

Agility 2017 Hands-on Lab Guide

DNS Services F5 Networks, Inc.

900

).O

Rahma (15) Rahma

Contents:

5

2	Clas	s 1 - Intro to GSLB 11
	2.1	Settings
	2.2	Listeners
		2.2.1 Logging
		2.2.2 DNS Profile
		2.2.3 UDP Profile
		2.2.4 TCP Profile
		2.2.5 UDP IP Address
		2.2.6 TCP IP Address
	23	Datacenters 28
	2.0	231 Servers 29
		2.3.1.1 atm1 site1 30
		2312 atm1 site2 35
		2.3.1.2 gitta.ba.pair 30
		$2.3.1.0$ site 1_1a-pair
		2.3.2 Dovice Trust 51
		2.3.2 Device flust
	0 /	
	2.4	FOOIS
	2.0	FQDN
	2.0	
		2.6.1 A Records
		2.6.2 Sub Domain
	0 7	2.6.3 CNAME
	2.7	Results
	2.8	Persistence
	2.9	LB Methods
3	Clas	s 2 - Advanced GSLB 83
	3.1	Transparent Cache
		3.1.1 Monitors
		3.1.2 Load Balancing
		3.1.3 Results
	3.2	Listeners

1 Lab Environment

	3.2.1	Log Profile
	3.2.2	DNS Profile
	3.2.3	UDP Profile
	3.2.4	TCP Profile
	3.2.5	UDP Listener
	3.2.6	TCP Listeners
	3.2.7	Results
3.3	Hidden	n Master
	3.3.1	Name Server
	3.3.2	DNS Express
	3.3.3	Results
3.4	DNSSe	ec
	3.4.1	Zone Signing Key
	3.4.2	Key Signing Key
	3.4.3	Signed Zone
	3.4.4	Results
3.5	Validat	ing Resolver
	3.5.1	Trust Anchors
	3.5.2	Modify DNS Profile
	3.5.3	Results
3.6	RPZ.	
	3.6.1	Zone Runner
	3.6.2	Name Server
	3.6.3	DNS Express
	3.6.4	Local Zone
	3.6.5	Walled Garden
	3.6.6	Results
3.7	URL C	ategorization
	3.7.1	Create an iRule
	3.7.2	iRule assignment
	3.7.3	Results

4 Credits

Lab Environment















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

• Convert the A record "www.example.com" to be a CNAME record pointing to www.gslb.example.com.

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

2.1 Settings

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

Navigate to: DNS >> Settings : GSLB : General

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

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



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

TMSH

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

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

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

2.2 Listeners

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

We will be creating both TCP and UDP based listeners.



2.2.1 Logging

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

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

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

Hostna IP Add	ame: gtm1.site1.example.com Da ress: 10.1.10.13 Tin	te: Jul 20, 2017 Use ne: 12:39 PM (CDT) Rol	er: admin le: Administrator			P
ſ	ONLINE (ACTIVE) Standalone					
Mai	n Help About	System » Logs : Col	nfiguration : Log Publishe	ers		
100 s	tatistics	🔅 👻 System	Captured Transaction	s Packet Filter	GSLB Aud	it
iA			Click "Cre	ate"	Create	1
😚 р	NS	🖌 🕈 Name			5	
6	SL Orchostrator	default-ipsec-log-p	oublisher			
U 3	SL Orchestrator	local-db-publisher				
(?) A	cceleration	sys-db-access-put	blisher			
		sys-sso-access-pu	ıblisher			
	evice Management	Delete				
<u></u> N	etwork					
8 🛉 S	ystem					
	Configuration					
	Pile Management					
	Certificate Management					
	Disk Management	Tu				
	Software Management					
	License	/ \				
	Resource Provisioning					
	Platform					
	High Availability					
	Archives 📀 🕨					
	Services	System				
	Preferences	Captured Transactions				
	sFlow	Packe Filter	Options			
	SNMP >	Local Traffic	Remote Logging			
	Crypto Offloading	GSLB	Log Filters			
	Users >	Audit 3	L 4 stinations	 Image: A start of the start of		
	Logs	Configuration	Log Publishers	•		

Create a local syslog publisher according to the table below:

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

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

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/system/log/create_publisher.jsp https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/system/log/create_publisher.jsp On both gtm1.site1 and gtm1.site run the following command:

TMSH

 $\label{eq:config} tmsh \ create \ sys \ log-config \ publisher \ local-syslog-publisher \ \{ \ destinations \ \{ \ local-syslog \ \} \ \} \ \}$

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

Hostname: gtm1.site1.example.com Dai IP Address: 10.1.10.13 Tin	e: Jul 20, 2017 ne: 12:49 PM (CDT)	User: admin Role: Administrator		
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » Delivery : I	Profiles : Other : DN	S Logging	
Mage Statistics	⇔ ▼ DNS	Protocol	✓ Other ✓	
iApps	ŀ		× Click "Create"	5 Create
S DNS	✓ ♦ Name			\$ Lo
Delivery	Listeners	>		
GSLB 2	Profiles	DNS	÷	
Zones	Load Balancing	Protocol	÷.	
Caches	iRules	Other	DNS Logging	•
Settings	Translation	3	4 Persistence	(\Rightarrow)
E con contractor	Nameservers	Figure 1	Statistics	\odot
SSL Orchestrator	Keys	×		
Acceleration				
Device Management				
Network				
System				

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

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

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

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

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

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

TMSH

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

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

2.2.2 DNS Profile

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

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

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



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

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

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Tim	e: Jul 20, 2017 User: admin e: 1:02 PM (CDT) Role: Administ	rator	
Standalone			
Main Help About	DNS » Delivery : Profiles : DN	IS » New DNS Profile	
Statistics	General Properties		
iApps	Name	example.com_dns_	
😚 dns	Parent Profile	dns	
Delivery	Denial of Service Protection	Custom	
GSLB	Rapid Response Mode	Disabled	
Zones	Rapid Response Last Action	Drop 🗸	
Caches	Hardware Acceleration		
octango	Protocol Validation	Disabled 🗸	
SSL Orchestrator	Response Cache	Disabled	
Acceleration	DNS Features		
Device Management	DNSSEC	Enabled 🔽	
	GSLB	Enabled V	
Network	DNS Express	Enabled V	
System	DNS Cache	Disabled	
	DNS Cache Name	Select 🗸	
	DNS IPv6 to IPv4	Disabled 🔽	
	Unhandled Query Actions		✓
	Use BIND Server on BIG-IP		
	DNS Traffic		
	Zone Transfer	Disabled	
	DNS Security	Disabled	
	DNS Security Profile Name	Select	
	Process Recursion Desired	Enabled 🔽	
	Logging and Reporting		
	Logging		✓
	Logging Profile	example_dns_logging_profile	1
	AVR Statistics Sample Rate	Enabled 1/ 1 queries sampled	

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/profile/dns/create.jsp https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/dns/profile/dns/create.jsp TMSH command for both gtm1.site1 and gtm1.site2:

TMSH

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

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

2.2.3 UDP Profile

A UDP profile is associated with a listener.

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

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Ti	ate: Jul 20, 2017 User: me: 1:11 PM (CDT) Role:	admin Administrator	
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Delivery : Prot	files : Protocol : UDP	Click "Create"
Statistics	⇔ v DNS	Protocol - Other	
iApps	ł	× Search	Create
😚 dns	🖌 🕈 Name		• •
Delivery 🔶	Listeners	>	
GSLB	Profiles	DNS 💮	
Zones	2 Load Balancing	Protocol	UDP 📀
Caches	iRules	3 Other 4	тср 🕣
Settings	translation		
B	Nameservers	>	
SSL Orchestrator	Keys	>	
Acceleration			
Device Management			
Network			
System			

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

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

Setting	Value
Name	example.com_udp-dns_profile
Parent Profile	udp_gtm_dns

Hostname IP Address	gtm1.site1.example.com s: 10.1.10.13	Date: Time:	Jul 20, 2017 Us 1:15 PM (CDT) Ro	er: admin le: Administra	tor		Partition: Common
6	ONLINE (ACTIVE) Standalone						
Main	Help About		DNS » Delivery : Pr	rofiles : Prot	ocol : UDP » New UDP Profile		
Magazina Stati	stics	1					
iApp	\$		General Properties		example.com_udp-		
😚 dns			Parent Profile		udp 🔽		
De	elivery	×	Settings		·		Custom 🗌
G	SLB	•	Proxy Maximum Seg	ment			
Zo	ones	×	Idle Timeout		Specify 🖌 60	seconds	
Ca	aches	•	IP ToS		Specify 🗸 0		
Se	ettings	•	Link QoS		Specify 🔽 0		
SSL	Orchestrator		Datagram LB				
	landian.		Allow No Payload				
Acce	eleration		TTL Mode		Proxy 🗸		
E Devi	ce Management		Don't Fragment Mode	9	PMTU 🔽		
e Netw	vork		Cancel Repeat	Finished			

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/profile/udp/create.jsp https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/dns/profile/udp/create.jsp TMSH command for both gtm1.site1 and gtm1.site2:

TMSH

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

2.2.4 TCP Profile

A TCP profile is associated with a listener.

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

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

Hostname: gtm1.site1.example.com Dai IP Address: 10.1.10.13 Tin	te: Jul 20, 2017 ne: 1:19 PM (CDT)	User: admin Role: Administrator		Partition: Common
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » Delivery	: Profiles : Protocol : T	СР	
Mage Statistics	DNS	Protocol	• Click "C	reate"
iApps	*		× Search	Create
S DNS	🖌 🕈 Name			Application Parent F
Delivery 1 >	Listeners	, t-tcp		tcp-legacy
GSLB	Profiles	DNS	÷	tcp-legacy
Zones	2 oad Balancing	Protocol	► UDP	() top
Caches	iRules	3 Other	ТСР	• tcp
Settings	Translation		- 4	tcp
C and and a starting	Nameservers	ied		tcp-legacy
SSL Orchestrator	Keys	₽		tcp-wan-or
Acceleration	tcp			(none)
Device Management	:::: tcp-lan-optimi	ized		tcp-legacy
berree munugement	tcp-legacy			tcp
Network	tcp-mobile-op	otimized		tcp-legacy
To System	tcp-wan-optin	nized		tcp-legacy

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

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

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Ti	ate: Jul 20, 2017 User: admin me: 1:23 PM (CDT) Role: Administ	rator	Partition: Common
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Delivery : Profiles : Pro	otocol : TCP » New TCP Profile	
Statistics	Concert Despertise		
iApps	Name	example.com_tc ×	
S DNS	Parent Profile	🗲 f5-tcp-wan	
Delivery	Timer Management		
GSLB	Close Wait	Specify 🔽 5 sec	conds
Zones	Fin Wait 1	Specify 🔽 5 sec	conds
Caches	Fin Wait 2	Specify 💙 300 see	conds
Settings	Idle Timeout	Specify V 300 seco	onds
SSL Orchestrator	Keep Alive Interval	Specify V 1800 seco	onds
Acceleration	Minimum RTO	500 milliseconds	
Dovice Management	Reset On Timeout	Enabled	
	Time Wait	Specify 🔽 2000 mil	lliseconds
Network	Time Scroll way do	wn to find the "Finish!	"button
System	Zero Window Timeout	Specify 20000 milli	seconds

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/profile/tcp/create.jsp https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/dns/profile/tcp/create.jsp TMSH Command for both gtm1.site and gtm1.site2:

TMSH

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

2.2.5 UDP IP Address

A UDP listener will receive and process DNS queries.

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

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

Hostname: gtm1.site1.example.com Dat IP Address: 10.1.10.13 Tim	e: Jul 20, 2017 User: au e: 1:29 PM (CDT) Role: A	d min dministrator			Partition: Common
Standalone					
Main Help About	DNS » Delivery : Listen	ers : Listener List		Click"Create	
Mag Statistics	🔅 👻 Listener List	Statistics			
iApps	*	×	Search		Create
S DNS	State 🗢 Name				Destination
Delivery	Listeners	Listener List	0		
GSLB	Profiles	Statistics	M		
Zones	Load salancing				
Caches	iRules >				
Settings	Translation >				
	Nameservers				
SSE OTCHER MALOI	Keys >				
Acceleration					
Device Management					
Network					
System					

Create a UDP listener according to the following table:

Setting		gtm1.site1	gtm1.site2]
Name		isp1_site1_ns1.example.com_udp_53_	vi ispa l_site2_ns2.example.com_udp_53_v	virtual
Destination		203.0.113.8	198.51.100.40	
Protocol	Profile	example.com_udp-dns_profile	example.com_udp-dns_profile	
(Client)				
DNS Profile		example.com_dns_profile	example.com_dns_profile	

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/listener/create.jsp https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/dns/listener/create.jsp

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Tin	te: Jul 20, 2017 User: admin ne: 1:32 PM (CDT) Role: Administ	trator Partition: Common		
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » Delivery : Listeners : L	istener List » New		
Magazina Statistics				
i i i i i i i i i i i i i i i i i i i	General			
TApps	Name	isp1_site1_ns1.example.com_udp_53		
S DNS	Description			
Delivery	State	Enabled V		
GSLB	Listener: Advanced			
Zones		Type: O Host O Network		
Caches	Destination	Address: 203.0.113.8		
Settings	Service Port	DNS 🔽 53		
SSL Orchestrator	VLAN Traffic	All VLANs		
	Source Address Translation	None		
Acceleration	Address Translation	Enabled		
Device Management	Port Translation	Enabled		
Network	Route Advertisement	Enabled		
25	Auto Last Hop	Default 🔽		
System	Last Hop Pool	None		
	Service: Advanced			
	Protocol	UDPV		
	Protocol Profile (Client)	example.com_udp-dns_profile		
	Protocol Profile (Server)	(Use Client Profile)		
	DNS Profile	example.com_dns_profile		

gtm1.site1 TMSH command:

TMSH

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

gtm1.site2 TMSH command:

TMSH

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

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

2.2.6 TCP IP Address

A TCP listener will receive and process DNS queries.

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

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

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Ti	ate: Jul 20, 2017 User: a me: 1:29 PM (CDT) Role: A	admin Administrator	Partition: Common
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Delivery : Listen	ners : Listener List	Click "Create"
Statistics		Statistics	
iApps	۴	× Search	Create
😚 dns	State 🗢 Name		▲ Destination 💠 F
Delivery	Listeners	Listener List 💽	
GSLB	Profiles	Statistics	
Zones >	Load Balancing		
Caches	iRules >		
Settings	Translation		
S SSI Orchantor	Nameservers		
SSL OICHERINATO	Keys		
Acceleration			
Device Management			
Network			
System			

Create a TCP listener.

Setting		gtm1.site1	gtm1.site2	
Name		isp1_site1_ns1.example.com_tcp_53_v	irt spa1 _site2_ns2.example.com_tcp_53_vi	irtua
Destination		203.0.113.8	198.51.100.40	
Protocol	Profile	example.com_tcp-dns_profile	example.com_tcp-dns_profile	
(Client)				
DNS Profile		example.com_dns_profile	example.com_dns_profile	

Hostname: gtm1.site1.example.com IP Address: 10.1.10.13	Date: Jul 20, 2017 User: admin Time: 2:18 PM (CDT) Role: Administ	trator Partition: Common
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » Delivery : Listeners : L	istener List » New
Statistics	General	
iApps	Name	isp1_site1_ns1.example.com_udp_53
S DNS	Description	
Delivery	State	Enabled V
GSLB	Listener: Advanced V	
Zones Caches	Destination	Type: Host O Network Address: 203.0.113.8
Settings	Service Port	DNS S3
SSL Orchestrator	VLAN Traffic	All VLANs 🔽
	Source Address Translation	None
	Address Translation	Enabled
Device Management	Port Translation	Enabled
Retwork	Route Advertisement	Enabled
	Auto Last Hop	Default Be sure to select "TCP"
System	Last Hop Pool	None
	Service: Advanced	
	Protocol	TCP
	Protocol Profile (Client)	example.com_tcp-dns_profile
	Protocol Profile (Server)	(Use Client Profile)
	DNS Profile	example.com_dns_profile
	Load Balancing	
	Default Pool	None
	Default Persistence Profile	None
	Fallback Persistence Profile	None

https://gtm1.site1.example.com/tmui/Control/jspmap/tmui/dns/listener/create.jsp https://gtm1.site2.example.com/tmui/Control/jspmap/tmui/dns/listener/create.jsp gtm1.site1 TMSH command:

TMSH

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

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

gtm1.site2 TMSH command:

TMSH

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

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

2.3 Datacenters

Datacenters are logical groupings of devices that share a gateway.

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

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

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Tir	te: Jul 20, 2017 User: ne: 1:45 PM (CDT) Role:	admin Administrator	Partition: Common
ONLINE (ACTIVE) Standalone			
Main Heip About	UNS » GSLB : Data C	enters : Data Center List	Click "Croate"
Statistics			Click-Create-
iApps	*	Search	Create
S DNS	Availability	Name	Location Links
Delivery	No records to display.		
GSLB	Wide IPs	e	
Zones 1	Pools	►	
Caches	iRules 🔶		
Settings	Data Centers	Data Center List 💽	
E sel contrata la	2 Servers	3 Statistics 🗵	
SSL Orchestrator	Links	Þ	
Acceleration	Prober Pools	Þ	
Device Management	Monitors 📀		
	Topology	►	
Network	Distributed Applications	►	
System			

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

Create two data centers according to the table below:

Setting	Value
Name	site1_datacenter
Name	site2_datacenter

Hos IP A	stname: gtm1.site1.example.com Address: 10.1.10.13	Date: Time:	Jul 20, 2017 1:48 PM (CDT)	User: Role:	admin Administrate	Partition: Common
ſ	Standalone					
			DNS » GSLB; I		enters : Da	
	Statistics		General Propertie	s		
	iApps		Name			site1_datacenter
5	DNS		Description			
	Delivery	×	Location			
	GSLB	×.	Contact			
	Zones	×	Prober Preference	е		Inside Data Center
	Caches	•	Prober Fallback			Any Available
	Settings	•	State			Enabled V
6	SSL Orchestrator		Cancel Repea	t Fi	nished	
	Acceleration					
	Device Management		Repeat	thi	s step	to create "site2_datacenter"
	Network					
3 -	System					
https	://gtm1.site1.example.co	m/tn	nui/Control/jsp	map	/tmui/glo	ballb/data_center/create.jsp

TMSH command for only site1.gtm1:

TMSH

tmsh create gtm datacenter site1_datacenter

TMSH

tmsh create gtm datacenter site2_datacenter

2.3.1 Servers

Server objects need to be defined and grouped into a Datacenter

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Tin	te: Jul 20, 2017 User: ao ne: 2:04 PM (CDT) Role: A	d min dministrator		Partition: Common
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » GSLB : Servers :	Server List		
Mage Statistics	🔅 👻 Server List	Trusted Server Certificate	s Statistics	
iApps	*	Search		Create
😚 dns	Status 🔺 Name	Device	es Address 💠 🛙	Data Center Virtual Servers
Delivery	No records to display.			
GSLB →	Wide IPs	ete		
Zones	Pools >			
Caches	iRules 🔶			
Settings	Data Centers			
E man	Servers	Server List 💽		
SSL Orchestrator	Links	Trusted Server		
Acceleration	Prober Pools	Statistics	1	
Device Management	Monitors 📀	Claided	2	
	Topology >			
Network	Distributed Applications >			
System				

Navigate to: DNS >> GSLB : Servers : Server List

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

2.3.1.1 gtm1.site1

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

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Tim	e: Jul 20, 2017 User: ad e: 2:00 PM (CDT) Role: Ad	imin Iministrator	Partition: Common
Standalone			
Main Help About	DNS » GSLB : Servers :	Server List	
Statistics	🔅 👻 Server List	Trusted Server Certificates	Statistics 🔎
iApps	*	Search	Create
S DNS	Status 🔺 Name	Devices	Address
Delivery	No records to display.		
GSLB	Enable Disable Delet	te	
Zones >			
Caches	Clic	k "Create" to d	efine atm1 site1
Settings >			guine
SSL Orchestrator			
Acceleration			
Device Management			
Network			
System			

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

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

1. Fill in the Name and Datacenter

Hostname: gtm1.site1.example.com Dat IP Address: 10.1.10.13 Tim	e: Jul 20, 2017 ie: 2:29 PM (CE	User:)T) Role:	admin Administrat	or	Parti
ONLINE (ACTIVE) Standalone					
Main Help About	DNS » G	SLB : Server	s : Server I	List >> New Server	
Statistics	Conoral Dr	portion			
iApps	Name	operues		gtm1.site1_server	
😚 dns	Product			BIG-IP System	
Delivery	Data Cer	ter		site1_datacenter	
GSLB	Prober Pre	eference		Inherit From Data Center 🗸	[
Zones	Prober Fa	llback		Inherit From Data Center 🗸	[
Caches	State			Enabled 🗸	
Settings	Devices			- Click-"Ad	a 2
SSL Orchestrator		Add 🗲			2 -
			Dev	ice Name	Address
Acceleration	BIG-IP	No data ava	ilable in tab	e	
Device Management	Devices				
Retwork					
System		Edit Delete			

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

Hostnan IP Addre	me: gtm1.site1.example.com ess: 10.1.10.13	Date: Jul 20, 2017 Time: 2:36 PM (CE	User:)T) Role:	admin Administrator		Parti
	ONLINE (ACTIVE) Standalone					
Main	Help About	DNS » G	SLB : Server	s : Server List » New	Server	
Ma Sta	atistics			Add BIG-IP	System Device	
iAp	pps	General Pro	operties	Device Nam Address:	e: gtm1.site1.example.com	
S) DN	IS	Product		Translation:		(Optional)
	Delivery	Click"	Add"	Link:	Auto-Select 🗸	
	GSLB	Prober Pre	eference	Add 3		
	Zones	Prober Fa	llback	203.0.113.7		
	Caches	State				
	Settings	>				
ss 🕄	L Orchestrator	Devices		Delete		OK Cancel
(Ac	celeration	BIG-IP	No data avai	De ilable in table		
📄 De	vice Management	System Devices				
e Ne	twork				CIICK OK	
Sy:	stem					

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

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Tin	ite: Jul 20, 2017 ne: 2:43 PM (Cl	' User: admin DT) Role: Administra	ator		Parti
CONLINE (ACTIVE) Standalone					
Main Help About	DNS » G	SLB : Servers : Serve	r List » New Server		
Statistics	General Pr	operties			
iApps	Name		gtm1.site1_server		
😚 dns	Product		BIG-IP System		
Delivery	Data Cer	nter	site1_datacenter		
GSLB	Prober Pr	eference	Inherit From Data Center 🗸		
Zones	Prober Fa	llback	Inherit From Data Center 🔽		
Caches	State		Enabled V		
Settings	Devices				
SSL Orchestrator		Add			
Acceleration		gtm1.site1.example.co	Device Name	Address 203.0.113.7	
Device Management	BIG-IN System Devices				
Network					
System		Edit Delete			
	Configurat	ion: Advanced 🔽			
	Health Mo	onitors	Selected	Available /Common gateway_icmp gtp http http_ http_head_f5	
	Availabilit	y Requirements	All Health Monitors		
	Limit Setti	ngs	Bits: Disabled Packets: Disabled Current Connections: Disabled	সাহায	
	iQuery Op	otions	Service Check 🖌 Path 🖌 SNMP 🖌		

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

TMSH

2.3.1.2 gtm1.site2

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



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

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

1. Fill in the Name and Datacenter

Hostname: gtm1.site1.example.com Dat IP Address: 10.1.10.13 Tim	e: Jul 20, 2017 e: 3:18 PM (CDT)	User: Role:	admin Administrate	pr	Pa	arti
Standalone						
Main Help About	DNS » GSI	.B : Server	s : Server l	.ist >> New Server		
Statistics	Concert Dece					
iApps	Name =	erues		gtm1.site2_server		
😚 dns	Product			BIG-IP System		
Delivery	Data Cente	r		site2_datacenter		
GSLB >	Prober Prefe	rence		Inherit From Data Center 🗸		
Zones	Prober Fallb	ack		Inherit From Data Center 🔽		
Caches	State			Enabled 🔽		
Settings	Dovices			<u></u>		
SSL Orchestrator	Devices	ral 👉		Click "Add"		
	f		Dev	ice Name	Address	
Acceleration	BIG-IP	lo data ava	ilable in tabl	e		
Device Management	System Devices					
Retwork						
System	E	dit Delete				

2. Click the "Add" button to define IP addresses
| Hostname: gtm1.site1.example.com [
IP Address: 10.1.10.13] | ate: Jul 20, 2017 User: admin
me: 3:30 PM (CDT) Role: Administrator | Parti |
|--|---|-----------|
| Standalone | | |
| Main Help About | DNS » GSLB : Servers : Server List » New Server | |
| Statistics | Add BIG-IP System Device | |
| iApps | General Properties Bayice Name: gtm1.site2.example.com Name Address: 198.51.100.39 Product |)ntional) |
| Delivery | | puonary |
| GSLR | | |
| 3000 | Add | |
| Zones | Prober Fallback 2 198.51.100.39 | |
| Caches | State | |
| Settings | and the second se | |
| SSL Orchestrator | | ancel |
| Acceleration | No data available in table | |
| Device Management | BIG-IP
System
Devices | |
| Retwork | | |
| System | Edit Delete | |

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



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

TMSH

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

2.3.1.3 site1_ha-pair

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



Create a Server Object as defined in the table below:

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

1. Fill in the Name and Datacenter

Host IP A	tname: gtm1.site1.example.com ddress: 10.1.10.13	Date: Time:	Jul 20, 2017 3:58 PM (CI	User: DT) Role:	admin Administrator			Parti
(Standalone	_ [DNS	61.0 - 6				
M	ain Heip About	1	UNS » G	SLB : Server	s : Server Li	st » New Server		
	Statistics		General Pr	onerties				
	iApps		Name		 [site1_ha-pair		
5	DNS		Product		[BIG-IP System		
	Delivery	•	Data Cer	nter	→	site1_datacenter		
	GSLB	÷	Prober Pr	eference	[nherit From Data Center 🔽		
	Zones		Prober Fa	llback	[nherit From Data Center 🔽		
	Caches	•	State		[Enabled 🔽		
	Settings	•	Devices					
6	SSL Orchestrator		Devices	Add 🗲		Click "Add"		
	Acceleration				Devid	e Name	Address	
	Device Management		BIG-IP System Devices	No data avai	ilable in table			
	Network							
87	System			Edit Delete				

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

Hostna IP Add	ame: gtm1.site1.example.com dress: 10.1.10.13	Date: Jul 20, 3 Time: 4:33 Ph	2017 User: M (CDT) Role:	admin Administrator				Pa
ſ	ONLINE (ACTIVE) Standalone							
Mai	in Help About	DNS	» GSLB: Server	rs : Server List	» New Server			
Ma s	tatistics			Ad	d BIG-IP System	Device		
	Apps	Genera	al Properties	De	vice Name: bigip1 dress: 1 203.0	.site1.example.com .113.5		
	NS	Produ	ict	Tra	inslation:		(Option	nal)
	Delivery	Data		Lin	k: Auto-S	Select 🗸		
	GSLB	Probe	er Preference		Add 2			
	Zones		ck"Add"	20	3.0.113.5			_
	Caches	State						
	Settings	•						
e		Device	s		elete			
L'S	SL Orchestrator					3	OK Cance	31
(?) A	cceleration		No data ava	De ailable in table				
	evice Management	BIG- Syst Devi			C	lick"OK"		
	etwork							
8 🛉 S	ystem							

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

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Time	e: Jul 20, 2017 User: admin e: 4:38 PM (CDT) Role: Adminis	Pai
Standalone		
Main Help About	DNS » GSLB : Servers : Serv	er List » New Server
Statistics	Conoral Properties	
iApps	Name	site1 ha-pair
S DNS	Product	BIG-IP System
Delivery	Data Center	site1_datacenter
GSLB →	Prober Preference	Inherit From Data Center
Zones	Prober Fallback	Inherit From Data Center
Caches	State	Enabled V
Settings >	Devices	Click "Add"again
SSL Orchestrator	Add	
Acceleration	bigind gited event	Dovise Name Address
	BIG-IF System	.com 203.0.113.5
Device Management	Devices	
Retwork		
System	Edit Delete	

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

Hostname: gtm1.site1.example.com IP Address: 10.1.10.13	Date: Jul 20, 2017 Time: 4:53 PM (CD	User: T) Role:	admin Administrator		Par
ONLINE (ACTIVE) Standalone					
Main Help About	DNS » G	SLB : Serve	rs : Server List » New S	Server	
Statistics			Add BIG-IP	System Device	
iApps	General Pro Name Product	operties	Address:	e: bigip2.site1.example.com	
Delivery	Click"		Link:	Auto-Select	aı)
Zones	Prober Eal		Add 203.0.113.6		
Caches Settings	> State				
SSL Orchestrator	Devices		Delete	OK Cancel	
Acceleration Device Management	BIG-IP System Devices	bigip1.site1.	example.com	20rd 113.5	
Network					

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

Hos IP A	stname: gtm1.site1.example.com Address: 10.1.10.13	Date: Time:	Jul 20, 2017 5:00 PM (C	' User: admin DT) Role: Administra	tor	Par
(ONLINE (ACTIVE) Standalone					
N	Main Help About		DNS » G	SLB : Servers : Server	List » New Server	
~	Statistics					
	iAnne		General Pr	operties		
100	ind ha		Name		site1_ha-pair	
5	DNS		Product		BIG-IP System	
	Delivery	•	Data Ce	nter	site1_datacenter	
	GSLB	•	Prober Pr	eference	Inherit From Data Center	
	Zones	•	Prober Fa	llback	Inherit From Data Center	
	Caches	•	State		Enabled V	
	Settings	•	Devices			
6	SSL Orchestrator		Devices	Add Two.d	evices belong to this HA-Pair	7
	Acceleration		I [bigip1.site1.example.co	om 203.0.113.5	
	Device Management		BIG-IF System Devices	bigip2.site1.example.co	om 203.0.113.6	
	Network					
	System			Edit Delete		
	dd the "bigip" He	alth		Advanced V		
2			Health Mo	pnitors	Selected Available //Common bigip < gateway_icmp gtp http http_head_f5	
			Availabilit	y Requirements	All Health Monitors	

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

Resource

lesources					
Virtual Server Discovery	Enabled				
Link Discovery	Enabled				
Cancel Repeat Finished					

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

TMSH

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

2.3.1.4 site2_ha-pair

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



Create a Server Object as defined in the table below:

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

1. Fill in the Name and Datacenter

Hostname: gtm1.site1.example.com Dat IP Address: 10.1.10.13 Tim	e: Jul 20, 2017 User: admin he: 5:52 PM (CDT) Role: Administra	tor
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » GSLB : Servers : Server	List » New Server
Magazine Statistics		
iAnne	General Properties	
induba induba	Name 🚽	site2_ha_pair
😚 dns	Product	BIG-IP System
Delivery	Data Center 🛑 🔶	site2_datacenter
GSLB	Prober Preference	Inherit From Data Center
Zones	Prober Fallback	Inherit From Data Center
Caches	State	Enabled V
Settings	Devices	Click "Add"
SSL Orchestrator		Add
		Device Name
Acceleration		No data available in table
Device Management	BIG-IP System Devices	
Retwork		
System		Edit Delete

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

Hostn IP Add	ame: gtm1.site1.example.o dress: 10.1.10.13	com Date: Time:	Jul 20, 2017 5:56 PM (CD	User: T) Role:	admin Administrator			Partition: Common
	ONLINE (ACTIVE Standalone)						
Ma	in Help	About	DNS » GS	SLB : Server	s : Server List	» New Server		
ν ν	tatistics Apps	-	General Pro	perties	Device Nan	ne: bigip1.site2.exan	nple.com	
S	ON S		Product		Translation	·		(Optional)
	Delivery	•	Data Cent		Link:	Auto-Select 🗸		
	GSLB	Clic	k"Ad		Add			
- F	Zones	,	Prober Fall	back	198.51.100	0.37		
	Caches	÷	State					
	Settings	•	Dovices		Delete			
6 s	SL Orchestrator		Jevices		Device N	lame		OK Cancel
A	cceleration			No data avai	ilable in table			
	evice Management		BIG-IP System Devices				Click "OK	P
<u>_</u> N	letwork							
87 S	system							

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

Hostname: gtm1.site1.example.com Dat IP Address: 10.1.10.13 Tim	e: Jul 20, 2017 User: admin e: 6:13 PM (CDT) Role: Admin	nistrator Partition: Commo
ONLINE (ACTIVE) Standalone		
Main Heip About	DNS » GSLB : Servers : Ser	rver List » New Server
Statistics	Conoral Droportion	
iApps	Name	site2_ha_pair
😚 dns	Product	BIG-IP System
Delivery	Data Center	site2_datacenter
GSLB >	Prober Preference	Inherit From Data Center
Zones	Prober Fallback	Inherit From Data Center
Caches	State	Enabled V
Settings	Dovices	
SSL Orchestrator	Add	
Acceleration	bigip1.site2.examp	Device name Address ble.com 198.51.100.37
Device Management	System Devices	
e Network		
System	Edit Delete	

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

Hostn IP Add	ame: gtm1.site1.example.co dress: 10.1.10.13	m Date: Time:	Jul 20, 2017 6:22 PM (CD1	User: T) Role:	admin Administrator			Partition: Common
	ONLINE (ACTIVE) Standalone							
Ma	in Help A	bout	DNS » GS	LB : Server	s : Server List »	New Server		
1 s	tatistics		_		Dovico Nam	ni higinî citaî avamal		
	Anne		General P <mark>ro</mark>	perties	1 1 1	e. bigipz.sitez.example	e.com	
L@ "	Apps		Name -		Address:	198.51.100.38		
()	N S		Product		Translation:			(Optional)
Г	Delivery	÷	Deta Cert	im.	2 ^{°k:}	Auto-Select 🗸		
	GSLB	CI	CK "Ad	d Ference	Add			
	Zones	+	Prober Fall	back	198.51.100	.38		
	Caches	÷	State					
	Settings	•	Devices		Delete			
🔓 s	SL Orchestrator						3	OK Cancel
	cceleration				Device N	lame		ddress
	oooloradion		BIG-IP	bigip1.site2.			198.51.1 (0.3)	~~~~
	evice Management		System Devices				Click	OK"
<u>_</u> N	letwork							
87 S	ystem							

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

Hos IP A	tname: gtm1.site1.example.com ddress: 10.1.10.13	Date: Time:	Jul 20, 2017 7:55 PM (C	User: DT) Role:	admin Administrate	or		Partition: Common
(ONLINE (ACTIVE) Standalone							
N	Main Help About		DNS » G	SLB : Server	s : Server I	List » New Server.		
	Statistics							
	iApps		General Pr	operties		alled he asis		
			Name			site2_na_pair		
\mathbf{S}	DNS		Product			BIG-IP System	\checkmark	
	Delivery	•	Data Cer	nter		site2_datacenter	~	
	GSLB	×	Prober Pr	eference		Inherit From Data C	Center 🔽	
	Zones	•	Prober Fa	llback		Inherit From Data C	Center 🔽	
	Caches	•	State			Enabled 🗸		
	Settings	•						
6	SSL Orchestrator		Devices	a sal				
-				Add	Des			
	Acceleration			bigip1.site2.	example.co	m	198.51.100	.37
	Device Management		BIG-IP System Devices	bigip2.site2.	example.co	m	198.51.100	.38
	Network							
	System			Edit Delete				
			Configurat	ion: Advance	ed 🗸			
			Health Mo	onitors		Selected /Common bigip	Availa	f5
			Availabilit	y Requiremen	ts	All Health Monitors	~	

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

Virtual Server Discovery Enabled Link Discovery Enabled Cancel Repeat

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

TMSH

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

2.3.2 Device Trust

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



Run the following command:

When prompted for a password use "default".

TMSH bigip_add



Navigate to: DNS >> GSLB : Servers : Trusted Server Certificates

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

Hostr IP Ad	name: gtm1.site1.exam idress: 10.1.10.13	ple.com Date: Time	: Jun 25, 2017 : 3:36 PM (CDT)	User: ad Role: Ad	admin Administrator
ſ	ONLINE (ACT Standalone	IVE)			
Ma	ain Help	About	DNS » GSLB:	Servers :	: Trusted Server Certificates
<u>M</u>	Statistics		🗱 👻 Server Lis	t	Trusted Server Certificates Statistics
i	Apps		General Propertie	5	
\$3 1	ONS		Name		server
	Delivery	۰.	Partition / Path		
	GSLB	•	Wide IPs	Þ	gtm1.site2.example.com, MyCompany bigip2.site1.example.com, MyCompany
	Zones		Pools	÷	bigip1.site2.example.com, MyCompany bigip2.site2.example.com, MyCompany
	Caches		iRules	\odot	gun I.site I.example.com, MyCompany
	Settings	•	Data Centers	÷	
C		7	Servers	•	Server List 📀
	SSL Orchestrator		Links		Trusted Server
	Acceleration	K	Prober Pools		Certificates 'GMT
0			Monitors	÷	Statistics
	Device Management		Topology		234963207
					Common Name: atm1 site2 example com

2.3.3 Sync Group

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

Changes will be automatically replicated across all F5 DNS servers.

Launch Putty and log in to gtm1.site2

Run the following command: Enter the password "default" when prompted.

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

TMSH

gtm_add 203.0.113.7



2.4 Pools

LTM virtual server objects are grouped together into GTM pools.

Navigate to: DNS >> GSLB : Pools : Pool List

Hostr IP Ad	name: gtm1.site1.e idress: 10.1.10.13	xample.com	Date Time	e: Jun 25, 2017 e: 3:57 PM (CDT)	User: a Role: A	d min dministrator	
	ONLINE (Standalor	ACTIVE) ne					
Ma	ain Help	About		DNS » GSLB:	Pools : P	ool List	
<u>~</u>	Statistics			🔅 👻 Pool List		Statistics	
a 1	iApps			*		×	Search
S	DNS			Status	Name	_	
	Delivery		•		www.exa	mple.com_pool	
	GSLB	-		Wide IPs		ete	
	Zones		•	Pools	7.	Pool List	0
	Caches			iRules	(\Rightarrow)	Statistics	7
	Settings			Jata Centers	Þ		
E				Servers	F		
	SSL Orchestrator			Links	F		
	Acceleration			Prober Pools	F		
	Douise Manager	ant		Monitors	(\Rightarrow)		
	Device managem	ent		Topology	Þ		
	Network			Distributed Applica	ations →		

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

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

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

DNS » GSL	B : Pools : Pool Lis	t » New Pool		
General Prope	erties			
Name		www.example.com_pool		
Туре 🔹	\longrightarrow	A		
State		Enabled		
Configuration				
Health Monitors		Selected Available Image: Common gateway_icmp structure gateway_icmp structure Image: Down Image: Common structure Image: Down Image: Common structure		
Availability R	equirements	All Health Monitors 🔽		
Limit Settings		Bits: Disabled Packets: Disabled Current Connections: Disabled		
Manual Resu	me			
TTL		30		
Dynamic Rati	io			
Maximum Answers Returned		1		
Verify Member Availability		$\mathbf{\nabla}$		
Members				
Load Balancing Method	Preferred: Round R Alternate: Round R Fallback: Return t	Robin V Robin V to DNS V		
Fallback IP	P 0.0.0			
	Virtual Server: Sele Ratio: 1 Add	ect		
Member	/Common/isp1_sit /Common/isp2_sit	e1_www.example.com_tcp_https_virtual (/Common/site1_ha-pair) - 203.0.113.9:443, Ratio(1) e2_www.example.com_tcp_https_virtual (/Common/site2_ha-pair) - 198.51.100.41:443, Ratio(1)		
	Delete Up Down			
Cancel Re	Finished			

TMSH command to run on only gtm1.site1:

TMSH

tmsh create gtm pool a www.example.com_pool { members add { site1_hapair:/Common/isp1_site1_www.example.com_tcp_https_virtual { member-order 0 } site2_hapair:/Common/isp2_site2_www.example.com_tcp_https_virtual { member-order 1 } } }

2.5 FQDN

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

Navigate to: DNS >> GSLB : Wide IPs : Wide IP List



Create an F5 "wide IP"

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

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

General Properties: Advanced	2
Name	www.example.com
Туре	
Description	
Alias List	Alias: Add Delete
State	Enabled V
Minimal Response	Enabled V
Return Code On Failure	Disabled 🔽
Load-Balancing Decision Log	Pool Selection Pool Traversal Pool Member Selection Pool Member Traversal
iRules	
iRule List	Selected Available
Pools	
Load Balancing Method	Round Robin
⁸ Persistence	Disabled V

Pool Select... 🗸

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

TMSH command to run on only gtm1.site1:

TMSH

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

2.6 Delegation

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



2.6.1 A Records

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

Setting	Value
ns1	203.0.113.8
ns2	198.51.100.40

	🖫 DC01 - 10.1.70.200 - Remote	Desktop Connection		
	å.	DNS Mana	ger	
BIG-IP Edge	File Action View Help	New Host 🗙		
Client	🗢 🔿 📶 🔀 🖾 🧔	Name (uses parent domain name if blank):		
		ns2	Data	Time:
agility pub.	a 📑 Eonward Lookun Zon	Fully qualified domain name (FQDN):		
	▶ C msdcs.EXAMPLE	ns2.EXAMPLE.COM.		
_	EXAMPLE.COM	IP address:		
2	⊳ 📑 _msdcs	198.51.100.40		
agility_prv	b C tcp	✓ Create associated pointer (PTR) record		
	⊳ <u>udp</u>	Allow any authenticated user to update DNS records with the		
	⊳ 🧰 branch01	same owner name		
4	⊳ 🦳 DomainDnsZo			
PUTTV (64-bi	▷ I ForestDnsZon		[152] de01 evenende sons	at the state
- 4111 (01-0	⊳ 🚞 mgmt		doll example.com	static
	⊳ 🔛 site1		ns1 branch01 example.com	static
07	þ 🧾 site2	Add Host Done	10 1 70 200	6/26/
	Reverse Lookup Zone		10.1.71.100	6/26/
Notepad++	Conditional Forwarde	rs dc01 Host (A)	10.1.70.200	static
	▶ III Global Logs	E www Hest (A)	203.0.113.9	static
	<	ns1 Host (A)	203.0.113.8	
- 7				
	< III	>		
Start 5	🥖 🍃 🖸 📬 💋	DC01 - 10.1.70.200 - Re		

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

2.6.2 Sub Domain

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

Image: Second system View Help Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second s	DNS Man	Data	Timestamp
File Action View Help Image: Second state stat	Туре	Data	Timestamp
 DNS DC01 Forward Lookup Zones Forward Lookup Zones Forward Lookup Zones Forward Lookup Zones Indexs, EXAMPLE.CC Indexs	Туре	Data	Timestamp
DNS DC01 Forward Lookup Zones Sites Sites EXAMPLE.CC Update Server Data File B	Туре	Data	Timestamp
A cw Mail Exchange (Pr) (Pr) (Pr) (Pr) (Pr) (Pr) (Pr) (Pr)	Start of Authority (SOA) Name Server (NS) Name Server (NS) Host (A) Host (A) Host (A) Host (A) Host (A)	[152], dc01.example.com., dc01.example.com. ns1.branch01.example.com. 10.1.70.200 10.1.71.100 10.1.70.200 203.0.113.8 198.51.100.40	static static static 6/26/2017 12:00:00 / 6/26/2017 12:00:00 / static

2. Create the "gslb" subdomain.



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

- 10.1.70.200 - Remote De	sktop Connection	
		DNS Manager
ction View Help		New Delegation Wizard
2 🗊 🗙 🗉 Q 🗟	Name	Name Servers You can select one or more name servers to host the delegated zone.
C01 Forward Lookup Zones C01 Constraints C	 msdcs sites tcp udp branch01 DomainDnsZones ForestDnsZones mgmt site1 site2 (same as parent folder) (client01) dc01 ns1 	Specify the names and IP addresses of the DN5 servers you want to have host the delegated zone. Name servers: Server Fully Qualified Domain Name (FQDN) IP Address ns1.example.com. Add Edit Remove Bac Next > Cancel
III >	ns2	Host (A) 198.51.100.40
. 2 📋		

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



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

0.1.70.200 - Remote De	sktop Connection					
DNS Mapager						
on View Help		New Delegation Wizard				
a 📰 🗶 📰 🧟 🖻		Name Servers You can select one or more name servers to host the delegated zone.				
11 Forward Lookup Zones Imsdcs.EXAMPLE.CCM EXAMPLE.COM Imsdcs Imsdcs <td>Name mades mades mades mades mathef{stress} mathef{stres</td> <td>Specify the names and IP addresses of the DNS servers you want to have host the delegated zone. Name servers: Server Fully Qualified Domain Name (FQDN) IP Address ns1.example.com. [203.0.113.8] ns2.example.com. [198.51.100.40]</td> <td></td>	Name mades mades mades mades mathef{stress} mathef{stres	Specify the names and IP addresses of the DNS servers you want to have host the delegated zone. Name servers: Server Fully Qualified Domain Name (FQDN) IP Address ns1.example.com. [203.0.113.8] ns2.example.com. [198.51.100.40]				
III >						
			•			

6. Click "Finish"



2.6.3 CNAME

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

😓 DC01 - 10.1.70.200 - Remote D	esktop Connection					
å.	DNS Manager					
File Action View Help						
🗢 🏟 🖄 📷 🗶 🖼 🔒 🛛						
 DNS DC01 Forward Lookup Zones Forward Lookup Zones EXAMPLE.COM EXAMPLE.COM Example.com sites sites sites sites b g udp b branch01 b DomainDnsZones ForestDnsZones forestDnsZones site1 site2 site2 site2 site2 site2 site2 forestDonsZones Trust Points Conditional Forwarders folobal Logs 	Name msdcs sites tcp udp branch01 DomainDnsZones ForestDnsZones rgmt site1 site2 gslb (same as parent folder) (same as parent folder) client01 dc01 ns1 ns2 www Delete	Type Start of Authority (SOA) Name Server (NS) Name Server (NS) Host (A) Host (A) Host (A) Host (A) Host (A)	Data [152], dc01.example.com., dc01.example.com. ns1.branch01.example.com. 10.1.70.200 10.1.71.100 10.1.70.200 203.0.113.8 198.51.100.40 203.0.113.9	Timestamp static static static 6/26/2017 12:00:00 / 6/26/2017 12:00:00 / static		
6	Properties					
Right Click - De	Help					
< III >						
Deletes the current selection.						
	.					

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



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



2.7 Results

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

2	
agility_prv	
_	
	Command Prompt
PuTTY (64-bit)	,, nou size redu. 72
	C:\Users\user.EXAMPLE>dig www.example.com
	; <<>> DiG 9.3.2 <<>> www.cxample.com ;; global options: printcmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 838
Notepaurr	;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
-	;; QUESTION SECTION: ;www.example.com. IN A
Mozilla Firef	HNSWER SECTION: www.example.com. 3600 IN CNAME www.gslb.example.com. www.gslb.example.com. 30 IN A 203.0.113.9
2	;; Query time: 31 msc. ;; SERVER: 10.1.70.200453(10.1.70.200) ;; WHEN: Sun Jun 25 71:37:31 2017 ;; MSG SIZE revd: 72
Google Chrome	C:\Users\user.EXP IPLE>dig www.example.com
Secucie Bin	
🖉 Start 🛛 🥭 Bi	1G-IP® - gtm1.site2.ex 🗦 🚺 🧔 😨 Command Prompt 💋 🎭 DC01 - 10.1.70.200 - Re

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

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

Hostname: gtm1.site1.example.com Dai IP Address: 10.1.10.13 Tin	te: Jul 17, 2017 User: a ne: 11:41 AM (CDT) Role: 7	admin Administrator			
ONLINE (ACTIVE) Standalone	DNS CSID : Wide IDe	- Mide ID List Despectice - many			
Main Help About	Properties	iRules Pools	Statistics •		
- Jausues			∧		
iApps	General Properties: Adva	nced			
S DNS	Name	www.gslb.example.com			
Delivery	Partition / Path	Common	Click Statistics		
GSLB →	Wide IPs →	Wide IP List 💮			
Zones	Pools	Statistics 🛛			
Caches	iRules 📀	Alias:			
Settings	Date centers	Add			
e l	Servers >				
SSL Orchestrapr	Links >				
Acceleration	Prober Pools	Delete			
Device Management	Monitors 💮	Available (Enabled) - Available	lable		
Solice munugement	Topology >	Enabled V			
Retwork	Distributed Applications	Enabled			
System	Return Code On Failure	Disabled			

Hostnar IP Addr	me: gtm1.site1.example.com ress: 10.1.10.13	Date: Time:	Jul 17, 2017 11:45 AM (CDT)	User: admi Role: Admi	i n inistrator			
ß	ONLINE (ACTIVE) Standalone							
Mair	h Help About		Statistics » Mode	ule Statisti	cs:DNS:GSLB » V	Vide IPs : www.gslb	.example.com : A	
Maga Sta	atistics		🔅 👻 Traffic Sum	mary 👻	DNS 👻	Network	Memory	Syst
	Dashboard	e.						
	Module Statistics		Display Options					
	Analytics		Data Format Normalized V					
	Performance		Auto Refresh Disabled V Refresh					
	pps		< Back Clear S	Statistics				
			Requests					
e			Total		12			
SS SS	SL Orchestrator		Persisted		0	0		
Ac	celeration		Resolved		12 🗲			
	Acceleration		Dropped 0					
📄 De	evice Management		Load Balancing					
📄 Ne	Network		Preferred		12			
हुक) System			Alternate		0			
			Fallback		0			
			CNAME Resolution	26	0			

TMSH

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

3. Observe WIDEIP statistics on gtm1.site2: Statistics >> Module Statistics : DNS : GSLB >> Wide IPs : www.gslb.example.com : A

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

4. Disable physical interfaces on gtm1.site2:

https://gtm1.site2.example.com/tmui/Control/form?__handler=/tmui/locallb/network/interface/list&__ source=disable&__linked=false&__fromError=false
gtm1.site2.example.con	II 17, 2017 User: ac 0.52 AM (CDT) Role: A	dmin dministrator			
10.1.10.23	Click refresh to s	ee updated interfa	ce status.		
Main Help About	Network » Interfaces : In	nterface List			
Statistics	🔅 👻 Interface List	Interface Mirrorin	g LLDP 🝷	Statistics 🔊	
iApps	Interfaces				
S DNS	✓ ≑ Status ▲ Name			MAC Address	Medi
E man	DISABLED 1.1			2c:c2:60:59:ec:f5	10000
SSL Orchestrator	DISABLED 1.2			2c:c2:60:62:ca:81	10000
Acceleration	DISABLED 1.3			2c:c2:60:4e:31:5c	10000
Device Management	Enable Disable				
Retwork		Sel	ect and disa	ble all interfa	aces
Interfaces	Interface List				
Router	Interface Mirroring				
Seff IPs 💿	LLDP >				
Proket Filters	Statistics 🔊				
Trunks					
Tunnels					
Route Domains (*)					

TMSH command to run on only gtm1.site2:

TMSH

tmsh modify net interface all disabled

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

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

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

TMSH command to run on only gtm1.site2:

TMSH

tmsh modify net interface all enabled

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

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

Hos IP A	stname: gtm1.site1.example.com Address: 10.1.10.13	Date: Jul 17, 2 Time: 12:32 P	2017 Us M (CDT) Ro	ser: admin ble: Administrator				Partit	on: Common	Ľ
ſ	ONLINE (ACTIVE) Standalone							_		
N	Main Help About	Statist	tics » Module	Statistics : DNS	GSLB » F	ools : www.exa	ample.com_pool : A			
<u>~</u>	Statistics	* -	Traffic Summa	iry 🔻 DNS	-	Network	Memory			
	Dashboard	e .								
	Module Statistics	Display	Options	_						
	Analytics	Data F	Format	Norr	nalized 🔽					
	Performance	Auto F	Refresh	Disa	bled 🔽	Refresh				
	iApps	<< Ba	ck							
53	DNS	Pool D	etails: "www.ex	ample.com_pool	: A"				L	d g
e	CEL Orohantenten	Status	Pool Memb	er	r ≎ Virt	ual Server			Preferred	¢ ₽
9	SSL Orchestrator	•	198.51.100.41	1:443 site2_ha	-pair /Com	mon/isp2_site2_	www.example.com_tcp_h	ttps_virtual	43	0
	Acceleration		203.0.113.9:4	43 site1_ha	-pair /Com	mon/isp1_site1_	www.example.com_tcp_h	ttps_virtual	44	0
	Device Management									
-	Network									
8 *	System									

show gtm pool a www.example.com_pool

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

TMSH

tail -f /var/log/ltm

2.8 Persistence

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

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

Hostname: gtm1.site1.example.com Dat IP Address: 10.1.10.13 Tim	e: Jul 17, 2017 User: admin ie: 4:14 PM (CDT) Role: Administrator	
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » GSLB : Wide IPs : Wide IP List	
Mage Statistics	transformation → Wide IP List Statistics	
iApps	Click www.gslb.example.c	:om
S DNS	Status - Name	Type
Delivery	www.gslb.example.com	A
GSLB	2 1de IPs 💦 🕢 Wide IP List 💽	
Zones	Pools > Statistics >	
Cache	indules 🛞	
Settinis	Data Centers	
	Servers >	
SSL OF CREATER	Links	
Acceleration	Prober Pools	
Device Management	Monitors 🕞	
	Topology	
Network	Distributed Applications	
System		

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

2. Click into the "Pools" tab:

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Time	: Jul 17, 2017 User: admin :: 4:18 PM (CDT) Role: Administr	ator
CONLINE (ACTIVE) Standalone		
Main Help About	BNS » GSLB : Wide IPS : Wide	s Pools Statistics
Statistics		
iApps	General Properties: Advanced	2
S DNS	Name	www.gslb.example.com
Delivery	Partition / Path	Common
GSLB	Туре	A
Zones	Description	
Caches		Alias:
Settings		Add
SSL Orchestrator	Alias List	
	Availability	Available (Enabled) - Available
Device Management	Otata	
Retwork	State	
	Minimal Response	Enabled
§ • System	Return Code On Failure	Disabled

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

3. Enable Persistence

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Tim	e: Jul 17, 2017 User: admin e: 4:53 PM (CDT) Role: Adminis	rator	
Standalone			
Main Help About	DNS » GSLB : Wide IPs : Wid	e IP List » Members : www.gslb.	example.com : A
Mage Statistics	Properties iRule	es Pools	Statistics -
iApps	Pools		
S DNS	Load Balancing Method	Round Robin	
Delivery	Persistence	Enabled 🔽	
GSLB →	Persistence TTL	3600 seconds	
Zones	Persist CIDR (IPv4)	32	
Caches	Persist CIDR (IPv6)	128	
Settings	Last Resort Pool	None	$\overline{}$
SSL Orchestrator	Update		
Acceleration	Pools		
Device Management	✓ ▲ Order ▼ Status ♦ Po	ol Name	
Retwork	Delete	example.com_pool	
System			

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

4. View Persistence Records

TMSH

tmsh show gtm persist

2.9 LB Methods

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

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

An ISP network outage can automatically cause DR activation.

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

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

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Tin	e: Jul 17, 2017 User: admin e: 1:33 PM (CDT) Role: Administrator
ONLINE (ACTIVE) Standalone	
Main Help About	DNS » GSLB : Pools : Pool List
Ma Statistics	Pool List Statistics
_	Click "www.example.com_pool"
iApps	* × Search
S DNS	✓ Status ≑ Name
Delivery	www.example.com_pool
GSLB	Wide IPs
Zones	Pools Pool List 📀
Caches	iRules 🕑 Statistics 🗵
Settings	Data Centers
e	Servers >
SSL Orchestrator	Links
Acceleration	Prober Pools
Device Management	Monitors 💿
berree management	Topology >
Network	Distributed Applications

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

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Time	e: Jul 17, 2017 User: admin e: 1:51 PM (CDT) Role: Administra	tor			
ONLINE (ACTIVE) Standalone				_	
Main Help About	DNS » GSLB : Pools : Pool Lis	t » Members : www.exa	mple.com_pool : #	`	
Magazina Statistics	🔅 🗸 Properties Memb	ers Statistics			
iApps	Load Balancing	Click	"Member	<mark>S</mark> "	
S DNS	Load Balancing Method	Preferred: Global Availab			-
Delivery		Fallback: Return to DNS			
GSLB	Fallback ID				
Zones >		10.0.0.0			
Caches	Update				
Settings	Members				
SSL Orchestrator	Member Order 💌 Status	Member	Member Address	Partition	Merr
	0	/Common/site1_ha-pair	203.0.113.9	Common	/Con
Acceleration	1	/Common/site2_ha-pair	198.51.100.41	Common	/Con
Device Management	Enable Disable Remove				
Network					

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

3. Introduce a network problem in the ISP at site1

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

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 17, 2017 User: admin Time: 8:42 PM (CDT) Role: Administrator
Standalone	
Main Help About	Network » Interfaces : Interface List
Statistics	☆ → Interface List Interface Mirroring LLDP ✓ Statistics Image: Compared to the state stat
iApps	Interfaces
S DNS	✓ ♦ Status ▲ Name
SSL Orchestrator	UP 1.1
Local Traffic	Disable Interface 1.6
Acceleration	UP 1.4
Device Management	DISABLED 1.6
Interfacer	Interface List
Routes	Interface Mirroring
Self IPs 🕞	LLDP
Powet Filters	Statistics 🗵
Trunks	

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

TMSH

tmsh modify interface 1.6 disabled

4. View the effect

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

Hostname: gtm1.site2.example.com Dat IP Address: 10.1.10.23 Tim	te: Jul 17, 2017 User: admin ne: 8:52 PM (CDT) Role: Administrator
ONLINE (ACTIVE) Standalone	
Main Help About	DNS » GSLB : Links : Link List
Statistics	tink List Statistics
iApps	* Search
	Status Address
Delivery	198.51.100.33 198.51.100.33
	Wide IPs 3.1 203.0.113.1
Zenes >	Pools
C ches	iRules 📀
S ttings	Data Centers
e .	Servers >
SS. Drchestrator	3 Links
	Prober Pools
Device Management	Monitors 💿
	Topology >
Network	Distributed Applications
System	

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

tmsh show gtm link

5. Set the site1 isp link back up

Log into the router and enable the interface 1.6 connecting ISP1 to site1 https://router01.branch01.example.com/tmui/Control/jspmap/tmui/locallb/network/interface/list.jsp

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 17, 2017 User: admin Time: 8:42 PM (CDT) Role: Administrator
Standalone	
Main Help About	Network » Interfaces : Interface List
Mage Statistics	to Therface List Interface Mirroring LLDP - Statistics
iApps	Interfaces
S DNS	✓ ♦ Status ▲ Name
SSL Orchestrator	UP 1.1
Local Traffic	Enable Interface 1.6
Acceleration	UP 1.4
Device Management	DISABLED to
etwork	Enable Disable
Interfacer 2	Interface List
Routes 🔄	Interface Mirroring
Self IPs 💿	LLDP >
Powet Filters	Statistics
Trunks	

tmsh modify interface 1.6 enabled

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

Class 2 - Advanced GSLB

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

The F5 device is directly connected to the internet.



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

1. Transparent Cache

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

3.1 Transparent Cache

3.1.1 Monitors

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



Navigate to: Delivery : Load Balancing : Monitors

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 18, 2017 Time: 1:30 PM (CDT)	User: admin Role: Administrator	Partition: Commo
Standalone			
Main Help About	DNS » Delivery : Loa	d Balancing : Monitors	
Statistics	🔅 👻 Monitor List		
iApps	P	× Search	Create
S DNS	✓ ▲ Name		Application Ty
Delivery 🔺 🕨 🕨	Listeners	>	Gatew
GSLB	Profiles	Þ	HTTP
Zones	Load Balancing	Pools	HTTP
Caches	iRules	Nodes	HTTP:
Settings	Translation	Monitors 📀	HTTP
R	NameServers		ICMP
SSL Orch Carcio	Keys	>	Inband
Local Traffic	real_server		Real S
Acceleration	snmp_dca		SNMP
Acceleration	🗆 tcp		TCP
Device Management	🗆 tcp_echo		TCP E
Network	tcp_half_open		TCP H

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

Create a monitor according to the following table:

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

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

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

TMSH

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

3.1.2 Load Balancing

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

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 18, 2017 Time: 1:22 PM (CDT)	User: admin Role: Administrator		
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » Delivery : Load	Balancing : Pools : Pool List		
Statistics	🔅 👻 Pool List	Statistics 🗾		
iApps	*	× Search		reate
S DNS	Status 🔺 Name			⇒ Des
Delivery	Listeners	ateway_pool		
GSLB	Profiles >			
Zones	2 Load Balancing	³ Pools →	Pool List 💮	
Caches	iRules	Nodes >	Statistics 🗵	
Settings >	Translon	Monitors (+)		
	Nameservers			
SSL Orchestrator	Keys >			
Local Traffic				
Acceleration				
Device Management				
Network				

Create a pool according to the following table:

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

Configuration: Advanced	
Name	branch01_dns_pool
Description	
Health Monitors	Active Available //Common example.com_dns_monitor >> //Common gateway_icmp http http_head_f5 https
Availability Requirement	All V 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	New Node O New FQDN Node O Node List Node Name: dc02.branch01.example.com_node (Optional) Address: 10.1.70.210 Service Port: 53 Select Add R:1 P:0 C:0 dc01.branch01.example.com_node 10.1.70.200 :53 R:1 P:0 C:0 dc02.branch01.example.com_node 10.1.70.210 :53 Create two nodes
	Edit Delete

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

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

3.1.3 Results

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

Click to select the branch01_dns_pool, and then click "Members"

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 18, 2017 Time: 3:41 PM (CDT)	User: admin Role: Administrator
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » Delivery : Loa	ad Balancing : Pools : Pool List
Magazine Statistics	🔅 👻 Pool List	Statistics
iApps	*	× Search
😚 dns	Status 🔺 Nan	me
Delivery 1	Listeners	_dns_pool
GSLB	Profiles	ateway_pool
Zones	oad Balancing	3 Jols 4 Pool List ⊙
Cachis	iRules	Nodes Statistics
Settilgs	translation	Monitors 🛞
G	Namervers	•
SSL rcb strate	Keys	5
Local Traffic		
Acceleration		
Device Management		
Network		

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 IP Address: 10.1.10.31	Date: Jul 18, 2017 U Time: 3:47 PM (CDT) F	User: admin Role: Administrator
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » Delivery : Load E	Balancing : Pools : Pool List » Properties : branch01_dns_pool
Mage Statistics	🔅 👻 Properties	Members Statistics I
iApps	General Properties	
S DNS	Name	branch01_dns_pool
Delivery	Partition / Path	Common
GSLB	Description	
Zones >	Availuoility	Available (Enabled) - The pool is available
Caches	C Ktion: T	embers"
Settings		Active Available
SSL Orchestrator	Health Monitors	example.com_dns_monitor example.com_dns_monitor s>
Local Traffic		nttps
	Availability Requirement	All Health Monitor(s)
	Allow SNAT	Yes
Device Management	Allow NAT	Yes
Network	Action On Service Down	None 🔽

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

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 18, 2017 User: admin Time: 4:54 PM (CDT) Role: Administrator	
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » Delivery : Load Balancing : Pools : Pool List	» Members : branch01_dns_pool
Marco Statistics	🔅 🗸 Properties Members Statistic	s 🗵
iApps	Load Balancing	
S DNS	Load Balancing Method Round Robin	V
Delivery >	Priority Group Activation Disabled	
GSLB	Update	
Zones Notice	that health monitors marked	d one server down
Caches	Current Members	
Settings	Status	▲ Address 🗢 Service Port 🗢 FQDN 🗢
8	dc01.branch01.example.com_node:53	10.1.70.200 53 No
SSL Orchestrator	dc02.branch01.example.com_node:53	10.1.70.210 53 No
Local Traffic	Enable Disable Force Offline Remove	
Acceleration	Maybe that's why users	are complaining. It
Device Management	seems that a local DNS s	server is failing.
Network		

tmsh show ltm pool branch01_dns_pool detail



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

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



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



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

Navigate to DNS >> Caches : Cache List

Create a transparent cache

Setting	Value
Name	transparent_cache
Resolver Type	Transparent

Hostname: IP Address:	router01.branch 10.1.10.31	01.example.com	Date: Jun 20, 2017 Time: 9:38 PM (CDT)	User: adr Role: Adr	min ministrator	
6	ONLINE (AC Standalone	rive)				
Main	Help	About	DNS » Caches : Cach	e List » 🖡	lew	
Magazina Statisti	ics					
-			General Properties			
iApps			Name	\rightarrow	transparent_cad	he
🌍 dns			Resolver Type	\rightarrow	Transparent (No	ne) 🗸
Deliv	very	Þ	DNS Cache			
Zone	es	Þ	Message Cache Size	_	1048576	bytes
Cac	hes		Cache List 🛛 🕣	Size	10485760	bytes
Jett	ings		Statistics		Enabled	
SSI of	chestrator		RRSet Rotate		none 🔽	
Local 1	Traffic		Cancel Repeat Fir	nished		
Accele	ration					

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

TMSH command for router01.branch01:

TMSH

tmsh create ltm dns cache transparent transparent_cache

3.2 Listeners

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

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

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

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



3.2.1 Log Profile

Configure DNS query and response logging.

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

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

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Time	: Jul 20, 2017 User: a 2: 12:39 PM (CDT) Role: A	admin Administrator		Р
ONLINE (ACTIVE) Standalone				
Main Help About	System » Logs : Config	uration : Log Publishers		
Statistics	🔅 🗸 System	Captured Transactions F	Packet Filter GSLB	Audit
iApps		Click "Creat	e"	Create
S DNS	🖌 🗢 Name		5	
SSI Orabastrator	default-ipsec-log-publi	isher		
SSL Orchestrator	local-db-publisher			
Acceleration	sys-db-access-publish	ner		
Device Management	sys-sso-access-publis	sher		
berree munugement	Delete			
Network				
System				
Configuration				
File Management				
Certificate Management				
Disk Management				
Software Management	/\\			
License				
Resource Provisioning				
Platform				
High Availability				
Archives				
Services	System			
Preferences	Captured Transactions		_	
sFlow	Packe Filter	Options		
SNMP	Local Traffic	Remote Logging		
Crypto Offloading	GSLB	Log Filters		
Users	Audit 3	L stinations		
Logs	Configuration →	Log Publishers 💽	have a line of	

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

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

Hostname: gtm1.site1.example.com Dai IP Address: 10.1.10.13 Tin	e: Jul 20, 2017 User: admin Pe: 12:43 PM (CDT) Role: Administrator P
ONLINE (ACTIVE) Standalone	
Main Help About	System » Logs : Configuration : Log Publishers
Statistics	
iApps	Name local-syslog-publisher
S DNS	Description
SSL Orchestrator	Log Destinations
Acceleration	Selected Available //Common local-syslog
Device Management	local-db
Network	Cancel Reneat Einished
System	
Configuration	
File Management	
Certificate Management	
Disk Management	
Software Management	

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

TMSH

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

2. Create a "Logging Profile"

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 19, 2017 Time: 12:09 PM (CDT)	User: admin Role: Administrator		
ONLINE (ACTIVE) Standalone		CI	ick"Create"	
Main Help About	DNS » Delivery : Profile	es : Other : DNS Logging		
Mage Statistics	⇔ - DNS	Protocol - Othe		
iApps	*	× Search		Create
🔁 Wizards	✓ ♦ Name			
	No records to display.			
	Delete			
Delivery 🔶 🕨 🕨	Listeners			
GSLB	Profiles	DNS 💮		
Zones	Load Balancing >>	Protocol >		
Caches	iRules	Other	DNS Logging 🛛 🤇	\mathbf{D}
Settings	Translation		Persistence	Ð
E	Nameservers		Statistics	Ð
SSL Orchestrator	Keys >			
Local Traffic				
Traffic Intelligence				
Acceleration				

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

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 19, 2017 User: 4 Time: 12:14 PM (CDT) Role: 7	admin Administrator
ONLINE (ACTIVE) Standalone	_	
Main Help About	DNS » Delivery : Profiles : Oth	er : DNS Logging » New
Mage Statistics		
	General Properties	
Log IApps	Name	example_dns_logging_profile
iii Wizards	Description	
S DNS	Configuration	
Delivery	Log Publisher	local-syslog-publisher
GSLB	Log Queries	☑ Enabled
Zones	Log Responses	Enabled
Caches	Log Fields	
Settings	Include Complete Answer	Enabled
SSI Orchestrator	Include Query ID	Enabled
332 Orchestrator	Include Source	Enabled
Local Traffic	Include Timestamp	Enabled
Traffic Intelligence	Include View	Enabled
Acceleration	Cancel Repeat Finished	

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

TMSH

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

3.2.2 DNS Profile

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

Navigate to: DNS >> Delivery : Profiles : DNS

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 19, 2017 Time: 12:19 PM (CDT)	User: admin Role: Administrator
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » Delivery : Profile	es : DNS
Mage Statistics	‡‡ - DNS	Protocol - Otomick Oreate
iApps	*	× Search Create
🔨 Wizards	✓ A Name	
	iii dns	
	Delete	
Delivery	Listeners	
GSLB	Profiles	
Zones	Load Balancing	Protocol
Caches	iRules	Other >
Settings	Translation >	
S col Contractor	Nameservers	
SSL Orchestrator	Keys	
Local Traffic		
Traffic Intelligence		
Acceleration		

Create a DNS profile as shown in the table below.

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 25, 2017 User: Time: 11:40 PM (CDT) Role:	admin Administrator Partition: Common	Log out
Standalone			
Main Help About	DNS » Delivery : Profiles : DI	NS » New DNS Profile	
Statistics	General Properties		
iApps	Name	example.com_dns_	
Wizards	Parent Profile	dns	
S DNS	Denial of Service Protection		Custom 🗌
Delivery	Rapid Response Mode	Disabled	
GSLB	Rapid Response Last Action	Drop 🔽	
Zones	Hardware Acceleration		
Caches	Protocol Validation	Disabled	
Settings	Response Cache	Disabled	
SSL Orchestrator	DNS Features		
Local Traffic	DNSSEC	Enabled V	
Traffic Intelligence	GSLB	Enabled V	
	DNS Express	Enabled V	
Acceleration	DNS Cache	Enabled	
Access	DNS Cache Name	transparent_cache	\checkmark
Device Management	DNS IPv6 to IPv4	Disabled 🔽	
	Unhandled Query Actions	Allow	
Network	Use BIND Server on BIG-IP		
System	DNS Traffic		
	Zone Transfer	Disabled 🗸	
	DNS Security	Disabled	
	DNS Security Profile Name	Select	
	Process Recursion Desired	Enabled 🔽	
	Logging and Reporting		
	Logging	Enabled V	→ 2
	Logging Profile	example_dns_logging_profile	\checkmark
	AVR Statistics Sample Rate	Enabled 1/ 1 queries sampled	

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

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

3.2.3 UDP Profile

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

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 19, 2017 Time: 12:27 PM (CDT)	User: admin Role: Administrator	
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Delivery : Prof	iles : Protocol : UDP	
Magazine Statistics	🔅 👻 DNS	Protocol - Othe	Click "Create"
iApps	ŕ	× Search	Create
📋 Wizards	🖌 🕈 Name		
	iii udp		
D N3	udp_decrement_ttl	_	
Delivery 1 >	Listeners		
GSLB	² Profiles	DNS 💮	
Zones	Load Balancing	Protocol	
Caches	iRules	Other >	тср 💮
Settings	Translation		
6 martin	Nameservers		
SSL Orchestrator	Keys		
Local Traffic			
Traffic Intelligence			
Acceleration			

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

Create a UDP profile as shown in the following table.

Setting	Value
Name	example.com_udp-dns_profile
Parent Profile	udp_gtm_dns

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 19, 2017 User: Time: 12:32 PM (CDT) Role:	admin Administrator	
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Delivery : Profiles : Pro	otocol : UDP » New UDP Profile	
Statistics	General Properties		
iApps	Name	example.com_udp-	
iii Wizards	Parent Profile	udp_gtm_dns	
S DNS	Settings		
Delivery	Proxy Maximum Segment		
GSLB	Idle Timeout	Specify 🔽 5 sec	conds
Zones	IP ToS	Specify 🗸 0	
Caches	Link QoS	Specify 🗸 0	
Settings	Datagram LB	Enabled	
SSI Orchostrator	Allow No Payload		
SSE OTCHESTIMO	TTL Mode	Proxy 🗸	
Local Traffic	Don't Fragment Mode	PMTU 🔽	
Traffic Intelligence	Cancel Repeat Finished		
Acceleration			

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

TMSH

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

3.2.4 TCP Profile

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

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 19, 2017 Time: 12:34 PM (CDT)	User: admin Role: Administrator		
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » Delivery : Profi	les : Protocol : TCP	Click"Cre	ate"
Statistics				
iApps	×	× Search		Create
🔁 Wizards	💌 🗢 Name			
	apm-forwarding-clie	nt-tcp		
UN3	apm-forwarding-ser	ver-tcp		
Delivery >	Listeners	s_profile		
GSLB	Profiles •	DNS 📀		
Zones	Load Balancing	Protocol >	UDP	 Image: A start of the start of
Caches	ikules	Other	ТСР	•
Setti	ranslation			
8	Nameservers	ed		
SSL Orchestrator	Keys	-tcp-lan_profile		
Local Traffic	spirtsession-default-	тср		
	tcp			
Traffic Intelligence	tcp-lan-optimized			
Acceleration	tcp-legacy			

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

Create a TCP profile as shown in the following table.

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 12, 2017 User: Time: 7:45 PM (CDT) Role:	admin Administrator	Partit
ONLINE (ACTIVE) Standalone			
Main Help About	Local Traffic » Profiles : Prot	ocol : TCP » New TCP Profile	
Statistics	Concert Descention		
iApps	Name	example.com_tcp-	
S DNS	Parent Profile	f5-tcp-lan	
SSL Orchestrator	Timer Management		
Contraction Contraction	Close Wait	Specify 5 seconds	
Notwork Man	Fin Wait 1	Specify 5 seconds	
Virtual Servers	Fin Wait 2	Specify 🔽 300 seconds	
Policies	Idle Timeout	Specify	
Profiles	Keep Alive Interval	Specify V 1800 seconds	
Ciphers	Minimum RTO	200 milliseconds	
iRules	Reset On Timeout	Enabled	
Pools	Time Wait	Specify 🔽 2000 milliseconds	
Nodes	Time Wait Recycle	Enabled	
Monitors (+)	Zero Window Timeout	Specify 20000 milliseconds	
Traffic Class (+)	Memory Management		
Address Translation	Auto Proxy Buffer		
Acceleration	Auto Receive Window		
Device Management	Auto Send Buffer		
Donce mundgement	Proxy Buffer High	65535 bytes	
Network	Proxy Buffer Low	32768 bytes	

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

TMSH

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

3.2.5 UDP Listener

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

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

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

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

Create two UDP listeners according to the tables below:

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

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

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

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

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

TMSH

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

3.2.6 TCP Listeners

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

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



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

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

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 19, 2017 User: a Time: 12:46 PM (CDT) Role: A	idmin Administrator
Standalone	-	
Main Help About	DNS » Delivery : Listeners : Lis	stener List » New
Statistics	General	
iApps	Name	DC01_tcp_53_virtual
🔨 Wizards	Description	
S DNS	State	Enabled
Delivery	Listener: Advanced	
GSLB	Destination	Type: O Host O Network Address: 10.1.70.200
Caches	Service Port	DNS 53
Settings	VLAN Traffic	Enabled on 🔽
SSL Orchestrator	VLANs and Tunnels	Selected Available //Common branch01_vlan <
Traffic Intelligence	Source Address Translation	None
Acceleration	Address Translation	Enabled
Access	Port Translation	Enabled
	Route Advertisement	
Device Management	Auto Last Hop	Default V
Network	Last Hop Pool	None
System	Service: Advanced 🗸	
	Protocol	
	Protocol Profile (Client)	example.com_tcp-dns_profile
	Protocol Profile (Server)	(Use Client Profile)
	DNS Profile	example.com_dns_profile
	Load Balancing	
	Default Pool	branch01_dns_pool
	Default Persistence Profile	None
	Fallback Persistence Profile	None

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

TMSH

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

TMSH

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

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

3.2.7 Results

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

Repeat some of the same queries multiple times

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

2. Viewing Cache Entries

Navigate to: DNS >> Caches : Cache List >> Properties : transparent_cache

Hostrano, router01.branch01.example.com IP ACTOSS: 10.1.10.31	Qate: Jun 27, 2017 Ime: 12:48 PM (CDT)	User: admin Role: Administrator			
ONLINE (ACTIVE) Standalone					
Main Help About	DNS » Caches : Cache	List » Properties : 1	transparent_cache		
Statistics	🔅 👻 Properties	Local Zones	Response Policy Zones	Statistics 🗵	
iApps	General Properties			7	
S DNS	Name	transparent_	_cache		
Delivery	Resolver Type	Transparent	(None)		
Zones	DNS Cache		Slick S	tatist	ICS
Caches	Message Cache Size	1048576	× bytes		
Settings	Resource Record Cache	Size 10485760	bytes		
SSL Orchestrator	Answer Default Zones	C Enabled			
	RRSet Rotate	none 🗸			
	Update Delete				
Acceleration					
Device Management					
Network					
System					

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

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

Hostr IP Ad	har couler01.branch01.example.com idr. 10.1.10.31	Date: Jun 27, 2017 Time: 12:50 PM (CDT)	User: admin Role: Administrat							Partition: Co	mmon	-
	ONLINE (ACTIVE) Standalone											
Ma	ain Help About	Statistics » Module St	tatistics : DNS : C	aches » Caches								
<u>M</u>	Statistics	🔅 👻 Traffic Summary	✓ DNS	✓ Local Traff	ic Ne	twork	Memory		System			
	Dashboard .=											
	Module Statistics	Display Options										
	Analytics >	Statistics Type	Caches									
	Performance >	Data Format	Normal	ized 🔽								
i ali	iApps	Auto Refresh	Disable	d V Refresh								
		/Common/transparent_ca	iche	Search Reset Sear	rch		DNS Quer	ies			Failure	es
5	DNS	✓ ▲ Name		Partition / Path	Details	Queries	Responses	\$ Sync	Async	Resolve	Connect	\$
6	SSL Orchestrator	transparent_cache	9	Common	View	7	4	4	0	0	0	0
	Local Traffic	Reset Clear Cache			~							
	Acceleration											
	Device Management		Cli	<u>ck Vi</u>	W							
	Network											
	System											

Host IP A	name: router01.branch01.example.com ddress: 10.1.10.31	Date: Jun 27, 2017 User Time: 12:52 PM (CDT) Role	: admin : Administrator			Partition: Co	mmon 🔽 Log out
	Standalone						
м	ain Help About	Statistics » Module Statistic:	s : DNS : Caches »	Caches : transparent cacl	10		
M	Statistics	🚓 👻 Summary					
-	Dashboard						
	Madula Otalialian	Display Options					
	Module Statistics	Data Format	Normalized V	[
	Analytics	Auto Refresh	Disabled	Refresh			
	Performance	Auto Reals	Disabled				
	iApps	< Back Clear Stausucs					
53	DNS	Query Details					
e		Queries 7					
	SSL Orchestrator	Responses	Responses 4				
0-0	Local Traffic	Synchronous Responses	4				
		Asynchronous Responses	0				
	Acceleration	Failure Details					
	Device Management	Resolve	0				
_		Connection	0				
	Network	Server	0				
	System	Send	0				
		Cache Details	flits	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				

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

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

TMSH

tmsh show Itm dns cache records rrset cache transparent_cache

[root@router01:Active	:Standa	alone] c	onfig #	tmsh show ltm dns cache records rrset cache transparent_cache				
Ltm::DNS-Cache/Resolve	≘r RR B	Records						
Owner	IIL	7.00	Class	rdata				
www.gslb.example.com	25	À	1.1	203.0.113.9				
www.example.com	3595	CNAME	7.4	www.gslb.example.com				
www.ncsu.clu	2500	~	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 TT	L Туре	e Class	rdata					
www.wikipedia.org 578	3 A	IN	198.3	5.26.96				
Total records returned (tmm0): 7								
[root@router01:Active	:Stands	alone] c	onfig #					

TMSH

show Itm dns cache transparent transparent_cache

3. Clearing Entire Cache

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

3.3 Hidden Master

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



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

3.3.1 Name Server

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

Navigate to DNS >> Delivery : Nameservers : Nameserver List

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 12, 2017 Time: 10:23 PM (CDT)	User: admin Role: Administrator	Partiti
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Delivery : Name	servers : Nameserver List	
Statistics	🔅 👻 Nameserver List	Statistics 🗩	
iApps	*	× Search	
S DNS	✓ A Name		Address Port TSIG Ke
Delivery >	Listeners		
GSLB	Profiles >		
Zones	Load Balancing		
Caches	iRules >		
Settings	Translation		
C sel curbustada	Nameservers	Nameserver List 💿	
SSL Orchestrator	Kevs	Statistics	
Local Traffic			
Acceleration			
Device Management			
Network			

Create a nameserver according to the following table:

Setting	Value
Name	dc01.example.com
Address	10.1.70.200

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Tin	ie: Jul 21, 2017 User: admin ie: 1:47 AM (CDT) Role: Administrator
ONLINE (ACTIVE) Standalone	
Main Help About	DNS » Delivery : Nameservers : Nameserver List » New Nameserver
Mage Statistics	
iAnne	General Properties
Tech tech	Name dc01.example.com
S DNS	Address 10.1.70.200 ×
Delivery	Service Port 53 Other:
GSLB	
Zones	Route Domain
Caches	
Settings	
SSL Orchestrator	Cancel Repeat Finished
Acceleration	
Device Management	
Network	
System	

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

TMSH

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

3.3.2 DNS Express

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

Navigate to DNS » Zones : Zones : Zone List

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 12, 2017 Time: 10:32 PM (CDT)	User: admin Role: Administrator	Partition: Common V
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Zones : Zones :	Zone List	
Statistics	🔅 👻 Zone List	Statistics 🗵	
a jánne			
(All the second	t	× Search	Create
😚 dns	✓ A Name		
Delivery	No records to display.		
GSLB	Delete		
Zones >	Zones	Zone List 💽	
Caches	NSSEC Zones	Statistics 2	
Settings	ZoneRunne >		
SSL Orchestrator			
Local Traffic			
Acceleration			
Device Management			
Network			

Create a DNS Express zone according to the following table:

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

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

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

TMSH

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

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

3.3.3 Results

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

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

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

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

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

dnsxdump less	
Examine the results	
🛃 router01	
DNS-Express DB Dump	
-= Årena Ållocator =-	
-= Region Stats =- memory: 484 objects (484 small/0 lan 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	ge), 22784 bytes allocated (778 wasted) in 6 chunks, 5 cleanups, 20 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
-= DB Dump =- Domain: . Domain: com. Domain: example.com.	
example.com. 3600 IN SOA	dc01.example.com hostmaster.example.com 209 900 600 86400 3600
example.com. 600 IN A	10.1.70.200
example.com. 3600 IN NS	dc01.example.com

3.4 DNSSec



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

3.4.1 Zone Signing Key

User: admin Role: Administrator router01.branch01.example.com Date: Jul 18, 2017 Time: 12:27 PM (CDT) Partition: Common ONLINE (ACTIVE) Standalone DNS » Zones : DNSSEC Zones : DNSSEC Zone List Main Help About DNSSEC Zone List **⇔** -Click "Create" m Statistics iApps Create .. Search S DNS V Status 🔺 Name Listeners ete... GSLB Profiles Zones Load Balancing iRules Caches Settings Translation Nameservers £ SSL Orchestrator TSIG Key List DNSSEC Key List Local Traffic \odot Acceleration Device Manageme Retwork

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

Create zone signing key according the following table:

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 18, 2017 User: ad Time: 1:40 PM (CDT) Role: Ad	min Iministrator
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » Delivery : Keys : DNSSE	C Key List » New DNSSEC Key
Mage Statistics		
	General Properties	
Ligit IApps	Name	example.com_ksk ×
S DNS	Туре	Zone Signing Key 🗸
Delivery	State	Enabled
GSLB	Hardware Security Module	None
Zones	Algorithm	RSA/SHA1
Caches	Key Management	Manual 🗸
Settings	Key Settings	
SSL Orchestrator	Certificate	default.crt
Local Traffic	Private Key	default.key
Acceleration	Cancel Repeat Finished	
Device Management		
Retwork		

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

TMSH

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

3.4.2 Key Signing Key

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 18, 2017 User: admin Partition: Common Time: 12:27 PM (CDT) Role: Administrator Partition: Common
ONLINE (ACTIVE) Standalone	
Main Help About	DNS » Zones : DNSSEC Zones : DNSSEC Zone List
Mage Statistics	DNSSEC Zone List Statistics
iApps	* Search Create
S DNS	Status - Name
Delivery	Listeners >
GSLB	Profiles etc
Zones	Load Balancing
Caches	iRules
Settings	Translation
C. C.C. Outburght	Nameservers
SSL Orchestrator	Keys TSIG Key List 🛞
Local Traffic	DNSSEC Key List 💿
Acceleration	
Device Management	
Network	

Create a key signing key according to the following table:

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 26, 2017 User: Time: 12:30 AM (CDT) Role:	admin Administrator	Partition:
Main Help About	DNS » Delivery : Keys : DNS	SEC Key List » New DNSSEC Key	
Statistics	General Properties		
iApps	Name	example.com_ksk	
Wizards	Туре	Key Signing Key 🔽	
S DNS	State	Enabled V	
Delivery	Hardware Security Module	None 🗸	
GSLB	Algorithm	RSA/SHA1	
Zones	Key Management	Manual 🔽	
Caches	Key Settings		
Settings	Certificate	default.crt 🗸	
SSL Orchestrator	Private Key	default.key	-
Local Traffic	Cancel Repeat Finished		
Traffic Intelligence			
Acceleration			

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

TMSH commands for Key Signing key creation:

TMSH

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

3.4.3 Signed Zone

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 18, 2017 User: admin Time: 3:09 PM (CDT) Role: Administrator Partition: Common
ONLINE (ACTIVE) Standalone	
Main Help About	DNS » Zones : DNSSEC Zones : DNSSEC Zone List
Mage Statistics	Image: Statistic st
iApps	* <u>Search</u>
S DNS	Status A Name
Delivery	No records to display.
GSLB	Enable Disable Delete
Zones 🗼 🕨	Zones
Caches	DNSSEC Zones → DNSSEC Zone List 📀
Settings	ZoneRunner > Statistics >
SSL Orchestrator	
Local Traffic	
Acceleration	
Device Management	
Retwork	

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

Create DNS Express zone signed by DNSSEC

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

I lostn IP Ad	ame: router01.branch01.example.com dress: 10.1.10.31	Date: Jul 18, 2017 Time: 3:18 PM (CDT)	User: admi Role: Admi	n inistrator		Partition:	Common
	ONLINE (ACTIVE) Standalone						
Ma	ain Heip About	DNS » Zones : DNSSE	C Zones : I	DNSSEC Zone Lis	T » NEW DNSSEC Z	one	
	Statistics	General Properties: Bas	sic 🔽	example com			
i 💭	Apps	Name		example.com			
()	DNS	State]	Enabled 🔽			
	Delivery >	Keys					
	GSLB →		_	Active	Av	ailable	_
	Zones >	Zone Signing Key			/Common example	com_zsk	
	Caches				>>		
	Settings >			Active	Av	ailable	
6	SSL Orchestrator	Key Signing Key	Г		/Common example	com_ksk	
(<u>)</u>	ocal Traffic		L		>>		
()	Acceleration	Cancel Repeat Fir	nished				
a (Device Management						
	Network						

TMSH commands for DNSSEC signed zone creation:

TMSH

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

3.4.4 Results

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



3.5 Validating Resolver

3.5.1 Trust Anchors

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

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

TMSH

dig dnskey . | grep 257 > /root/dnskey.txt dnssec-dsfromkey -f /root/dnskey.txt .

🛃 router01
[root@router01:Eval:Active:Standalone] config #
[root@router01:Eval:Active:Standalone] config # dig dnskey . grep 257 > /root/dnskey.txt
[root@router01:Eval:Active:Standalone] config # dnssec-dsfromkey -f /root/dnskey.txt .
. IN DS 19036 8 1 B256BD09DC8DD59F0E0F0D8541B8328DD986DF6E
. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
. IN DS 20326 8 1 AE1EA5B974D4C858B74OBD03E3CED7EBFCBD1724
. IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
[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"

Hos IP A	stname: gtm1.site1.example.com Address: 10.1.10.13	Date: Time:	Jul 21, 2017 1:28 AM (CDT)	User: Role:	admin Administrator		Partition: Commor
(ONLINE (ACTIVE) Standalone						
	Main Help About		DNS » Caches	: Cach	e List		
~	Statistics		🚓 👻 Cache Li	st	Statistics		
	iApps		*			Search	
5	DNS		✓ ♦ Name				Resolver
	Delivery	•	validating-re	solver_	cache		Validating F
	GSLB	•	Delete				
	Zones	•					
	Caches	•	Cache List	0	Eliek '	validating-resolver_	_cache"
	Settings	•	tatistics	Z			
6	SSL Orchestrator	/					
	Acceleration	/					
	Device Management						
	Network						
89	System						

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



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

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

DNS » Caches : Cache List

Add Trust Anchor	
Trust Anchor	. IN DS 19036 8 1 B256BD09DC8DD59F0E0F0D8541B8328DD986DF6E
Cancel Repeat Finished	
🛃 router01	
[root@routerO1:Eval:Acti [root@routerO1:Eval:Acti [root@routerO1:Eval:Acti 210:domain ip-protocol t rofile () } translate-a [root@routerO1:Eval:Acti [root@routerO1:Eval:Acti [root@routerO1:Eval:Acti [root@routerO1:Eval:Acti [root@routerO1:Eval:Acti [root@routerO1:Eval:Acti [root@routerO1:Eval:Acti	<pre>ve:Standalone] config # ve:Standalone] config # ve:Standalone] config # tmsh create ltm virtual DC02_tcp_53_virt cp mask 255.255.255.255 profiles add { example.com_dns_profile { ddress_disabled_vlans_add { branch01_vlan } vlans-enabled pool b ve:Standalone] config # ve:Standalone] config # ve:Standalone] config # tmsh create ltm dns cache validating-res cones yes ve:Standalone] config # ve:Standalone] conf</pre>
<pre>[root@router01:Eval:Acti [root@router01:Eval:Acti [root@router01:Eval:Acti]root@router01:Eval:Acti]. IN DS 19036 8 1 B256BD . IN DS 19036 8 2 49AAC1 . IN DS 20326 8 1 AE1EAS . IN DS 20326 8 2 E06D44 [root@router01:Eval:Acti [root@router01:Eval:Acti [root@router01:Eval:Acti</pre>	<pre>ve:Standalone] config # ve:Standalone] config # dig dnskey . grep 257 > /root/dnskey.t ve:Standalone] config # dnssec_safromkey -f /root/dnskey.txt . O9DC8DD59F0E0F0D8541E8328DD986DF6E 1D7B6F6446702E54A160737160741441855200FD2CE1CDDE32F24E8FB5 B974D4C858B740BD03E3CED7EBFCBD1724 B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D ve:Standalone] config # ve:Standalone] config # ve:Standalone] config # </pre>

DNS » Caches : Cache List » Trust Anchors : validating-resolver_cache									
🔅 👻 Properties	Trust Anchors	DLV Anchors	Local Zones	Forward Zones	Response Policy Zones				
Statistics									
Trust Anchors Add									
Trust Anchor									
. IN DS 19036 8 1 B256BD09DC8DD59F0E0F0D8541B8328DD986DF6E									
. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5									
. IN DS 20326 8 1 AE1EA5B974D4C858B740BD03E3CED7EBFCBD1724									
. IN DS 20326 8 2 E0	6D44B80B8F1D39A	95C0B0D7C65D0845	58E880409BBC6834	57104237C7F8EC8	D				
Remove									

1

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

3.5.2 Modify DNS Profile

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

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



Select the profile "example.com_dns_profile"

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 19, 2017 User: a Time: 1:07 PM (CDT) Role: A	dmin dministrator
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » Delivery : Profiles : DN	S » Properties : example.com_dns_profile
Statistics	🚓 👻 Properties	
-		
iApps	General Properties	
🔁 Wizards	Name	example.com_dns_profile
	Partition / Path	Common
Delivery	Parent Profile	dns 🔽
	Denial of Service Protection	
Zones	Rapid Response Mode	Disabled 🗸
Caches	Rapid Response Last Action	Drop
Settings	Hardware Acceleration	
e	Protocol Validation	Disabled V
SSL Orchestrator	Response Cache	
Local Traffic	Selec	t the "validating-resolver cache"
Traffic Intelligence	DNSSEC	
	GSLB	
	DNS Express	
Access	DNO Express	
Device Management	DNS Cache	
	DNS Cache Name	Validating-resolver_cache
Network	DNS IPv6 to IPv4	
System	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 V
	Logging and Reporting	
	Logging	Enabled V
	Logging Profile	example_dns_logging_profile
	AVR Statistics Sample Rate	Enabled 1/ 1 queries sampled

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

TMSH

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

3.5.3 Results

From the CLI on the router01.branch01 BIGIP run

tail -f /var/log/ltm

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



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



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

🖾 Command Prompt	
C:\Users\user.EXAMPLE>dig dnssec-deployment.org +dnssec	
; <<>> DiG 9.3.2 <<>> dnssec-deployment.org +dnssec ;; global options: printcmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1568 ;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 1	
;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags: do; udp: 4096 ;; QUESTION SECTION: ;dnssec-deployment.org. IN A	
;; ANSWER SECTION: dnssec-deployment.org. 294 IN A 46.43.37.10 dnssec-deployment.org. 294 IN RRSIG A 5 2 300 20170801204001 2017071 8204001 36518 dnssec-deployment.org.fcsC4irvKmAp0c+39rYtx+tWzp9cPb6I/MRVeG9gun wWXkGNFXuJwUl +eBsy6NRNW184maIW7vY0bmwJkgsET2okUCcEP00/BzY/RFPHmzBsG5N Bxhg+0Lei MUYp/gHiDX0tGQVMvMgn6Z3oeqD4Ut6FJEcLuyGED0cRYNB yBc=	
;; AUTHORITY SECTION: dnssec-deployment.org. 294 IN NS ns1.sea1.afilias-nst.info. dnssec-deployment.org. 294 IN NS ns1.mia1.afilias-nst.info. dnssec-deployment.org. 294 IN NS ns1.yy21.afilias-nst.info. dnssec-deployment.org. 294 IN NS ns1.hkg1.afilias-nst.info. dnssec-deployment.org. 294 IN NS ns1.afilias-nst.info. dnssec-deployment.org. 294 IN NS ns1.afilias-nst.info. dnssec-deployment.org. 294 IN RSIG NS 5 2 300 20170801204001 201707 18204001 36518 dnssec-deployment.org. Jr13JdhS8T+ScKm+ZRpweEMywc1h0LM6T/5032dwp5	₽rv
<pre>/ul 19 13:07:46 router01 info tmm[12513]: 2017-07-19 13:07:45 router01.branch01.examp .16 from 10.1.71.100#65485: view none: query: dnssec-deployment.org IN & + (10.1.70.2 /ul 19 13:07:46 router01 info tmm[12513]: 2017-07-19 13:07:45 router01.branch01.examp .16 to 10.1.71.100#65485: [NOERROR qr,rd,ra] response: dnssec-deployment.org. 300 IN .0; /ul 19 13:07:52 router01 info tmm[12513]: 2017-07-19 13:07:52 router01.branch01.examp .568 from 10.1.71.100#65486: view none: query: dnssec-deployment.org IN & +ED (10.1.7 /ul 19 13:07:52 router01 info tmm[12513]: 2017-07-19 13:07:52 router01.branch01.examp .568 to 10.1.71.100#65486: view none: query: dnssec-deployment.org IN & +ED (10.1.7 /ul 19 13:07:52 router01 info tmm[12513]: 2017-07-19 13:07:52 router01.branch01.examp .568 to 10.1.71.100#65486: [NOERROR qr,rd,ra,ad] response: dnssec-deployment.org .294 J7.10; dnssec-deployment.org. 294 IN RRSIG & 5 2 300 20170801204001 20170718204001 3 deployment.org fceSC4irvKmAp0c+39rYtx+Ux299cPb6I/MRVeG9gvnWMKkGNFXuJwV1+eBsy6NRNW184 lkqsET2okVCcEP00/BzY/RFPHmzBsG5NBxhg+0LeiMUYp/gHiDX0tGQVMvMgn623oeqD4Vt6FJEcLuyGEDUCR</pre>	ole.com qid (OO%O) ole.com qid A 46.43.37. ole.com qid (O.200%O) ole.com qid i IN A 46.43 6518 dnssec imalWayODmw RYNByBc=;

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

C:\Users\user.EXAMPLE>dig dnssec-failed.org +dnssec	s Local Zones
; <<>> DiG 9.3.2 <<>> dnssec-failed.org +dnssec ;; global options: printcmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: STRUFAIL, 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 rovd: 35	
C:\Users\user.EXAMPLE>	
Jul 20 11:49:38 router01 info tmm[12352]: 2017-07-20 11:49:38 router01.branch01.ex 5 from 10.1.71.100#61266: view none: query: dnssec-failed.org IN & +ED (10.1.70.20	ample.com qid 63 D%O)
Jul 20 11:49:38 router01 info tmm[12352]: 2017-07-28 11:49:38 router01.branch01.exe	ample.com qid 63
5 to 10.1.71.100#61266: [SERVFAIL dr,rd,rat 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

Hos IP A	tname: ddress:	router01.branch 10.1.10.31	01.example.com	ı	Date: 、 Time: (Jul 16, 2017 5:47 PM (CD	Т)	User: Role:	admin Administrator		
ſ	5	ONLINE (AC	NVE)								
N	lain	Help	About		DNS »	Caches :	Cache	List			
M	Statisti	ics			⇔ -	Cache List	-	Sta	tistics		
G	iApps				*				×	Sea	irch
S DNS			✓ ♦ Name								
	Deli	very	•		No reco	ords to disp	lay.				
	GSL	.B	•		Delete						
	Zon	es	Þ								
	Cac	hes	Þ	7	Cache Li	ist	•				
	Sett	ings			Statistics	;	Z				
6	SSL O	rchestrator									
69	Local 1	Traffic									
	Accele	ration									

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

Create a validating resolver cache according to the table below:

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

General Properties

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

DNS Cache

Message Cache Size	1048576	bytes
Resource Record Cache Size	10485760	bytes
Name Server Cache Count	16536	entries
DNSSEC Key Cache Size	1048576	bytes
Answer Default Zones	🗹 Enabled 룾	
RRSet Rotate	none 🗸	

DNS Resolver

Use IPv4	Enabled
Use IPv6	Enabled
Use UDP	Enabled
Use TCP	☑ Enabled
Max. Concurrent UDP Flows	8192
Max. Concurrent TCP Flows	20
Max. Concurrent Queries	1024
Unsolicited Reply Threshold	0
Allowed Query Time	200
Randomize Query Character Case	Enabled
Root Hints (Optional: Leave blank for defaults)	IP Address: Add
140	
DNSSEC Validator	

DNSSEC Validato

Deefedala Ka	

.

Enabled

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

TMSH

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

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

3.6 RPZ

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



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

3.6.1 Zone Runner

Customers will subscribe to their RPZ vendor of choice.

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

Navigate to DNS >> Zones : ZoneRunner : Zone List

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

Hos IP A	tname: router01.branch01.example.com ddress: 10.1.10.31	n	Date: Jul 12, 2017 Time: 9:19 PM (CDT)	U	lser: admin ole: Administra	tor			Partition:	Common	-	Log out]
ſ	ONLINE (ACTIVE) Standalone												
Main Help About			DNS » Zones : Zor	neRun	ner : Zone Lis	t							
Mage Statistics			🚓 🚽 Resource Re	cord Li	st Zone List		View List	nam	ied Configuratio	n			
iApps			Find Zones										
S DNS			View Name		All	\sim							
	Delivery	Þ	Zone Name		*		Search	Reset Sear	rch				
	GSLB	ŀ									(Create	D
	Zones	ŀ	Zones	•					Zone Type	View Name	Resour	ce Records	1
	Caches		DNSSEC Zones	•									
	Settings	*	ZoneRunner	•	Resource Re List	cord 🕂)						
6	SSL Orchestrator			→	Zone List	•							
				View List	÷)							
				named Confi	guration								
Acceleration													
Device Management													
Network													
System													

Create a zone according to the following table:

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

General Properties						
View Name	external V					
Zone Name	rpz.example.com					
Zone Type	Master V NO COL AL UIE EIIC					
Configuration						
Records Creation Method	Manual					
Zone File Name	db.external.rpz.example.com					
Options						
Create Reverse Zone						
Records Creation	Records Creation Dots at the end					
SOA Record	TTL 300 Master Server router01.branch01.example.com. Email Contact hostmaster.example.com. Serial Number 2017071801 Refresh Interval 10800 Retry Interval 3600 Expire 604800 Negative TTL 86400					
NS Record	TTL 300 Nameserver router01.branch01.example.com					
Create A Record	Enable					
A Record	IP Address 10.1.71.1					

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

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

Hostnai IP Addr	me: router01.branch01.example.com ess: 10.1.10.31	Date: Jul 12, 2017 Us Time: 10:06 PM (CDT) Ro	er: admin Ie: Administrator		Partition: Co		
ſ	ONLINE (ACTIVE) Standalone						
Mair	Help About	DNS » Zones : ZoneRunne	r : Resource Record	l List			
Statistics		🚓 👻 Resource Record List	Zone List	View List	named Configuration		
	pps	Find Records					
S DNS		View Name	All 🔽	All			
Delivery		Zone Name	All Zones (Sele	All Zones (Select a View to search a specific zone)			
	GSLB >	Туре	All				
Zones >		Name	*	*			
Caches		RDATA					
Settings		Search Reset Search C	create				
SSL Orchestrator							
Local Traffic							
Acceleration							
De	vice Management						

Create a resource record according to the following table:

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 18, 2017 Us Time: 11:29 PM (CDT) Ro	ser: admin ble: Administrator		
ONLINE (ACTIVE) Standalone		ar - Resource Record List	-	
Statistics	Resource Record List	Zone List View	v List named Configura	tion
iApps	Find Records			
S DNS	View Name	All		
Delivery	Zone Name	All Zones (Select a V	(iew to search a specific zone)	
GSLB	Туре	All		
Zones	Name	*		
Caches	RDATA	*		
Settings	Search Reset Search	Create.		
SSL Orchestrator		-Click	"Searc	n "
Cocal Traffic	✓ ▲ Name	View Name	Zone Name	\$
	suns.com.rpz.example.	com. external	rpz.example.com.	30
Acceleration	rpz.example.com.	external	rpz.example.com.	30
Device Management	Delete	external	rpz.example.com.	30
Network				

3.6.2 Name Server

Navigate to DNS >> Delivery : Nameservers : Nameserver List

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

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

Create a nameserver according to the following table:

Setting	Value
Name	localhost

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 18, 2017 User. Time: 11:33 PM (CDT) Role:	admin Administrator
Standalone		
Main Help About	DNS » Delivery : Nameservers	: Nameserver List » New Nameserver
Magazine Statistics		
	General Properties	
iApps	Name	localhost
S DNS	Address	127.0.0.1
Delivery	Service Port	53 Other: 🔽
GSLB	Configuration	
Zones >	Route Domain	
Caches	TSIG Key	
Settings	1510 Key	
SSL Orchestrator	Cancel Repeat Finished	
Local Traffic		
Acceleration		
Device Management		
Network		

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

TMSH

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

3.6.3 DNS Express

Navigate to DNS >> Zones : Zones : Zone List

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

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

Create a DNS Express zone according to the following table:

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

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

TMSH

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

3.6.4 Local Zone

Navigate to: DNS >> Caches : Cache List

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 18, 2017 User: admin Time: 11:40 PM (CDT) Role: Administrator
Standalone	
Main Help About	DNS » Caches : Cache List
Statistics	🚓 🚽 Cache List Statistics 🗵
iApps	* Search
S DNS	Anne State S
Deliverv	transparent_cache
GSLB	validating-resolver_cache
Zones	Delete Click "validating-resolver cache
Caches	Cache List
Settings	Statistics
SSL Orchestrator	
Local Traffic	
Acceleration	
Device Management	
Network	

Select validating-resolver_cache, click "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

Host IP A	name: router01.branch01.example.com ddress: 10.1.10.31	Date: Jul 18, 2017 Time: 11:45 PM (CDT)	User: admin Role: Administrator		Pa	rtition: Common
ſ	ONLINE (ACTIVE) Standalone					
M	ain Help About	DNS » Caches : Cach	e List » Local Zones	: validating-resol	ver_cache	
1	Statistics	🔅 👻 Properties	Trust Anchors	DLV Anchors	Local Zones	Forward Z
	iApps	Response Policy Zones	Statistics 🔎		/0	
\bigcirc	DNS	Local Zones				Add
	Delivery	✓ Name				2
	GSLB	No records to display.		Select "I	ocal Zone	s"
	Zones >	Delete		Then clic	k "Add"	2
	Caches >					
	Settings >					
	SSL Orchestrator					
	Local Traffic					
	Acceleration					
	Device Management					
	Network					

Create a local zone entry according to the following table:

Setting	Value
Name	sorry.example.com
Туре	Static
Records	sorry.example.com. IN A 10.1.71.21

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

TMSH commands for router01.branch01:

3.6.5 Walled Garden

Navigate to: DNS >> Caches : Cache List

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

Click "validating-resolver_cache"

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 18, 2017 Time: 11:40 PM (CDT)	User. admin Role: Administrator
Standalone		
Main Help About	DNS » Caches : Cache	List
Mage Statistics	🔅 🚽 Cache List	Statistics 🔎
iApps	ŀ	× Search
S DNS	✓ ♦ Name	
Delivery	transparent_cache	
GSLB	validating-resolver_ca	ache
Zones >	Delete	Click "validating-resolver_cache
Caches >	Cache List 💽	g
Settings	Statistics 🗵	
SSL Orchestrator		
Local Traffic		
Acceleration		
Device Management		
Network		

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

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 13, 2017 User: adm Time: 3:48 PM (CDT) Role: Adm	hin hinistrator	Partition: Common V Log out
CONLINE (ACTIVE) Standalone			
Main Help About	DNS » Caches : Cache List » R	esponse Policy Zones : resolver_cache	
Ma Statistics	🚓 🗸 Properties Local Z	ones Forward Zones Response Po	Dicy Zones Statistics 🗩
iApps	Response Policy Zones		_Add
S DNS	✓ A Name	♦ <u>Action</u> ♦ Willed Gar	den 💠 Logs and Stats Only Fartition / Path
Delivery	No records to display.		2 /
GSLB	Delete Click	"Response Policy Zor	ne" Click "Add"
Zones		0	
Caches			
Settings			
SSL Orchestrator			
Local Traffic			
Acceleration			
Device Management			

Create a local zone entry according to the following table:

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

Response Policy Zone							
Zone	rpz.example.com						
Action	Walled Garden 🗸						
Walled Garden	sorry.example.com						
Logs and Stats Only							

TMSH commands for router01.branch01:

TMSH

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

3.6.6 Results

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



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

dig www.f5.com

3.7 URL Categorization

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



3.7.1 Create an iRule

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 18, 2017 Time: 8:30 PM (CDT)	User: admin Role: Administrator			
ONLINE (ACTIVE) Standalone					
Main Help About	DNS » Delivery : iRule	s : iRule List			
Market Statistics	🔅 👻 iRule List	Data Group List iFi	le List	Statistics	
iApps	ŀ	× Searc	:h		
🚯 DNS	✓ ▲ Name		Verification		\$
Delivery >	Listeners >	9	None		
GSLB	Profiles	eSupport_OA_BasicAuth	F5 Verified		f5
Zones	Load Balancing	eSupport_OA_NtImAuth	F5 Verified		f5-
Cachos	iDulos	sSupport holpor	F5 Verified		f5-
Caches		IRUIE LISI	F5 Verified		f5-
Settings	Translation	Data Group List	F5 Verified		f5-
SSI Orchostrator	Nameservers	iFile List 📀 F5 Verified			f5-
33E Orchestrator	Keys 🔸	Statistics	F5 Verified		f5-
Local Traffic	sys_auth_ldap		F5 Verified		f5-
Acceleration	sys_auth_radius		F5 Verified		f5-
Acceleration	sys_auth_ssl_cc_ld	ар	E F5 Verified		f5
Device Management	sys_auth_ssl_cridp		F5 Verified		f5-
-	sys_auth_ssl_ocsp		F5 Verified		f5-
Network					

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

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

Setting	Value
Name	DNS-query-filtering

```
when RULE_INIT {
# Set categories to block for DNS hosts
 set static::blocked_categories {
   /Common/Bot_Networks
   /Common/Spyware
   /Common/Malicious_Web_Sites
   /Common/Adult_Content
   /Common/Sex
 }
 # CONFIGURATION
 # Check all requests by default
 set static::request_check 1
 # If the category returns as blocked, return NXDOMAIN (1)
 # Otherwise if (0), return a statically defined IP address
 set static::request_return_nxdomain 0
 set static::request_redirect_to "10.1.71.21"
```

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

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

TMSH

tmsh create Itm rule DNS-query-filtering

3.7.2 iRule assignment

Repeat the following steps for all 4 DNS listeners. Navigate to: **DNS** >> **Delivery : Listeners : Listener List**

1.000	across _ coutorΩ4 broocbΩ4 oversets across	n Dete: 10149-0047	Lloor edmin			1
	Idress: 10.1.10.31	Time: 8:59 PM (CDT)	Role: Administrator			
ſ	ONLINE (ACTIVE) Standalone					
Ma	ain Help About	Local Traffic » iRules	s : iRule List			
Ma :	Statistics	🚓 👻 iRule List	Data Group List	iFile List	Statistics 🗵	
i 🔊	Apps	*		Gearch		
S 1	DNS	Name		Verification		\$
	Delivery	▶ Listeners	▶ Listener List	€ F5 Verified		f5
	GSLB	Profiles	Statistics	F5 Verified		f5
	Zones	Load Balancing	soupport_neiper	F5 Verified		f5
	Caches	iRules	Support_main	F5 Verified		f5
	Settings	> Translation	SAML_BasicAuth	F5 Verified		f5
		Nameservers	C ▶ to	F5 Verified		15
	SSL Orchestrator	Keys	ile ▶	F5 Verified		CI 45
(<u>)</u>	Local Traffic	sys_auth_radius		F5 Verified		f5
		sys_auth_ssl_cc_	Idap	F5 Verified		f5
		sys_auth_ssl_crld	lp	F5 Verified		f5
	Device Managemen	sys_auth_ssl_ocs	p	F5 Verified		f5
	lotwork	sys_auth_tacacs		F5 Verified		f5
	NELWOIN					

Navigate to the listener DC01_udp_virtual

DNS » Delivery : Listeners : Listener List								
tistener List Statistics								
* × Search			Create					
State + Name	 Destination 	+ Protocol	Partition / Path					
Enabled DC01_tcp_virtual	10.1.70.200	TCP	Common					
Enabled DC01_udp_virtual	10.1.70.200	UDP	Common					
Enabled BC02_tep_virtual	10.1.70.210	TCP	Common					
Enabled DC02_udp_virtual	10.1.70.210	UDP	Common					
Enable Disable Delete								

Navigate to iRules section

DNS » Delivery : Listeners : Listener List » Properties : DC01_udp_virtual						
🔅 🚽 Properties Loa	d Balancing iRules Dtatistics 🗵					
General						
Name	DC01_udp_virtual					
Partition	Common					
Description						
State	Enabled					
Listener: Advanced						
Destination	Type: Host O Network Address: 10.1.70.200					
Service Port	DNS 🔽 53					
VLAN Traffic	Enabled on					
VLANs and Tunnels	Selected Available /Common < branch01_vlan < >> //Common >> //Common AD_vlan >> http-tunnel isp1_site1_vlan					
Source Address Translation	None					
Address Translation	Enabled					
Port Translation	Enabled					
Route Advertisement	Enabled					

Navigate to Manage

DNS :	DNS » Delivery : Listeners : Listener List » iRules : DC01_udp_virtual								
\$ +	Properties	Load Balancing	iRules	Statistics					
Statisti	cs								
Static	tice Drofile	Nono							
otatis	ucs Frome	INOTE	•						
Updat	te								
iRules						Manage			
Name									
No rec	ords to display.								
-									

https://router01.branch01.example.com/tmui/Control/form?__handler=/tmui/dns/listener/irules&__source=Manage...&__lin Highlight DNS-query-filtering iRule and move it to Selected column

DNS	DNS » Delivery : Listeners : Listener List » Properties : DC01_udp_virtual									
⇔ -	Properties	Load	Balancing	iRules		Statistics				
iRule N	lanagement									
			Sele	ted			Available			
iRules	3				>>	Common DNS-query-filte _sys_APM_Exc _sys_APM_Exc _sys_APM_Exc	ring changeSupport_(changeSupport_(changeSupport_h	DA_BasicAuth DA_NtImAuth nelper	$\hat{}$	
			Up	Down						
Updat	te									

TMSH commands for router01.branch01

TMSH

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

3.7.3 Results

From the CLI on the router01.branch01 BIGIP run

tail -f /var/log/ltm

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

🔤 Command Prompt					_ 🗆 🗙			
<pre><<>> 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</pre>								
;; 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 ;; SERUER: 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 & + (10.1.70.200%0) Jul 18 22:06:35 router01 info tmm3[11519]: Rule /Common/DNS-guery-filtering <dns_request>: C ategory /Common/Information_Technology matching example.com is not filtered Jul 18 22:06:35 router01 info tmm[11519]: 2017 07-10-22:06:34 router01.branch01.example.com qid 116 to 10.1.71.100#49954: [NOERROR qr,aa,rd] response: example.com. 600 IN & 10.1.70.200 ;</dns_request>								
Update	Delete							

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

📾 Command Prompt	_ 🗆 🗵	
C:\Users\user.EXAMPLE> C:\Users\user.EXAMPLE> C:\Users\user.EXAMPLE> C:\Users\user.EXAMPLE> C:\Users\user.EXAMPLE>dig porno.com		
; <<>> DiG 9.3.2 <<>> porno.com ;; global options: printcmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2037 ;; flags: gr 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>		.)
		:55
Jul 18 22:09:12 router01 info tmm[11519]: 2017-07-18 22:09:12 router01.bran	nchO1.exam	ple.com
qid 2037 from 10.1.71.100#49955: view none: query: porno.com IN A + (10.1.7 Jul 18 22:09+12 router01 info tmm2[11519]: Rule /Common/DNS-query-filtering	70.200%0) g <dns_req< td=""><td>UEST>: B</td></dns_req<>	UEST>: B
LOCKED Category /Common/Sex matching porno.com is filtered. Jul 18 22 :09:12 router01 info tmm[11519]: 2017-07-18 22:09:12 router01.bran	nch01.exam	ple.com
qid 2037 to 10.1.71.100#49955: [NOERKOR qr,rd] response: porno.com. 111 IN	A 10.1.71	.21;
Update Delete		

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 13, 2017 Time: 8:30 PM (CDT)	User: admin Role: Administrator			
ONLINE (ACTIVE) Standalone					
Main Help About	DNS » Delivery : iRule	s : iRule List			
Statistics	🔅 👻 iRule List	Data Group List iFile	List	Statistics (
iApps	*	× Search			
S DNS	Name	4	Verification		\$
Delivery >>	Listeners >	9 N	lone		
GSLB	Profiles >>	eSupport_OA_BasicAuth	F5 Verified		f5
Zones	Load Balancing	eSupport_OA_NtImAuth	F5 Verified		f5
Cachoc	iPulos	iPulo List	F5 Verified		f5-
Caches	ikules P		F5 Verified		f5-
Settings	Translation	Data Group List (+)	F5 Verified		f5-
	Nameservers	iFile List 🔶	F5 Verified		f5-
SSE Orchestrator	Keys	Statistics	F5 Verified		f5-
Coral Traffic	sys_auth_Idap		F5 Verified		f5
Acceleration	sys_auth_radius	0	F5 Verified		f5-
Acceleration		lap	F5 Verified		f5-
Device Management	sys_auth_ssl_cridp	9	5 Verified		f5-
	sys_auth_ssl_ocsp		F5 Verified		f5-
Network					

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/Adult_Content 8 /Common/Adult_Content 8 /Common/News_and_Media 9 /Common/News_and_Media 10 # 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_retirect_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 } { 27 28 29 29 20 20 20 20 20 20 20 20 20 20 20 20 20</pre>					
Ignore Signature/Check	sum 🗖					

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



4 Credits

• Agility 2017:

Bill Wester

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









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.