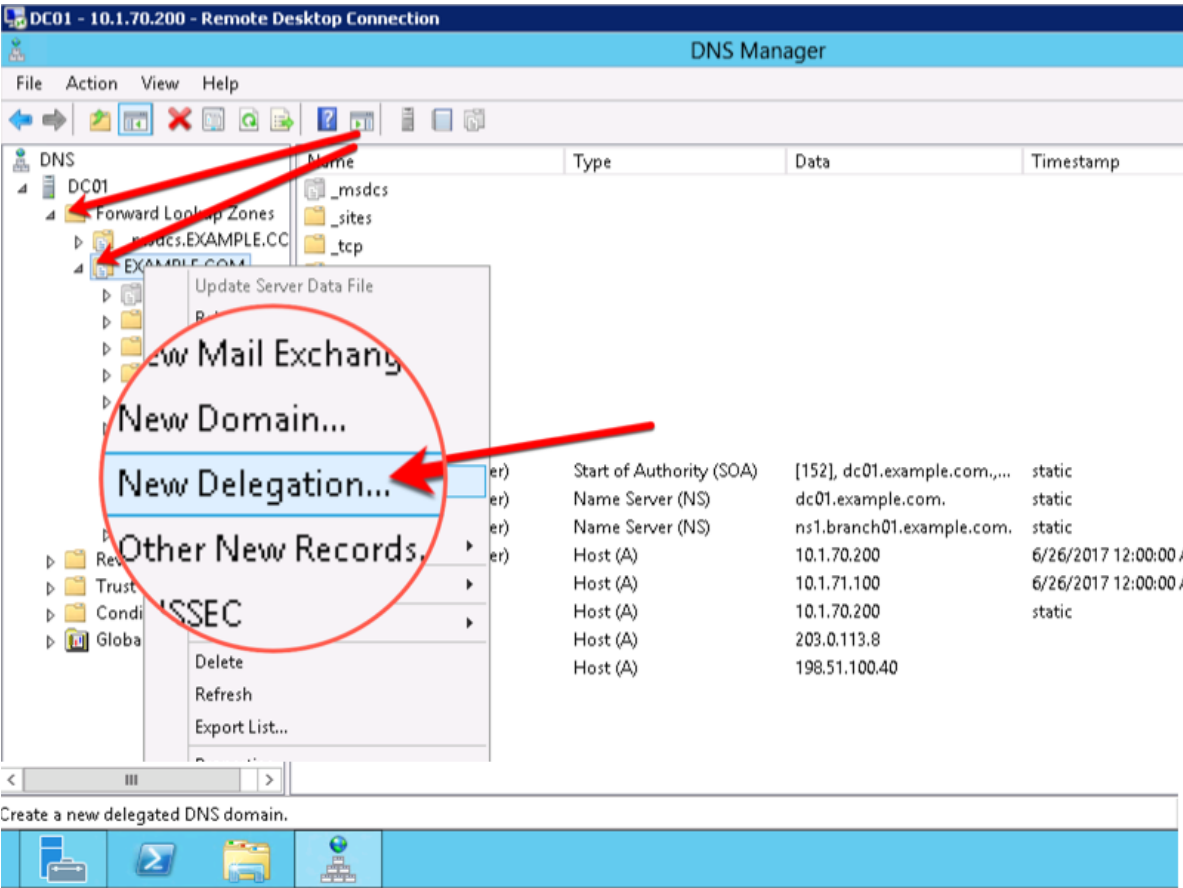
Create ns2.example.com



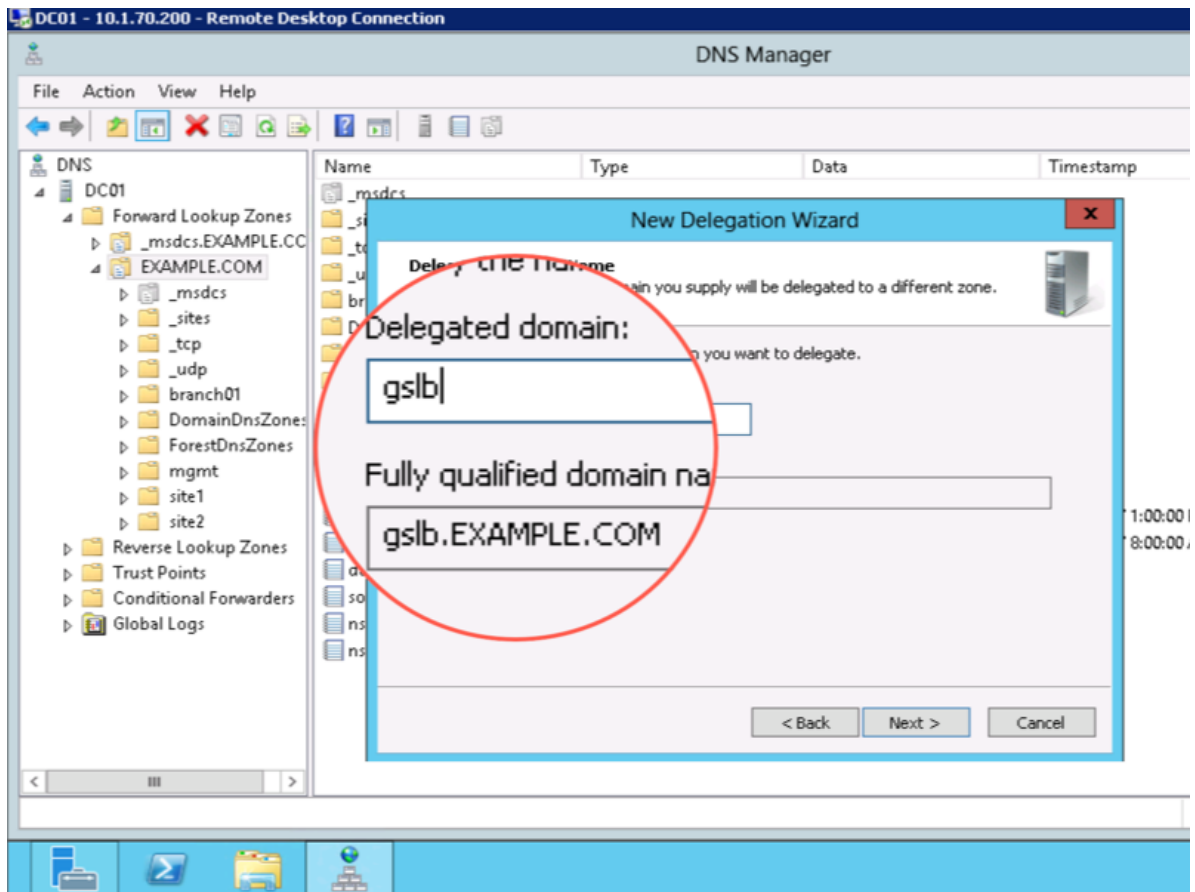
2.1.8.2 Sub Domain

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

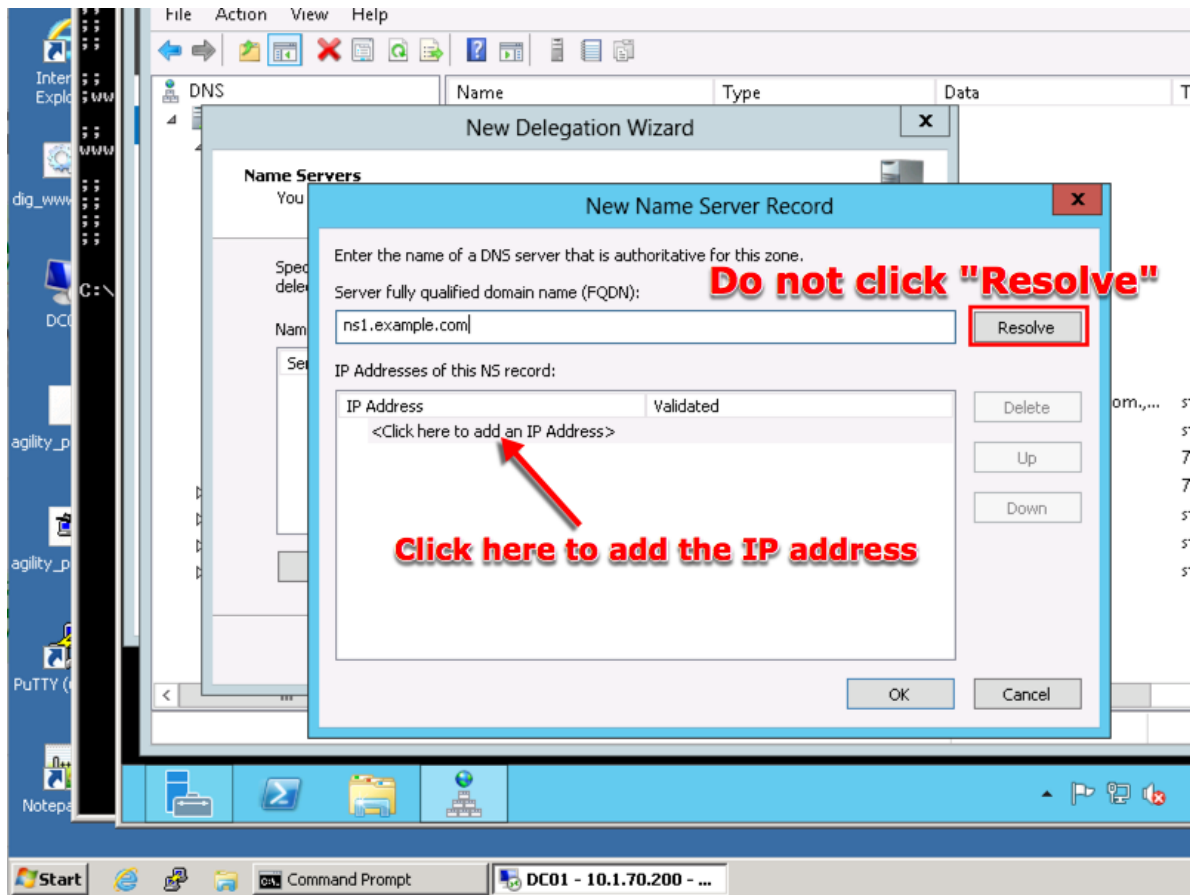
1. Expand "Forward Lookup Zones", and right click on "EXAMPLE.com"



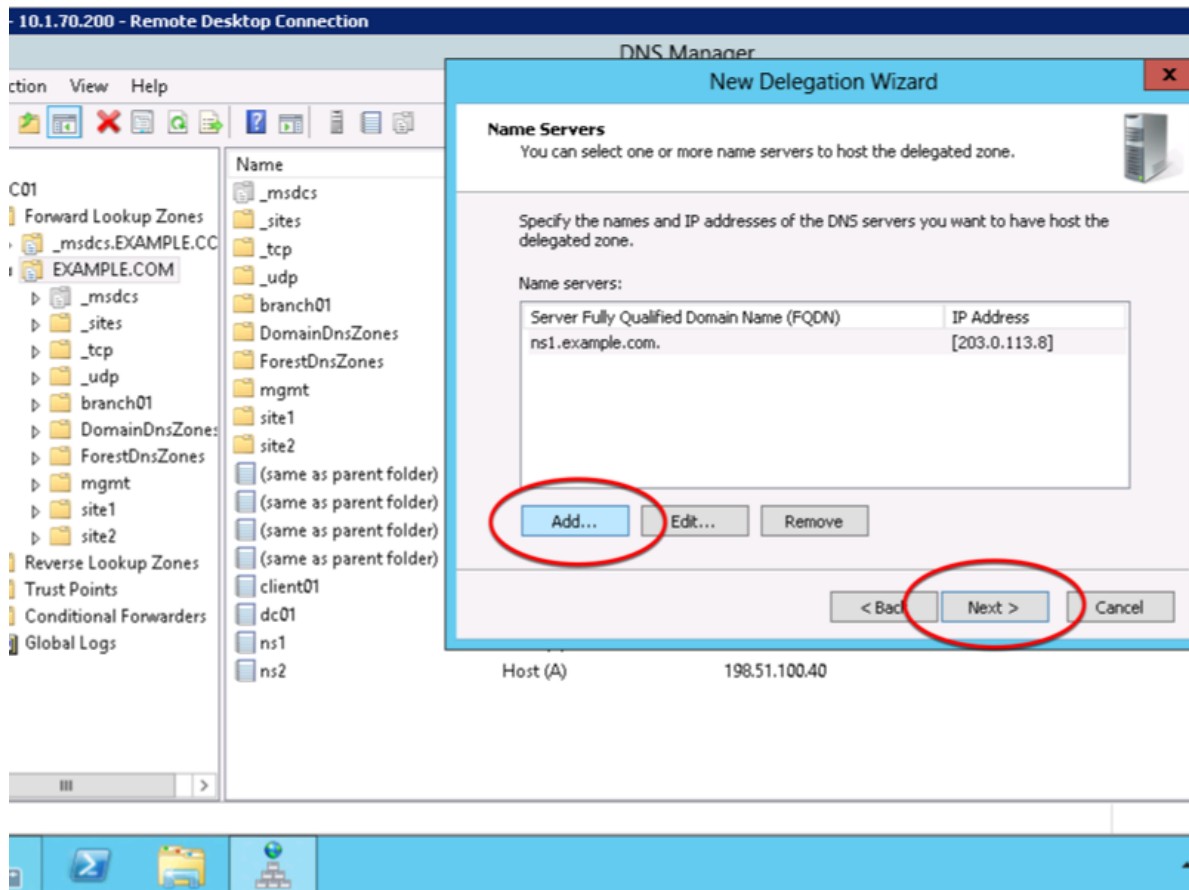
2. Create the “gslb” subdomain.



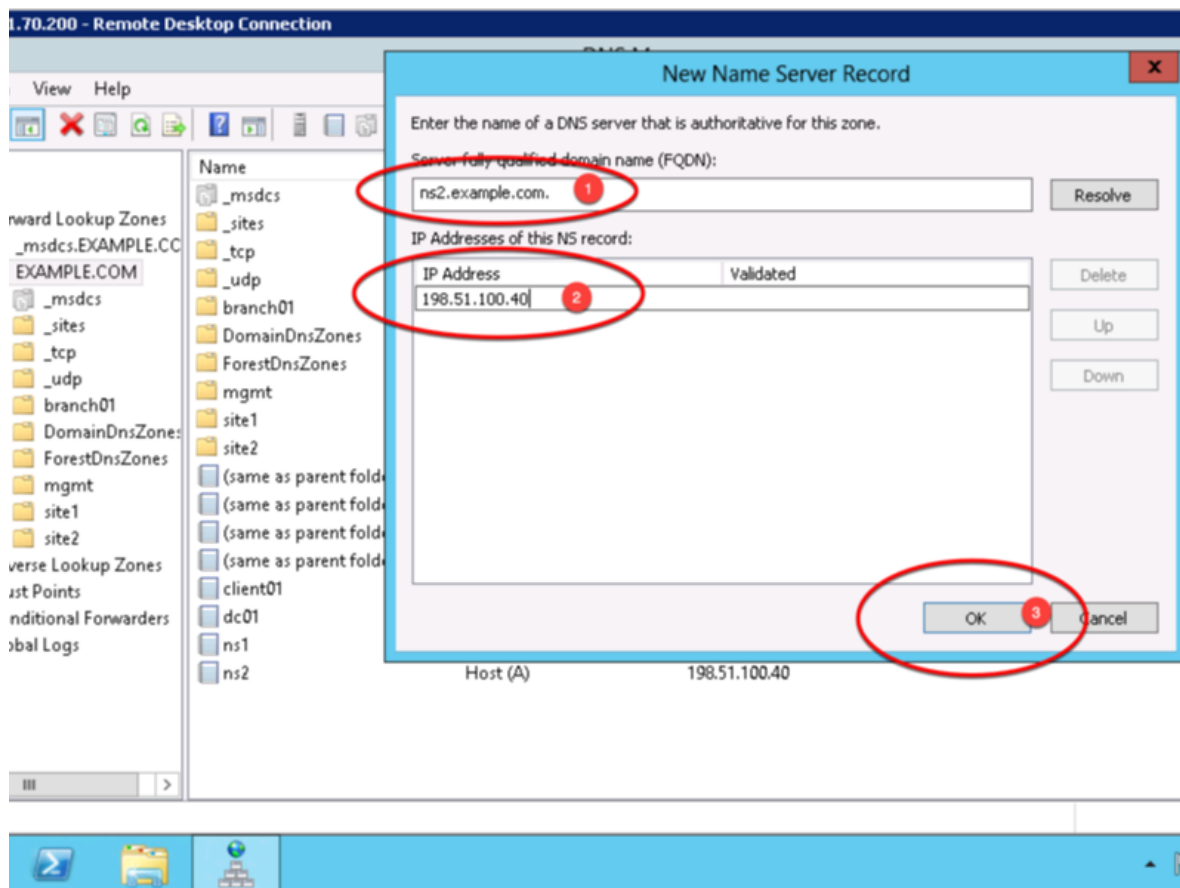
3. Step through the Delegation Wizard. Add "ns1.example.com - 203.0.113.8"



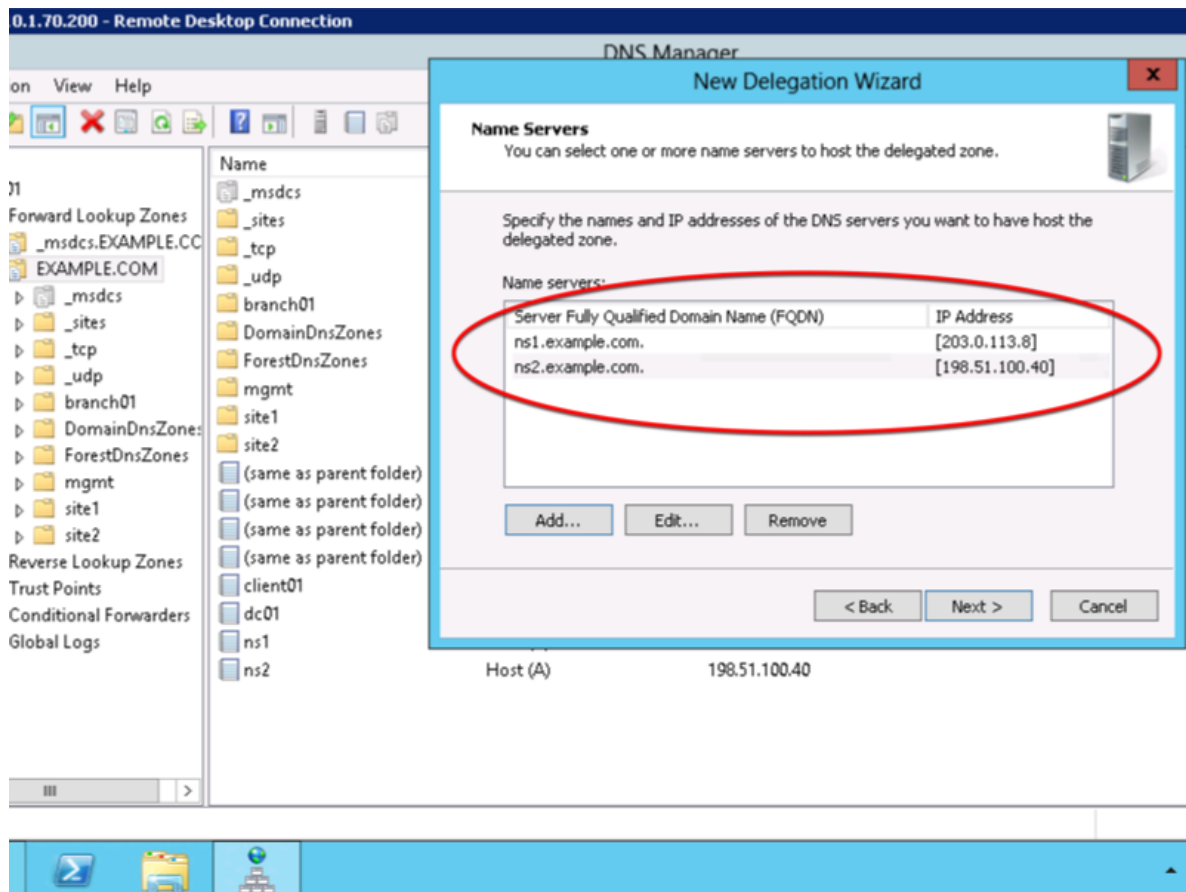
Repeat to add ns2.example.com



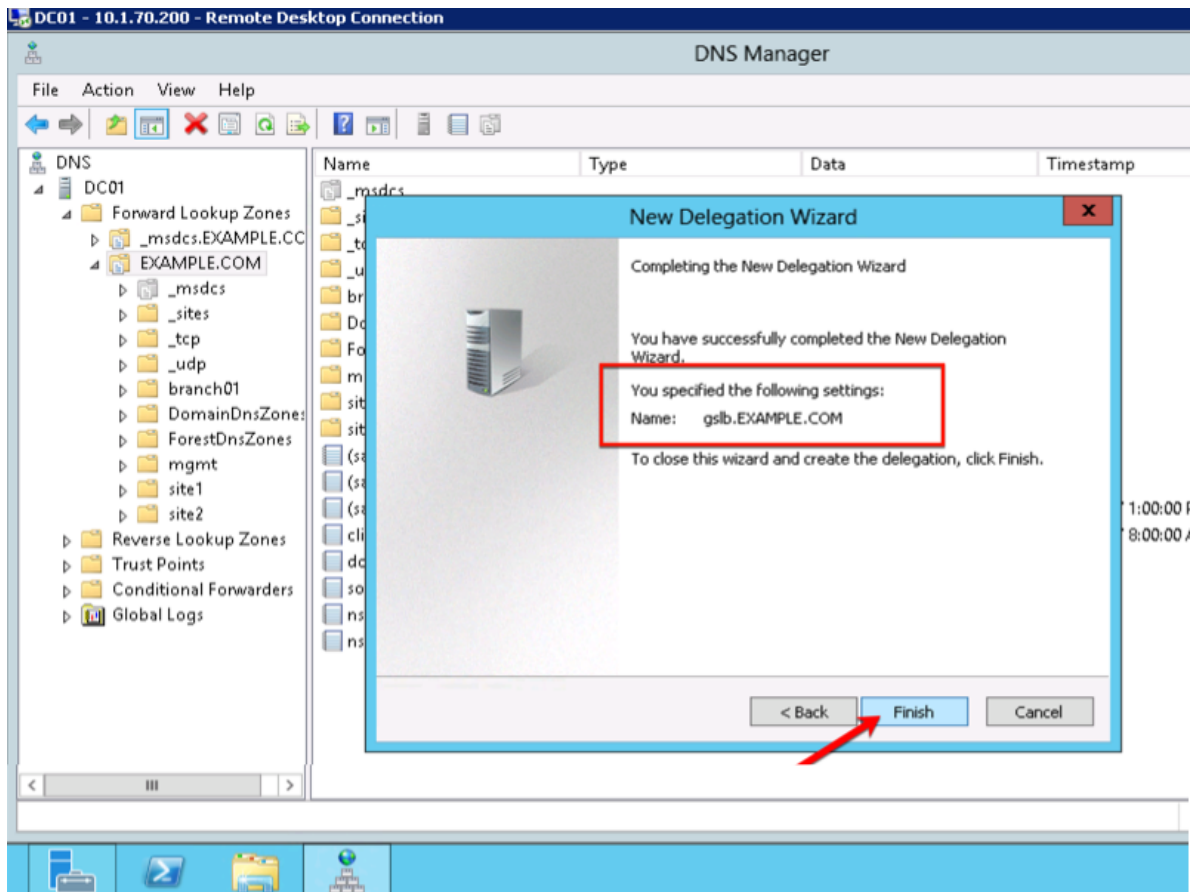
4. Also add "ns2.example.com - 198.51.100.40"



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



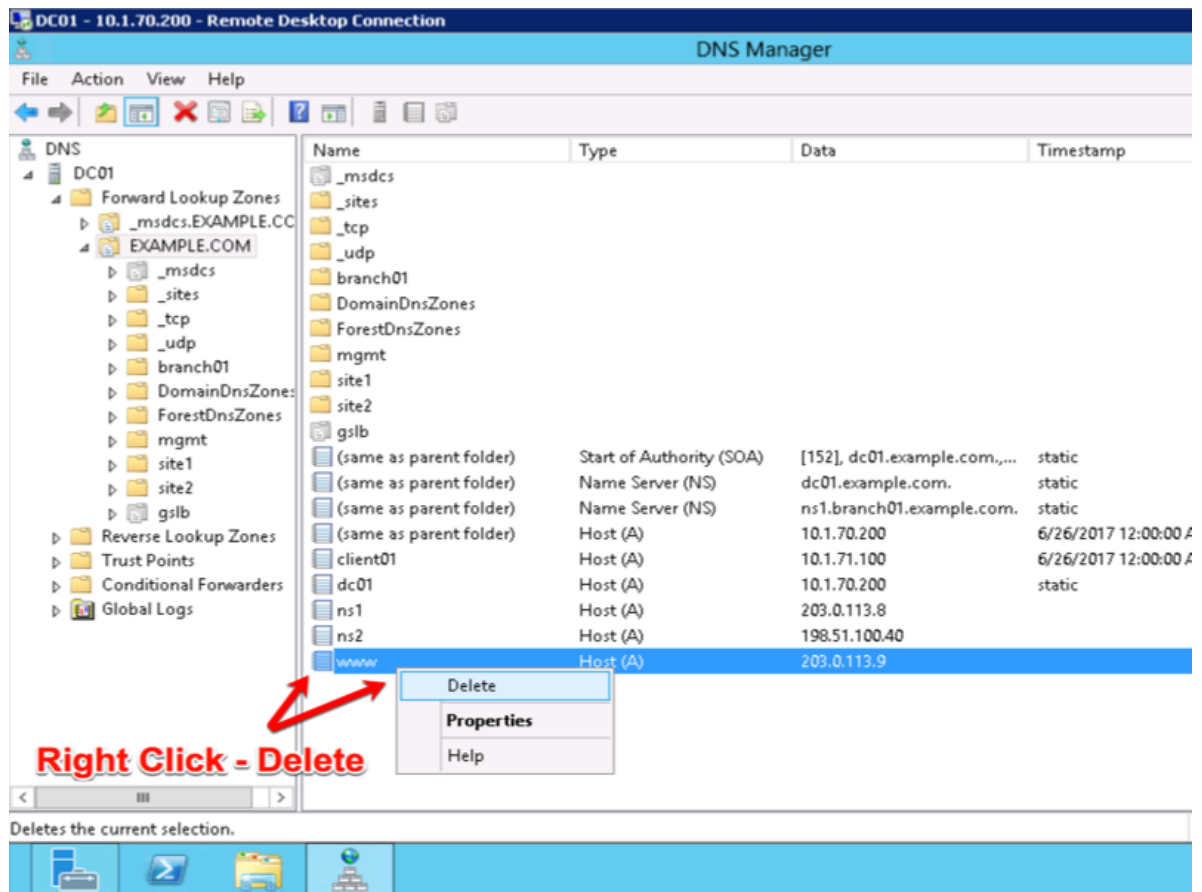
6. Click "Finish"



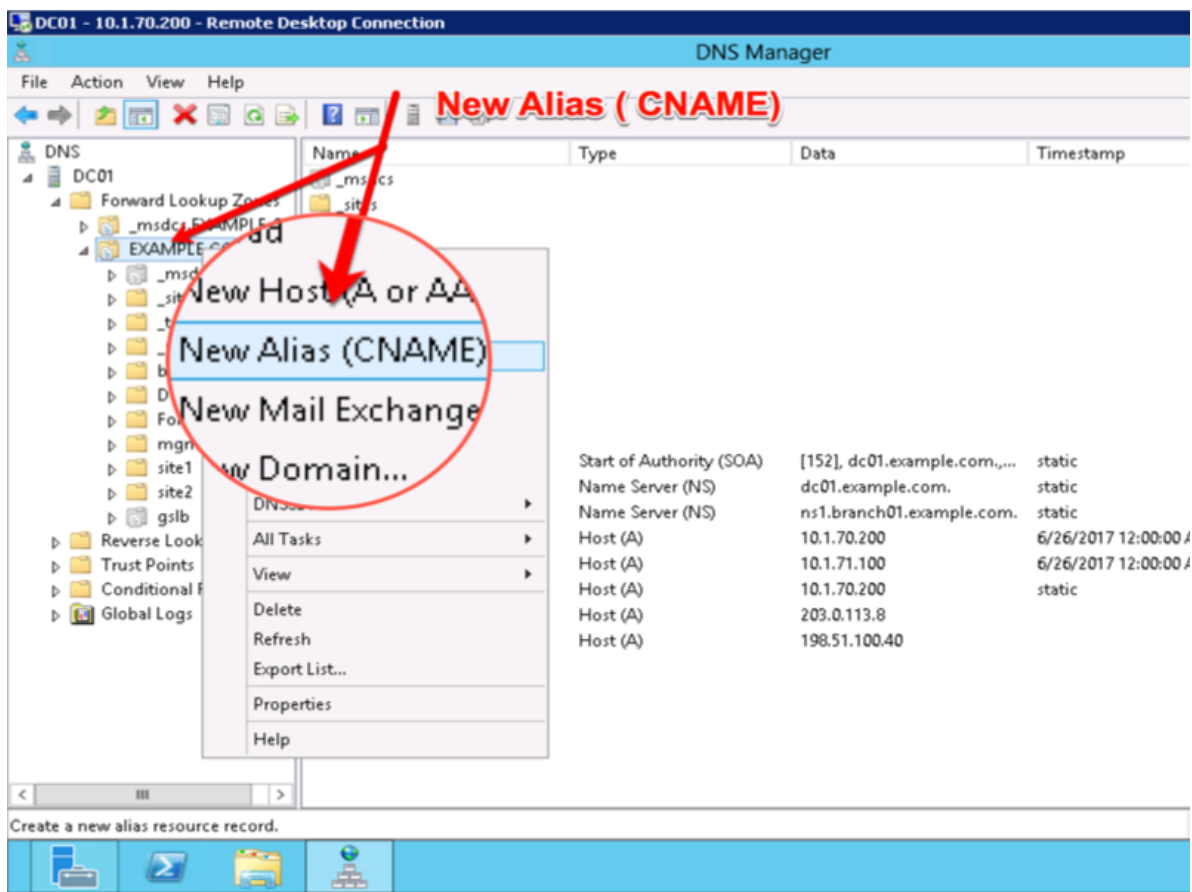
2.1.8.3 CNAME

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

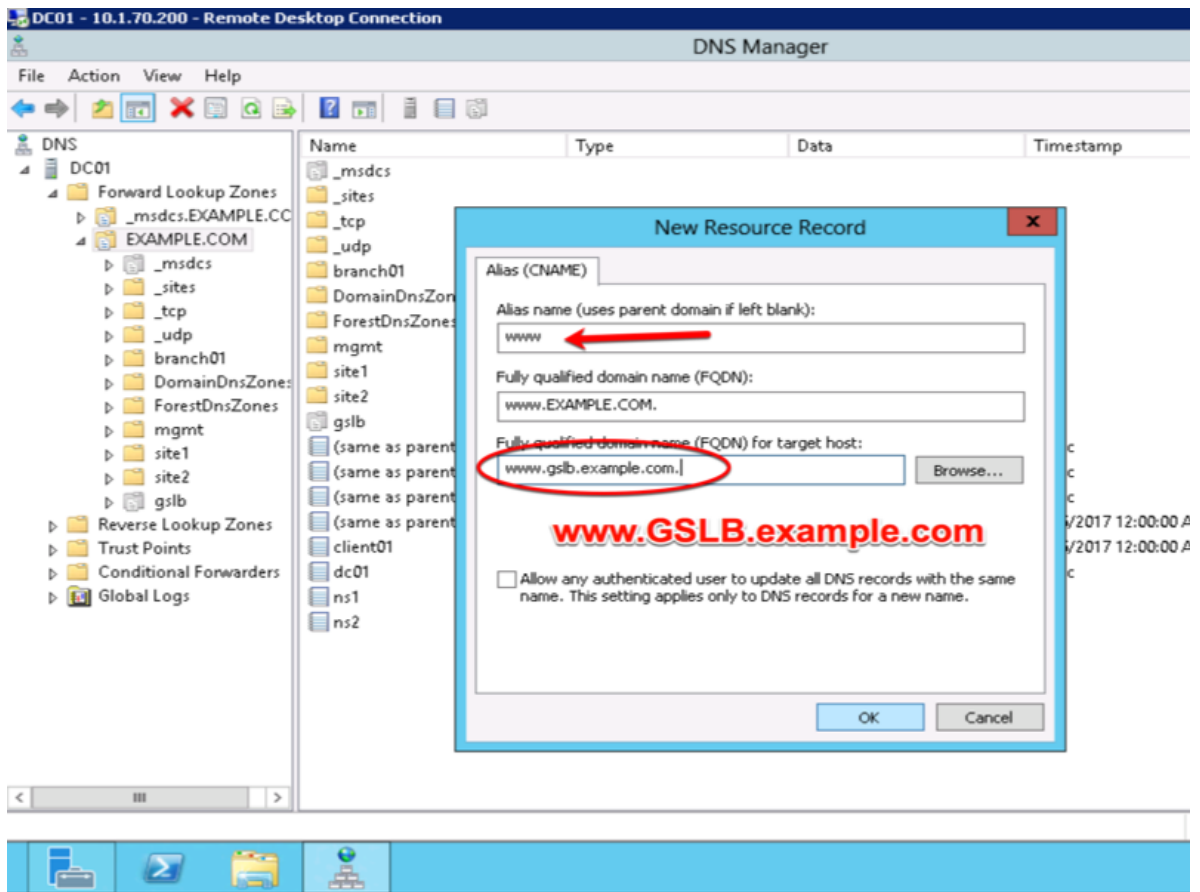
1. Make sure “Forward Lookup Zones” and “EXAMPLE.COM” is expanded. Right click on “www”, and select delete.



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



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



2.1.8.4 Results

From the Jumpbox use “dig” from the CMD prompt

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

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

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

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

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

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

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

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

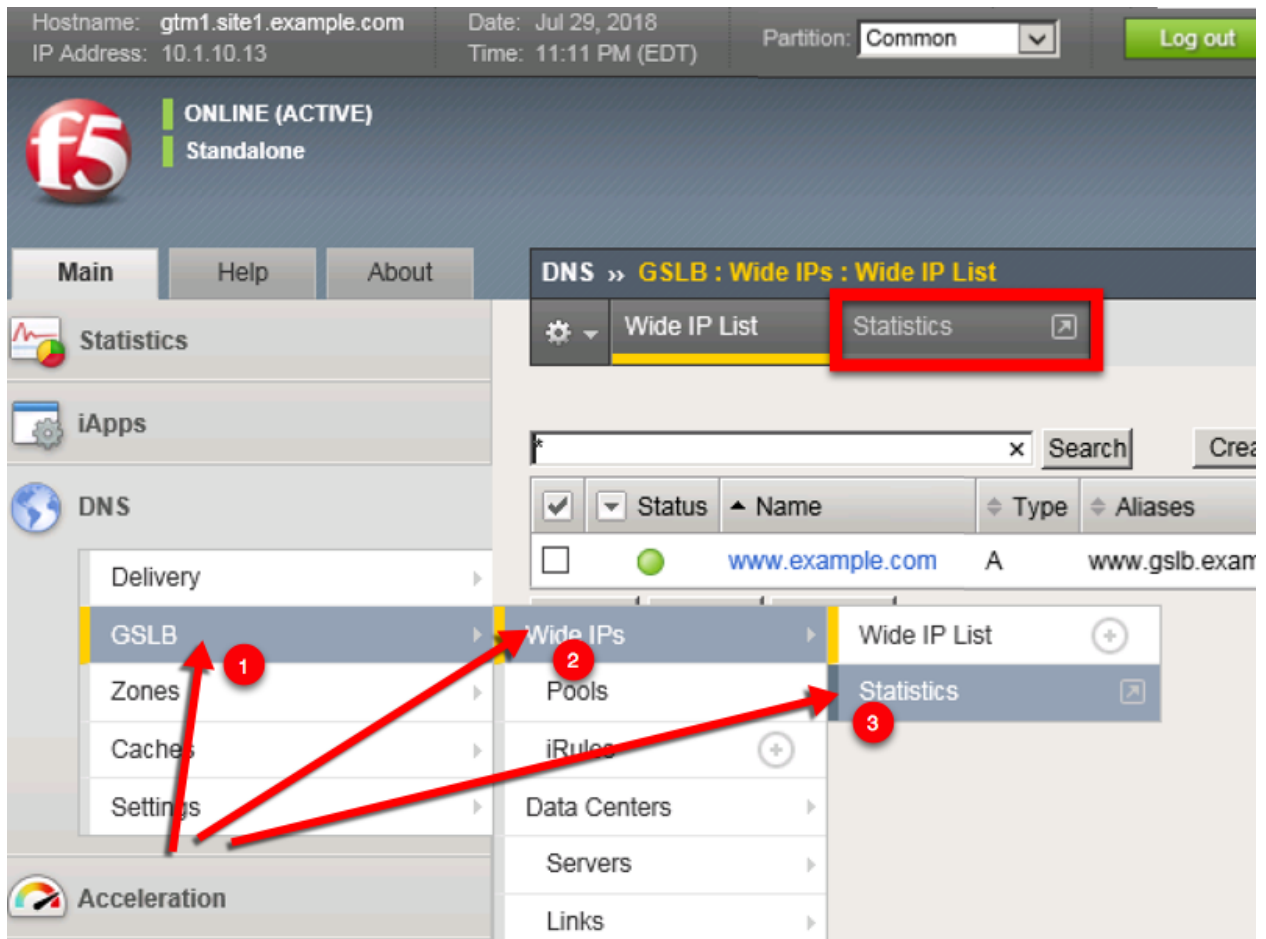
;; <<>> DiG 9.3.2 <<>> www.example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 593
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

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

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

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

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



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

f5 ONLINE (ACTIVE)
Standalone

Main Help About

Statistics » Module Statistics : DNS : GSLB

Statistics Traffic Summary DNS Subscriber Management Network

Statistics

- Dashboard
- Module Statistics
- Analytics
- Performance

iApps

DNS

Acceleration

Device Management

Network

System

Display Options

Statistics Type: Wide IPs

Data Format: Normalized

Auto Refresh: Disabled Refresh

* Search

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

Reset

For more details click

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

TMSH

tmsh show gtm wideip A www.example.com detail

```

gtm1.SITE1
[root@gtm1:Active:Standalone] config # tmsh show gtm wideip A www.example.com detail

Gtm::WideIp::A www.example.com
-----
Status
  Availability : available
  State       : enabled
  Reason      : Available

Requests
  Total       44
  Persisted   0
  Resolved    44
  Dropped     0

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

-----
| Gtm::Pool::A www.example.com_pool
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Available
|
| Load Balancing
|   Preferred   44
|   Alternate   0
|   Fallback    0
|   Returned from DNS 0
|   Returned to DNS 0
|   Dropped     0
|
-----
| Gtm::Pool Member: www.example.com_pool:A isp1_site1_www.example.com_tcp_https_virtual:site1_ha-pair
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Available
|
| Load Balancing
|   Preferred   35
|   Alternate   0
|   Fallback    0
|
-----
| Gtm::Virtual Server: isp1_site1_www.example.com_tcp_https_virtual
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Monitor /Common/bigip from 203.0.113.5 : UP
|   Destination : 203.0.113.9:443
|   Up Time     : 10:18
|
| Link Name      203.0.113.1
|
| Global
|   Picks        35
|   Connections  0
|   Virtual Server Score 1
|
| Throughput
|   In  Out
|   Bits/sec  0  0
|   Packets/sec 0  0
|
-----
| Gtm::Pool Member: www.example.com_pool:A isp2_site2_www.example.com_tcp_https_virtual:site2_ha-pair
-----
| Status
|   Availability : available
|   State       : enabled
|   Reason      : Available

```

TMSH

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

```
gtm1.SITE1
[root@gtm1:Active:Standalone] config # tail -f -n 12 /var/log/ltm
Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com qid 991 from 198.51.100.68#64119: view none: query: www.gslb.example.com IN A + (203.0.113.8%0)
Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com qid 991 from 198.51.100.68#64119 [www.gslb.example.com A] [round robin selected pool (www.example.com_pool)] [pool member check succeeded (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9) - pool member state is available (green)] [round robin selected pool member (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9)]
Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com qid 991 to 198.51.100.68#64119: [NOERROR qr,aa,rd] response: www.gslb.example.com. 30 IN A 203.0.113.9;
Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 from 198.51.100.68#64120: view none: query: www.gslb.example.com IN A + (203.0.113.8%0)
Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 from 198.51.100.68#64120 [www.gslb.example.com A] [round robin selected pool (www.example.com_pool)] [pool member check succeeded (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9) - pool member state is available (green)] [round robin selected pool member (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9)]
Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 to 198.51.100.68#64120: [NOERROR qr,aa,rd] response: www.gslb.example.com. 30 IN A 203.0.113.9;
Jul 30 00:23:44 gtm1 info tmm[11966]: 2018-07-30 00:23:43 gtm1.site1.example.com qid 261 from 203.0.113.68#64121: view none: query: www.example.com IN A + (203.0.113.8%0)
Jul 30 00:23:44 gtm1 info tmm[11966]: 2018-07-30 00:23:43 gtm1.site1.example.com qid 261 from 203.0.113.68#64121 [www.example.com A] [round robin selected pool (www.example.com_pool)] [pool member check succeeded (isp2_site2_www.example.com_tcp_https_virtual:198.51.100.41) - pool member state is available (green)] [round robin selected pool member (isp2_site2_www.example.com_tcp_https_virtual:198.51.100.41)]
Jul 30 00:23:44 gtm1 info tmm[11966]: 2018-07-30 00:23:43 gtm1.site1.example.com qid 261 to 203.0.113.68#64121: [NOERROR qr,aa,rd] response: www.example.com. 30 IN A 198.51.100.41;
Jul 30 00:23:50 gtm1 info tmm[11966]: 2018-07-30 00:23:50 gtm1.site1.example.com qid 97 from 203.0.113.68#64122: view none: query: www.example.com IN A + (203.0.113.8%0)
Jul 30 00:23:50 gtm1 info tmm[11966]: 2018-07-30 00:23:50 gtm1.site1.example.com qid 97 from 203.0.113.68#64122 [www.example.com A] [round robin selected pool (www.example.com_pool)] [pool member check succeeded (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9) - pool member state is available (green)] [round robin selected pool member (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9)]
Jul 30 00:23:50 gtm1 info tmm[11966]: 2018-07-30 00:23:50 gtm1.site1.example.com qid 97 to 203.0.113.68#64122: [NOERROR qr,aa,rd] response: www.example.com. 30 IN A 203.0.113.9;
```

2.1.9 Failure Condition

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

```
Command Prompt
:: MSG SIZE rcvd: 72

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

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

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

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

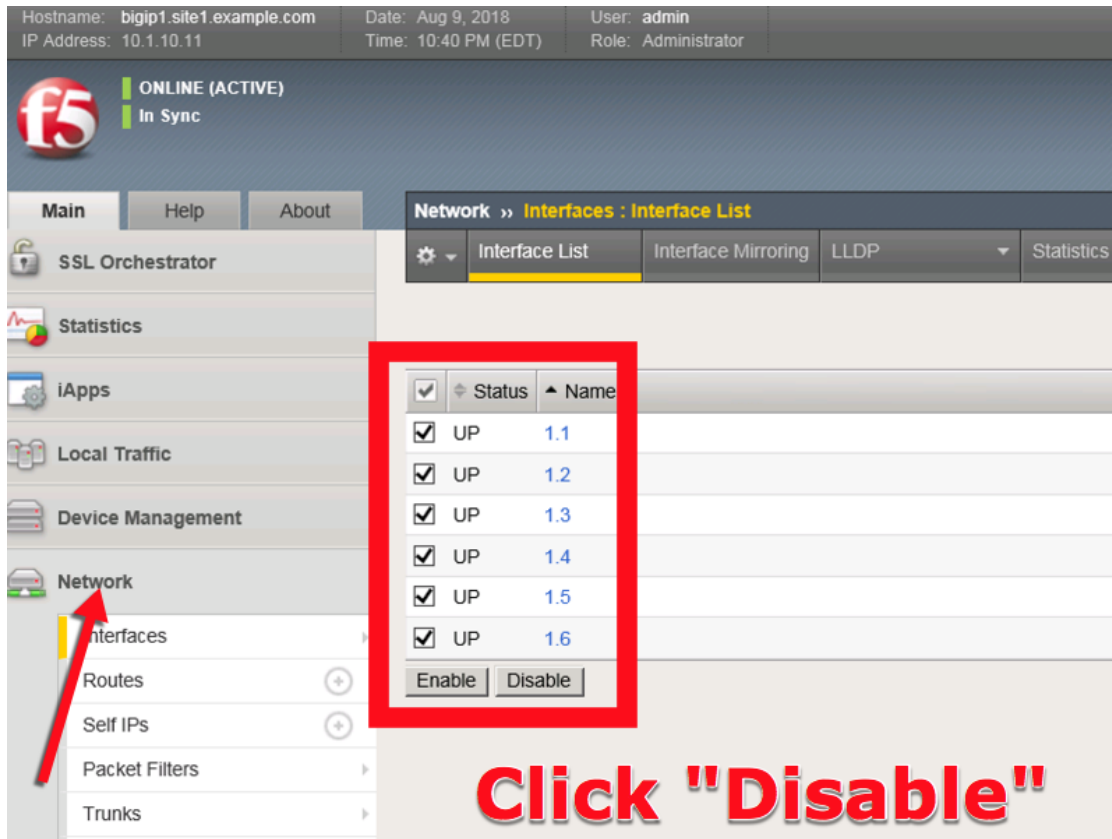
;; Query time: 31 msec
;; SERVER: 10.1.70.200#53(10.1.70.200)
;; WHEN: Sun Jun 25 21:37:31 2017
;; MSG SIZE rcvd: 72

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

Log into both the Active and the Standby ADC device in SITE1 and disable all interfaces.

<https://bigip1.site1.example.com/tmui/Control/jspmap/tmui/local/b/network/interface/list.jsp>

<https://bigip2.site1.example.com/tmui/Control/jspmap/tmui/local/b/network/interface/list.jsp>



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

TMSH

tmsh modify interface all disabled

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

Hostname: gtm1.site1.example.com Date: Aug 9, 2018 User: admin
IP Address: 10.1.10.13 Time: 11:01 PM (EDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

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

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

Server List Trusted Server Certificates Statistics

Search

<input checked="" type="checkbox"/>	Status	Name	Devices	Address
<input type="checkbox"/>		gtm1.site1_server	1	201.10.10.10
<input type="checkbox"/>		gtm1.site2_server	1	192.168.1.10
<input type="checkbox"/>		site1_ha-pair	2	201.10.10.10
<input type="checkbox"/>		site2_ha-pair	2	192.168.1.10

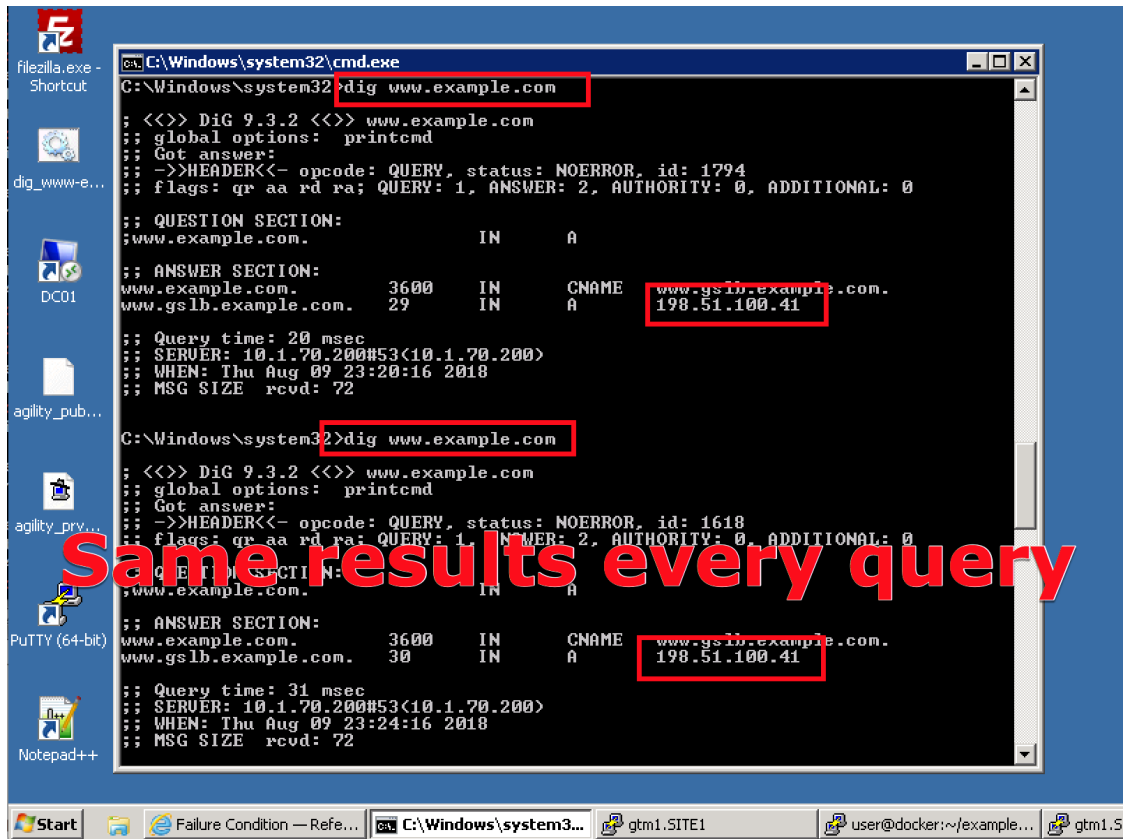
Enable Disable Delete...

Site1 HA pair is Down

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

TMSH

tmsh show gtm server



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

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

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

TMSH

tmsh modify interface all enabled

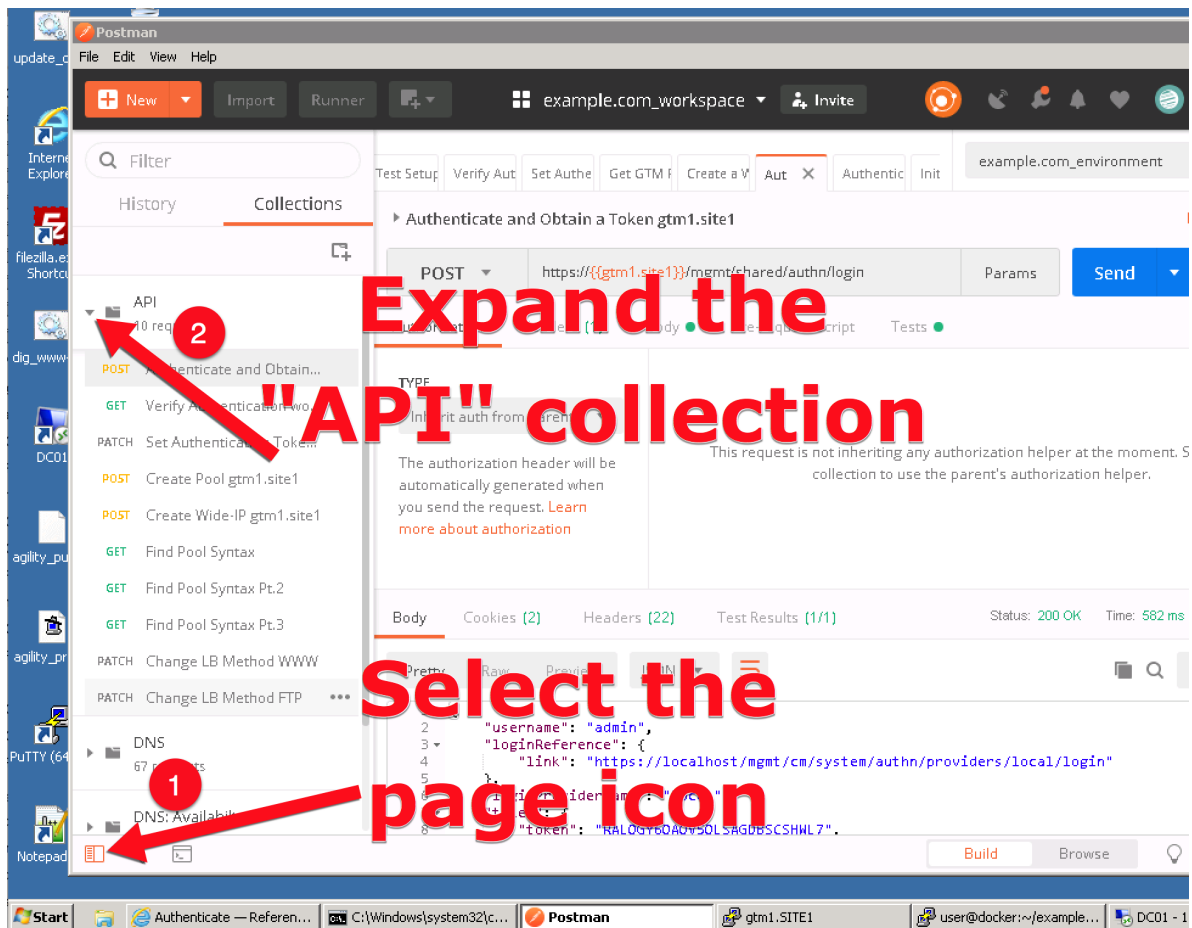
2.1.10 Rest API

2.1.10.1 Authenticate

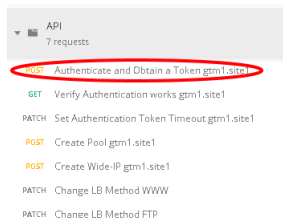
From the Jumpbox using the Postman application navigate to the “API” section under the Collections on the left.

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

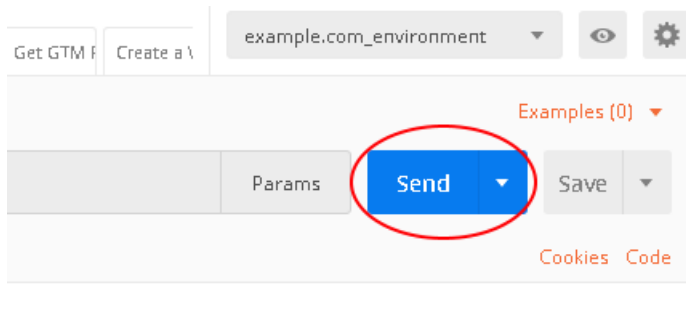
1. Reveal the navigation panel in Postman



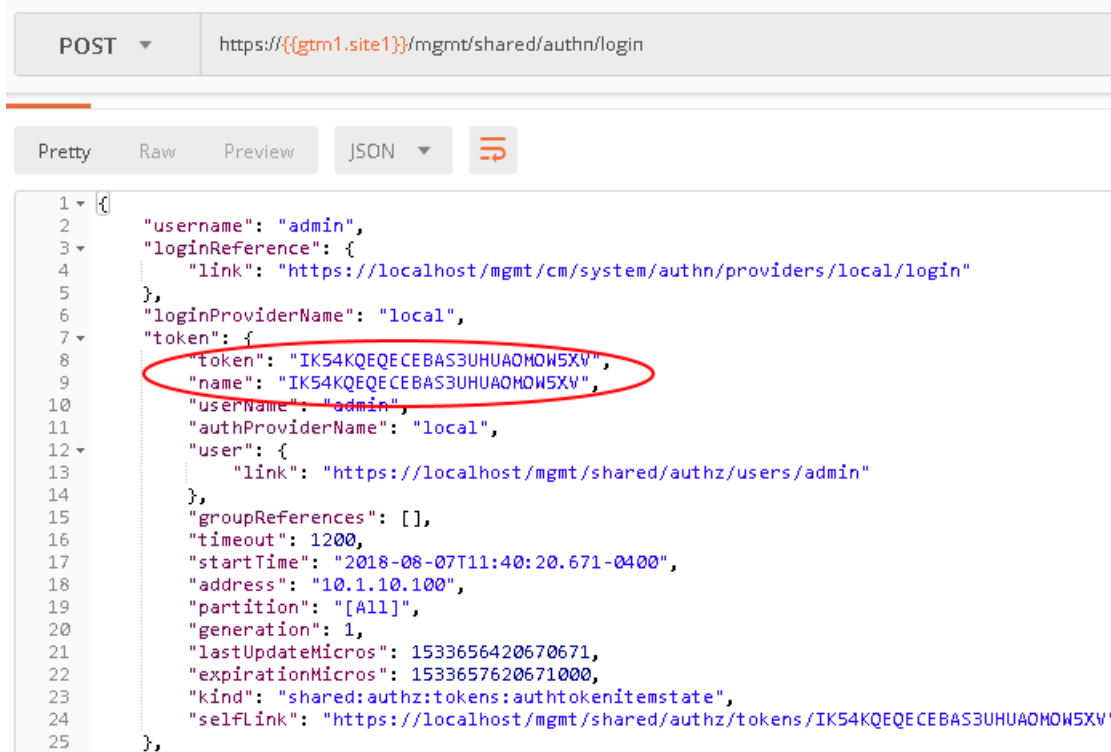
2. Click on “Authenticate and Obtain Token from gtm1.site1”.



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



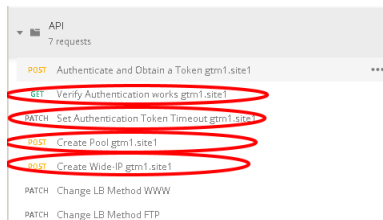
4. Open the response body and observe the received token. The token value is dynamic and your result will not be the same as illustrated below. The token received will be used for all subsequent authenticated actions with the BIG-IP DNS.



2.1.10.2 POST

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

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

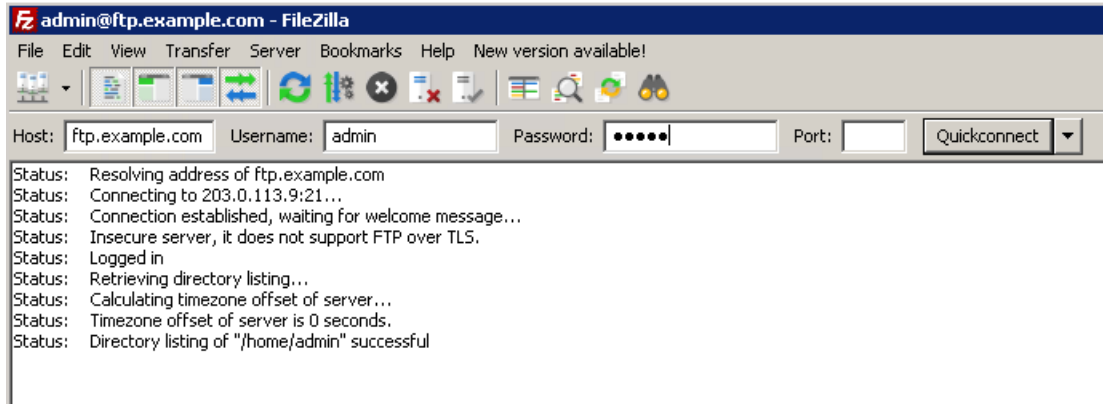


Once complete, login to gtm1.site1 via Web interface and look for the new configuration elements to confirm that they were successfully created. Do the same on gtm1.site2.

2.1.10.3 Results

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

Note: Use FTP credentials admin/admin



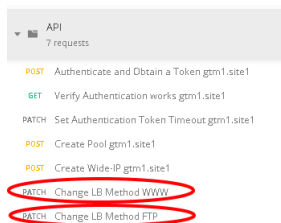
You've just successfully created a new highly available service on BIG-IP DNS all with only a few very simple API commands.

2.1.10.4 Active/Standby

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

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

Open Postman and send both of the patch commands below.



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

2.1.10.5 API Extras (Optional)

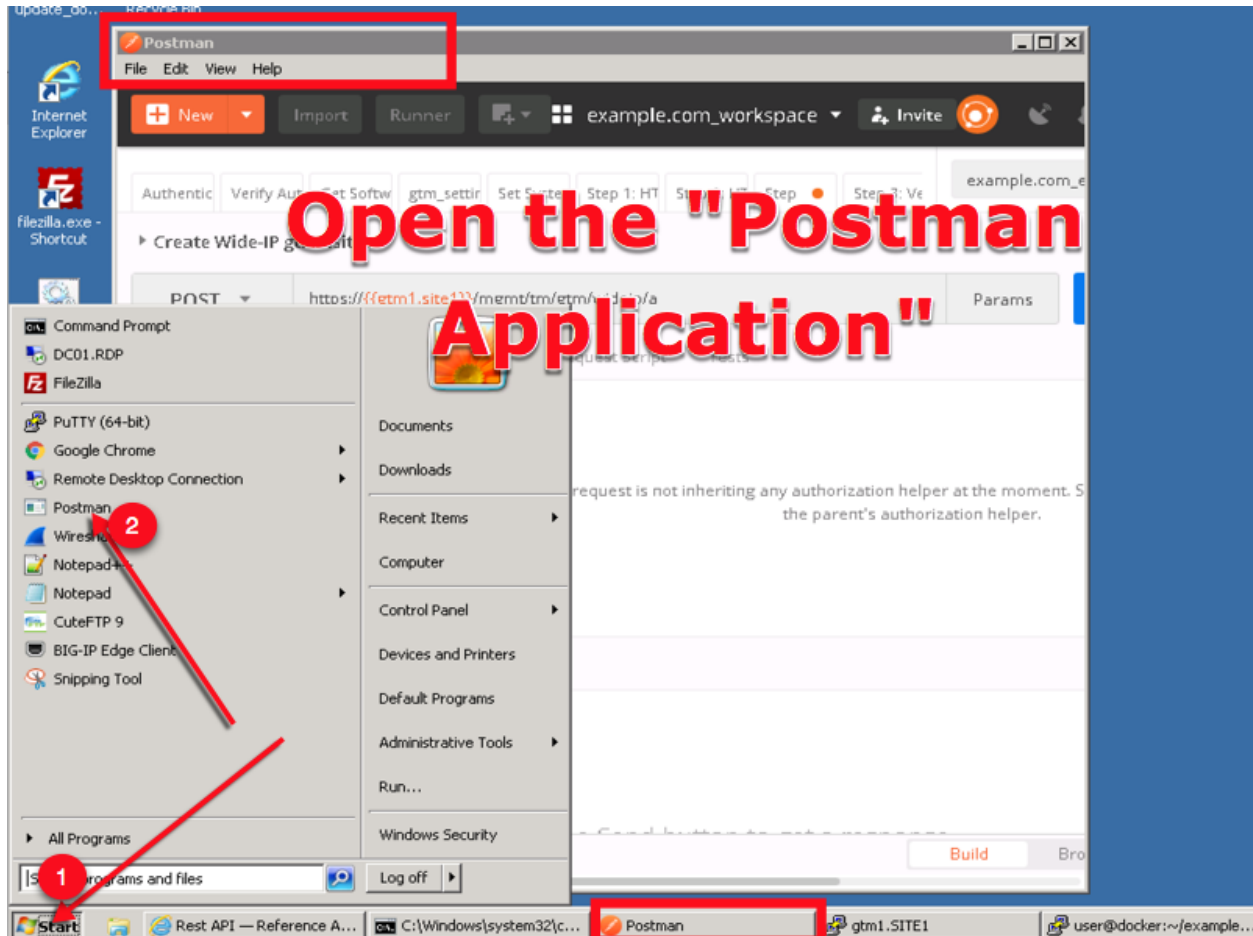
In Postman, feel free to browse the other collections and experiment with additional REST commands.

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



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

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

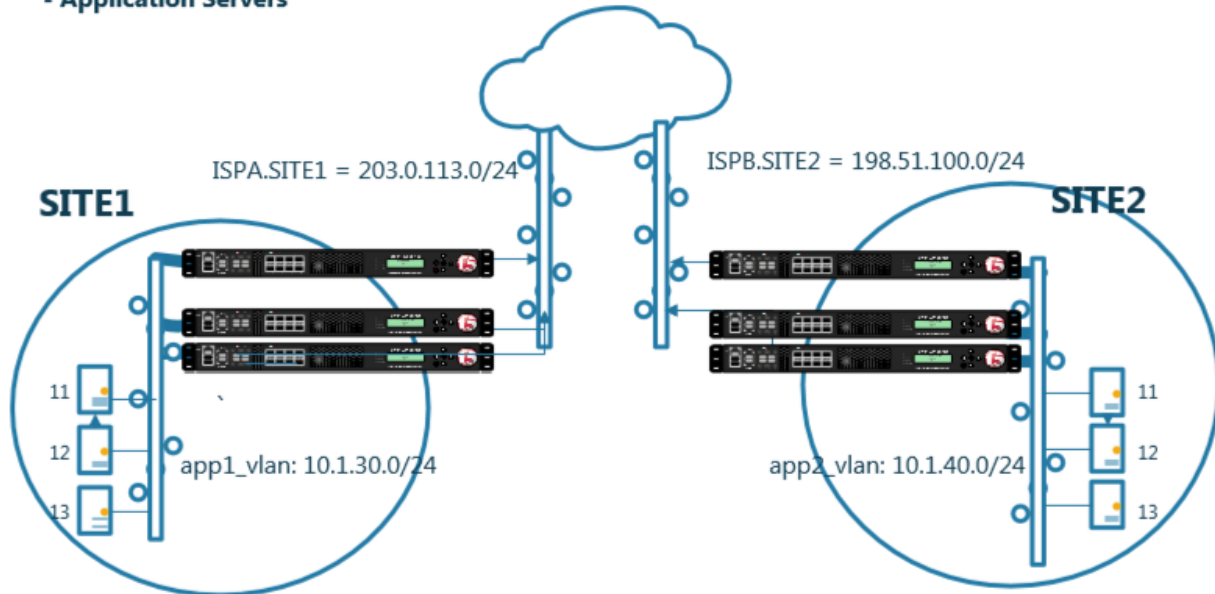


2.1.11 Congratulations

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

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

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



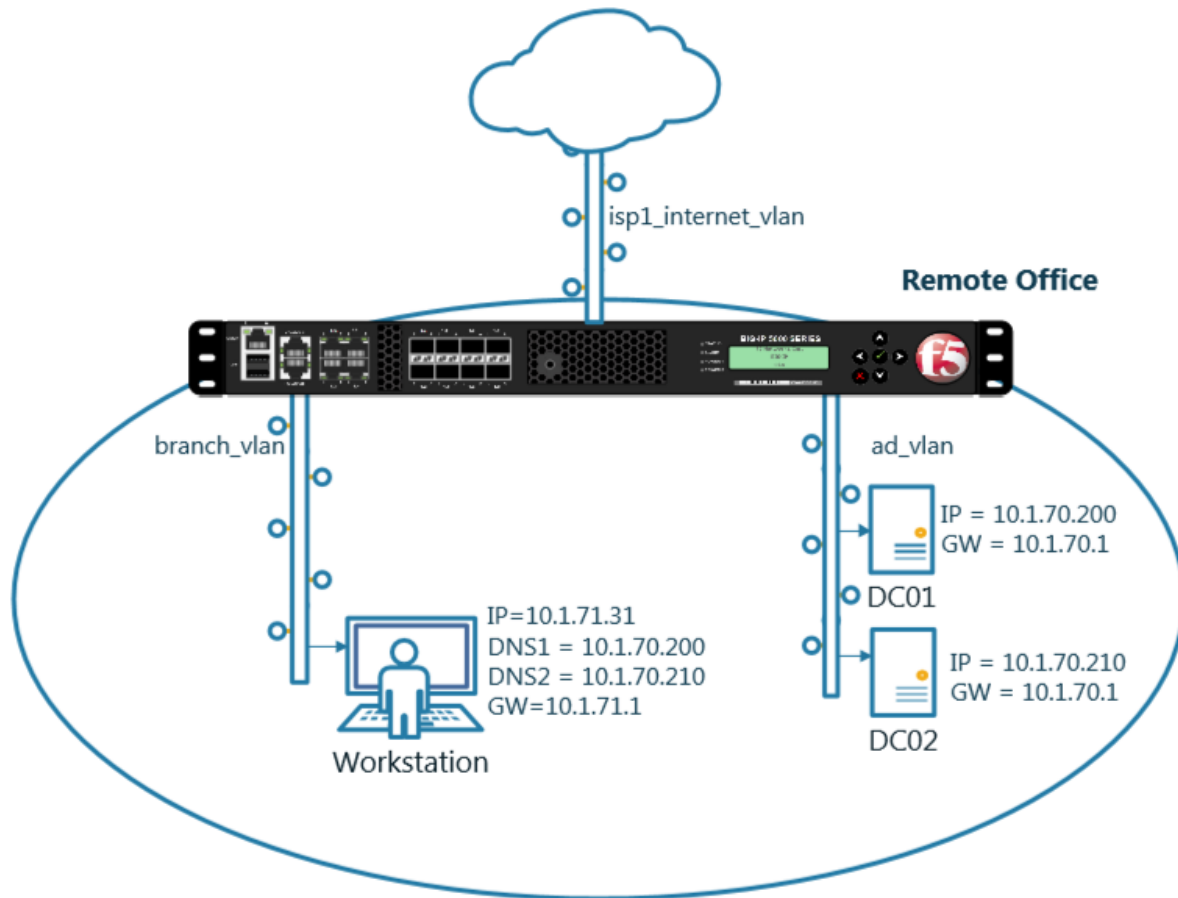
- Students will configure F5 DNS servers to support GSLB (Global Services Load Balancing) on a single device in site1.
- Join an additional F5 DNS server in site2 to the GSLB cluster.
- An Internal group of DNS servers is authoritative for the zone example.com and contains a static A record for “www.example.com”,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

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

2.2 Security

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

The F5 device is directly connected to the internet.



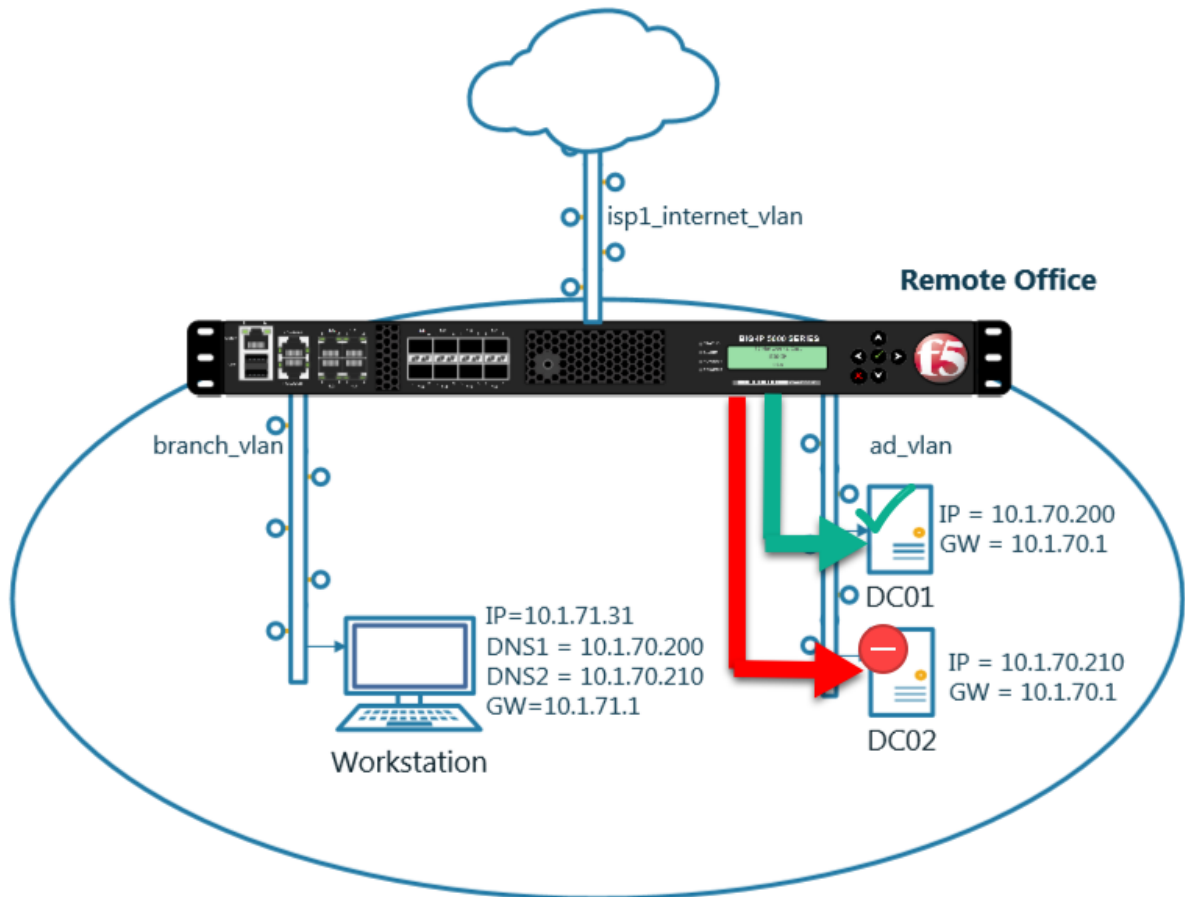
Students will work with the following concepts as part of a group of lab exercises.

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

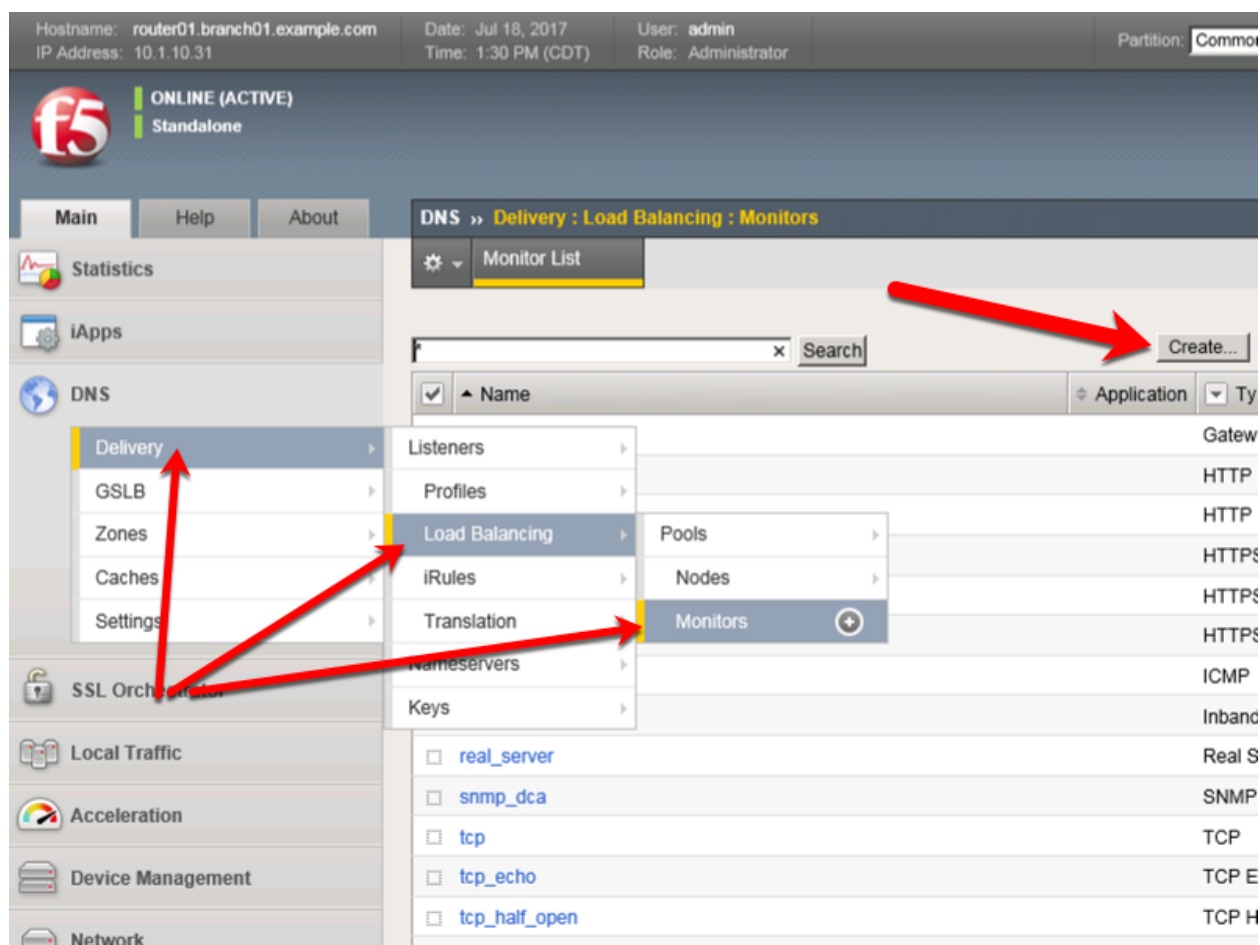
2.2.1 Transparent Cache

2.2.1.1 Monitors

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



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



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

Create a monitor according to the following table:

Field	Value
Name	example.com_dns_monitor
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>

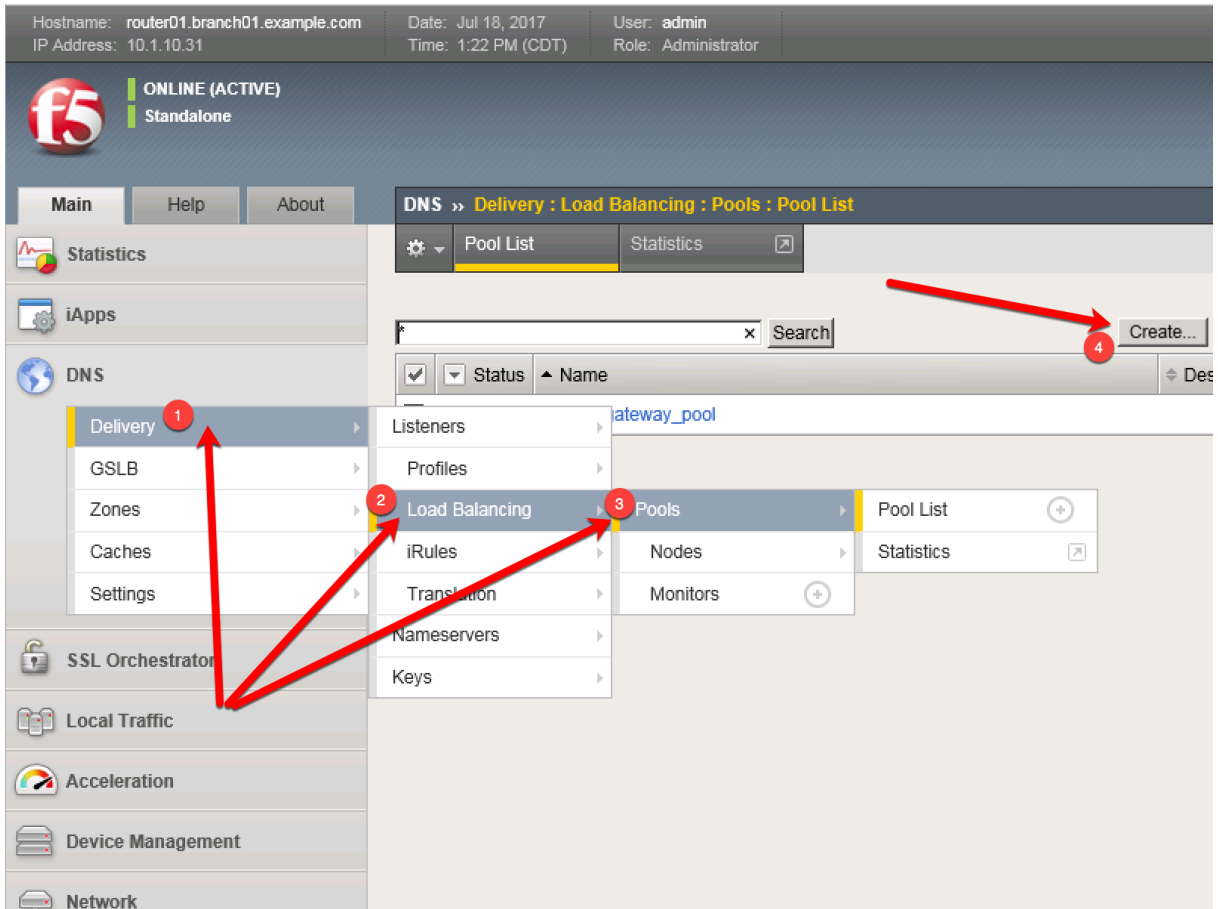
TMSH

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

2.2.1.2 Load Balancing

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

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



Create a pool according to the following table:

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

Configuration: **Advanced** ▼

Name	branch01_dns_pool
Description	
Health Monitors	<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>v</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

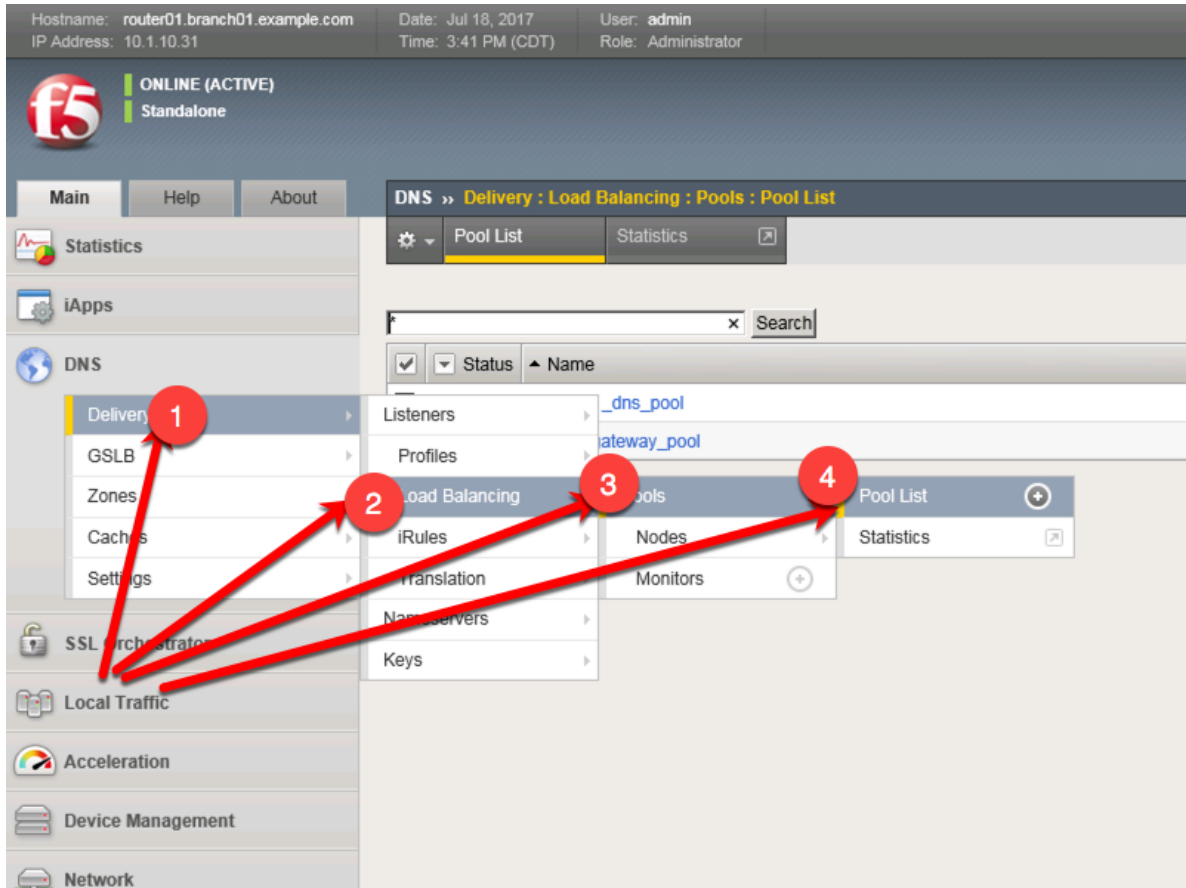
```
tmsl create ltm pool branch01_dns_pool members add { dc01.branch01.example.com_node:53 { address 10.1.70.200 } dc02.branch01.example.com_node:53 { address 10.1.70.210 } } monitor exam-
```

ple.com_dns_monitor

2.2.1.3 Results

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

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



<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

ONLINE (ACTIVE)
Standalone

Main Help About

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

Properties Members Statistics

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

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

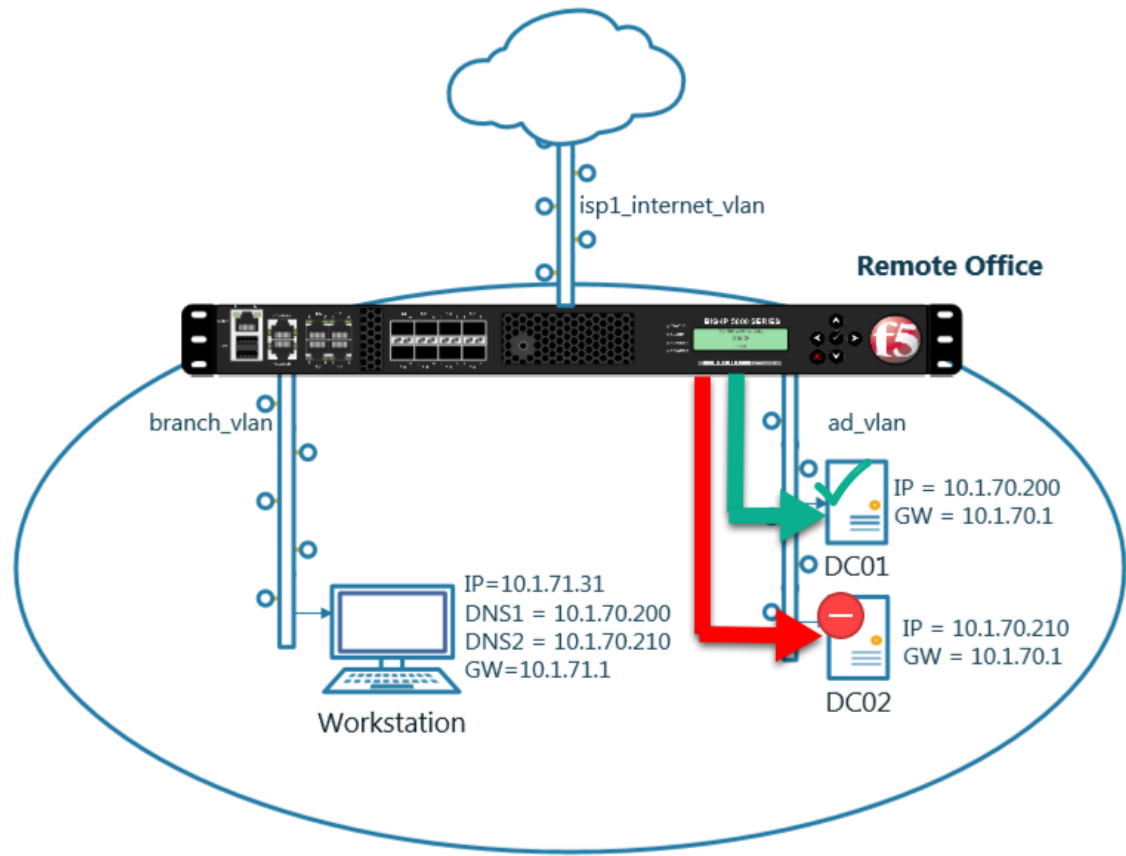
<input checked="" type="checkbox"/>	Status	Member	Address	Service	Port	FQDN
<input type="checkbox"/>		dc01.branch01.example.com_node:53	10.1.70.200	53		Nc
<input type="checkbox"/>		dc02.branch01.example.com_node:53	10.1.70.210	53		Nc

Enable Disable Force Offline Remove

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

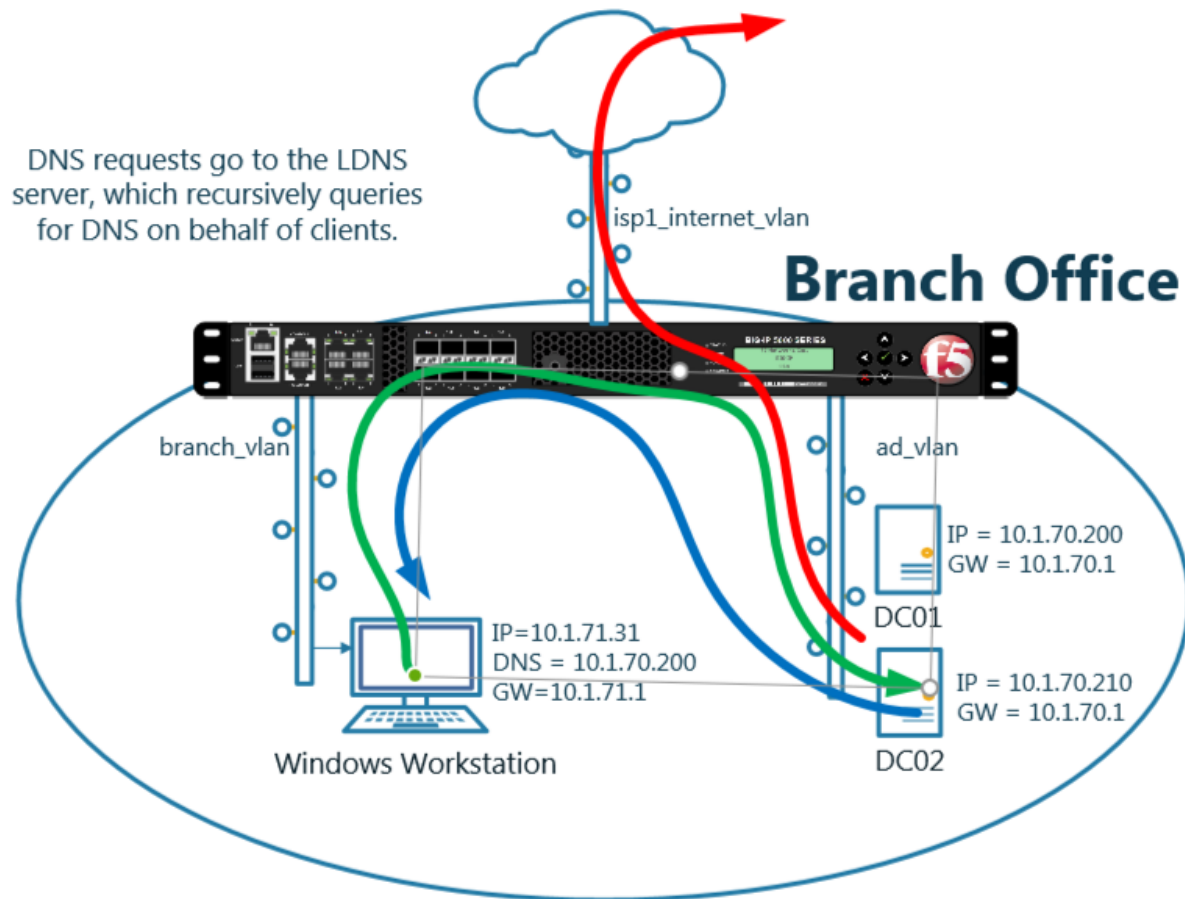
TMSH

tmsh show ltm pool branch01_dns_pool detail

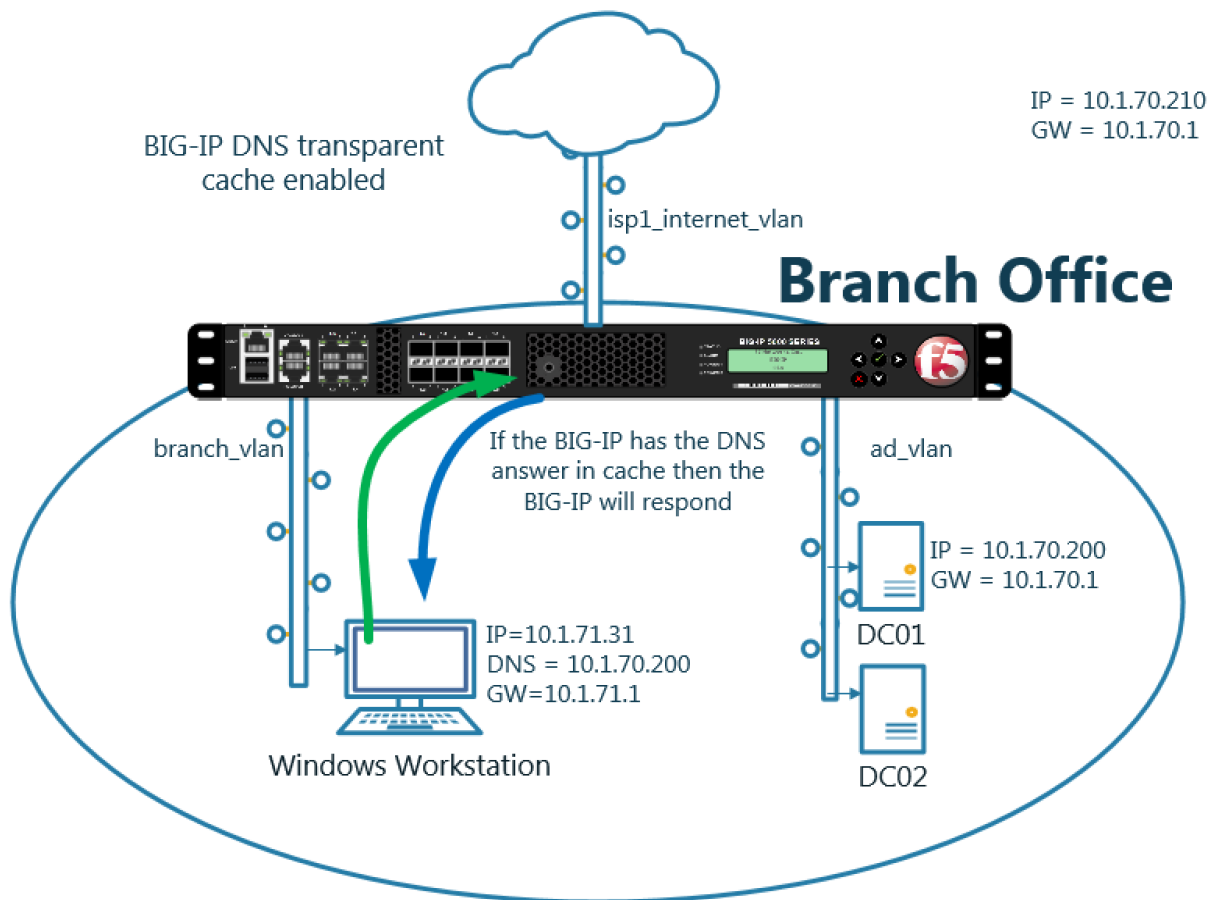


In this module we will prepare the objects required to build a transparent cache.

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

Field	Value
Name	transparent_cache
Resolver Type	Transparent

Hostname: router01.branch01.example.com Date: Jun 20, 2017 User: admin
IP Address: 10.1.10.31 Time: 9:38 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About DNS » Caches : Cache List » New...

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

General Properties

Name transparent_cache
Resolver Type Transparent (None)

DNS Cache

Message Cache Size 1048576 bytes
Cache List 10485760 bytes
Size 10485760 bytes
☐ Enabled
RRSet Rotate none

Cancel Repeat Finished

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

TMSH command for router01.branch01:

TMSH

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

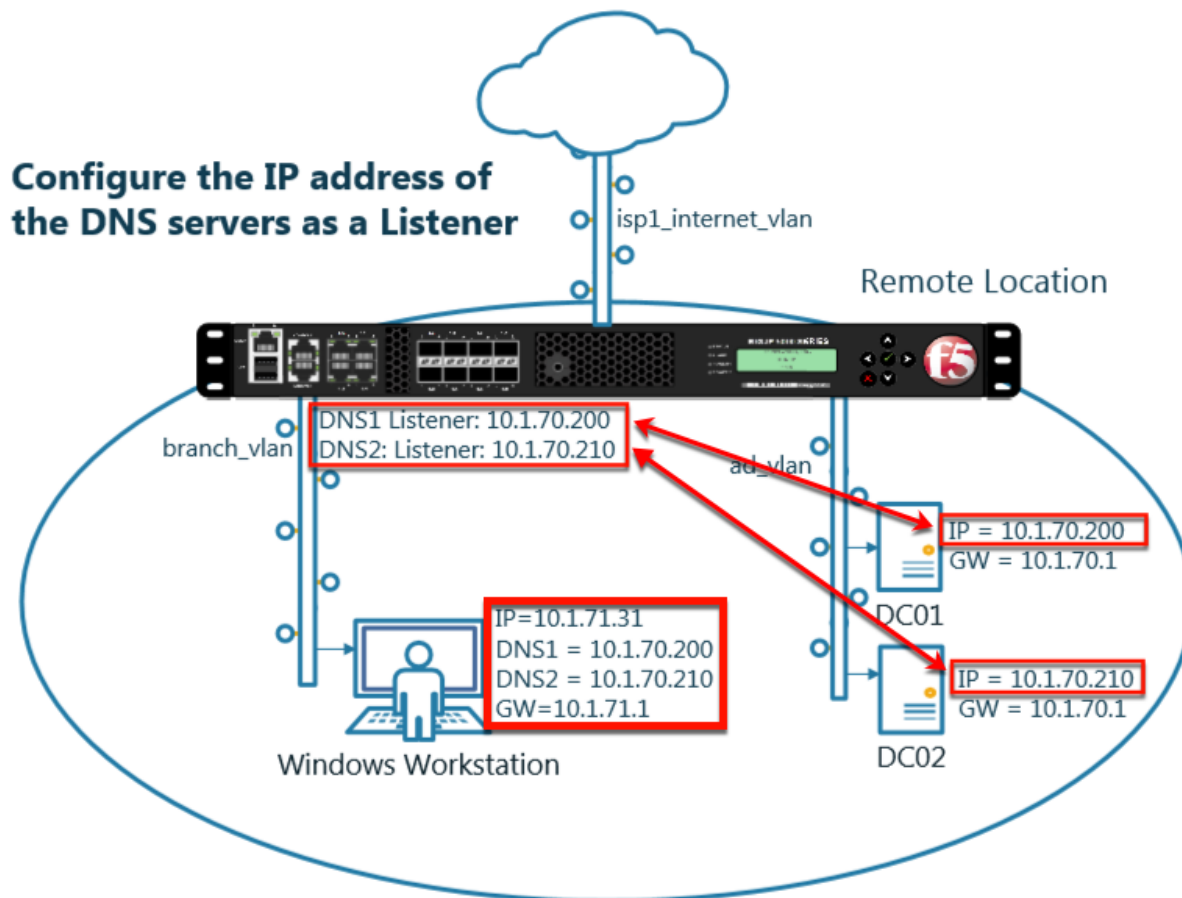
2.2.2 Listeners

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

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

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

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

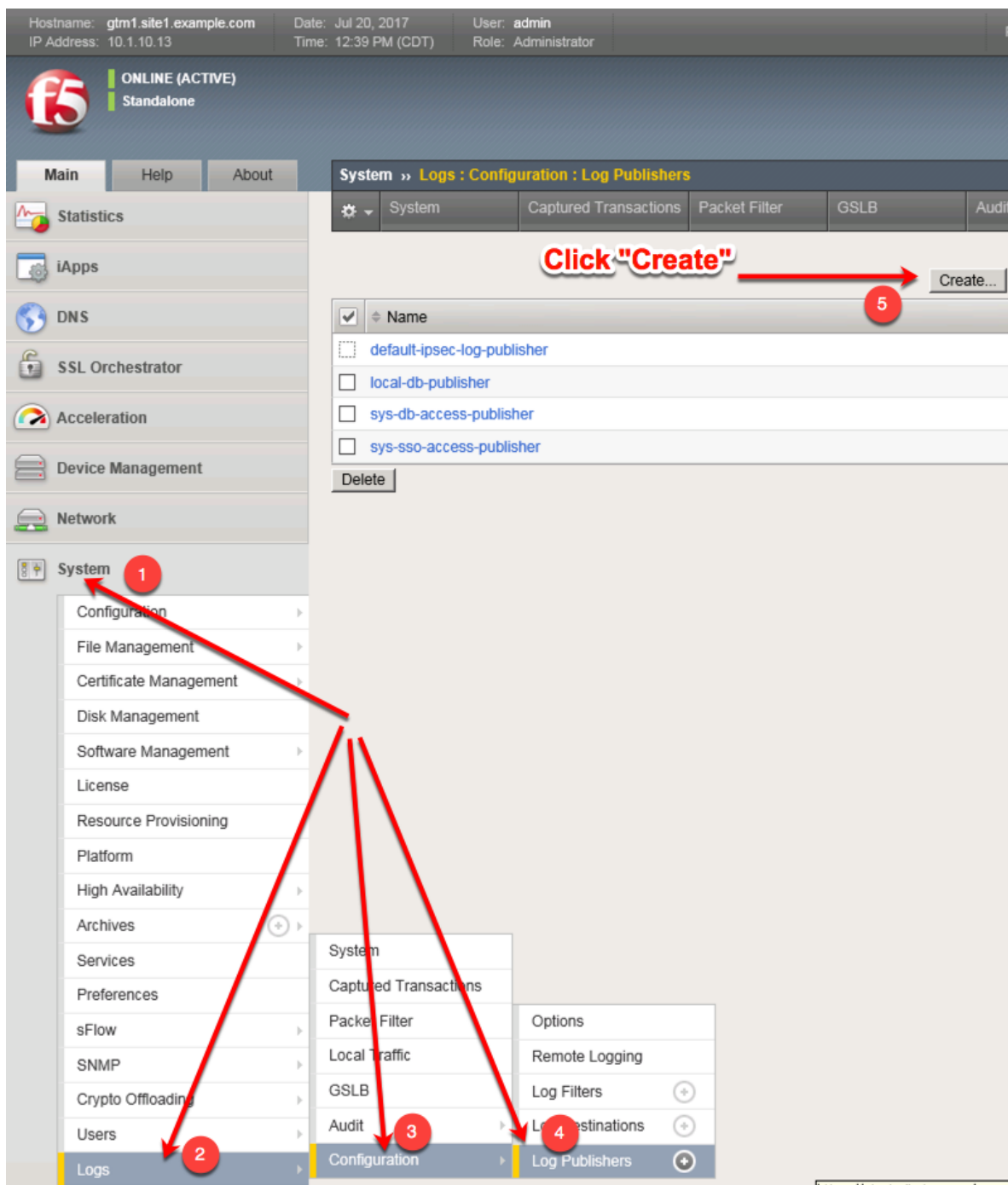


2.2.2.1 Log Profile

Configure DNS query and response logging.

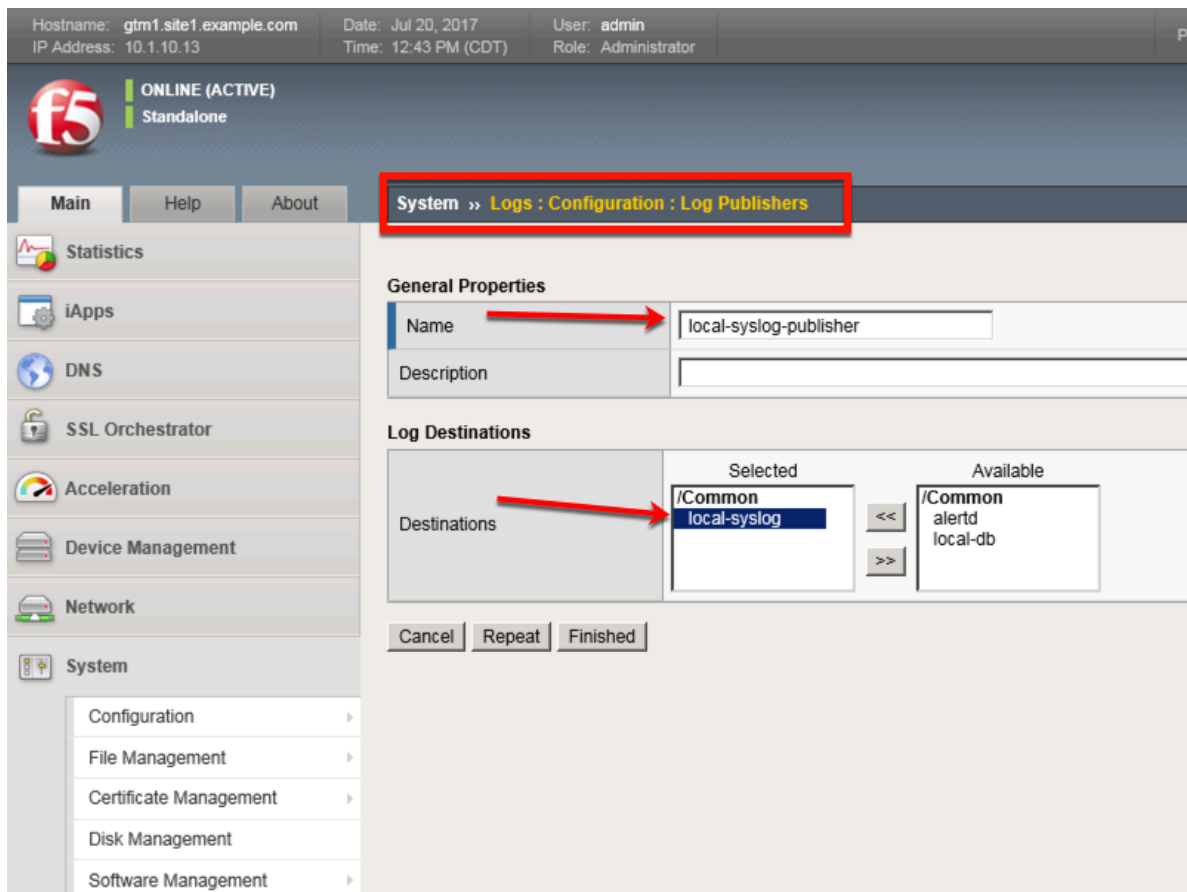
1. Create a "Log Publisher" for local syslog.

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



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

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



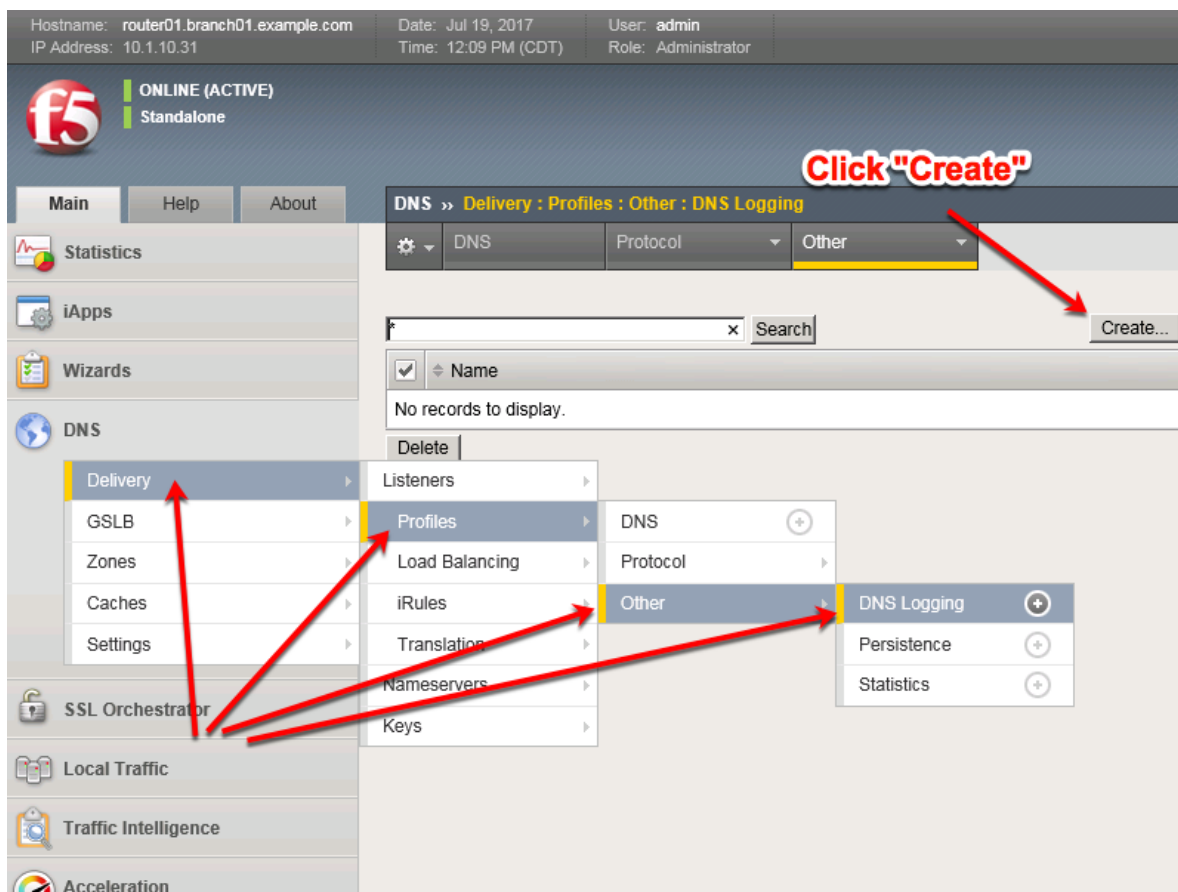
https://router01.branch01.example.com/tmui/Control/jspmap/tmui/system/log/create_publisher.jsp

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:

Field	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	example_dns_logging_profile
Description	

Configuration

Log Publisher	local-syslog-publisher
Log Queries	<input checked="" type="checkbox"/> Enabled
Log Responses	<input checked="" type="checkbox"/> Enabled

Log Fields

Include Complete Answer	<input checked="" type="checkbox"/> Enabled
Include Query ID	<input checked="" type="checkbox"/> Enabled
Include Source	<input checked="" type="checkbox"/> Enabled
Include Timestamp	<input checked="" type="checkbox"/> Enabled
Include View	<input checked="" type="checkbox"/> Enabled

Cancel Repeat Finished

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

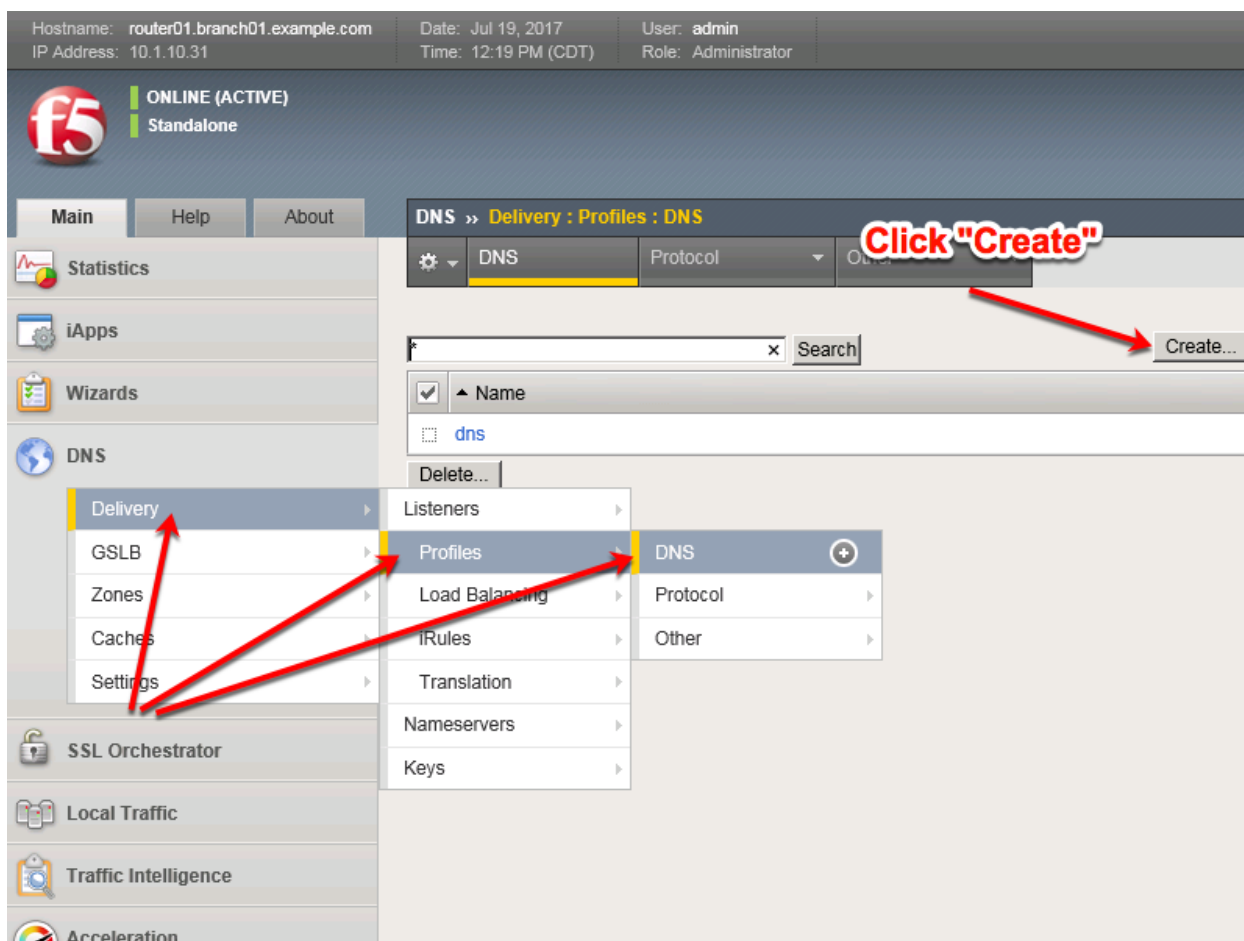
TMSH

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

2.2.2.2 DNS Profile

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

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



Create a DNS profile as shown in the table below.

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

Hostname: router01.branch01.example.com Date: Jul 25, 2017 User: admin
IP Address: 10.1.10.31 Time: 11:40 PM (CDT) Role: Administrator Partition: Common Log out


f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

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

General Properties

Name: example.com_dns_ 
Parent Profile: dns



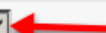


Denial of Service Protection Custom ☐

Rapid Response Mode: Disabled ☐
Rapid Response Last Action: Drop ☐

Hardware Acceleration

Protocol Validation: Disabled ☐
Response Cache: Disabled ☐





DNS Features

DNSSEC: Enabled ☐
GSLB: Enabled ☐
DNS Express: Enabled ☐
DNS Cache: Enabled ☐  ☒ 
DNS Cache Name: transparent_cache ☐  ☒
DNS IPv6 to IPv4: Disabled ☐
Unhandled Query Actions: Allow ☐
Use BIND Server on BIG-IP: Disabled ☐  ☒ 

DNS Traffic

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

Logging and Reporting

Logging: Enabled ☐  ☒ 
Logging Profile: example_dns_logging_profile ☐  ☒
AVR Statistics Sample Rate: ☒ Enabled 1/ 1 queries sampled 

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

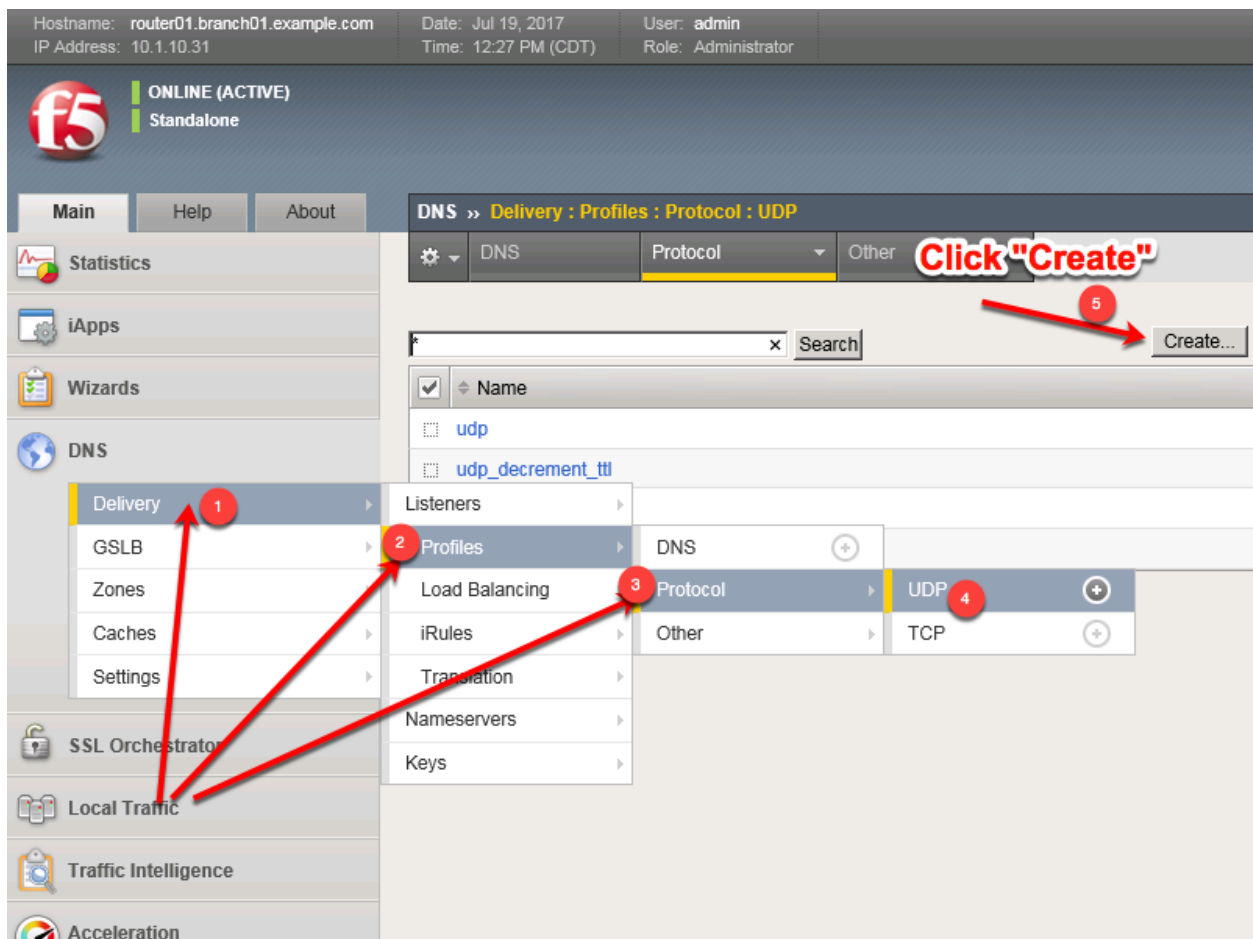
TMSH

```
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 }
```

2.2.2.3 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.

Field	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>

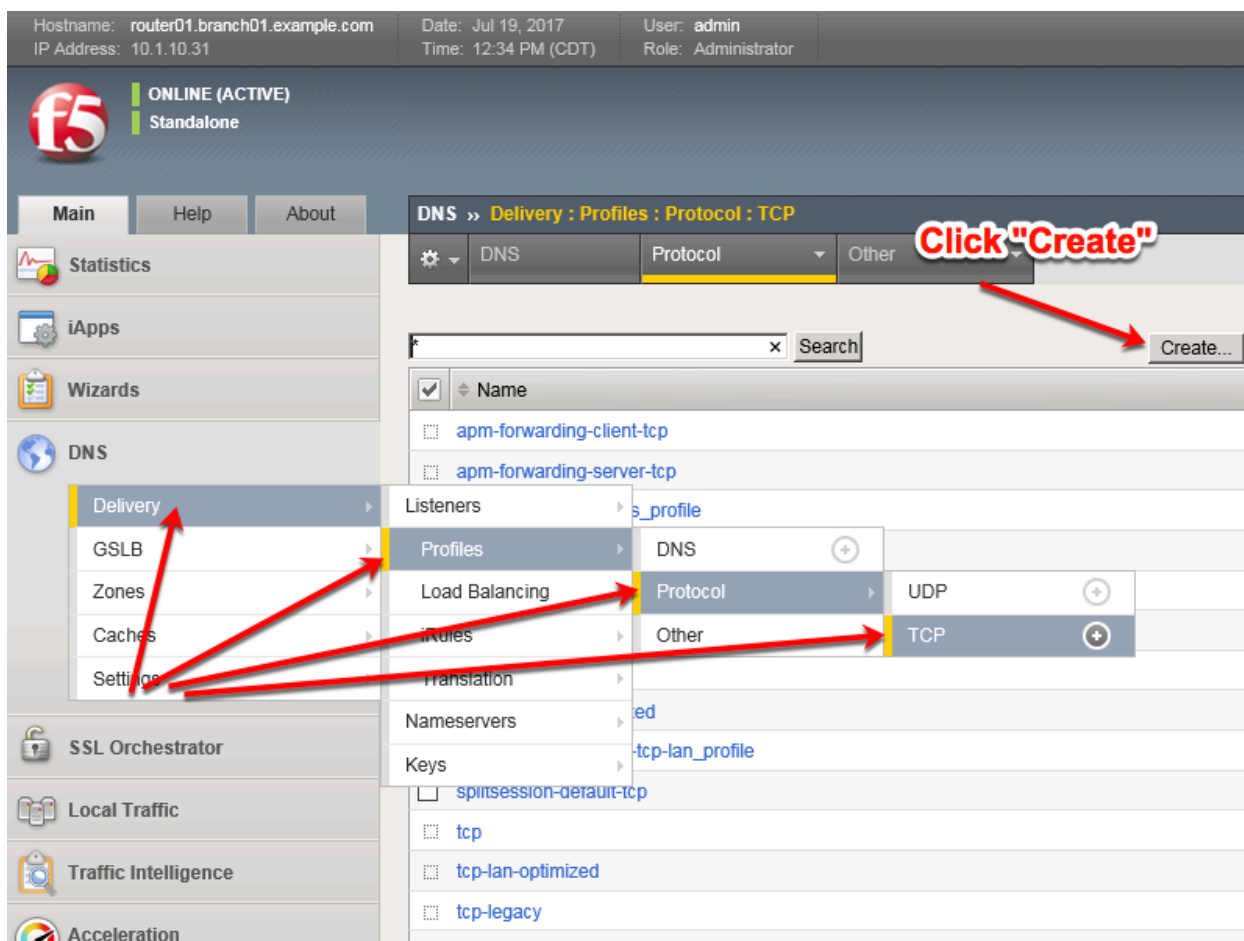
TMSH

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

2.2.2.4 TCP Profile

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

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



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

Create a TCP profile as shown in the following table.

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

Hostname: router01.branch01.example.com Date: Jul 12, 2017 User: admin
IP Address: 10.1.10.31 Time: 7:45 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About Local Traffic » Profiles : Protocol : TCP » New TCP Profile...

Statistics
iApps
DNS
SSL Orchestrator
Local Traffic
Network Map
Virtual Servers
Policies
Profiles
Ciphers
iRules
Pools
Nodes
Monitors
Traffic Class
Address Translation
Acceleration
Device Management
Network

General Properties

Name example.com_tcp-1
Parent Profile f5-tcp-lan

Timer Management

Close Wait Specify... 5 seconds
Fin Wait 1 Specify... 5 seconds
Fin Wait 2 Specify... 300 seconds
Idle Timeout Specify... 300 seconds
Keep Alive Interval Specify... 1800 seconds
Minimum RTO 200 milliseconds
Reset On Timeout ☒ Enabled
Time Wait Specify... 2000 milliseconds
Time Wait Recycle ☒ Enabled
Zero Window Timeout Specify... 20000 milliseconds

Memory Management

Auto Proxy Buffer ☐
Auto Receive Window ☐
Auto Send Buffer ☐
Proxy Buffer High 65535 bytes
Proxy Buffer Low 32768 bytes

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

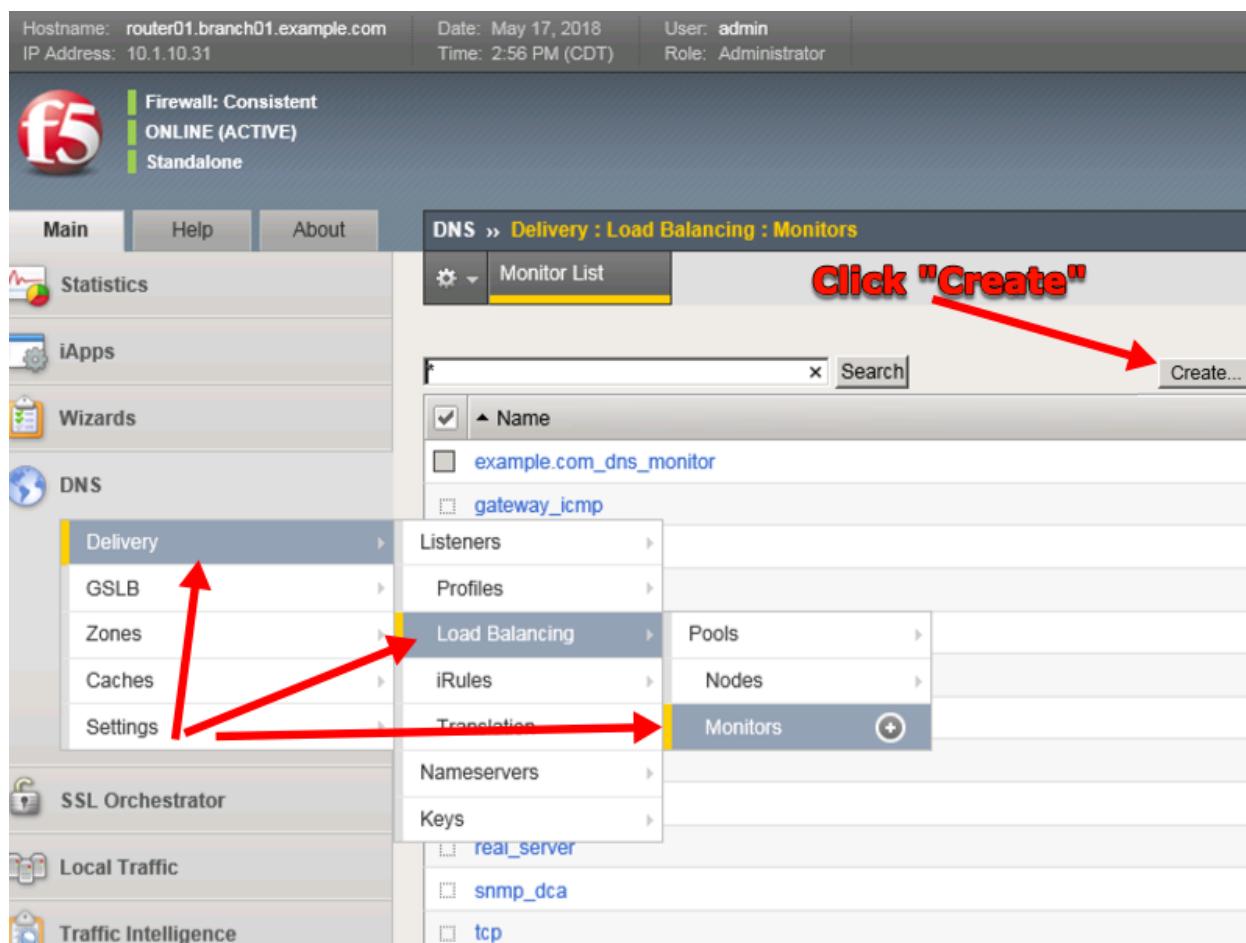
TMSH

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

2.2.2.5 DNS Servers

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

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



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

Create a DNS monitor according to the table below:

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

Hostname: router01.branch01.example.com Date: May 17, 2018 User: admin
IP Address: 10.1.10.31 Time: 4:12 PM (CDT) Role: Administrator

f5 Firewall: Consistent
ONLINE (ACTIVE)
Standalone

Main Help About DNS » Delivery : Load Balancing : Monitors » New Monitor...

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

General Properties

Name	example.com_dns_monitor
Description	
Type	DNS
Parent Monitor	dns

Configuration: Advanced

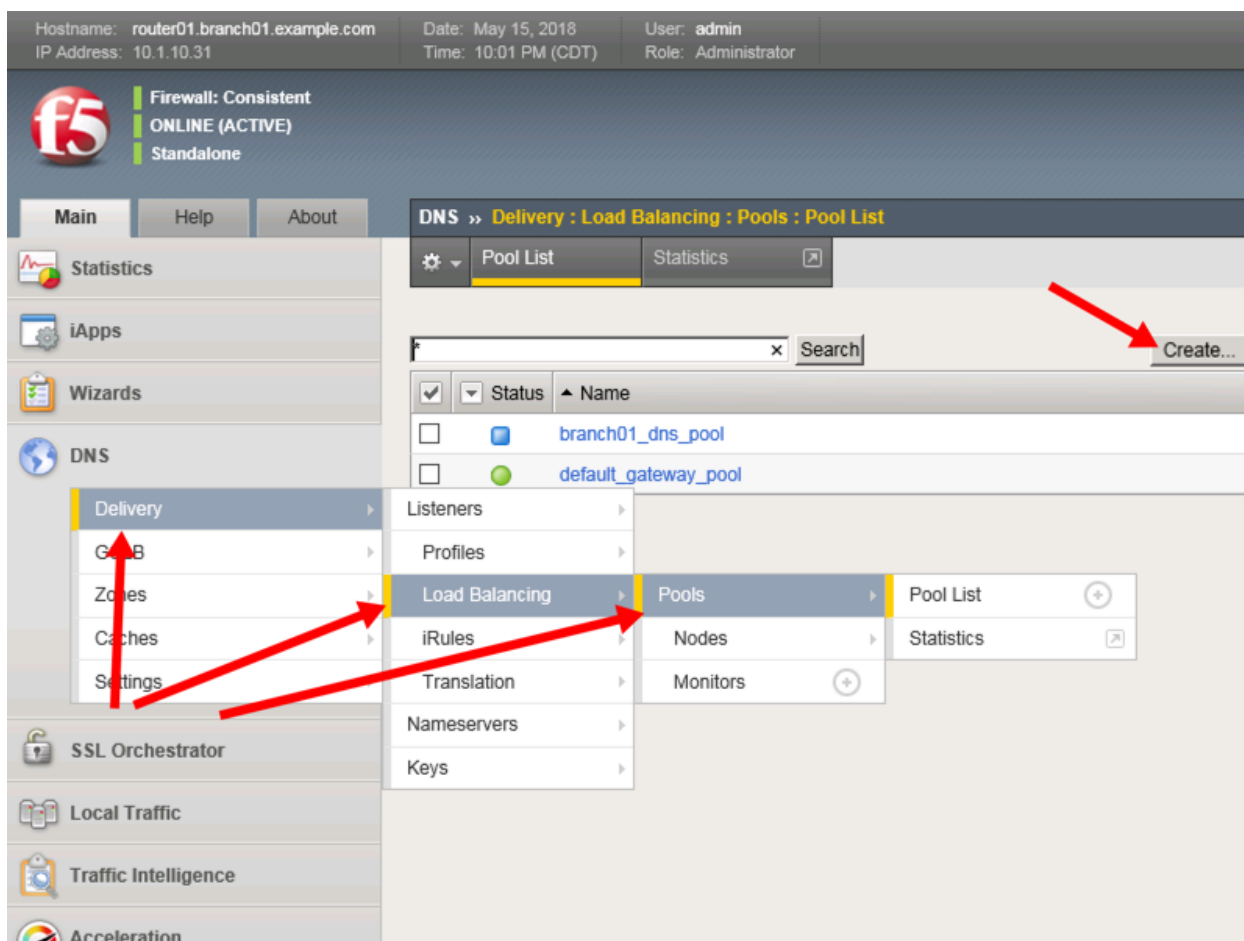
Interval	5 seconds
Up Interval	Disabled
Time Until Up	0 seconds
Timeout	16 seconds
Manual Resume	<input type="radio"/> Yes <input checked="" type="radio"/> No
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
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

Cancel Repeat Finished

TMSH

```
tmsl create ltm monitor dns example.com_dns_monitors qname www.example.com
```

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



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

Create a DNS pool according to the table below:

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

Hostname: router01.branch01.example.com Date: May 15, 2018 User: admin
IP Address: 10.1.10.31 Time: 10:13 PM (CDT) Role: Administrator

Firewall: Consistent
ONLINE (ACTIVE)
Standalone

Main Help About DNS » Delivery : Load Balancing : Pools : Pool List » New Pool...

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

Configuration: Basic

Name: example.com_dns_pool

Description:

Health Monitors

Active: /Common/example.com_dns_monitor

Available: /Common/gateway_icmp, http, http_head_f5, https

Resources

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

New Node New FQDN Node Node List FQDN Node List

Node Name: dc02.example.com_node (Optional)

Address: 10.1.70.210

Service Port: 53

Add

New Members

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
dc01.example.com_node	10.1.70.200	53		0
dc02.example.com_node	10.1.70.210	53		0

Edit Delete

Cancel Repeat Finished

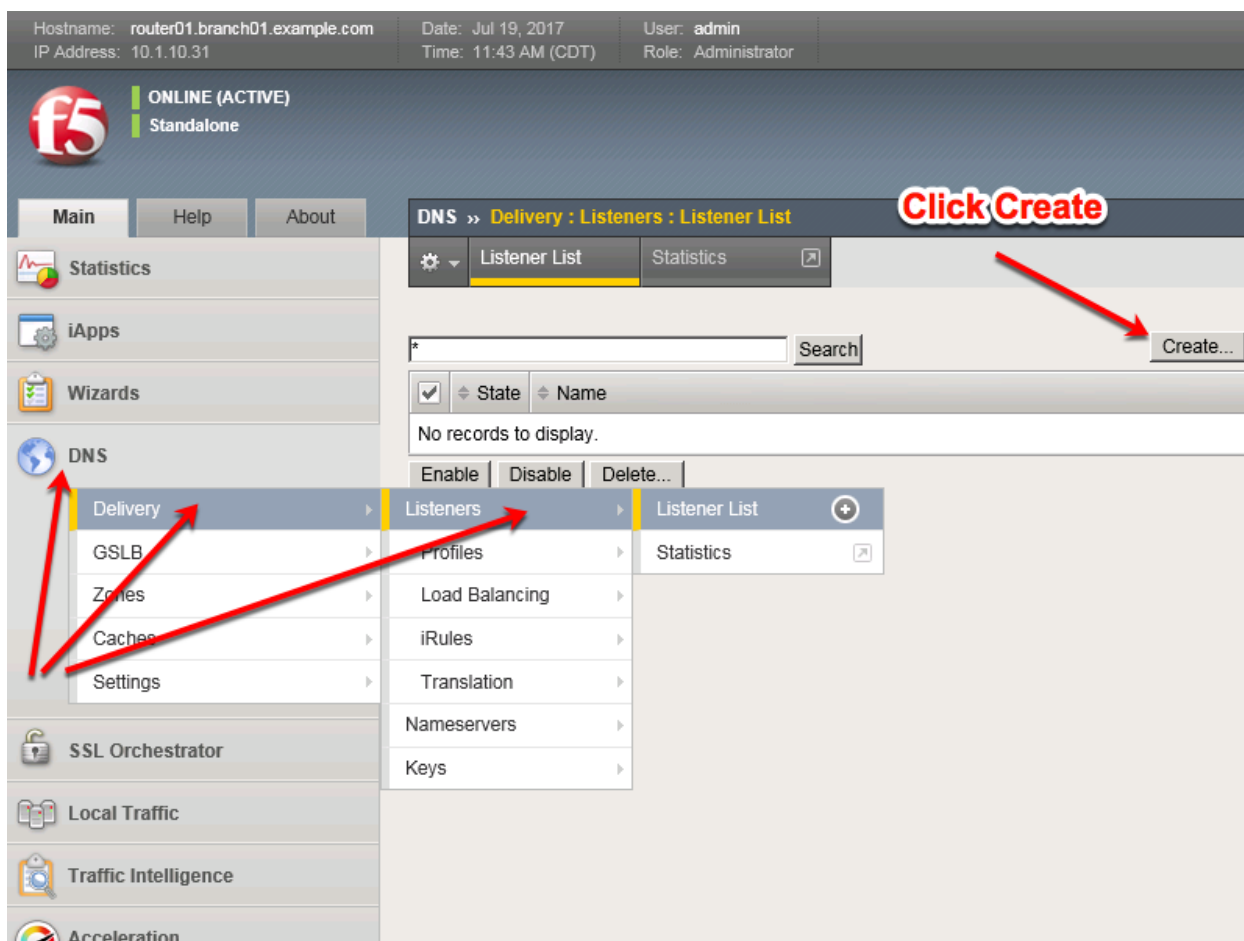
TMSH

```
tmsh create ltm pool example.com_dns_pool members add { dc01.example.com_node:53 { address 10.1.70.200 } dc02.example.com_node:53 { address 10.1.70.210 } } monitor example.com_dns_monitor
```

2.2.2.6 UDP Listener

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

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



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

Create two UDP listeners according to the tables below:

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

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

Hostname: router01.branch01.example.com Date: Jul 19, 2017 User: admin
IP Address: 10.1.10.31 Time: 12:01 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About 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

Name: DC01_udp_53_virtual
Description:
State: Enabled

Listener: Advanced

Destination: Address: 10.1.70.200
Type: Host Network
Service Port: DNS 53
VLAN Traffic: Enabled on...
VLANs and Tunnels: /Common branch01_vlan
Source Address Translation: None
Address Translation: Enabled
Port Translation: Enabled
Route Advertisement: Enabled
Auto Last Hop: Default
Last Hop Pool: None

Service: Advanced

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

Load Balancing

Default Pool: branch01_dns_pool
Default Persistence Profile: None
Fallback Persistence Profile: None

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

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

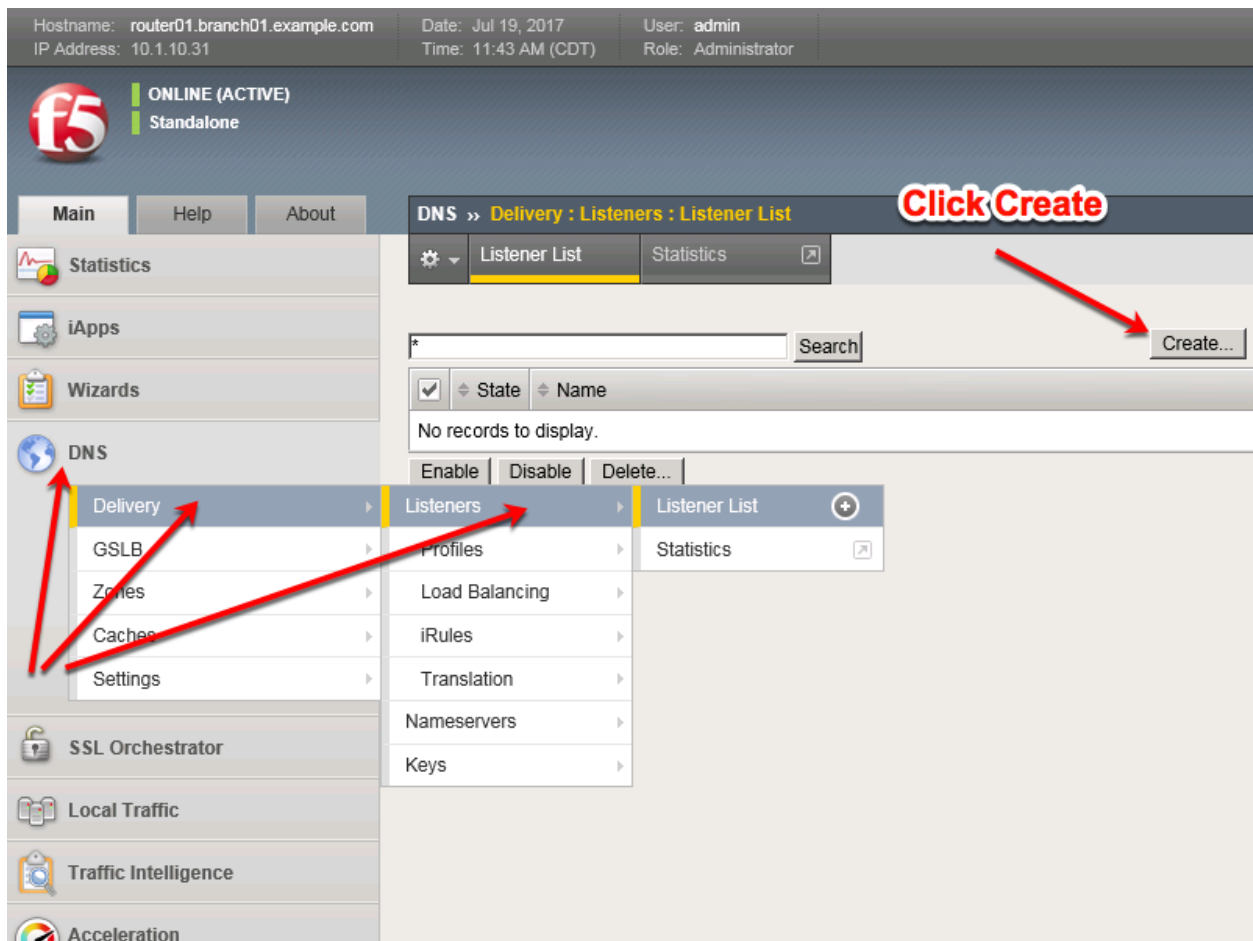
TMSH

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

2.2.2.7 TCP Listeners

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

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



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

Create two TCP listeners according to the table below:

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

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

Hostname: router01.branch01.example.com Date: Jul 19, 2017 User: admin
IP Address: 10.1.10.31 Time: 12:46 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About **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

Name: DC01_tcp_53_virtual
Description:
State: Enabled

Listener: Advanced

Destination: Address: 10.1.70.200
Type: Host Network

Service Port: DNS 53

VLAN Traffic: Enabled on...

VLANs and Tunnels: Selected: /Common branch01_vlan Available: /Common AD_vlan external_vlan http-tunnel isp1_site1_vlan

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: branch01_dns_pool
Default Persistence Profile: None
Fallback Persistence Profile: None

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

TMSH

2.2. Security

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

TMSH

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

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

2.2.2.8 Results

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

Repeat some of the same queries multiple times

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

2. Viewing Cache Entries

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

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 Caches Settings SSL Orchestrator Local Traffic Acceleration Device Management Network System

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

Display Options

Statistics Type	Caches
Data Format	Normalized
Auto Refresh	Disabled Refresh

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

Summary

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**

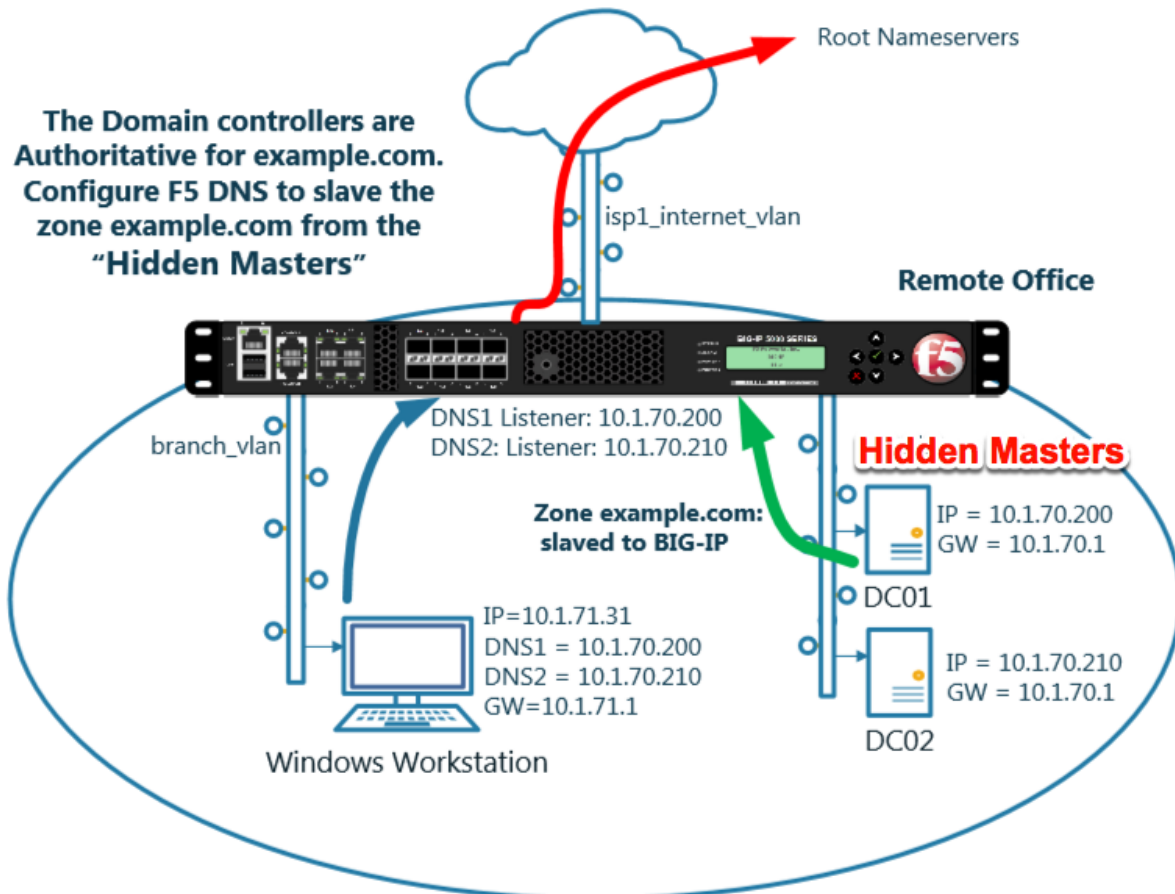
Set “Statistics Type” to “Caches”.

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

2.2.3 Hidden Master

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

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

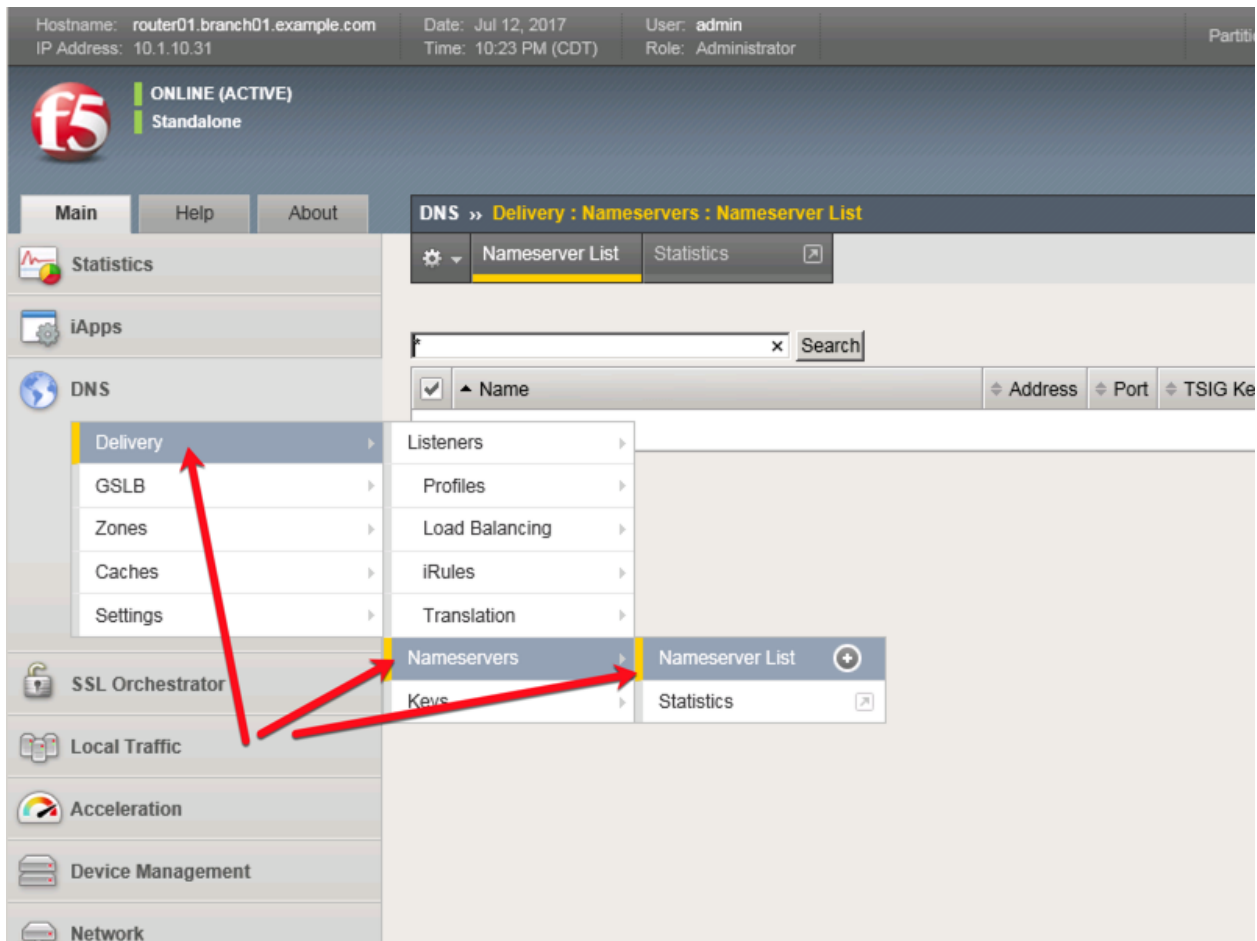


https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/dns-services-implementations-11-6-0/2.html#unique_1658664851

2.2.3.1 Name Server

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

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



Create a nameserver according to the following table:

Field	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
Address
Service Port Other:

Configuration

Route Domain
TSIG Key

Cancel Repeat Finished

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

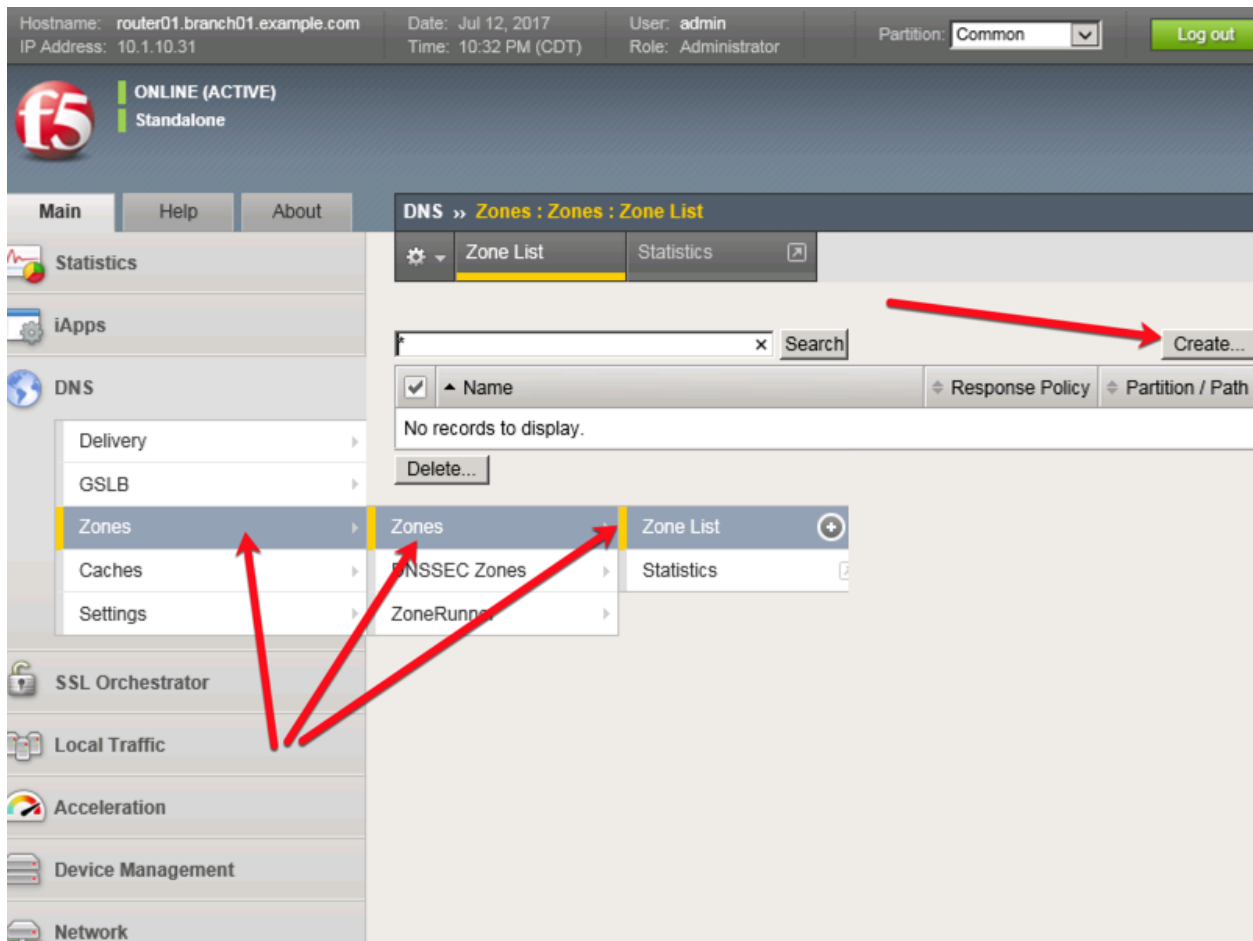
TMSH

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

2.2.3.2 DNS Express

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

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



Create a DNS Express zone according to the following table:

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

Hostname: gtm1.site1.example.com Date: 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>

<https://www.unbound.net>

2.2.3.3 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

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

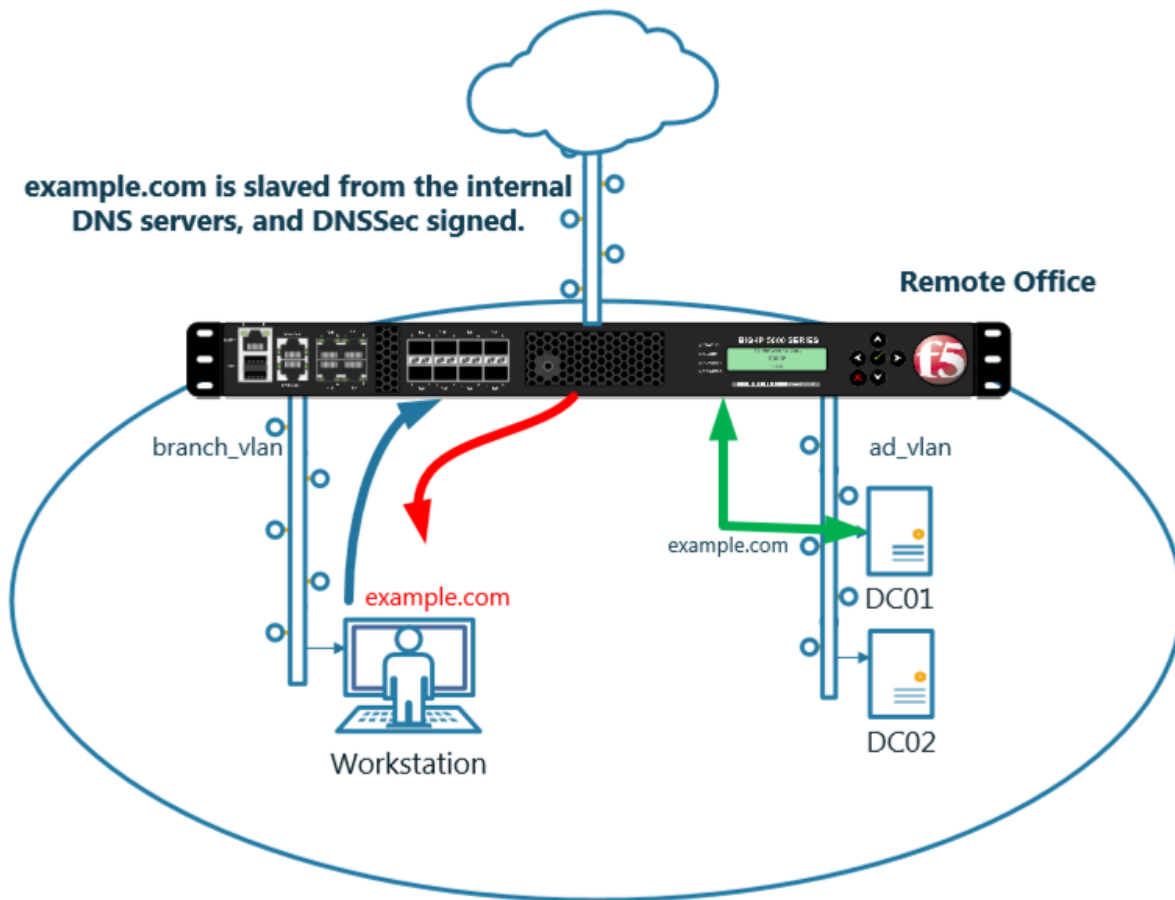
Run the following command to see the contents of the DNS Express database:

```
dnsxdump | less
```

Examine the results

[illegible]

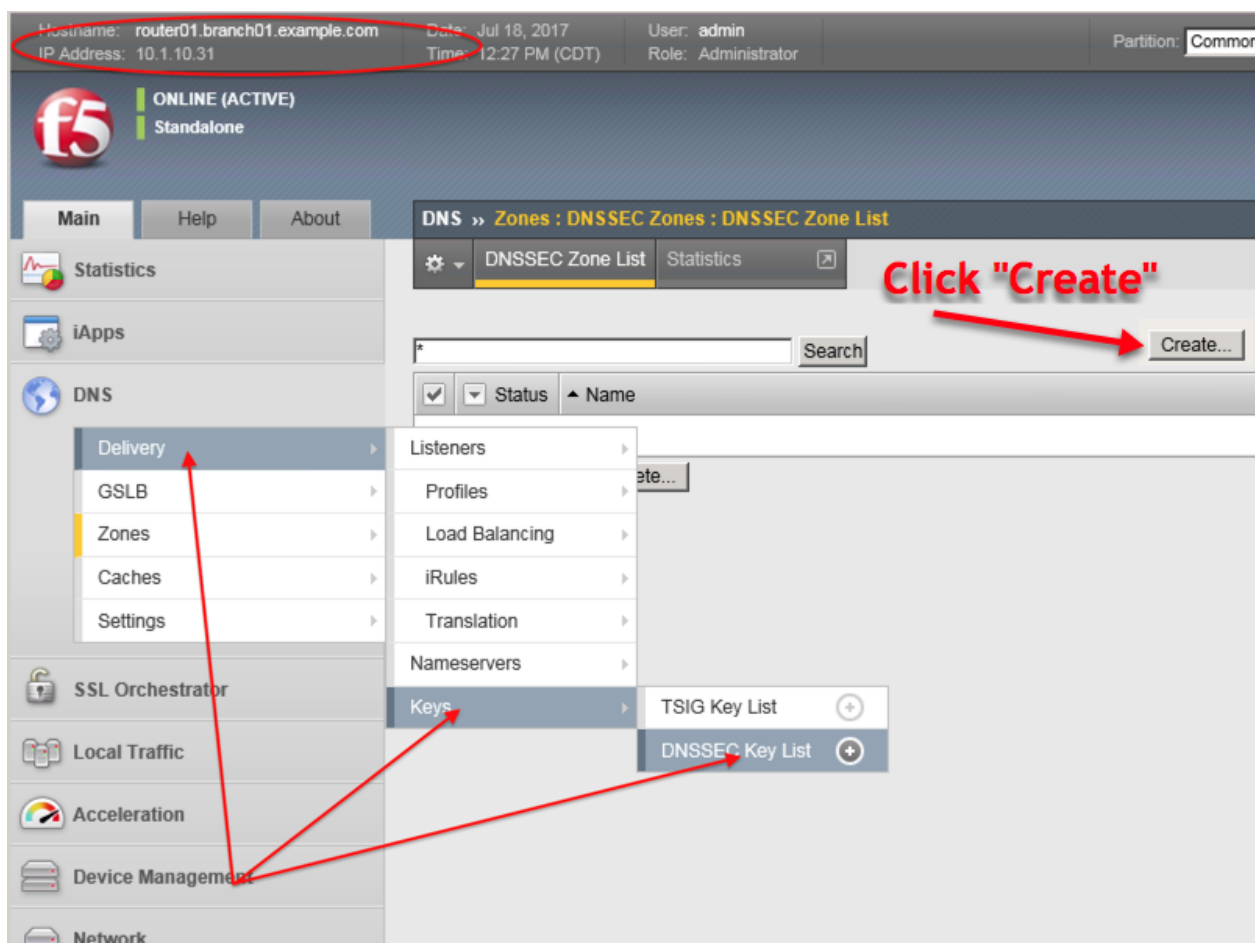
2.2.4 DNSSec



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

2.2.4.1 Zone Signing Key

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



Create zone signing key according the following table:

Field	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

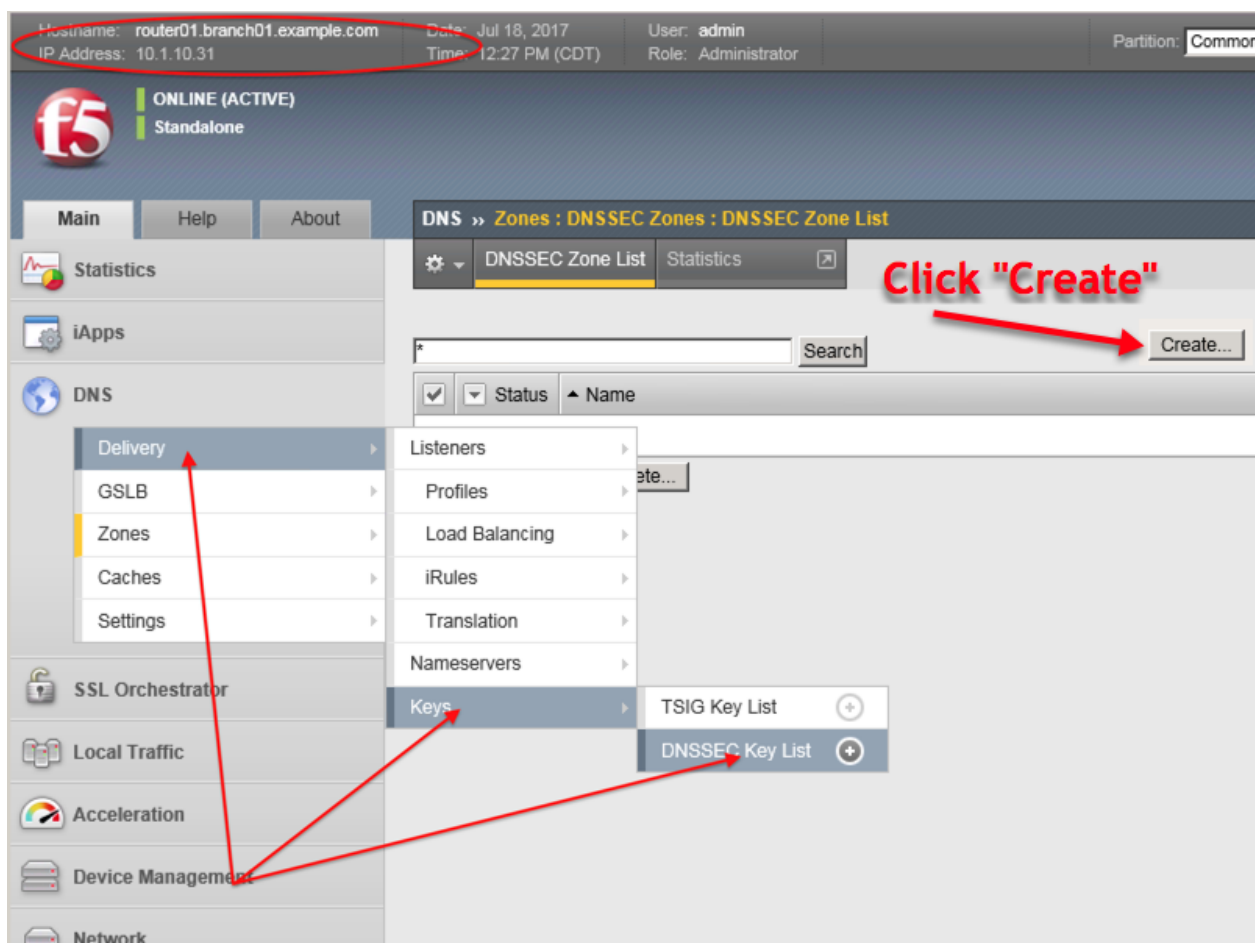
https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/dnssec_key/create.jsp

TMSH

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

2.2.4.2 Key Signing Key

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



Create a key signing key according to the following table:

Field	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

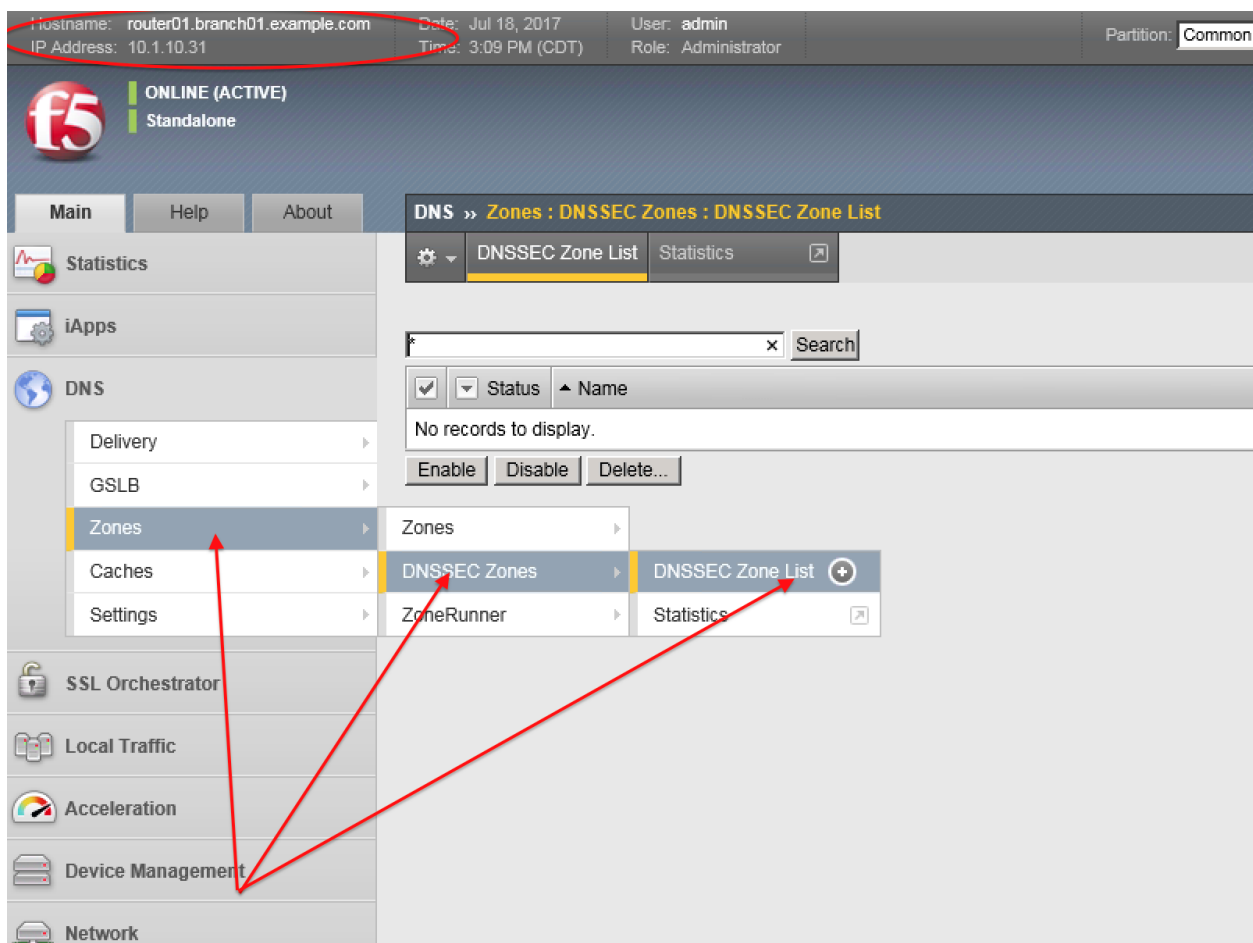
TMSH commands for Key Signing key creation:

TMSH

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

2.2.4.3 Signed Zone

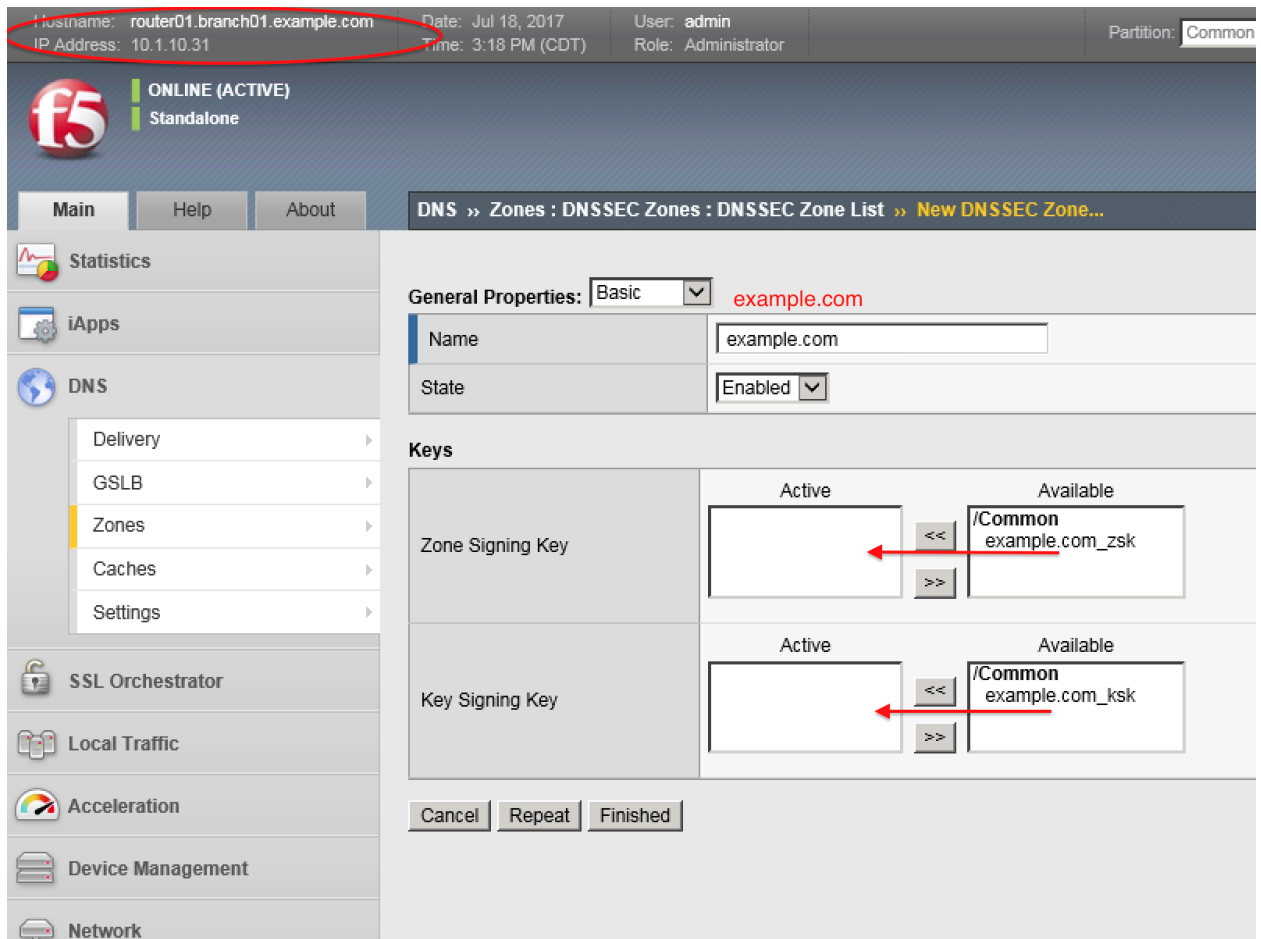
Navigate to: **DNS » Zones : DNSSEC Zones : DNSSEC Zone List**



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

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



TMSH commands for DNSSEC signed zone creation:

TMSH

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

2.2.4.4 Results

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

From the Workstation CMD prompt run: `"dig example.com +dnssec"`

```

C:\Users\user.EXAMPLE>dig example.com +dnssec

; <<>> DiG 9.3.2 <<>> example.com +dnssec
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 614
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;example.com.                IN      A

;; ANSWER SECTION:
example.com.                 600     IN      A      10.1.70.200
example.com.                 600     IN      RRSIG   A 7 2 600 20170725202837 20170718202837 64508 example.com. meABj54Ex3yhrSxn5YnlJ+u4+J3XAP4r2P4NcJyAKZo/NpwFf2I/UBp+RFJ9TmoXTZMU5WgpAbWwzEY2UUY0kUUm2o7brqfG4pdzIcX6UMgY2/J Xbx51IQ3rrLz+tbUhpZdH8ueDBUm1SXqb0YTxPUfcQDMUCthCNbe3SR5 gg5HmRL0TvCcx0i6/49hNL6oXJH5nDQNsoGTS/keZWgdf6DI0vk19Bpt R7q0KJ3F0PRnXpgsx5lgn83QLIu3nWOGjGa02WbAVN4hQdlyu2h0xqL xTFfBBBCMSi/MA2b3FrTGTxCTkfzc00JDKc9+uGzRuFEHhms9014NEK7 2yPXkw==

;; AUTHORITY SECTION:
example.com.                 3600    IN      NS      dc01.example.com.
example.com.                 3600    IN      RRSIG   NS 7 2 3600 20170725202837 20170718202837 64508 example.com. MFjHTouNuAf4Gpv15aFD6P+C7AXjAAZF6KIRs4G3uWgNUIy4MmN20k5 QGg20w517/eNnIAvjsmggYAU5d15v1640JSbm4i1eLUTQBMMbNdi0S03i yFi2Cs/Xb0ZGaROx1NIxKPrqk6ssNh/tS01Gg0Qlaki/dCL5N4DmeH60 HsrDzNxRa74RFQ10QyFhAcKAHgenWTgdoH6eUsw/Dn9zLIdUcOZtFb0ll TCZDUEf4bHL18B0Uu918xGut iHtMmMo/GN4/z4MSrCeUEBw3t+uR+icTM0w EwG2bt

router01
Jul 18 15:41:18 router01 info tmm[11375]: 2017-07-18 15:41:17 router01.branch01.example.com q
id 614 from 10.1.71.100#52224: view none: query: example.com IN A +ED (10.1.70.200%)
Jul 18 15:41:18 router01 info tmm[11375]: 2017-07-18 15:41:17 router01.branch01.example.com q
id 614 to 10.1.71.100#52224: [NOERROR qr,aa,rd,do] response: example.com. 600 IN A 10.1.70.20
0; example.com. 600 IN RRSIG A 7 2 600 20170725202837 20170718202837 64508 example.com meABj5
4Ex3yhrSxn5YnlJ+u4+J3XAP4r2P4NcJyAKZo/NpwFf2I/UBp+RFJ9TmoXTZMV5WgpAbWwzEY2UUY0kVUm2o7brqfG4p
dzIcX6UMgY2/JXbx51IQ3rrLz+tbUhp2dH8ueDBUm1SXqb0YTxPUfcQDMUCthCNbe3SR5gg5HmRL0TvCcx0i6/49hNL6o
XJH5nDQNsoGTS/keZWgdf6DI0vk19BptR7q0KJ3F0PRnXpgsx5lgn83QLIu3nWOGjGa02WbAVN4hQdlyu2h0xqLxTFf
BBBCMSi/MA2b3FrTGTxCTkfzc00JDKc9+uGzRuFEHhms9014NEK72yPXkw==;

```

2.2.5 Validating Resolver

2.2.5.1 Trust Anchors

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

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

TMSH

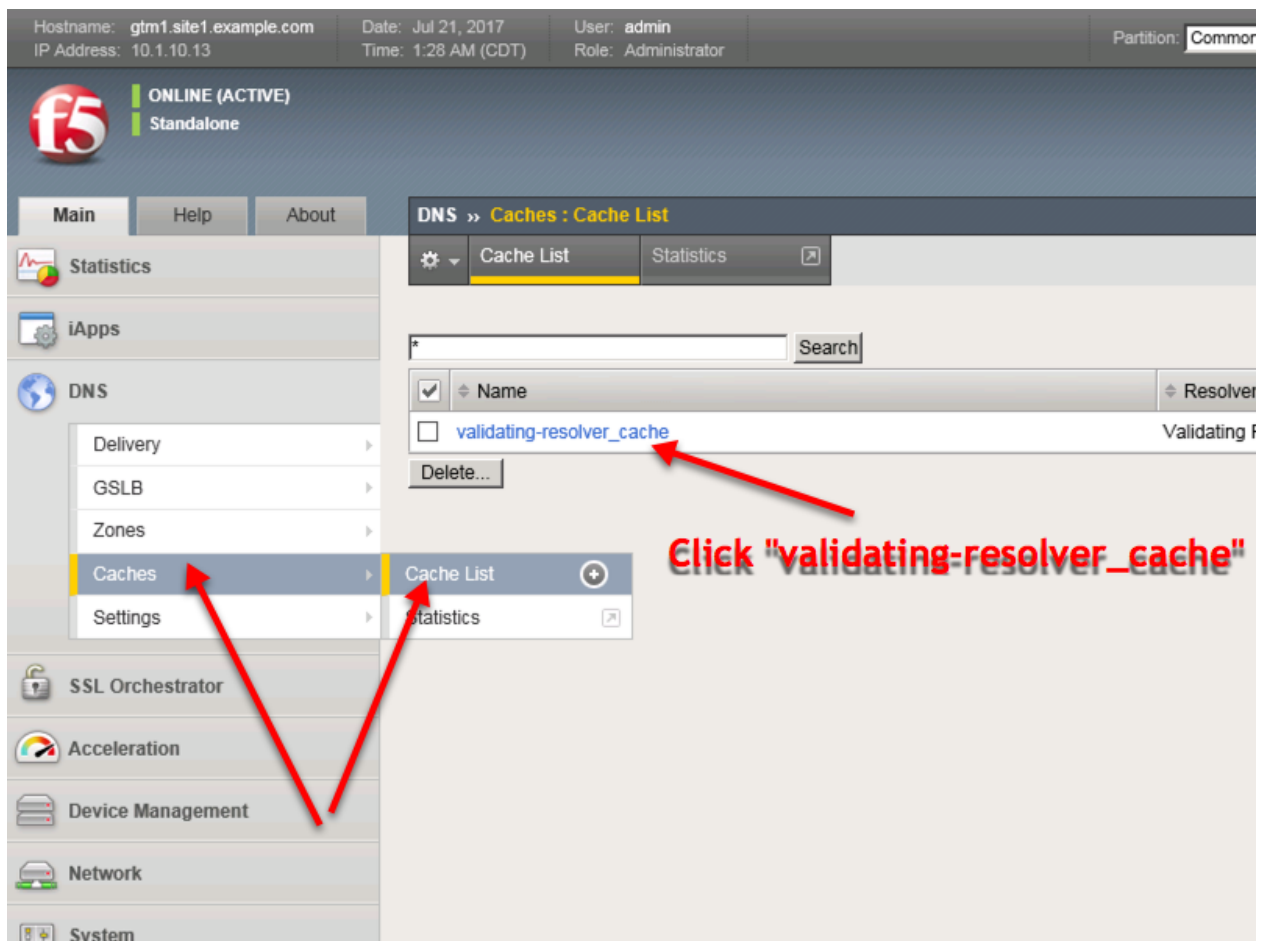
```
dig dnskey . | grep 257 > /root/dnskey.txt
```

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

```
router01
[root@router01:Eval:Active:Standalone] config #
[root@router01:Eval:Active:Standalone] config #
[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 # dnstool-dsfromkey -f /root/dnskey.txt .
. IN DS 19036 8 1 B256BD09DC8DD59F0E0FOD8541B8328DD986DF6E
. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A4185520OFD2CE1CDDE32F24E8FB5
. IN DS 20326 8 1 AE1EA5B974D4C858B740BD03E3CED7EBFCBD1724
. IN DS 20326 8 2 E06D44B80B8FD139A95COBOD7C65D08458E880409BBC683457104237C7F8EC8D
[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 #
```

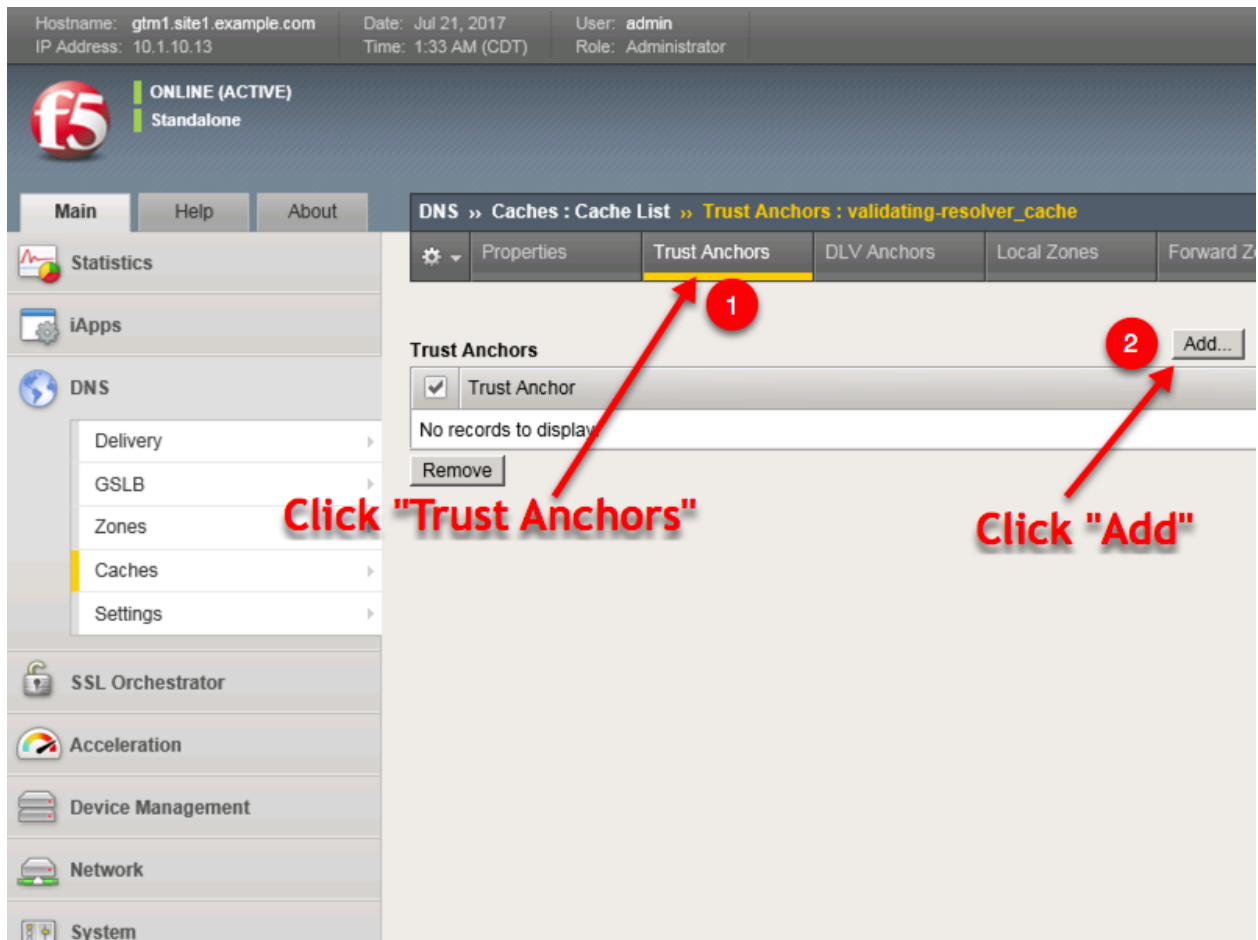
Navigate to: **DNS » Caches : Cache List » validating-resolver_cache : Trust Anchors**

Select the validating-resolver_cache and click “Trust Anchors”



https://router01.branch01.example.com/tmui/Control/ispmap/tmui/dns/cache/trust_anchor/list.isp?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:

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

Trust Anchors

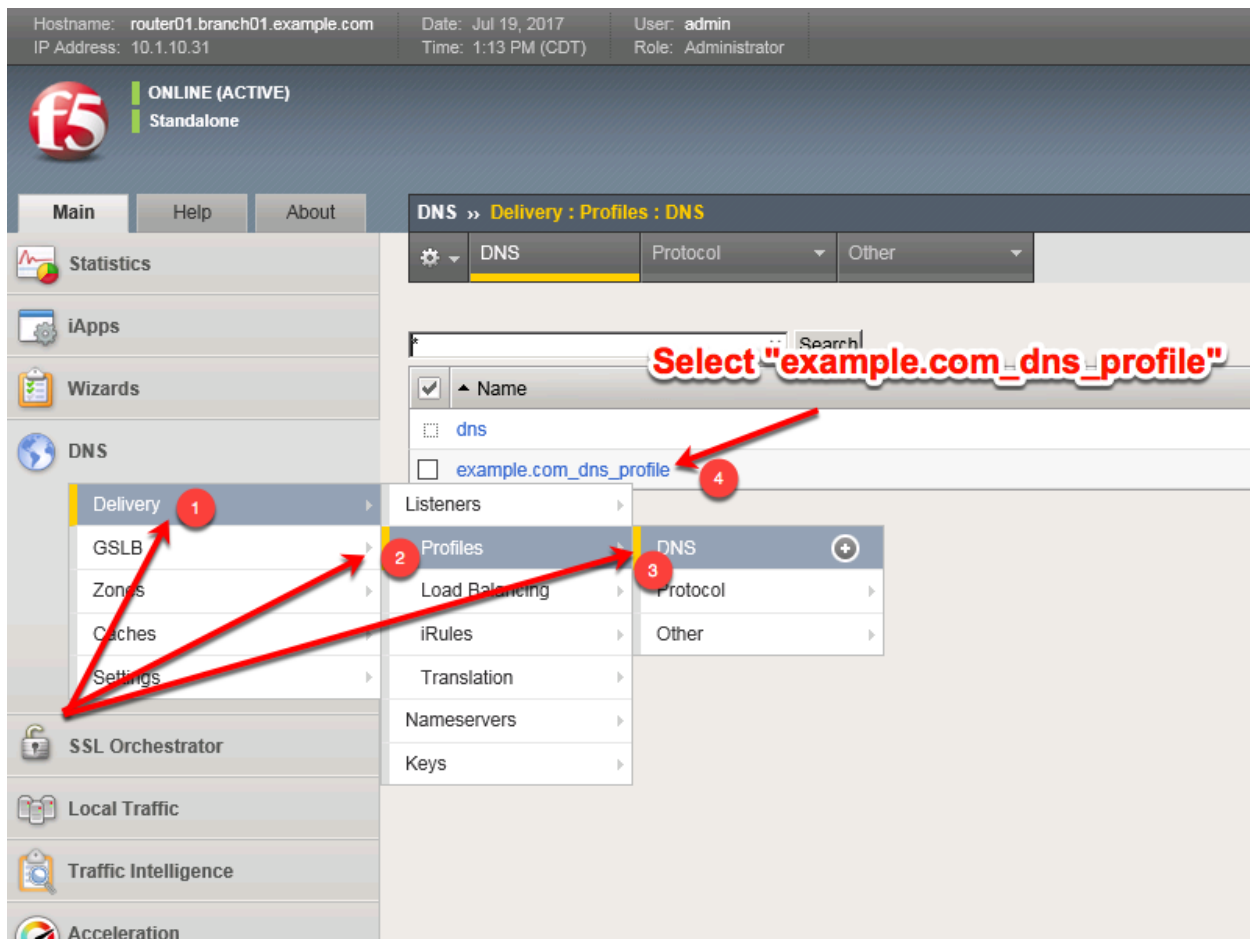
<input checked="" type="checkbox"/>	Trust Anchor
<input checked="" type="checkbox"/>	. IN DS 19036 8 1 B256BD09DC8DD59F0E0F0D8541B8328DD986DF6E
<input type="checkbox"/>	. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
<input type="checkbox"/>	. IN DS 20326 8 1 AE1EA5B974D4C858B740BD03E3CED7EBFCBD1724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

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

2.2.5.2 Modify DNS Profile

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

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



Select the profile “`example.com_dns_profile`”

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

Hostname: router01.branch01.example.com Date: Jul 19, 2017 User: admin
IP Address: 10.1.10.31 Time: 1:07 PM (CDT) Role: Administrator

f5 ONLINE (ACTIVE)
Standalone

Main Help About

DNS » Delivery : Profiles : DNS » Properties : example.com_dns_profile

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

Properties

General Properties

Name	example.com_dns_profile
Partition / Path	Common
Parent Profile	dns

Denial of Service Protection

Rapid Response Mode	Disabled
Rapid Response Last Action	Drop

Hardware Acceleration

Protocol Validation	Disabled
Response Cache	Disabled

DNS Features

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

DNS Traffic

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

Logging and Reporting

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

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

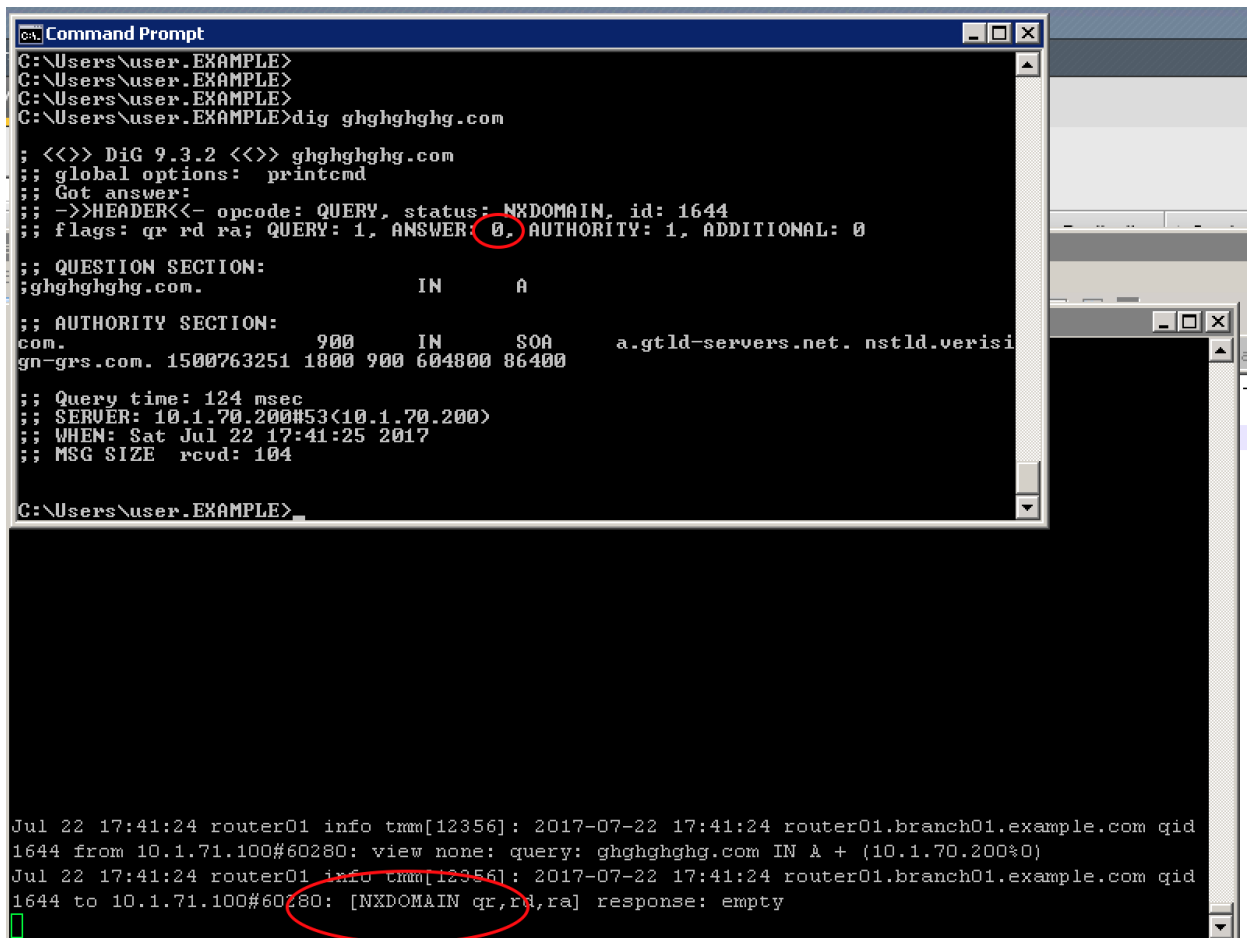
tmsh modify ltm profile dns example.com_dns_profile cache validating-resolver_cache

2.2.5.3 Results

From the CLI on the router01.branch01 BIGIP run

tail -f /var/log/ltm

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



```
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.verisign-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"


```

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"

```

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/MRvEG9gvnwNKKGNFXuJwVl+eBsy6NRNW184maIW7vY0bmwJkqsET2okUCcEP00/BzY/RFPHmzBsG5N Bxhg+0LeiMUYp/gHidX0tGQVMvMgn6Z3oeqD4Vt6FJEcLuyGED0cRYNB yBc=

;; AUTHORITY SECTION:
dnssec-deployment.org.  294     IN      NS      ns1.sea1.afiliast.net.info.
dnssec-deployment.org.  294     IN      NS      ns1.mia1.afiliast.net.info.
dnssec-deployment.org.  294     IN      NS      ns1.yyz1.afiliast.net.info.
dnssec-deployment.org.  294     IN      NS      ns1.hkg1.afiliast.net.info.
dnssec-deployment.org.  294     IN      NS      ns1.ams1.afiliast.net.info.
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/MRvEG9gvnwNKKGNFXuJwVl+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>

```

```

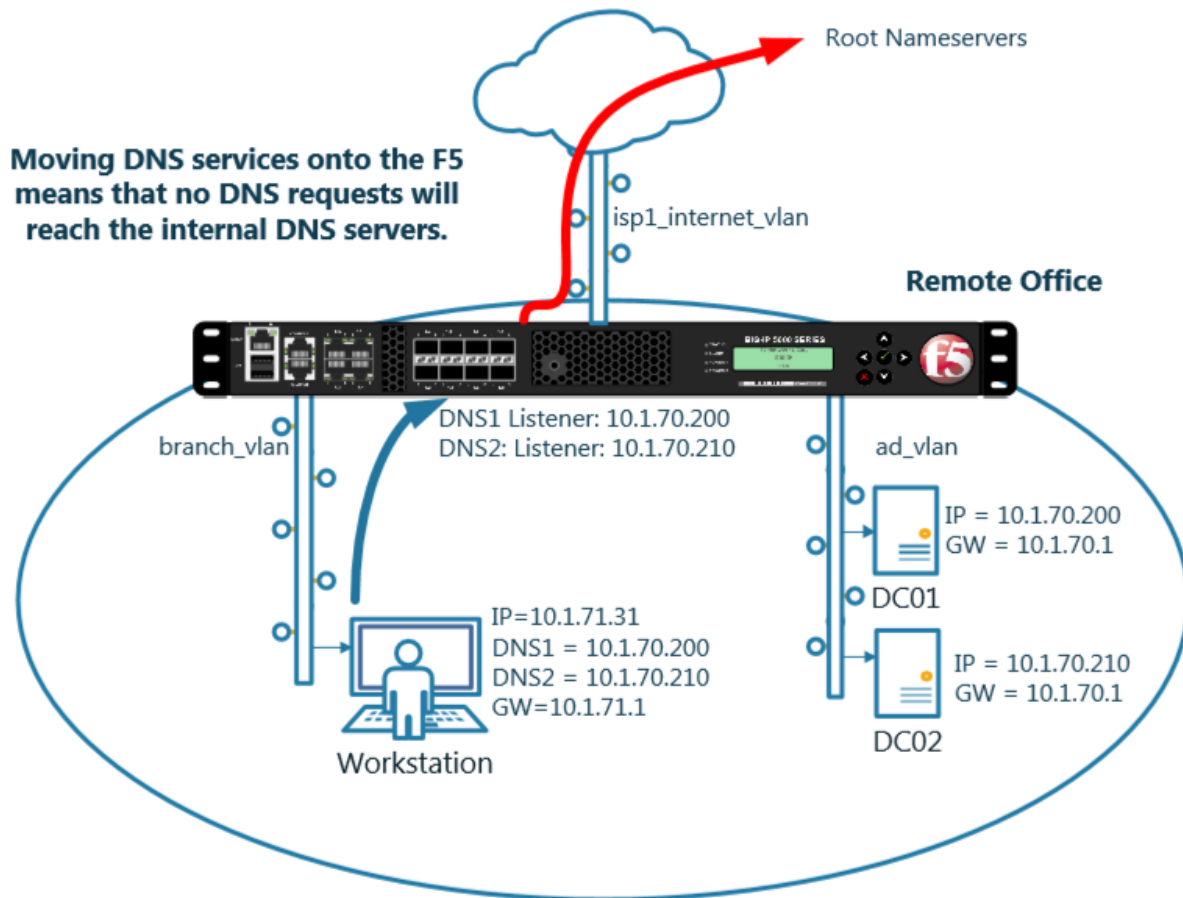
Jul 20 11:49:38 router01 info tmm[12352]: 2017-07-20 11:49:38 router01.branch01.example.com qid 63
5 from 10.1.71.100#61266: view none: query: dnssec-failed.org IN A +ED (10.1.70.200%0)
Jul 20 11:49:38 router01 info tmm[12352]: 2017-07-20 11:49:38 router01.branch01.example.com qid 63
5 to 10.1.71.100#61266: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

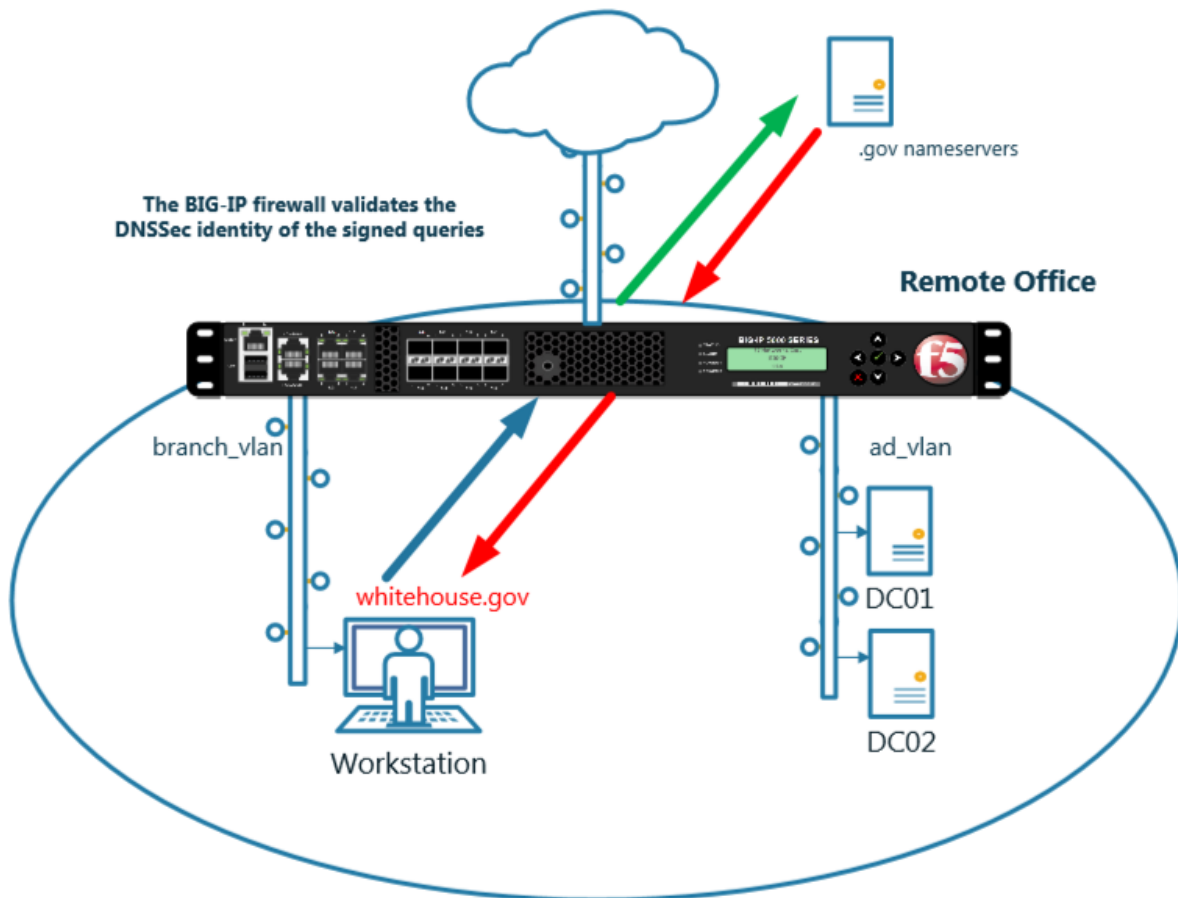
```

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

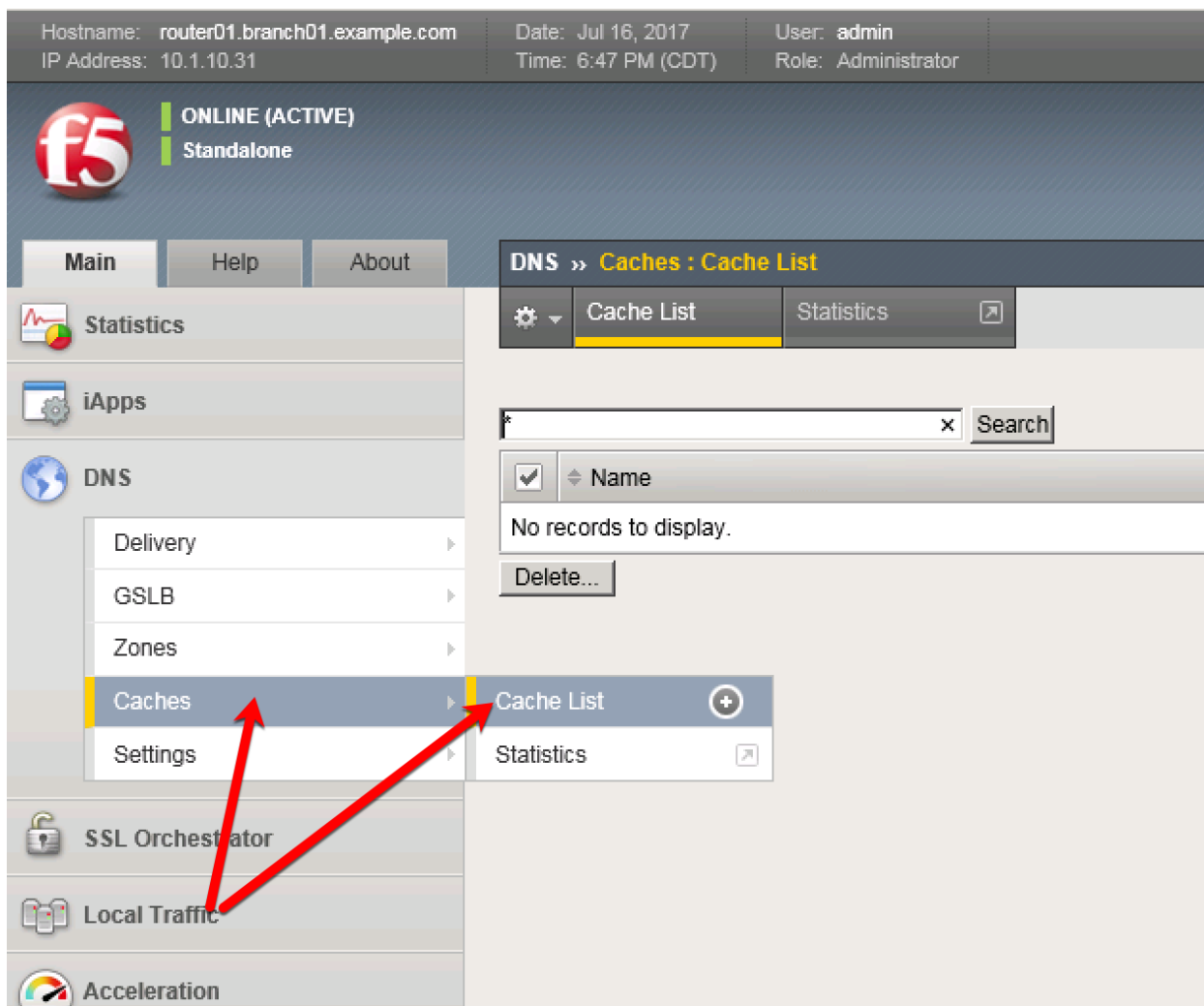
Configure a validating resolver cache on the BIG-IP® system to recursively query public DNS servers, validate the identity of the DNS server sending the responses, and then cache the responses.

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





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






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



Create a validating resolver cache according to the table below:

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

General Properties

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

DNS Cache

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

DNS Resolver

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

DNSSEC Validator

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

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

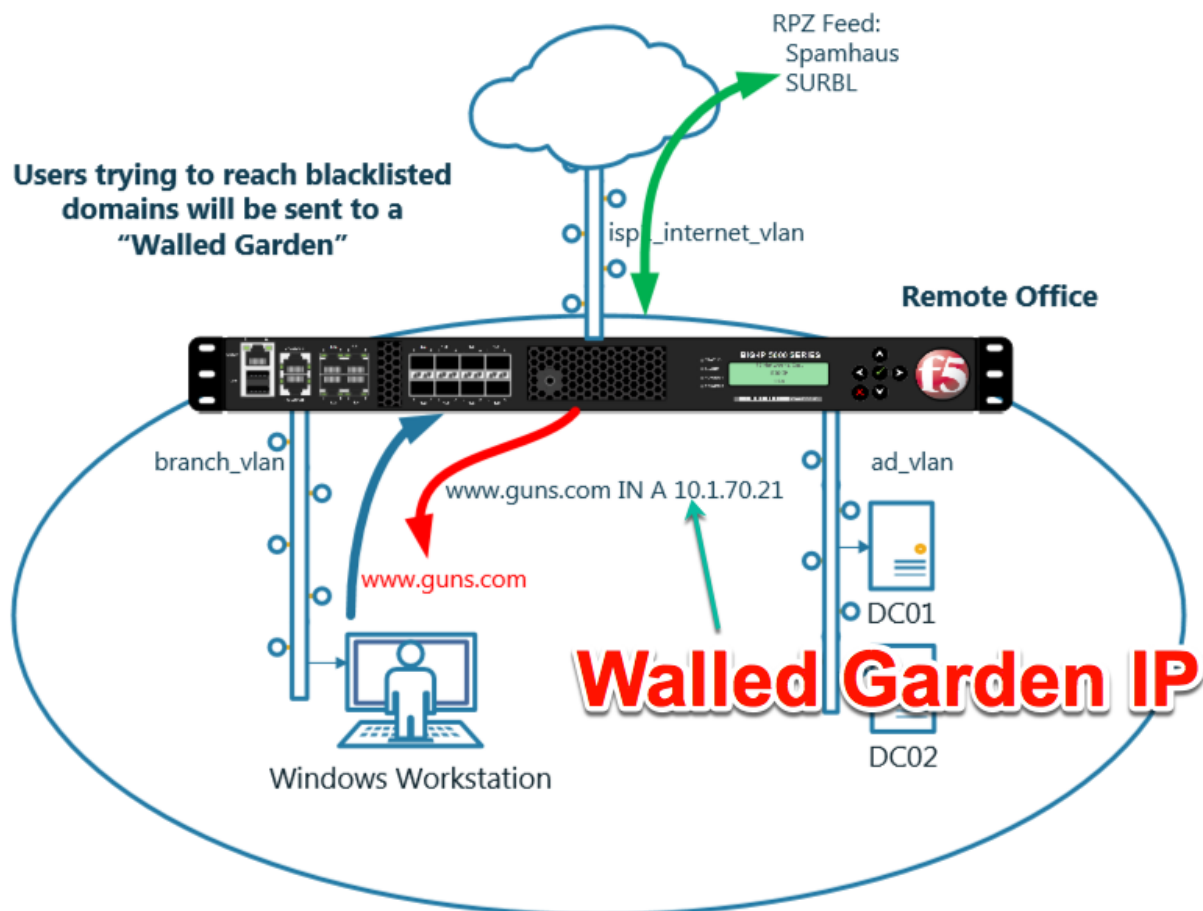
TMSH

```
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>

2.2.6 RPZ

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



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

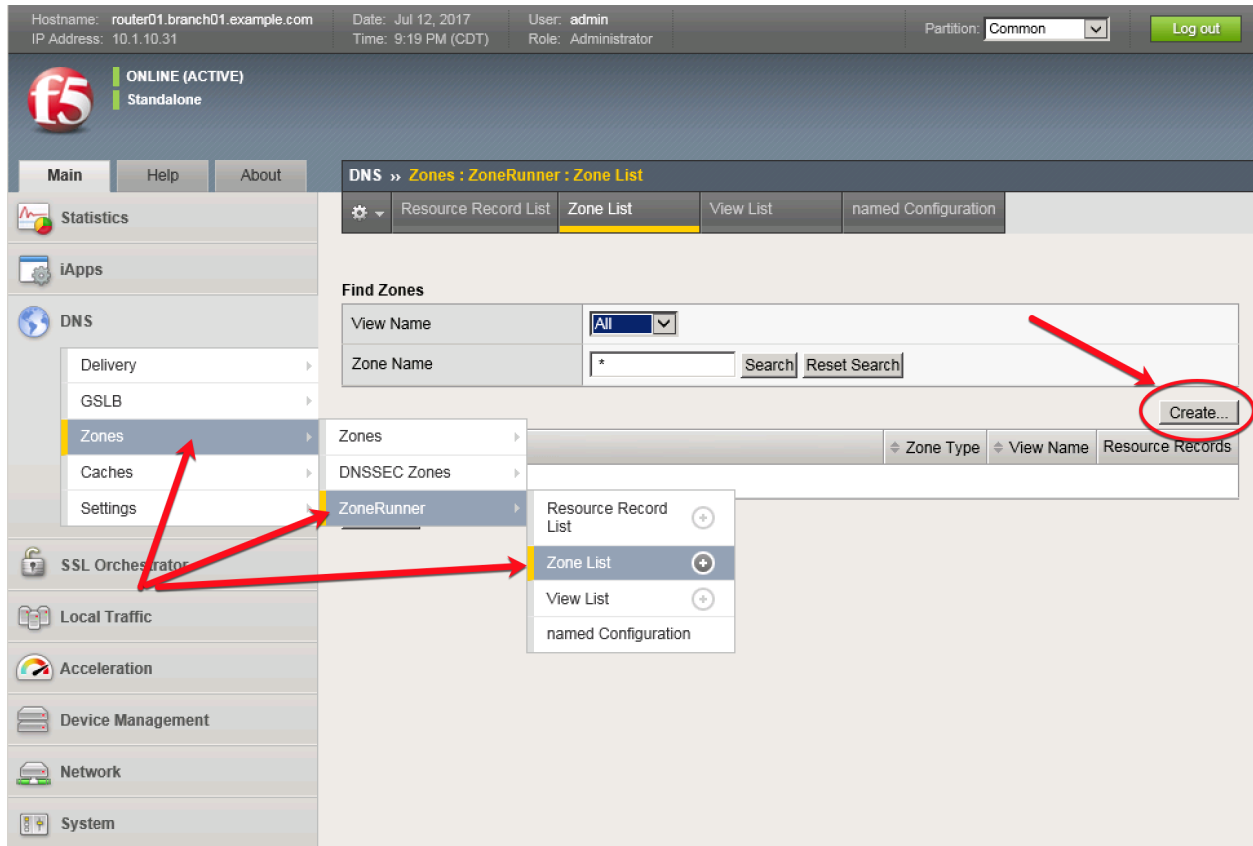
2.2.6.1 Zone Runner

Customers will subscribe to their RPZ vendor of choice.

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

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

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



Create a zone according to the following table:

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

The screenshot shows a web-based DNS configuration interface. It is divided into three main sections: General Properties, Configuration, and Records Creation. Red arrows and text annotations highlight specific fields and their formatting requirements.

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	

Annotations:

- No dot at the end:** Points to the 'external' dropdown in 'View Name' and the 'rpz.example.com' text field in 'Zone Name'.
- Dots at the end:** Points to the 'router01.branch01.example.com.' text fields in 'Master Server', 'Nameserver', and 'Email Contact'.

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

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

Hostname: router01.branch01.example.com Date: Jul 12, 2017 User: admin
 IP Address: 10.1.10.31 Time: 10:06 PM (CDT) Role: Administrator Partition: Co

f5 ONLINE (ACTIVE)
Standalone

Main Help About

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

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...

Create a resource record according to the following table:

Field	Value
View Name	external
Zone Name	rpz.example.com
Name	*.guns.com.rpz.example.com.
TTL	300
Type	CNAME
CNAME	.

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

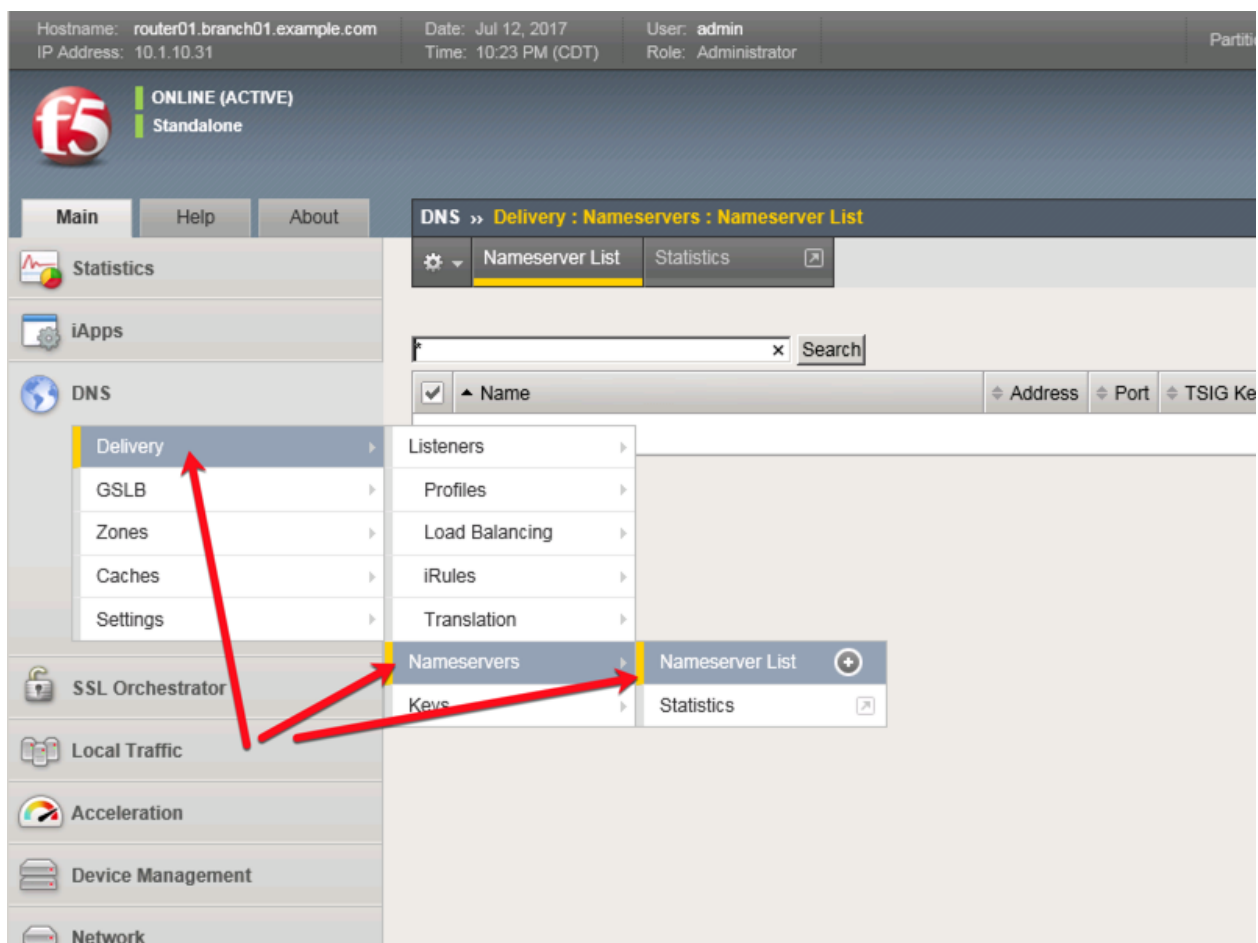
Click "Search"

<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...

2.2.6.2 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:

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

Configuration

Route Domain	<input type="text" value="0"/>
TSIG Key	<input type="text" value="None"/>

Cancel Repeat Finished

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

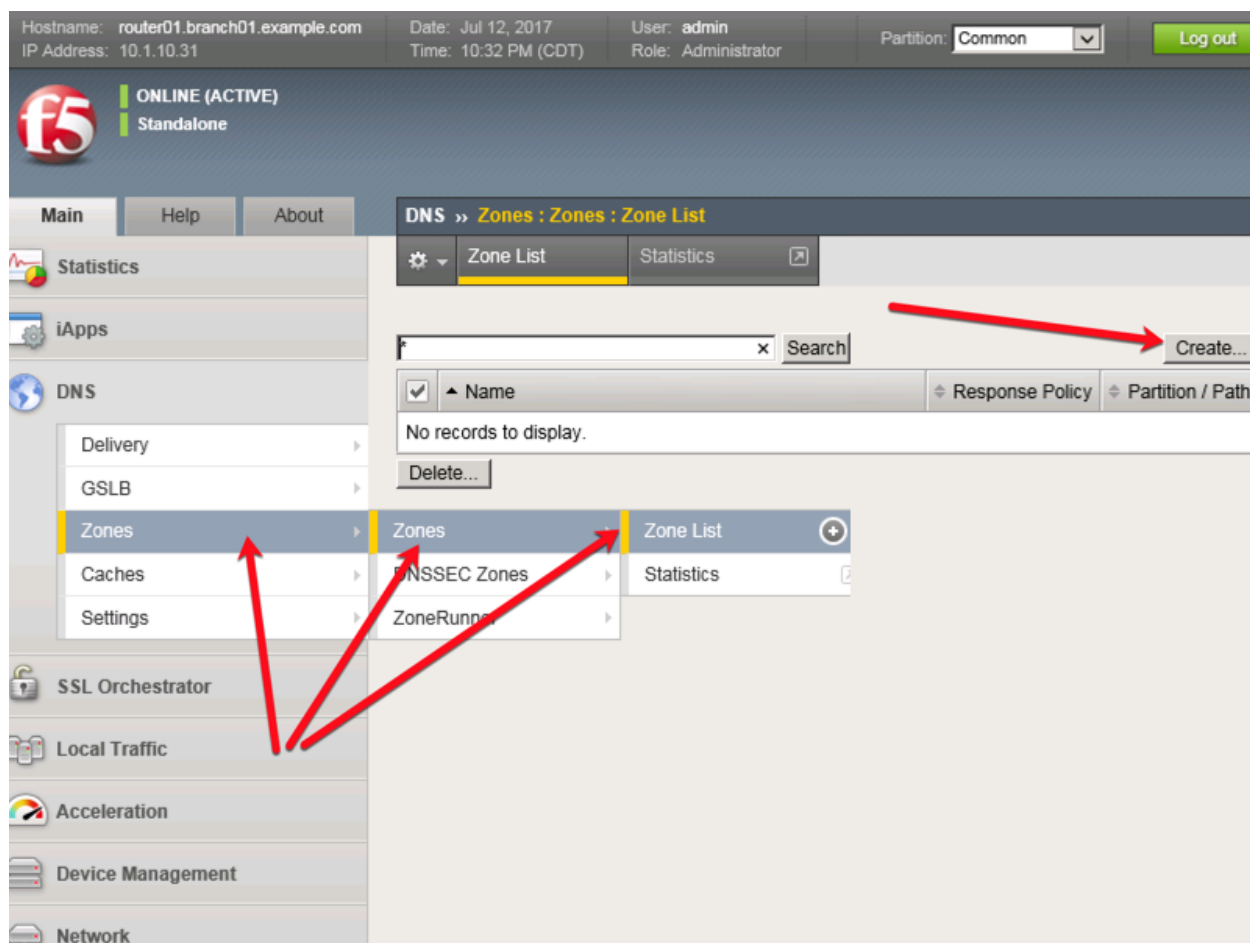
TMSH

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

2.2.6.3 DNS Express

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

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



Create a DNS Express zone according to the following table:

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

Hostname: router01.branch01.example.com Date: Jul 18, 2017 User: admin
IP Address: 10.1.10.31 Time: 11:37 PM (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
Local Traffic
Acceleration
Device Management
Network
System

General Properties

Name

DNS Express

Server

Availability ☐ Unknown

State

Notify Action

Address:

127.0.0.1

Allow NOTIFY From

Verify Notify TSIG ☐

Response Policy ☒

Zone Transfer Clients

Nameservers

Active

Available

/Common
dc01.example.com
localhost

TSIG

Server Key

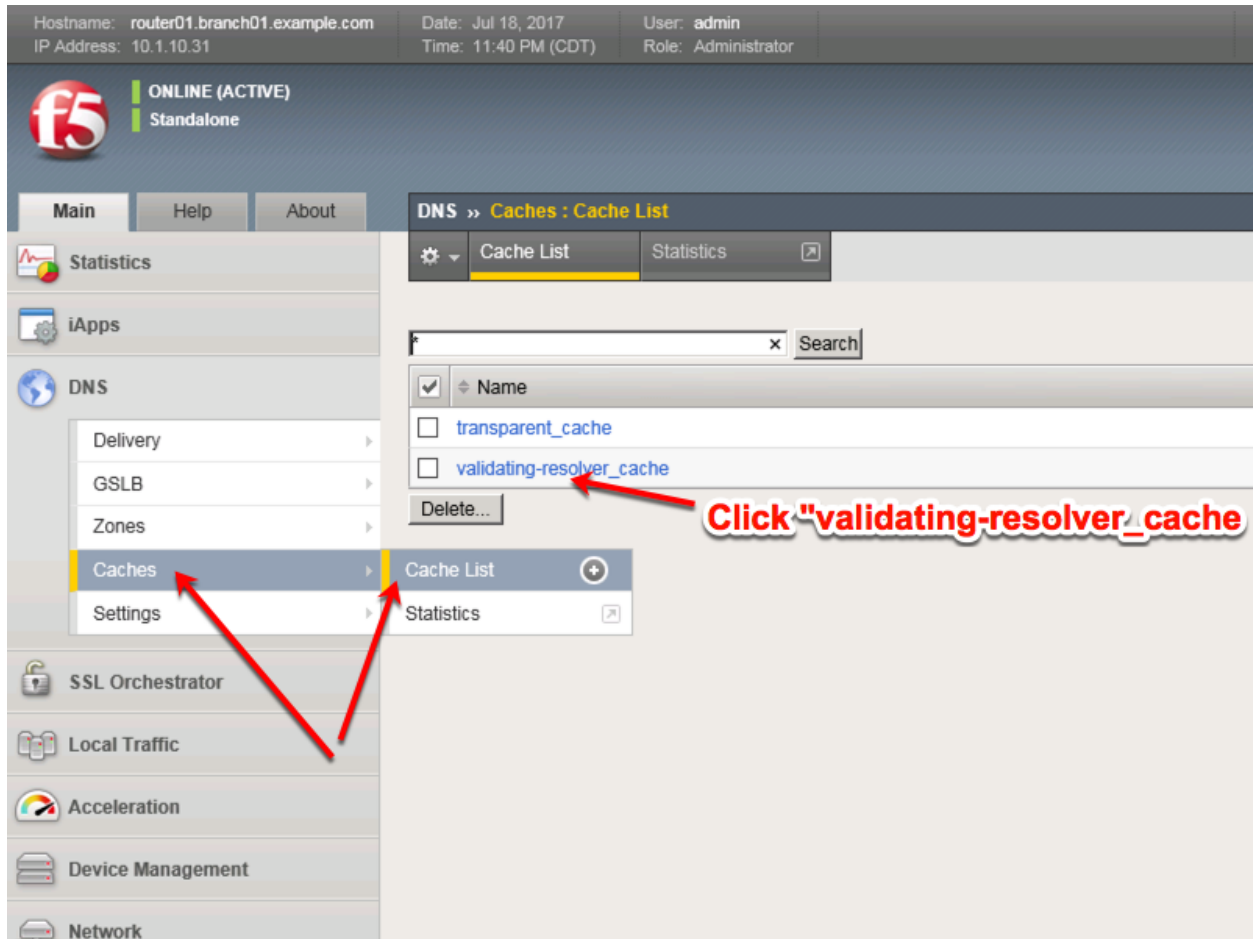
TMSH

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

2.2.6.4 Local Zone

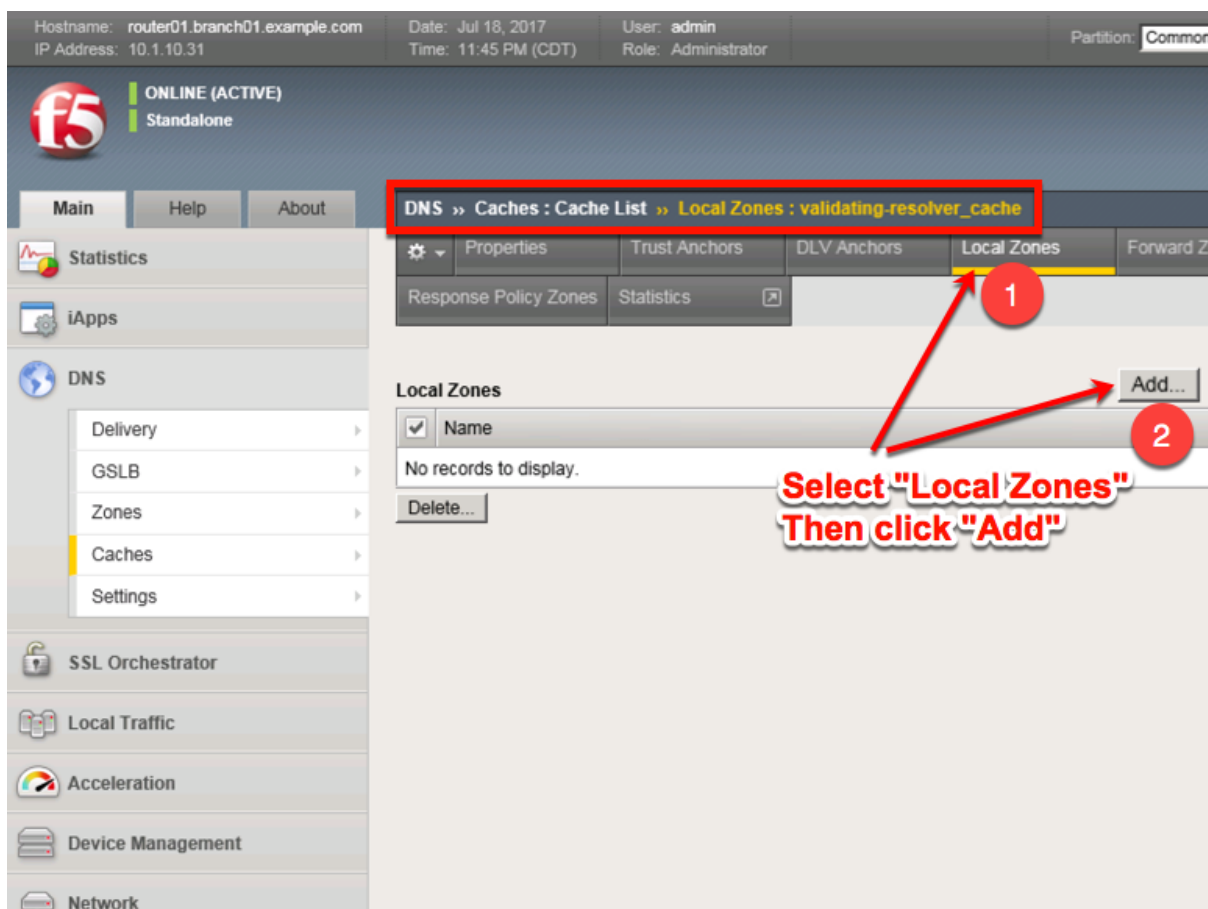
Navigate to: **DNS » Caches : Cache List**

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



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:

Field	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 } }
```

(continues on next page)

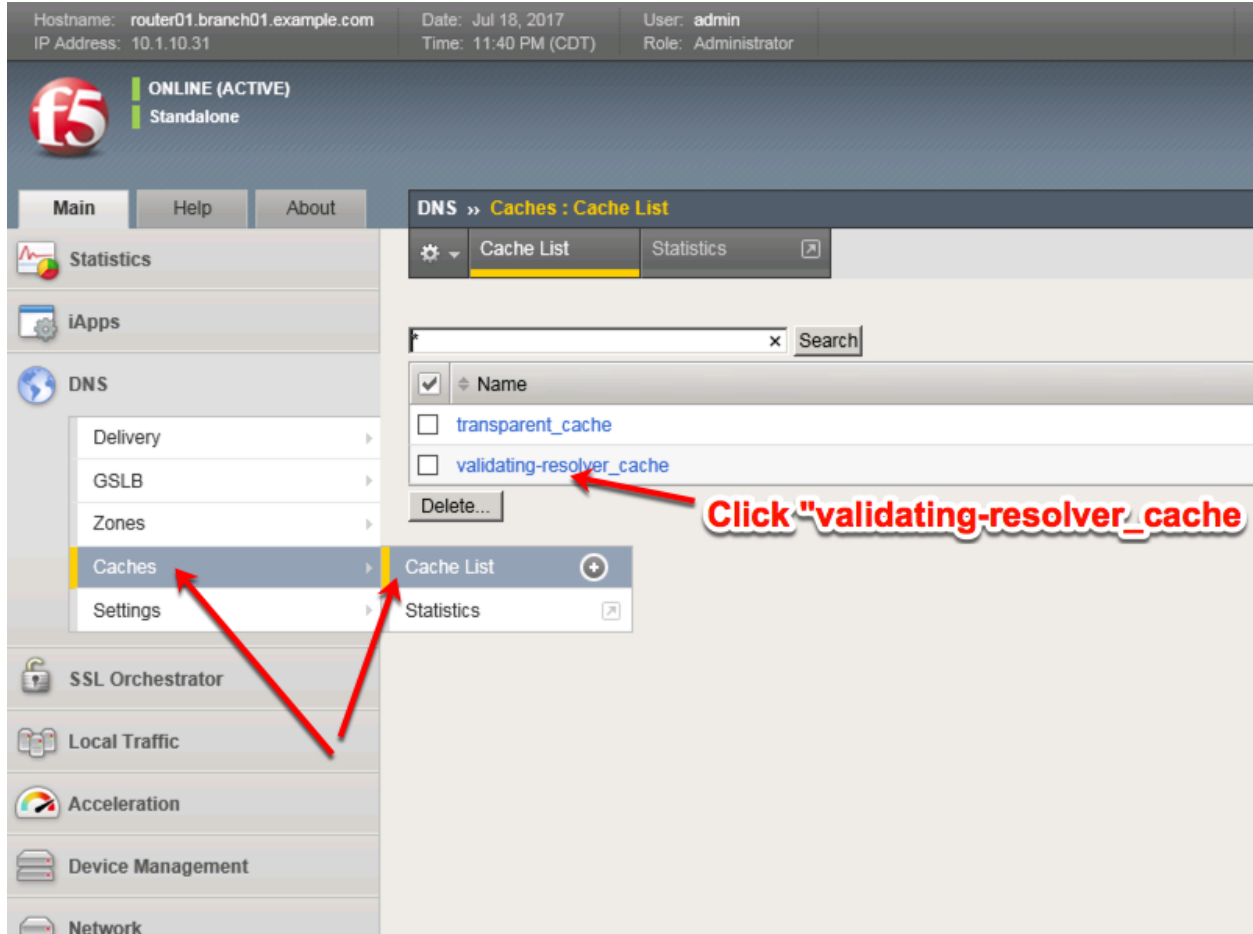
(continued from previous page)

2.2.6.5 Walled Garden

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

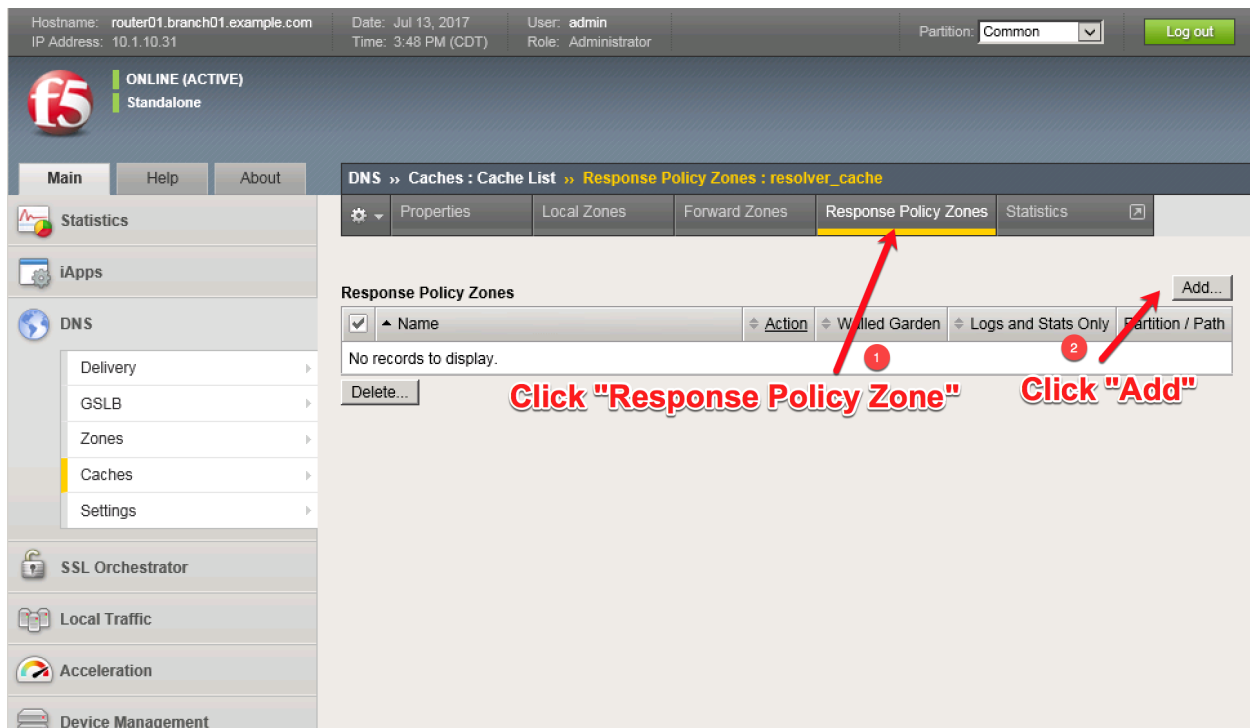
<https://router01.branch01.example.com/tmui/Control/jspmap/tmui/dns/cache/list.jsp>

Click “validating-resolver_cache”



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:

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

Response Policy Zone

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

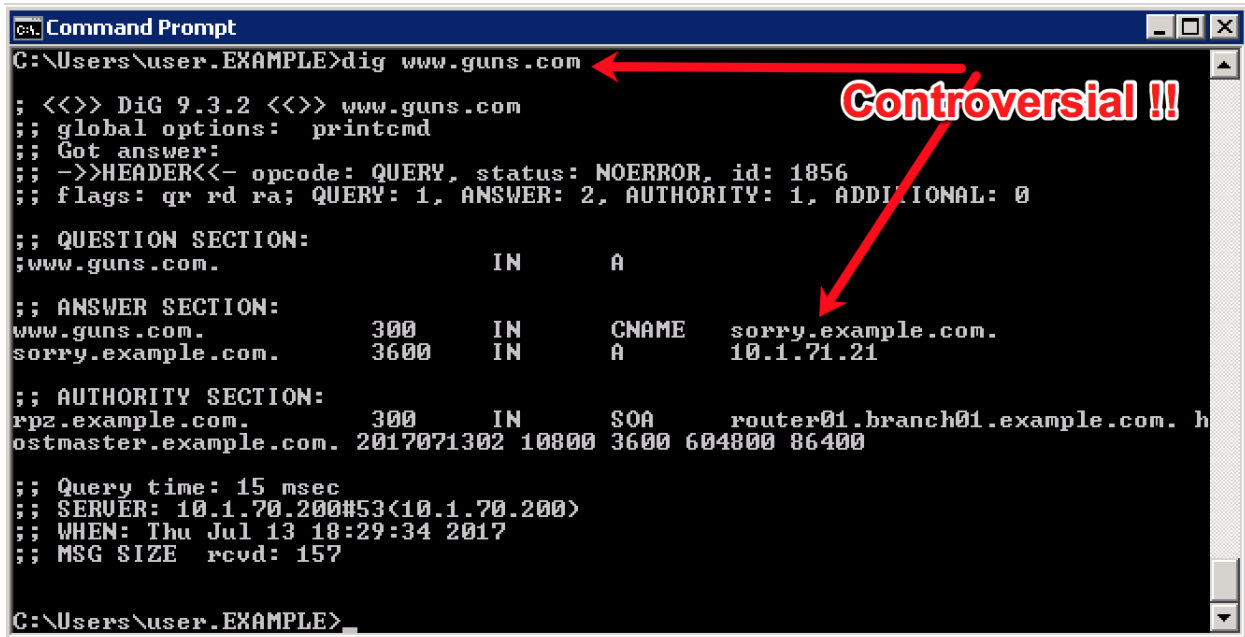
TMSH commands for router01.branch01:

TMSH

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

2.2.6.6 Results

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



```

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>

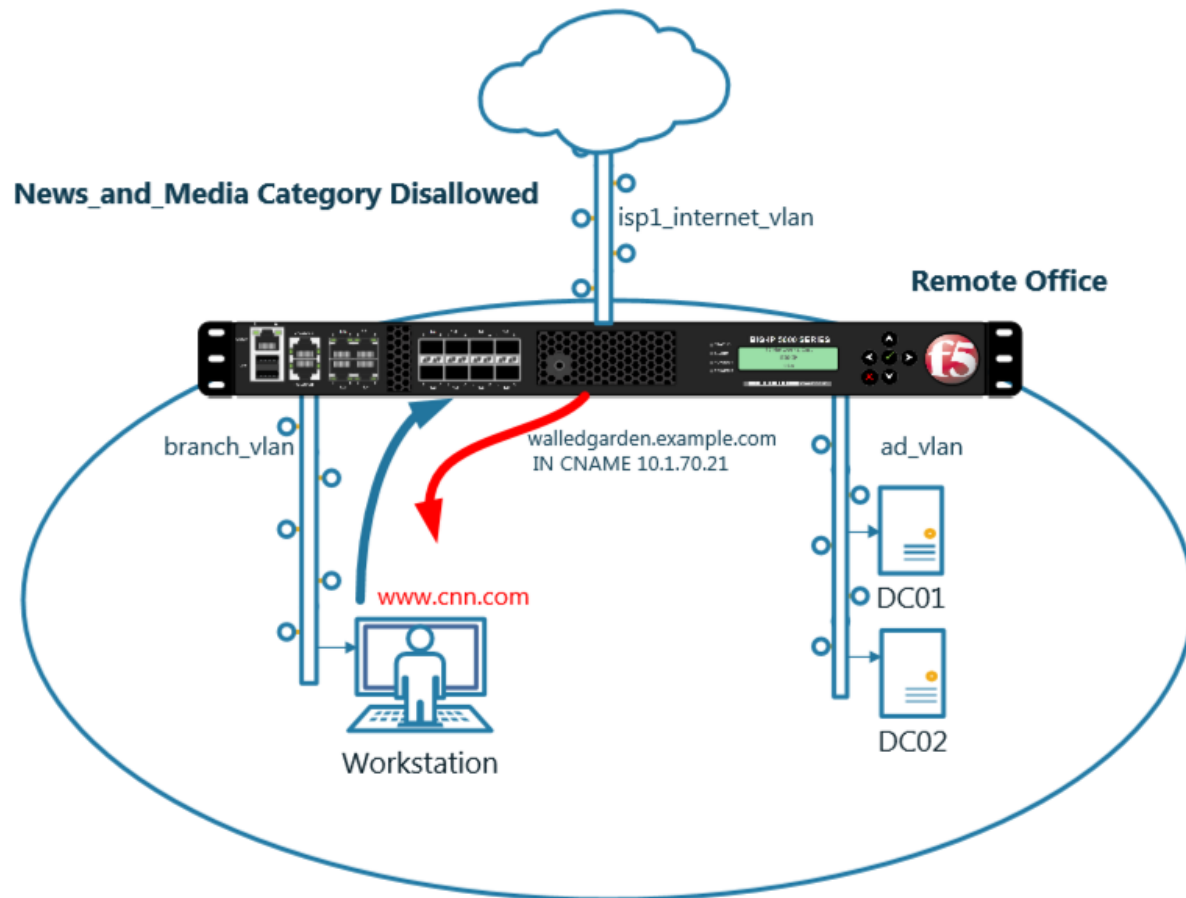
```

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

dig www.f5.com

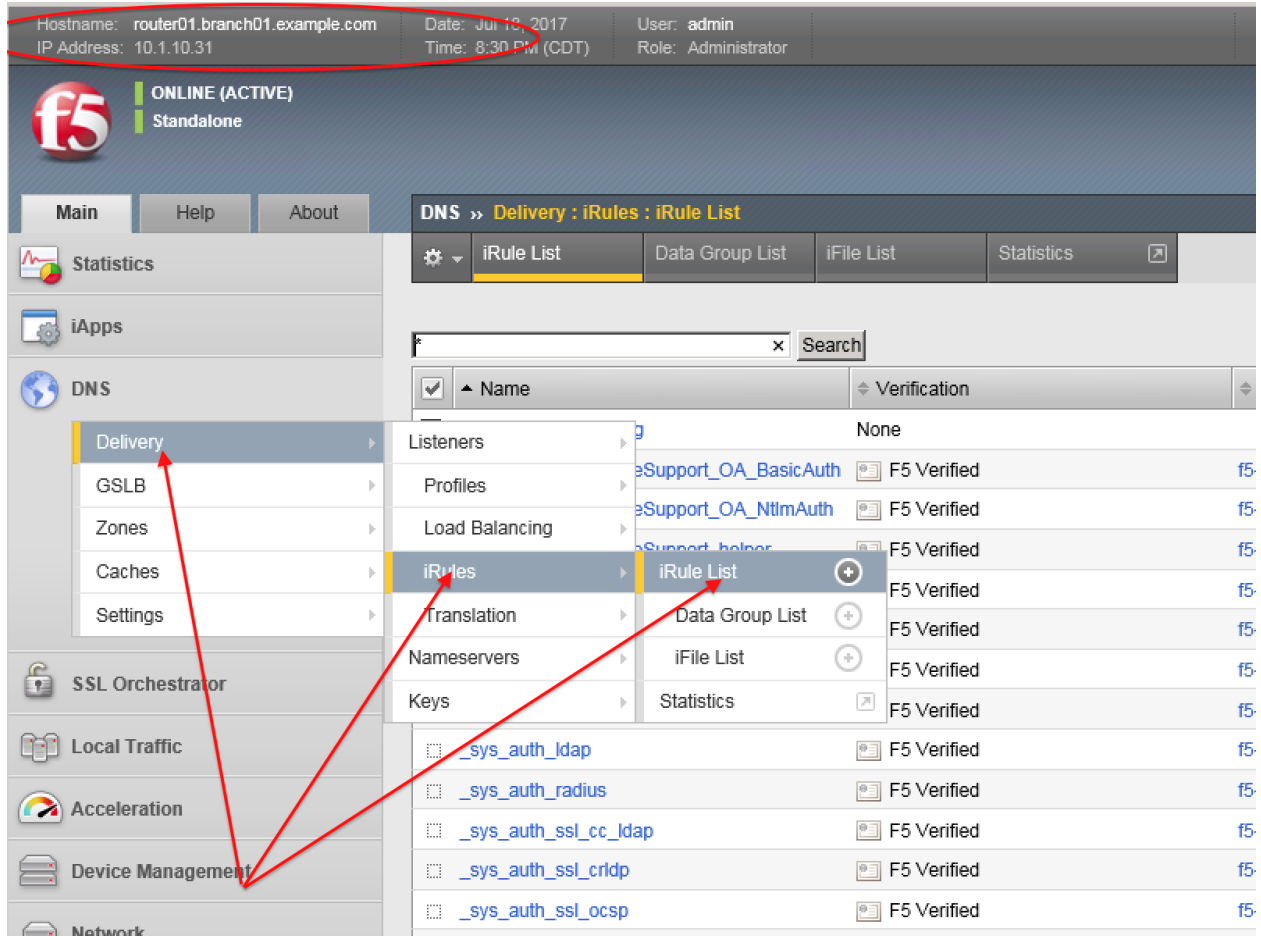
2.2.7 URL Categorization

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



2.2.7.1 Create an iRule

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



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

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

Field	Value
Name	DNS-query-filtering

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

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

(continues on next page)

(continued from previous page)

```

set static::request_redirect_to "10.1.71.21"
# Toggle for debug logs
set static::request_debug 1
}

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

2.2.7.2 iRule assignment

Repeat the following steps for all 4 DNS listeners.

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

Hostname: router01.branch01.example.com Date: Jul 18, 2017 User: admin
IP Address: 10.1.10.31 Time: 8:56 PM (CDT) Role: Administrator

ONLINE (ACTIVE)
Standalone

Main Help About

Local Traffic > iRules : iRule List

iRule List Data Group List iFile List Statistics

Search

✓	Name	Verification
	Listeners	F5 Verified 15
	Profiles	F5 Verified 15
	Load Balancing	F5 Verified 15
	iRules	F5 Verified 15
	Translation	F5 Verified 15
	Nameservers	F5 Verified 15
	Keys	F5 Verified 15
	_sys_auth_radius	F5 Verified 15
	_sys_auth_ssl_cc_ldap	F5 Verified 15
	_sys_auth_ssl_crdp	F5 Verified 15
	_sys_auth_ssl_ocsp	F5 Verified 15
	_sys_auth_tacacs	F5 Verified 15

Navigate to the listener DC01_udp_virtual

DNS > Delivery : Listeners : Listener List

Listener List Statistics

Search Create...

✓	State	Name	Destination	Protocol	Partition / Path
<input type="checkbox"/>	Enabled	DC01_tcp_virtual	10.1.70.200	TCP	Common
<input type="checkbox"/>	Enabled	DC01_udp_virtual	10.1.70.200	UDP	Common
<input type="checkbox"/>	Enabled	DC02_tcp_virtual	10.1.70.210	TCP	Common
<input type="checkbox"/>	Enabled	DC02_udp_virtual	10.1.70.210	UDP	Common

Enable Disable Delete...

Navigate to iRules section

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

Properties Load Balancing **iRules** Statistics

General

Name	DC01_udp_virtual
Partition	Common
Description	
State	Enabled

Listener: **Advanced**

Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.1.70.200
Service Port	DNS 53
VLAN Traffic	Enabled on...
VLANs and Tunnels	<div>Selected: /Common branch01_vlan</div> <div>Available: /Common AD_vlan external_vlan http-tunnel isp1_site1_vlan</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

Properties Load Balancing **iRules** Statistics

Statistics

Statistics Profile: None

Update

iRules

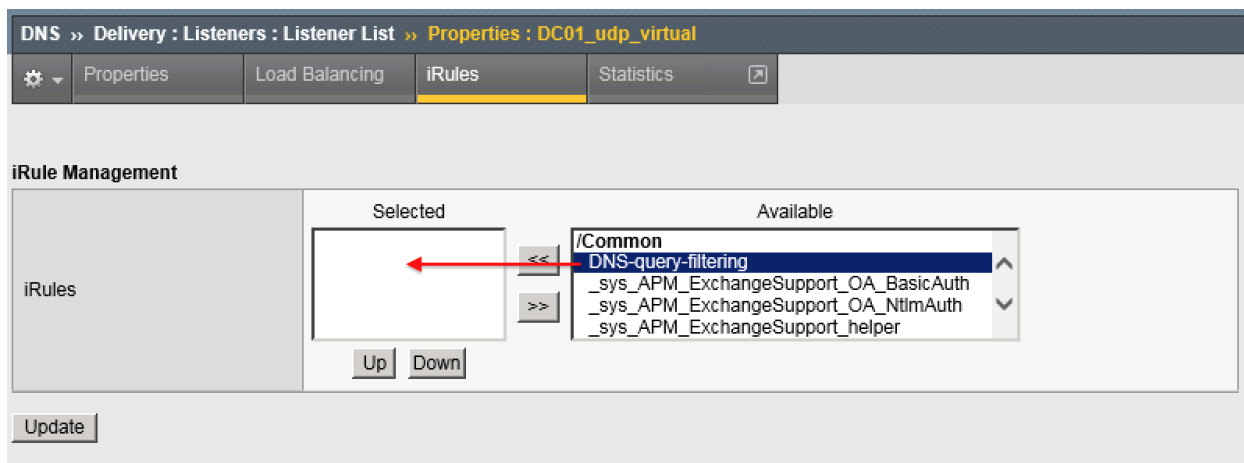
Manage...

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 }
```

2.2.7.3 Results

From the CLI on the router01.branch01 BIGIP run

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

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

```

C:\Users\user.EXAMPLE>dig <<>> 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-query-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
;

```

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

The image shows two overlapping windows. The top window is a Windows Command Prompt titled 'Command Prompt' with the following text:

```

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>

```

The bottom window is a network device console showing log messages. A red circle highlights the following line:

```

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.

```

Below the console output, there are two buttons: 'Update' and 'Delete'.

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

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	
_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> <p><input type="checkbox"/> Wrap Text <input type="checkbox"/> Show Print Margin</p>
Ignore Signature/Checksum	<input type="checkbox"/>

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

```

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;

```

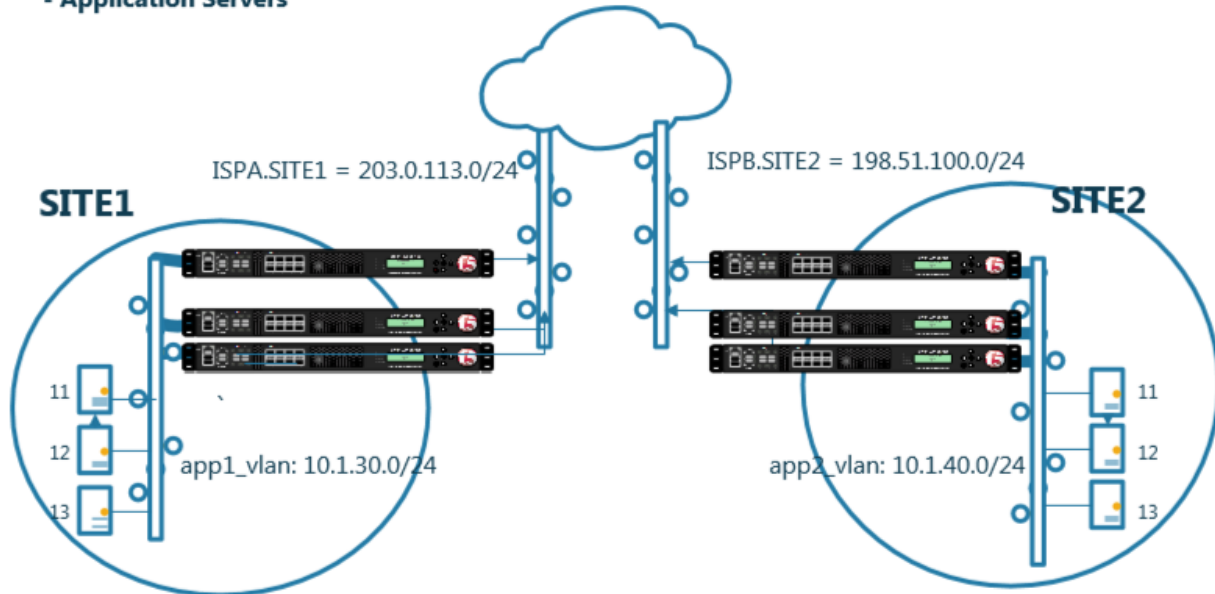
Update Delete

2.2.8 Title

Here's some stuff.

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

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



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.