DNS Documentation

F5 Networks, Inc.

Jun 03, 2020



Agility 2020 Hands-on Lab Guide

DNS



Contents:

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

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: S	ystem » Log	gs : Conf	iguration :	Log	Publishers
--	----	----------------	-------------	-----------	-------------	-----	------------

Hostna IP Add	ame: gtm1.site1.example.com Dat Iress: 10.1.10.13 Tim	te: Jul 20, 2017 User: : ne: 12:39 PM (CDT) Role: .	admin Administrator	Р
ſ	ONLINE (ACTIVE) Standalone			
Mai	in Help About	System » Logs : Config	uration : Log Publishers	
100 s	tatistics	🔅 🚽 System	Captured Transactions Packet Filter	GSLB Audit
i/	Apps		Click "Create"	Create
5 D	NS	🖌 🗢 Name		5
6	SL Orchostrator	default-ipsec-log-publ	lisher	
U 3	SE Orchestrator	local-db-publisher		
ᢙ A	cceleration	sys-db-access-publis	her	
	anian Managana d	sys-sso-access-publis	sher	
	evice Management	Delete		
<u></u> N	etwork			
S + 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 Astinations	
	Logs	Configuration +	Log Publishers 💿	
				https://start.skat.sussals.sas

Create a local syslog publisher according to the table below:

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

Hostname: gtm1.site1.example.com Dat IP Address: 10.1.10.13 Tim	e: Jul 20, 2017 User: admin e: 12:43 PM (CDT) Role: Administrator P
ONLINE (ACTIVE) Standalone	
Main Help About	System » Logs : Configuration : Log Publishers
Statistics	Conseril Dranadian
iApps	Name local-syslog-publisher
S DNS	Description
SSL Orchestrator	Log Destinations
Acceleration	Selected Available
Device Management	Destinations
Retwork	
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

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 Dat IP Address: 10.1.10.13 Tim	e: Jul 20, 2017 e: 12:49 PM (CDT)	User: admin Role: Administrator			
ONLINE (ACTIVE) Standalone					
Main Help About	DNS » Delivery :	Profiles : Other : D	NS Logging		
Mage Statistics	DNS	Protocol	✓ Other		
iApps	ł		× Click "Cre	ate"	Create
S DNS	✓ ♦ Name				\$ Lo
Delivery	Listeners	+			
GSLB 2	Profiles	DNS	(*)		
Zones	Load Balancing	Protocol			
Caches	iRules	Other	DNS L	.ogging 💿	
Settings >	Translation	3	4 Persis	tence 🔶	
SSI Orchestrator	Nameservers		Statist	ics 📀	
G 33E Orchestrat	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 Da IP Address: 10.1.10.13 Tir	te: Jul 20, 2017 User: admin ne: 12:52 PM (CDT) Role: Administ	rator
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » Delivery : Profiles : Oth	er : DNS Logging » New
Mage Statistics		
iAnns	General Properties	
- in the	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	Les Fielde	
C SSI Orchastrator	Log Fields	
SSL Orchestrator	Include Complete Answer	
Acceleration	Include Query ID	
	Include Source	✓ Enabled
Device Management	Include Timestamp	Enabled
Retwork	Include View	Enabled
To 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

Main Help About	DNS » Delivery : Profiles : D	NS >> Properties : example.com_dns_profile	
Mage Statistics	🔅 🚽 Properties		
iApps	General Properties		
😚 dns	Name	example.com_dns_profile	
Delivery	Partition / Path	Common	
GSLB	Parent Profile	dns 🔽	
Zones	Denial of Service Protection		Custom 🗌
Caches	Rapid Response Mode	Disabled 🗸	
Settings	Rapid Response Last Action	Drop	
Acceleration	Hardware Acceleration		
Device Management	Protocol Validation	Disabled	
	Response Cache	Disabled	
Network	DNS Features		
System	DNSSEC	Disabled V	
	GSLB	Enabled V	
	DNS Express	Disabled V	
	DNS Cache	Disabled 🗸	
	DNS Cache Name	Select	
	DNS IPv6 to IPv4	Disabled 🔽	
	Unhandled Query Actions	Drop V	
	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	
	Logging Profile	example_dns_logging_profile	
	AVR Statistics Sample Rate	Enabled 1/ 1 queries sampled	V

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

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

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

TMSH

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

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

2.2.3 UDP Profile

A UDP profile is associated with a listener.

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

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

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Tin	te: Jul 20, 2017 U ne: 1:11 PM (CDT) R	lser: admin tole: Administrator	
ONLINE (ACTIVE) Standalone	_		
Main Help About	DNS » Delivery : I	Profiles : Protocol : UDP	Click "Create"
Statistics	DNS	Protocol - Oth	er 🗸
iApps	ŀ	× Search	Create
S DNS	✓ \$ Name		÷.
Delivery	Listeners	>	
GSLB	Profiles	DNS 💮	
Zones	2 Load Balancing	Protocol	UDP 💿
Caches	iRules	³ Other	4 TCP 💮
Settings	rranslation	•	
SSI Orchastrator	Nameservers	•	
33L Orchestrator	Keys	•	
Acceleration			
Device Management			
Network			
System			

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 10.1.10.13	n Date Time	: Jul 26, 2018 :: 8:17 AM (EDT)	User: admin Role: Administra	tor Partition: Common	$\overline{}$	Log out
6	ONLINE (ACTIVE) Standalone						
Main	Help Ab	out	DNS » Delivery	y : Profiles : Prot	ocol : UDP » New UDP Profile		
Magazina Statisti	ics		0				
iApps			Name =	es	example.com_udp-dns_profile		
😚 dns			Parent Profile		udp_gtm_dns		
Deli	very	÷	Settings			(Custom 🗌
GSL	B	•	Proxy Maximum	Segment			
Zone	es	÷	Idle Timeout		Specify 🔽 5	seconds	
Cac	hes	•	IP ToS		Specify V		
Sett	ings	•	Link QoS		Specify V 0		
Accele	ration		Datagram LB		Enabled		
Device.			Allow No Payloa	d			
E Device	Management		TTL Mode		Proxy 🗸		
Networ	rk		Don't Fragment	Mode	PMTU 🔽		
Systen	1		Max Buffer Byte	s	655350		
			Max Buffer Pack	ets	0		

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 D IP Address: 10.1.10.13 T	ate: Jul 20, 2017 īme: 1:19 PM (CDT)	User: admin Role: Administrator		Partition: Common
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » Delivery	: Profiles : Protocol : TCI	P	
Mage Statistics	DNS	Protocol	Click "C	reate"
iApps	ř	×	Search	Create
S DNS	✓ ⇒ Name			
Delivery 1	Listeners	, t-tcp		tcp-legacy
GSLB	Profiles	DNS	÷	tcp-legacy
Zones	2 Joad Balancing	Protocol	> UDP	(+) top
Caches	iRules	3 Other	ТСР	e tcp
Settings	Translation		- 4	tcp
B an a bat a	Nameservers	ed		tcp-legacy
SSL Orchestrator	Keys) ₽		tcp-wan-or
Acceleration	tcp			(none)
Dovice Management	tcp-lan-optim	ized		tcp-legacy
Device Management	tcp-legacy			tcp
Retwork	tcp-mobile-op	ptimized		tcp-legacy
E Sustam	tcp-wan-optin	mized		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 Date IP Address: 10.1.10.13 Time	e: Jul 20, 2017 User: admin e: 1:23 PM (CDT) Role: Administr	ator	Partition: Common
Standalone			
Main Help About	DNS » Delivery : Profiles : Pro	tocol : TCP » New TCP Profile	
Mage Statistics			
	General Properties		
IApps	Name	example.com_tcp-dns_profile	
😚 dns	Parent Profile	f5-tcp-wan	
Delivery	Timer Management		
GSLB	Close Wait	Specify 🗹 5 se	conds
Zones	Fin Wait 1	Specify 🖌 5 se	conds
Caches	Fin Wait 2	Specify 🔽 300 se	conds
Settings	Idle Timeout	Specify V 300 sec	onds
SSL Orchestrator	Keep Alive Interval	Specify V 1800 sec	onds
Acceleration	Minimum RTO	500 milliseconds	
Device Management	Reset On Timeout	Enabled	
	Time Wait	Specify 🔽 2000 mi	lliseconds
Network	Time Scroll way dow	wn to find the "Einish"	"button
System	Zero Window Timeout	Specify 20000 milli	iseconds

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 Da IP Address: 10.1.10.13 Tir	te: Jul 20, 2017 User: au ne: 1:29 PM (CDT) Role: A	d min dministrator	Partition: Common
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Delivery : Listen	ers : Listener List	Click"Create"
Mage Statistics	🔅 🚽 Listener List	Statistics 🗵	
iApps	٢	× Search	Create
S DNS	State 🗢 Name		▲ Destination 💠 F
Delivery	Listeners	Listener List 📀	
GSLB	Profiles	Statistics 🦻	
Zones	Load Balancing >		
Caches	iRules >		
Settings	Translation >		
	Nameservers >		
SSL OICHER WILDI	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_	virtua
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: Administr	rator Partition: Common		
CONLINE (ACTIVE) Standalone				
Main Help About	DNS » Delivery : Listeners : L	istener List » New		
Mage Statistics				
itana	General			
TApps	Name	isp1_site1_ns1.example.com_udp_53		
S DNS	Description			
Delivery	State	Enabled V		
GSLB	Listener: Advanced			
Zones >		Type: Host O Network		
Caches	Destination	Address: 203.0.113.8		
Settings	Service Port	DNS 53		
SSL Orchestrator	VLAN Traffic			
A surfacetion	Source Address Translation	None		
Acceleration	Address Translation	Enabled		
Device Management	Port Translation	Enabled		
Network	Route Advertisement	Enabled		
	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 Tin	te: Jul 20, 2017 User: ne: 1:29 PM (CDT) Role:	admin Administrator	Partition: Common
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Delivery : Liste	eners : Listener List	Click "Create"
Magazine Statistics	🔅 👻 Listener List	Statistics 💌	
iApps	ł	× Search	Create
😚 dns	State 🗢 Name		▲ Destination 💠 F
Delivery	Listeners	Listener List 📀	
GSLB	Profiles	Statistics	
Zones	Load alancing		
Caches	iRules		
Settings	Translation		
E SSI Orabellar	Nameservers		
SSL OICHANNALOI	Keys		
Acceleration			
Device Management			
Network			
System			

Create a TCP listener.

Setting		gtm1.site1	gtm1.site2	
Name		isp1_site1_ns1.example.com_tcp_53_v	ir tspa1 _site2_ns2.example.com_tcp_53_v	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 Dat IP Address: 10.1.10.13 Tin	te: Jul 20, 2017 User: admin he: 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
😚 dns	Description	
Delivery	State	Enabled 🔽
GSLB	Listener: Advanced V	
Zones >	Destination	Type: Host O Network Address: 203.0.113.8
Settings	Service Port	DNS 🔽 53
SSL Orchestrator	VLAN Traffic	
Appalaration	Source Address Translation	None
Acceleration	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 E IP Address: 10.1.10.13 T	ate: Jul 20, 2017 ime: 1:45 PM (CDT)	User: admin Role: Administrator		Partition: Common
ONLINE (ACTIVE) Standalone				
Main Heip About	UNS » GSLB:	tor List Statistics	nter List	Click "Create"
Statistics		ler List Statistics		Click-Create-
iApps	*		Search	Create
S DNS	Availabili	ity A Name		Location Links
Delivery	No records to dis	play.		
GSLB	Wide IPs	ie		
Zones	Pools	•		
Caches	iRules	\odot		
Settings	Data Centers	Data Center I	List 💽	
E SSI Orghantraar	2 Servers	3 Statistics	7	
SSL Orchestrator	Links	Þ		
Acceleration	Prober Pools	•		
Device Management	Monitors	\odot		
	Topology			
Network	Distributed Applica	tions >		
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

Hosi IP A	tname: gtm1.site1.example.com ddress: 10.1.10.13	Date: Time:	Jul 20, 2017 U : 1:48 PM (CDT) R	lser: admin ole: Administral	tor	Partition: Common
(Standalone					
M	lain Help About		DNS » GSLB : Dat	ta Centers : D	ata Center List	
~	Statistics					
	ið en e		General Properties			
Lø	IApps		Name		site1_datacenter	-
\bigcirc	DNS		Description			
	Delivery	•	Location			
	GSLB	F	Contact			
	Zones	×	Prober Preference		Inside Data Center	
	Caches	×	Prober Fallback		Any Available	
	Settings	•	State		Enabled V	
6	SSL Orchestrator		Cancel Repeat	Finished		
	Acceleration					
	Device Management		Repeat t	his step	to create "site2_datacer	iter
	Network					
34	System					
https	://gtm1.site1.example.co	m/tn	nui/Control/jspm	ap/tmui/gl	oballb/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

Hos IP A	tname: gtm1.site1.example.com ddress: 10.1.10.13	Date: Jul 20, 2017 Time: 2:04 PM (CDT)	User: a Role: A	dmin dministrator				Partition: Common
(Standalone							
N	lain Help About	DNS » GSL	B: Servers :	: Server List				
	Statistics	🔅 👻 Serve	r List	Trusted Server	Certificates	Statistics		
3	iApps	*			Search			Create
0	DMS				Devices	Addross	A Data Contor	Virtual Servers
$\mathbf{\bullet}$	DNS	V Statt			Devices	Address	Vala Ceriler	viitual Servers
	Delivery	No records to	display.	- 1				
	GSLB	Wide IPs	F	ete				
	Zones	Pools	Þ					
	Caches	iRules	÷					
	Settings	Data Centers	F					
e		Servers	5	Server List	⊙			
	SSL Orchestrator	Links	-	Trusted Server Certificates				
	Acceleration	Prober Pools	· ·	Statistics	7			
	Device Management	Monitors	(+)					
		Topology	Þ					
	Network	Distributed App	olications >>					
3	System							

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

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

gtm1.site1

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

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Time	:: Jul 20, 2017 User: admi a: 2:00 PM (CDT) Role: Adm	nin ninistrator	Partition: Common			
Standalone						
Main Help About	DNS » GSLB : Servers : Se	erver List				
Mage Statistics	🔅 🚽 Server List	Trusted Server Certificates	Statistics 🔊			
iApps	*	Search	Create			
😚 dns	Status 🔺 Name	Devices	Address			
Delivery	No records to display.					
GSLB	Enable Disable Delete					
Zones						
Caches	Click	c-"Create"-to.d	efine.atm1.site1			
Settings >						
SSL Orchestrator						
Acceleration						
Device Management						
Retwork						
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 e: 2:29 PM (CC	User:)T) Role:	admin Administrati	or		Parti
ONLINE (ACTIVE) Standalone						
Main Help About	DNS » G	SLB : Server	s : Server I	List » New Server		
Market Statistics						
iðans.	General Pr	operties				
indups.	Name		\rightarrow	gtm1.site1_server		
S DNS	Product			BIG-IP System		
Delivery	Data Center 🛑 🔶		site1_datacenter			
GSLB →	Prober Pre	Prober Preference		Inherit From Data Center		
Zones >	Prober Fa	rober Fallback Inherit From Data Center		Inherit From Data Center 🔽		
Caches	State		Enabled V			
Settings	Dovices			Click#Ad		
SSL Orchestrator	Devices			CIICK AU	<u>u</u> -	
		Add	Dev	ico Namo	Addrose	
Acceleration		No data ava	ilable in tabl	e	Address	
Device Management	BIG-IP System Devices					
e Network						
System		Edit Delete				

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

Hostname: gtm1.site1.ex IP Address: 10.1.10.13	ample.com Date: Time:	Jul 20, 2017 2:36 PM (CDT)	User: Role:	admin Administrator			Parti
ONLINE (# Standalon	ACTIVE) 1e						
Main Help	About	DNS » GSL	.B : Server	s : Server List	» New S	erver	
Ma Statistics				Add	i Big-ip s	System Device	
iApps		General Pron	erties	Devi	ice Name: ress:	gtm1.site1.example.com 1 203.0.113.7 2	
S DNS		Product		Tran	nslation:		(Optional)
Delivery		Click"A		Link		Auto-Select	
GSLB	•	Prober Prefe		A	dd 3		
Zones	•	Prober Fallba	ack	203	3.0.113.7		
Caches	•	State					
Settings	• •	Douises		De	Noto		
SSL Orchestrator		A			siele	OK	Cancol
Acceleration			o data avai	De ilable in table		4	Cancer
Device Manageme	ent	BIG-IP System Devices					
Network		2011003				Click"OK"	
System		E					

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 (CI	User: admin DT) Role: Administra	ator	Part		
ONLINE (ACTIVE) Standalone						
Main Help About	DNS » G	SLB : Servers : Serve	r List » New Server			
Statistics	General Pr	operties				
iApps	Name		gtm1.site1_server			
S DNS	Product		BIG-IP System			
Delivery	Data Cer	nter	site1_datacenter			
GSLB	Prober Pro	eference	Inherit From Data Center 🔽			
Zones	Prober Fa	llback	Inherit From Data Center 🔽			
Caches	State		Enabled V			
Settings	Devices					
SSL Orchestrator		Add				
Acceleration		Device Name Address dtm1 site1 example com 203 0 113 7				
Device Management	BIG-IF System Devices	es l				
Retwork						
System		Edit Delete				
	Configurat	ion: Advanced 🗸				
	Health Mo	onitors	Selected	Available Common gateway_icmp gtp http http_head_f5		
	Availability	/ Requirements	All Health Monitors			
	Limit Setti	ngs	Bits: Disabled Packets: Disabled Current Connections: Disabled	সসম		
iQuery Options			Service Check 🖌 Path 🖌 SNMP 🖌			

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

TMSH

tmsh create gtm server gtm1.site1_server datacenter site1_datacenter devices add { gtm1.site1.example.com { addresses add { 203.0.113.7 } } } monitor bigip product bigip
gtm1.site2

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



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

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

1. Fill in the Name and Datacenter

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Time	e: Jul 20, 2017 e: 3:18 PM (CD)	User: T) Role:	admin Administrator			Parti
ONLINE (ACTIVE) Standalone						
Main Help About	DNS » GS	LB : Server	s : Server List	» New Server		
Statistics						
iApps	General Pro	perties	 g	tm1.site2_server		
S DNS	Product		В	G-IP System		
Delivery	Data Cent	er	si	te2_datacenter		
GSLB >	Prober Pret	ference	In	herit From Data Center 🔽		
Zones >	Prober Fall	back	In	herit From Data Center 💌		
Caches	State		E	nabled 🔽		
Settings	Daviana					
SSI Orchestrator	Devices			Click "Add"		
	j	Add	Device	Name	Address	
Device Management	BIG-IP System	No data avai	lable in table			
Network	Devices					
System		Edit Delete				

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

Hostname: gtm1.site1.example.com IP Address: 10.1.10.13	Date: Jul 20, 2017 Time: 3:30 PM (CD	User: admin T) Role: Admin	istrator	Parti
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » G	SLB : Servers : Sei	rver List » New Server	
Statistics			Add BIG-IP System Device	
iApps	General Pro Name Product		Address: 198.51.100.39 Translation:	ample.com) (Optional)
Delivery GSLB	Prober Pre	k"Add"	Link: Auto-Select	2
Zones Caches	Prober Fal State	lback	2 98.51.100.39	
Settings	•			
SSL Orchestrator	Devices		Delete	3 OK Cancel
Acceleration	BIG-IP	No data available i	n table	
Device Management	System Devices		Gilck	
System				

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

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Tin	te: Jul 20, 2017 ne: 3:37 PM (CDT)	User: admin Role: Administra	ator		Parti	
ONLINE (ACTIVE) Standalone						
Main Help About	DNS » GSLI	B : Servers : Server	r List » New Server			
Statistics	General Prope	erties				
iApps	Name		gtm1.site2_server			
😚 dns	Product		BIG-IP System			
Delivery	Data Center		site2_datacenter			
GSLB	Prober Prefer	ence	Inherit From Data Center 🗸			
Zones	Prober Fallba	ck	Inherit From Data Center 🔽			
Caches	State		Enabled 🔽			
Settings	Devices					
SSL Orchestrator	Ac	id D	evice Name	Address	-	
Acceleration	BIG-IE gtr	gtm1.site2.example.com 198.51.1				
Device Management	System Devices	System Devices				
Network						
System	Ec	dit Delete				
_	Configuration	Advanced 🗸				
	Health Monito	ors	Selected /Common bigip <	Available /Common gateway_icmp gtp http http_head_f5		
-	Availability Re	equirements	All Health Monitors			
	Limit Settings		Bits: Disabled Packets: Disabled Current Connections: Disabled			
	iQuery Option	15	Service Check 🖌 Path 🖌 SNMP 🖌			

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

TMSH

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

site1_ha-pair

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



Create a Server Object as defined in the table below:

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

1. Fill in the Name and Datacenter

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Time	:: Jul 20, 2017 :: 3:58 PM (CD	User:)T) Role:	admin Administrate	or	Partil
Main Help About	DNS » G	SI R : Server	: Server I	ist » New Server-	
Statistics	General Pro	operties			
iApps	Name			site1_ha-pair	
S DNS	Product			BIG-IP System	
Delivery	Data Cen	ter		site1_datacenter	
GSLB →	Prober Pre	eference		Inherit From Data Center 🔽	
Zones >	Prober Fa	llback		Inherit From Data Center 🔽	
Caches	State			Enabled 🔽	
Settings	Devices				
SSL Orchestrator		Add 🗲			
Acceleration		No data avai	Dev ble in tabl	ice Name	Address
Device Management	BIG-IP System Devices				
Retwork					
System		Edit Delete			

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

Hostname: gtm1.site1.example.com D IP Address: 10.1.10.13 T	ate: Jul 20, 2017 ime: 4:33 PM (CDT)	User: admin Role: Administrator	Pa
Standalone			
Main Help About	DNS » GSL	.B : Servers : Server Lis	st » New Server
Statistics		^	Add BIG-IP System Device
iApps	General Prop Name	erties	ddress: 1 203.0.113.5
5 DNS	Product	т	ranslation: (Optional)
Delivery	Data Center	r u	ink: Auto-Select
GSLB	Prober Prefe	rence	Add 2
Zones	Click"	Add"	203.0.113.5
Caches	State		
Settings			4
e	Devices	-	Delete
SSL Orchestrator	A	dd	3 _ OK Cancel
Acceleration		Der Le date quaitable in table	
_	BIG-IP	lo data avallable in table	
Device Management	System Devices		ClickTOKT
Retwork			
System	E		

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	: Jul 20, 2017 User: admin :: 4:38 PM (CDT) Role: Administra	lor
Standalone		
Main Help About	DNS » GSLB : Servers : Server	List » New Server
Statistics	General 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	BIG-IF	m 203.0.113.5
Device Management	System Devices	
Network		
System	Edit Delete	

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

Hostname: gtm1.si IP Address: 10.1.10	e1.example.com 13	Date: Jul 20, 2017 Time: 4:53 PM (Cl	User: DT) Role:	admin Administrator			Par
	NE (ACTIVE) dalone						
Main H	elp About	DNS » G	SLB : Server	s : Server List	» New S	erver	
Statistics				Ad	d BIG-IP S	System Device	
iApps		General Pr Name	operties	Dev Ado	vice Name dress:	bigip2.site1.example.com	
S DNS		Product		Tra	nslation:		(Optional)
Delivery		Click"	Adar -	Link	k:	Auto-Select	(-p,
GSLB		 Proper Pr 	elerence	A	Add		
Zones		Prober Fa	llback	20	3.0.113.6		
Caches		State					
Settings		> -					
SSL Orchestr	ator	Devices			elete		
					_	0	K Cancel
Acceleration		BIGJP	bigip1.site1.	example.com		20.0.113.5	
Device Manag	jement	System Devices				Click"OK"	
Network							
System							

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

Hostname: gtm1.site1.example.com IP Address: 10.1.10.13	Date: Jul 20, 2 Time: 5:00 PM	017 User: admin (CDT) Role: Administra	Pa			
CONLINE (ACTIVE) Standalone						
Main Help About	DNS >	GSLB : Servers : Server	List » New Server			
Statistics	Genera	Properties				
iApps	Name	•	site1_ha-pair			
S DNS	Produc	:t	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					
SSL Orchestrator	Devices	Add Two d	evices belong to this HA-Pair			
Acceleration		bigip1.site1.example.co	om 203.0.113.5			
Device Management	Syste	bigip2.site1.example.co	om 203.0.113.6			
Retwork						
System		Edit Delete				
Add the "bigip" He	alth Mo	nitor				
	Health	Monitors	Selected Available //Common //Common bigip < >> //Endote ptp http http_head_f5			
	Availa	bility Requirements	All Health Monitors			

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

Resource

sources					
Virtual Server Discovery	Enabled				
Link Discovery	Enabled				
Cancel Repeat Finished					

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

TMSH

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

site2_ha-pair

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

Hos IP A	stname: gtm1.site1.example.com Address: 10.1.10.13	Date: J Time: 5	ul 20, 2017 :47 PM (CDT)	User: ad Role: Ad	min Iministrator				
ſ	ONLINE (ACTIVE) Standalone					(Click"Cr	eate"	
N	Main Help Abo	out 🛛	DNS » GSLB	: Servers :	Server List				
	Statistics		🛱 👻 Server L	.ist	Trusted Server Cert	ificates S	Statistics		
6	iApps	F			×S	earch		Cre	ate
5	DNS		🖌 🔽 Status	▲ Name		Devices	Address	Data Center	Virtual
	Delivery	, [gtm1.site1	_server	1	203.0.113.7	site1_datacenter	0
	GSLB	· · · ·		gtm1.site2	_server	1	198.51.100.39	site2_datacenter	0
	Zones	•		site1_ha-p	air	2	203.0.113.5 203.0.113.6	site1_datacenter	0
	Caches	· · 1	Enable Disal	ble Delet	ie				
	Settings	•							
6	SSL Orchestrator								
	Acceleration								
	Device Management								
	Network								
8 🕈	System								

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 e: 5:52 PM (CDT) Role: Administra	lor
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » GSLB : Servers : Server	List » New Server
Magazine Statistics		
	General Properties	
IApps	Name	site2_ha_pair
S 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
Assolution		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 Ad	ame: gtm1.site1.example.com dress: 10.1.10.13	Date: Time:	Jul 20, 2017 5:56 PM (CDT)	User: Role:	admin Administrator		Partition: Common
	ONLINE (ACTIVE) Standalone	_					
Ma	in Help About		DNS » GSLE	3 : Server	s : Server List » New Server.	••	
s 🔁 ا	Statistics Apps	-	General Prope	rties	Address: 198.51.100	.example.com .37]
S C	DNS		Product		Translation:		(Optional)
Ĭ	Delivery	×	Data Center		Link: Auto-Select	\checkmark	
	Zanao	Clic	k"Add		198.51.100.37		
	Zones		Prober Fallba				
	Caches	<u> </u>	State				
	Settings	•	Devices		Delete		
6	SSL Orchestrator				Design House		OK Cancel
A 💫	Acceleration		No	data ava	lable in table		iress
	Device Management					Click"OK	•
	letwork						
8 P 5	System						

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	: Jul 20, 2017 User: admin a: 6:13 PM (CDT) Role: Administra	tor Partition: Common
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » GSLB : Servers : Server	List » New Server
Statistics		
iApps	General Properties	
	Name	sitez_na_pair
S 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		
C	Devices	lick "Add"
SSL Orchestrator	Add	
Acceleration	De	vice name Auuress
Acceleration	bigip1.site2.example.co	om 198.51.100.37
Device Management	System	
Network		
System	Edit Delete	

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

Hostr IP Ad	name: gtm1.site1.example.com Idress: 10.1.10.13	Date: Time:	Jul 20, 2017 6:22 PM (CD1	User: T) Role:	admin Administrator			Partition: Common
ſ	ONLINE (ACTIVE) Standalone							
Ma	ain Help About		DNS » GS	LB : Server	s : Server List »	New Server		
<u>~</u>	Statistics		_		-Dovico Namo	v higin] oito] overnel		1
I	Apps		General Pro	perties	Address:	198.51.100.38	e.com]
()	DNS		Product		Translation:			(Optional)
	Delivery	è.		in .	2 ^{1k:}	Auto-Select 🗸		
	GSLB	C		erence	Add			
	Zones	÷	Prober Fall	back	198.51.100.3	38		
	Caches	•	State					
	Settings	•	Devices		Delete			
6	SSL Orchestrator						3	OK Cancel
	Acceleration		r	bigip1.site2.e	Device Na example.com	ame	198.51.1 0.37	ddress
a (Device Management		BIG-IP System Devices				Click"	<mark>ok"</mark>
	Network							
80	System							

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

Hostname: gtm1.site1.example.com Dai IP Address: 10.1.10.13 Tim	te: Jul 20, 2017 ne: 7:55 PM (CI	'User: admin DT) Role: Administra	tor	Partition: Common	
ONLINE (ACTIVE) Standalone					
Main Help About	DNS » G	SLB : Servers : Server	List » New Server		
Statistics	General Pr	operties			
iApps	Name		site2_ha_pair		
S DNS	Product		BIG-IP System	2	
Delivery	Data Cer	nter	site2_datacenter		
GSLB	Prober Pro	eference	Inherit From Data Center	Y	
Zones	Prober Fa	llback	Inherit From Data Center	v	
Caches	State		Enabled V		
Settings	Devices				
SSL Orchestrator		Add			
Acceleration		bigip1.site2.example.co	om	198.51.100.37	
Device Management	BIG-IP System	bigip2.site2.example.com 198.51.		198.51.100.38	
Natwork	Devices				
Network		Edit Delete			
System					
	Configurat	ion: Advanced			
	Health Mo	onitors	Selected //Common bigip	Available /Common gateway_icmp y http / v http_head_f5	
	Availability	y Requirements	All Health Monitors		

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

Resources Virtual Server Discovery Enabled Link Discovery Enabled Cancel Repeat

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	ame: gtm1.site1.exam dress: 10.1.10.13	ple.com Date: Time	Jun 25, 2017 3:36 PM (CDT)	User: ad Role: Ad	idmin Administrator
C	ONLINE (ACT Standalone	TVE)			
Ma	in Help	About	DNS » GSLB:	Servers :	: Trusted Server Certificates
M_ 1	Statistics		🔅 🚽 Server Lis		Trusted Server Certificates Statistics
I	Apps		General Propertie	s	
\$3 I	DNS		Name		server
	Delivery	•	Partition / Path		
	GSLB	•	Wide IPs	F	gtm1.site2.example.com, MyCompany bigip2.site1.example.com, MyCompany
	Zones		Pools	F	bigip1.site2.example.com, MyCompany bigip2.site2.example.com, MyCompany
	Caches		iRules	\odot	gun iste i.example.com, wycompany
	Settings	F	Data Centers	Þ	
E		7	Servers	×	Server List 🕘
	SL Orchestrator		Links		Trusted Server
	Acceleration	K	Prober Pools	,	Certificates GMT
			Monitors	(\cdot)	Statistics
	Device Management		Topology		234963207
					Common Name: atm1 site? 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**

Hostname: gtm1.site1.example.com IP Address: 10.1.10.13	Date: Jul 26, 2018 Time: 3:58 PM (EDT) Partition: Commo	Don 🔽 Log out
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » GSLB : Pools : Pool List	
Statistics	Pool List Statisti	cs 🔎
iApps	k	× Search Create
S DNS	Status 🗢 Name 💠	Type Members
Delivery	No records to display.	
GSLB 🚹 🔺	Wide IPs	
Zones	Pools Pool L	ist 💿
Caches	iRules 📀 Statist	ics 🗵
Settings	Data Centers	
	Servers	
Acceleration	Links	
Device Management	Prober Pools	

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

IP A	name: g ddress: 1	ptm1.site1.exam 10.1.10.13	i ple.com Da Tir	ate: Jul 26, 2018 me: 4:11 PM (EDT)	User: admin Role: Administr	ator			Partition	Common	$\mathbf{\overline{\mathbf{v}}}$	Log out
	5	ONLINE (ACT Standalone	TVE)									
м	lain	Help	About	DNS » GSLB	: Pools : Pool Li	st » New Pool						
	Statistic	CS		General Proper	ties							
	iApps			Name		www.example.com	_pool	×				
5	DNS			State		Enabled V						
	Deliv	ery	>	Configuration								
	GSLE	В	÷	Configuration		Selected		Available				
	Zone	s	Þ			Selected	/Co	ommon				
	Cach	les	•	Health Monitor	5		<u><</u> 9	ateway_icmp tp	^			
	Settir	ngs	+				>> n h	ttp_head_f5	~			
	Acceler	ation				Up Down						
	Accelet	auon		Availability Rec	quirements	All Health Monitors	~					
	Device	Management				Bits:	Disabled V	1				
	Networi	k		Limit Settings		Packets: Current Connections	Disabled V Disabled V	l I				
8	System			Manual Resum	1e							
				TTL		30						
				Dynamic Ratio								
				Maximum Ans	wers Returned	1						
				Verify Member	Availability	•						
				Members		Selec	t two	LTM VI	P's i	and cl	i ck "/	Add"
				Load Balancing Method	Preferred: Roun Alternate: Roun Fallback: Retur	d Robin V d Robin V n to DNS V						
				Fallback IP	0.0.0.0							
				Member List	Virtual Server: s Ratio: Add /Common/isp1_ /Common/isp2 Delete Up Do	elect 1 site 1_www.example.co site 2_www.example.co	m_tcp_https_ m_tcp_https_	virtual (/Comm virtual (/Comm	on/site1_ on/site2_	ha-pair) - 203 ha-pair) - 196	.0.113.9:4 .51.100.4	43, Ratio(1) 1:443, Ratio(1)

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".

Hostname: gtm1.site1.example.com IP Address: 10.1.10.13	Date: Jun 25, 2017 User: admin Fime: 8:49 PM (CDT) Role: Administrator
ONLINE (ACTIVE) Standalone	
Main Help About	DNS » GSLB : Wide IPs : Wide IP List
Statistics	transformation and the statistics Image: The statistics Image: The statistic and th
iApps	* × Search
S DNS	Status 🔺 Name
Delivery	www.gslb.example.com
GSLB	Vide IPs → Wide IP List 💽
Zones	Pools > Statistics >
Caches	IRules 📀
Settings	Data Centers
SSI Orchestrator	Servers
33E Orchestrator	Links
Acceleration	Prober Pools
Device Management	Monitors 🕞
	Topology
Network	Distributed Applications
System	

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 Documentation

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Tim	te: Jul 29, 2018 User: admin ne: 4:13 PM (EDT) Role: Administra	ator Partition: Common V
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » GSLB : Wide IPs : Wide	PList » New
Statistics		
iAnns	General Properties: Advanced	
Co Indulto	Name	www.example.com
S DNS	Туре	A
Delivery	Description	
GSLB		Alias: www.gslb.example.com
Zones		Add
Caches	Alias List	www.gsib.example.com
Settings		
Acceleration		Delete
Device Management	State	Enabled V
	Minimal Response	Enabled V
Network	Return Code On Failure	Disabled
System	Load-Balancing Decision Log	 ✓ Pool Selection ✓ Pool Traversal ✓ Pool Member Selection ✓ Pool Member Traversal
	iRules	
		Selected Available
For trouble	eshooting enable	<
verbose	logging	Selected Available
	iRule List	Vp Down
	Pools	
	Load Balancing Method	Round Robin
	Persistence	Disabled
58		Chapter 2. Class 1 - Intro to GSLB 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	Deskton Connection		
		DNS Mana	ger	
BIG-IP Edge	File Action View Help	New Host 🛛 🗙		
Client	🗢 🔿 🗾 🖬 🖸	Name (uses parent domain name if blank):		
agility_pub	▲ DNS ▲ ☐ DC01 ▲ ☐ Forward Lookup Zon	ns2 Fully qualified domain name (FQDN):	Data	Time:
1	▷ _msdcs.EXAMPLE ▲ C EXAMPLE.COM ▷ msdcs	IP address: [198.51.100.40]		
agility_prv	▷	✓ Create associated pointer (PTR) record Allow any authenticated user to update DNS records with the same owner name		
Putty (64-bi	▷ ☐ ForestDnsZon ▷ ☐ mgmt ▷ ☐ site1 ▷ ☐ site2 ▷ ☐ Reverse Lookup Zone	Add Host Done	[152], dc01.example.com., dc01.example.com. ns1.branch01.example.com. 10.1.70.200	static static static 6/26/
Notepad++	 ▷ ⁽¹⁾ Trust Points ▷ ⁽¹⁾ Conditional Forwarde ▷ ⁽¹⁾ Global Logs 	rs dc01 Host (A)	10.1.71.100 10.1.70.200 203.0.113.9	6/26/ static static
P	< III	Host (A)	203.0.113.8	
/// Start	🥖 🏹 🖸 💿 📼 🖉			

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

堤 DC01 - 10.1.70.200 - Remote Desktop Connection			
ă.	DNS Mar	nager	
File Action View Help			
◆ → 2 📷 🗙 🖬 Q 🕞 🛛 🚛 🗄 🖬 🖏			
DNS DC01 Forward Lookup Zones Forward Lookup Zones Condi Con	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	Timestamp static static static 6/26/2017 12:00:00 / 6/26/2017 12:00:00 / static
Lreate a new delegated DNS domain.			

2. Create the "gslb" subdomain.



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

- 10.1.70.200 - Remote Desktop Connection	
	DNS Manager
ction View Help	New Delegation Wizard
	Name Servers You can select one or more name servers to host the delegated zone.
Forward Lookup Zones sites tcp EXAMPLE.COM udp	Specify the names and IP addresses of the DNS servers you want to have host the delegated zone. Name servers:
 Conditional Forwarders Conditional Forwarders Conditional Forwarders Conditional Forwarders Conditional Forwarders DemainDacos DomainDnsZones DomainDnsZones DomainDnsZones DomainDnsZones PorestDnsZones PorestDn	Server Fully Qualified Domain Name (FQDN) IP Address ns1.example.com. [203.0.113.8] Add Edit Remove Add Edit Cancel
	Host (A) 198.51.100.40

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 Manager	
on View Help		New Delegation Wizard	x
I Forward Lookup Zones msdcs.EXAMPLE.CC EXAMPLE.COM Campados Sites	Name msdcs sites tcp udp branch01 DomainDnsZones ForestDnsZones	Name Servers You can select one or more name servers to host the delegated zone. 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]	
 iiii branch01 iiii DomainDnsZones iiiiii ForestDnsZones iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	 mgmt site1 site2 (same as parent folder) client01 dc01 	Add Edit Remove < Back Next > Can	cel
Global Logs	ns1 ns2	Host (A) 198.51.100.40	
			•

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 De	sktop Connection			
å.		DN	IS Manager	
File Action View Help				
🗢 🔿 🖄 📷 🗶 🖼 🔒 🛽	? 🖬 🗎 🗐 🖏			
 DNS DC01 Forward Lookup Zones msdcs.EXAMPLE.CC EXAMPLE.COM msdcs sites sites sites pomainDnsZones ForestDnsZones mgmt site1 site2 gibb Reverse Lookup Zones Trust Points Conditional Forwarders file Global Logs 	Name	der) Start of Authority (der) Name Server (NS) der) Name Server (NS) der) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A)	(SOA) [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 Å 6/26/2017 12:00:00 Å static
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"

File Action View Help File DNS Image: Constrained action Image: Const
File Action View Help Image: Second sec
Image: Second
Name Type Data Timestamp Image: DC01 Image: DC01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01 Image: Dc01
Conditional Forwarders Conditional Forwarders Conditional Forwarders Conditional Logs Conditional Logs Conditional Logs Conditional Forwarders Conditional Forw

2.7 Results

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

2.	Command Prompt
(64-bit)	;; MSG SIZE rcvd: 72 C:\Users\user.EXAMPLE>dig www.example.com
} ad++	; <<>> DiG 9.3.2 <<>> www.cxample.com ;; global options: printcmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 838 ;; flags: gr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
	;; QUESTION SECTION: ;www.example.com. IN A
Firef	WWW.example.com. 3600 IN CNAME www.gslb.example.com. 300 IN A 203.0.113.9
gle	;; Query time: 31 msc. ;; SERUER: 10.1.70.209 53(10.1.70.200) ;; WHEN: Sun Jun 25 21:37:31 2017 ;; MSG SIZE rcvd: 72
me	C:\Users\user.EXPIPLE>dig www.example.com
le Bin	

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 Da IP Address: 10.1.10.13 Tin	te: Jul 17, 2017 User: ad ne: 11:41 AM (CDT) Role: Ad	I min Iministrator	
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » GSLB : Wide IPs :	Wide IP List » Properties : www.	gslb.example.com : A
Magazina Statistics	🔅 👻 Properties	iRules Pools	Statistics
iApps	General Properties: Advance	ced 🗸	
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	Data centers	Add	
6 martin	Servers		
SSL Orchestrapr	Links		
Acceleration	Prober Pools	Delete	
Device Management	Monitors 🕞	Available (Enabled) - Avail	able
bence management	Topology >		
Retwork	Distributed Applications	Enabled V	
System	Return Code On Failure	Disabled	

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Ti	ate: Jul 17, 2017 User: admir me: 11:45 AM (CDT) Role: Admir	n nistrator			
ONLINE (ACTIVE) Standalone	_				
Main Help About	Statistics » Module Statistic	s:DNS:GSLB » V	Vide IPs : www.gslb	.example.com : A	
Statistics	🔅 🗸 Traffic Summary 👻	DNS -	Network	Memory	Syst
Dashboard					
Module Statistics	Display Options				
Analytics	Data Format	Normalized 🗸			
Performance	Auto Refresh	Disabled 🗸	Refresh		
iApps	<< Back Clear Statistics				
S DNS	Requests				
e	Total	12			
SSL Orchestrator	Persisted	0			
Acceleration	Resolved	12	_		
_	Dropped	0			
Device Management	Load Balancing				
Network	Preferred	12			
TE Custom	Alternate	0			
System	Fallback	0			
	CNAME Resolutions	0			

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 1 2:52 AM (CDT)	User: admin Role: Administrat				
10.1.10.23	Click refi	resh to see updat	ed interface	status.		
Main Help About	Network » Intert	aces : Interface	List			
Mage Statistics	🔅 👻 Interface L	ist Interfac	e Mirroring	LLDP 👻	Statistics	
iApps	Interfaces					
S DNS	🖌 🗢 Status -	 Name 			MAC Address	A Medi A
SSI Orchestrator	DISABLED	1.1			2c:c2:60:59:ec:f5	10000
33L 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					
Network			Sele	ct and disa	ble all interf	aces
Interfaces	Interface List					
Router	Interface Mirroring					
Setf IPs 📀	LLDP	•				
Preket 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

IP #	stname: gtm1.site1.example.com I Address: 10.1.10.13	Date: Jul 17, 2 Time: 12:32 Pl	017 User: M (CDT) Role:	admin Administrator			Partitio	n: Common	L C
ſ	ONLINE (ACTIVE) Standalone								
N	Main Help About	Statist	ics » Module St	atistics : DNS : GS	LB » Pools : www.ex	ample.com_pool : A			
	Statistics	* •	Traffic Summary	▼ DNS	 Network 	Memory			
	Dashboard								
	Module Statistics	Display	Options						
	Analytics	Data F	ormat	Normaliz	ed 🔽				
	Performance	Auto R	tefresh	Disabled	✓ Refresh				
-	iApps	<< Ba	<u>ck</u>						
53	DNS	Pool De	tails: "www.exan	nple.com_pool : A"			_	Lo	n Po
e		Status	Pool Member	Server	Virtual Server			Dreferred	1 A 6
the second se	6.61 Orchostrator							· Fieleneu	
	SSL Orchestrator	•	198.51.100.41:44	43 site2_ha-pair	/Common/isp2_site2_	www.example.com_tcp_https_	virtual	43	0
	SSL Orchestrator	0	198.51.100.41:44 203.0.113.9:443	43 site2_ha-pair site1_ha-pair	/Common/isp2_site2 /Common/isp1_site1	www.example.com_tcp_https_ www.example.com_tcp_https_	virtual virtual	43 44	0
	SSL Orchestrator Acceleration Device Management	•	198.51.100.41:4- 203.0.113.9:443	43 site2_ha-pair site1_ha-pair	/Common/isp2_site2_ /Common/isp1_site1_	www.example.com_tcp_https_ www.example.com_tcp_https_	virtual	43 44	0
	SSL Orchestrator Acceleration Device Management Network	0	198.51.100.41:4 203.0.113.9:443	43 site2_ha-pair site1_ha-pair	/Common/isp1_site1_ /Common/isp1_site1_	www.example.com_tcp_https_ www.example.com_tcp_https_	virtual	43 44	0
	SSL Orchestrator Acceleration Device Management Network System	•	198.51.100.41:4 203.0.113.9:443	43 site2_ha-pair site1_ha-pair	/Common/isp2_site2_ /Common/isp1_site1_	www.example.com_tcp_https_ www.example.com_tcp_https_	virtual (43 44	0
	SSL Orchestrator Acceleration Device Management Network System	•	198.51.100.41:4 203.0.113.9:443	43 site2_ha-pair site1_ha-pair	/Common/isp2_site2_ /Common/isp1_site1_	www.example.com_tcp_https_ www.example.com_tcp_https_	virtual (43 44	0

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 e: 4:14 PM (CDT) Role: Administrator	
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » GSLB : Wide IPs : Wide IP List	
Mage Statistics	₩ Wide IP List Statistics	
iApps	Click www.gslb.example.c	:om
😚 dns	Status - Name	Type
Delivery	www.gslb.example.com	A
GSLB	🛛 ide IPs 💦 🚽 🔞 Wide IP List 💿	
Zones	Pools Statistics	
Cache	itales 🕢	
Settin s	Data Centers	
6 martin	Servers >	
SSL Or negadior	Links	
Acceleration	Prober Pools	
Device Management	Monitors 📀	
Derice munugement	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: :: 4:18 PM (CDT) Role:	admin Administrator
Standalone		
Main Help About	DNS » GSLB: Wide IP	Ps : Wide IP List » Properties : www.gslb.example.com : A
Market Statistics	🚓 👻 Properties	iRules Pools Statistics -
iApps	General Properties: Adv	vanced
S DNS	Name	www.gslb.example.com
Delivery	Partition / Path	Common
GSLB	Туре	A
Zones	Description	
Caches		Alias:
Settings		Add
SSL Orchestrator	Alias List	
Acceleration		Delete
Device Management	Availability	Available (Enabled) - Available
	State	Enabled 🔽
Network	Minimal Response	Enabled 💌
System	Return Code On Epilure	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 Time	: Jul 17, 2017 User: admin : 4:53 PM (CDT) Role: Administra	ator	
CONLINE (ACTIVE) Standalone			
Main Help About	DNS » GSLB : Wide IPs : Wide	IP List » Members : www.gslb.	example.com : A
Mage Statistics	Properties iRules	e 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	~
SSL Orchestrator	Update		
Acceleration	Pools		
Device Management	✓ A Order Status \$ Pool	Name	
Network	Delete	xample.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 Tir	te: Jul 17, 2017 User: admin ne: 1:33 PM (CDT) Role: Administrator
ONLINE (ACTIVE) Standalone	
Main Help About	DNS » GSLB : Pools : Pool List
Statistics	Pool List Statistics I
iApps	* Search
S DNS	Status 🗢 Name
Delivery	www.example.com_pool
GSLB	Wide IPs
Zones	Pools Pool List 💿
Caches	iRules 🛞 Statistics 🗵
Settings	Data Centers
B. Market	Servers >
SSL Orchestrator	Links
Acceleration	Prober Pools
Device Management	Monitors 🕙
	Topology >
Retwork	Distributed Applications

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

Hostname: gtm1.site1.example.com Dat IP Address: 10.1.10.13 Tim	e: Jul 17, 2017 User: admin e: 1:51 PM (CDT) Role: Administra	ator			
Standalone				_	
Main Help About	DNS » GSLB : Pools : Pool Lis	t » Members : www.exa	mple.com_pool : /	λ.	
Mage Statistics	🔅 👻 Properties Memb	oers Statistics			
iApps	Load Balancing	Click	"Member	<mark>s</mark> "	
S DNS	Load Balancing Method	Preferred: Global Availat Alternate: Round Robin			-
Delivery		Fallback: Return to DNS	s 🔽		
GSLB	Fallback IP	0000			
Zones					
Caches	Update				
Settings					
e	Members				
SSL Orchestrator	Member Order Status	Member	Member Address	Partition	Merr
Acceleration	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
ONLINE (ACTIVE) Standalone	
Main Help About	Network » Interfaces : Interface List
Statistics	
iApps	Interfaces
S DNS	Status A Name
SSL Orchestrator	UP 1.1
Local Traffic	Disable Interface 1.6
Acceleration	UP 14
Device Management	DISABLED 1.6
	Enable Disable
Interfacer	anterface List
Routes	Interface Mirroring
Self IPs 📀	LLDP
Porket 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	e: Jul 17, 2017 User: admin ie: 8:52 PM (CDT) Role: Administrator
ONLINE (ACTIVE) Standalone	
Main Help About	DNS » GSLB : Links : Link List
Mage Statistics	tink List Statistics
iApps	* Search
(S) DN1	Status Address
Delivery	198.51.100.33 198.51.100.33
	Wide IPs
Zenes >	Pools
C ches	iRules 🕞
S ttings	Data Centers
e	Servers >
SS. Drchestrator	3 Links
Act Press	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
Main Statistics	terrace List Interface Mirroring LLDP - Statistics
iApps	Interfaces
S DNS	✓ ♦ Status ▲ Name
SSL Orchestrator	UP 1.1 UP 1.2
Local Traffic	□ UP 1.3 Enable Interface 1.6
Acceleration	UP 1.4
Device Management	
	UP 1.7 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 - Next Generation DNS Services

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

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

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

The F5 device is directly connected to the internet.

Below is a lab diagram and connectivity information:



3.1 Lab Components

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

Component	VLAN/IP Address(es)	Credentials
BIG-IP DNS	 Management: 10.1.1.4 External Self: 10.1.10.6 Internal Self: 10.1.20.6 	admin/agility2020
Ubuntu Desktop	 Management: 10.1.1.6 External: 10.1.10.4 	ubuntu/agility2020
Ubuntu server	 Management: 10.1.1.5 Internal: 10.1.20.4 	ubuntu/agility2020

Follow these steps to get your lab started:

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

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

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

3.1.1 Transparent Cache

Monitors

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

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

ONLINE (ACTIVE) Standalone				
Main Help About	DNS » Delivery : Load	Balancing : Monitors		
Magazina Statistics	🔅 👻 Monitor List			
iApps	1	× Search	Cre	ate
S DNS	✓ A Name		Application	💌 Ту
Delivery 🔒 🔋 🕨	Listeners			Gatew
GSLB	Profiles			HTTP
Zones	Load Balancing	Pools		HTTP
		Nadas		HTTP
Caches	IRules >	Nodes		HTTPS
Settings	Translation	Monitors 💽		HTTPS
Barrow	wameservers			ICMP
SSL OFCH PALLA	Keys >			Inband
Local Traffic	real_server			Real S

Create a new monitor according to the following settings:

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 🗸	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	ww.example.com					
Query Name	www.example.com						
Query Type	a 🔽						
Answer Section Contains	Query Type 🗸						
Accept RCODE	No Error 🔽						
Receive String							
Adaptive	Enabled						

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

Load Balancing

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

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

C		(ACTIVE) one							
Ma	ain Help	About	DNS » Delivery :	: Load I	Balancing : Po	ols : Pool List			
<u>~</u>	Statistics		🔅 👻 Pool List		Statistics				
i	iApps		*			× Search			Create
S	DNS		🗹 💌 Status 🔺	Name					\$ Des
	Delivery 1	•	Listeners	Þ	ateway_pool				
	GSLB	÷	Profiles	Þ					
	Zones		² Load Balancing		³ Pools		Pool List	÷	
	Caches		iRules		Nodes	F	Statistics		
	Settings		Trans' aion	Þ	Monitors	÷			
£	CCL Orehestert		Nameservers	÷.					
	SSL Orchestrato		Keys	Þ					
() ()	Local Traffic								

Create a pool according to the following table:

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

DNS » Delivery : Load Balanc	ing : Pools : Po	ool List » New P	ool			
Configuration: Basic 🔶						
Name	dns_pool	dns_pool				
Description						
		Active		Available		
Health Monitors	/Common example.	/Common /Common example.com_dns_monitor <				
Resources						
Load Balancing Method	Round Robi	n		¢		
Priority Group Activation	Disabled	¢				
	Node Name:	New Node Node N dns01_node	ew FQDN Noc	de (Optiona	l)	
	Address:	10.1.20.4				
New Members	Add	53 Sele	ect ¢			
	Node Name	Address/FQDN	Service Port	Auto Populate	Priority	
	dns01_node	10.1.20.4	53		0	
	Edit	elete				
Cancel Repeat Finished						

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

Results

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

CONLINE (ACTIVE) Standalone	
Main Help About	DNS » Delivery : Load Balancing : Pools : Pool List
Mage Statistics	
iApps	* × Search
S DNS	Status - Name
Delivery 1	Listeners
GSLB	Profiles ateway_pool
Zones	2 Load Balancing 3 Jols 4 Pool List 📀
Cachis	iRules Nodes Statistics 2
Settings	manslation Monitors 📀
SSL reportate	Nacruservers Keys
Local Traffic	

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

DNS	NS » Delivery : Load Balancing : Pools : Pool List » Members : dns_pool											
☆ -	Properties	Members	Statistics									
Load E	Balancing											
Load	Load Balancing Method Round Robin											
Priori	ty Group Activation	Disabled	•									
Upda	te											
Currer	Current Members Add											
	Status 🗢 Memb	er			 Address 	Service Port		Ephemeral	Ratio	Priority Group	Connection Limit	Partition / Path
	Image: optimized state dns01_node:53 10.1.20.4 53 No 1 0 (Active) 0 Common											
Enabl	Enable Disable Force Offline Remove											

tmsh show Itm pool dns_pool detail

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

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



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

Navigate to $\ensuremath{\text{DNS}}$ $\ensuremath{\text{\sc sc hes}}$ $\ensuremath{\text{\sc sc hes}}$ Cache List

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

Setting	Value
Name	transparent_cache
Resolver Type	Transparent

ONLINE (ACTIV	'E)	
Main Help	About	DNS » Caches : Cache List » New
Mage Statistics		
_		General Properties
iApps		Name transparent_cache
S DNS		Resolver Type Transparent (None)
Delivery	Þ	DNS Cache
Zones	×	Message Cache Size 1048576 bytes
Caches		Cache List O Size 10485760 bytes
rettings		Statistics
SSI orchestrator		RRSet Rotate none
Local Traffic		Cancel Repeat Finished

tmsh create ltm dns cache transparent transparent_cache

3.1.2 Listeners

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

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

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

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



Log Profile

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

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

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

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

CONLINE (AC	:TIVE)						
Main Help	About S	system » Lo	ogs : Config	uration : Log Publisher	S		
Mage Statistics		🔅 🚽 System		Captured Transactions	Packet Filter	GSLB	Audit
iApps				Click "Cre	ate"		reate
S DNS		A Name				5	
	C	default-ip	sec-log-publ	isher			
SSL Orchestrator		local-db-p	oublisher				
Acceleration		sys-db-ad	cess-publist	ner			
Device Managemen		sys-sso-a	ccess-publis	sher			
Device management	<u> </u>	Delete					
Retwork							
System 1 Configuration File Management Certificate Manage Disk Management Software Manage License Resource Provisio Platform High Availability Archives Services Preferences sFlow SNMP Crypto Offloadir Users Logs	ment mining Sy Ca	stem ptu ed Trans cke Filter cal Traffic SLB dit 3 annfiguration	actions	Options Remote Logging Log Filters (L 4 stinations (Log Publishers (9		

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

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

ONLINE (ACTIVE) Standalone	
Main Help About	System
Statistics	
_	General Properties
iApps	Name local-syslog-publisher
S DNS	Description
SSL Orchestrator	Log Destinations
Acceleration	Selected Available
Device Management	Destinations
Network	
System	Cancer Repeat Pinished

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
				_	- 33 3

ſ	Stand	NE (ACTIVE) Jalone				CI	ick"Creat	te"	
N	lain H	elp About	DNS » Delivery :	Profile	s : Other : DNS	5 Logging			
M	Statistics		DNS		Protocol	→ Othe	ir 🔹		
6	iApps		4			× Search			Create
Ê	Wizards		🖌 🕈 Name						
	DNC		No records to displa	ay.					
	DNS		Delete						
	Delivery	•	Listeners	÷					
	GSLB	Þ	Profiles	•	DNS	÷			
	Zones		Load Balancing	Þ	Protocol	Þ			
	Caches		iRules		Other		DNS Logging	•	
	Settings		Translation	Þ			Persistence	÷	
e		1/-	Nameservers	Þ			Statistics	(\cdot)	
	SSL Orchestr	ator	Keys	F					
<u>(</u>	Local Traffic								

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

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

ONLINE (AC' Standalone	TIVE)				
Main Help	About	DNS » Delivery : Profiles : Othe	er : DNS Logging » New		
Statistics		General Properties			
iApps		Name	example_dns_logging_profile		
Wizards		Description			
Configuration					
Delivery	•	Log Publisher	local-syslog-publisher		
GSLB	•	Log Queries	✓ Enabled		
Zones	•	Log Responses	Enabled		
Caches	÷	Log Fields			
Settings	•	Include Complete Answer	C Enabled		
SSI Orchestrator		Include Query ID	🗹 Enabled		
33L Orchestrator		Include Source	Z Enabled		
Local Traffic		Include Timestamp	I Enabled		
Traffic Intelligence		Include View	Enabled		
Acceleration		Cancel Repeat Finished			

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

DNS Profile

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

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

Navigate to: DNS >> Delivery : Profiles : DNS

ONLINE (ACTIVE) Standalone	
Main Help About	DNS » Delivery : Profiles : DNS
Mage Statistics	
iApps	* × Search Create
izards	✓ ▲ Name
😚 dns	Delete
Delivery >	Listeners
GSLB	Profiles ONS 📀
Zones	Load Balancing
Caches	iRules > Other >
Settings	Translation
6 martine	Nameservers
SSL Orchestrator	Keys >
Local Traffic	

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

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

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

Hostname: router01.branch01.example.com IP Address: 10.1.10.31	Date: Jul 25, 2017 User: Time: 11:40 PM (CDT) Role:	admin Partition: Common V	out
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Delivery : Profiles : DI	NS » New DNS Profile	
Statistics	General Properties		
iApps	Name	example.com_dns_	
E Wizards	Parent Profile	dns	
S DNS	Denial of Service Protection	Custo	m 🗆
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	
	GSLB	Enabled 🔽	
	DNS Express	Enabled 🔽	
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	Disabled V	
System	DNS Traffic		
	Zone Transfer	Disabled	
	DNS Security	Disabled	
	DNS Security Profile Name	Select	
	Process Recursion Desired	Enabled V	
	Logging and Reporting		
	Logging		
	Logging Profile	example_dns_logging_profile	1
	AVR Statistics Sample Rate	Enabled 1/ 1 queries sampled	

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

UDP Profile

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

(5	NLINE (AC tandalone	TIVE)									
N	Nain	Help	About		DNS » Delive	ry : Profile	s : Protocol :	UDP				
~	Statistics				DNS		Protocol	-	Other	Click	"Create	۳
	iApps				ł			× Searc	:h			Create
Ê	Wizards				Aname 🖉							
	DNS				🛄 udp							
					udp_decre	ment_ttl						
	Delivery				Listeners	Þ						
	GSLB	T-		-	2 Profiles	•	DNS	(Ð			
	Zones			Λ	Load Balancing	,	Protocol		•	UDP 4	•	
	Caches			•	iRules		Other			ТСР	÷	
	Settings			\mathbf{F}	Translation	Þ						
e				/	Nameservers	Þ						
	SSL Urche	strato			Keys	Þ						
C -D	Local Traf	fič										

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

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

Setting	Value
Name	example.com_udp-dns_profile
Parent Profile	udp_gtm_dns

ONLINE (ACTIVE) Standalone							
Main Help About DNS » Delivery : Profiles : Protocol : UDP » New UDP Profile							
Statistics							
	General Properties						
IApps	Name	example.com_udp-					
izards 📔	udp_gtm_dns						
😚 dns	Settings						
Delivery	Proxy Maximum Segment						
GSLB	Idle Timeout	Specify 5 seconds					
Zones	IP ToS	Specify 🔽 0					
Caches	Link QoS	Specify 🔽 0					
Settings	Datagram LB	Enabled					
S man had	Allow No Payload						
SSL Orchestrator	TTL Mode	Proxy 🗸					
Local Traffic	Don't Fragment Mode	PMTU 🔽					
Traffic Intelligence	Cancel Repeat Finished						

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

TCP Profile

Like the UDP profile, a TCP profile controls properties of TCP connections on the BIG-IP. Navigate to: **DNS** >> **Delivery : Profiles : Protocol : TCP**

ONLINE (ACTIVE) Standalone							
Main Help About	DNS » Delivery : Pro	files : Protocol : TCP					
Mage Statistics	DNS	Protocol - Othe	Click "Create"				
iApps	r × Search Create						
iii Wizards	Vame 🖉						
	apm-forwarding-client-tcp						
DNS	apm-forwarding-server-tcp						
Delivery >	Listeners	▶ s_profile					
GSLB	Profiles	DNS 💮					
Zones	Load Balancing	≽ Protocol 🛛 🔸	UDP 💮				
Caches	ixules	> Other	тср 💿				
Setti	ranslation	•					
e	Nameservers	ed					
SSL Orchestrator	Keys	-tcp-lan_profile					

Create a TCP profile as shown in the following table.

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

	ONLINE (ACTIVE) Standalone		
Ma	ain Help About	Local Traffic » Profiles : Proto	col : TCP » New TCP Profile
Statistics		General Properties	
i 🤤	Apps	Name	example.com_tcp-
()	DNS	Parent Profile	f5-tcp-lan
6	SSL Orchestrator	Timer Management	
		Close Wait	Specify 5 seconds
	Natural Mar	Fin Wait 1	Specify V 5 seconds
	Virtual Sonrors	Fin Wait 2	Specify 💙 300 seconds
	Policies	Idle Timeout	Specify V 300 seconds
	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 V 20000 milliseconds
Traffic Class			

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

UDP Listener

Now that all of our profiles are created, we can create our listeners starting with the UDP listener. Navigate to: **DNS** >> **Delivery : Listeners : Listener List**



Create a UDP listener according to the tables below:

Setting	Value
Name	udp_53_virtual
Destination Address	10.1.10.53
Service Port (Advanced Settings)	DNS 53
VLAN and Tunnel Traffic -> Enabled on	external
Address Translation	Enabled
Protocol	UDP
Protocol Profile (Client)	example.com_udp-dns_profile
DNS Profile	example.com_dns_profile
Default Pool	dns_pool

Main Help About	DNS » Delivery : Listeners : Listener List » New						
Mage Statistics							
-	General						
iApps	Name	udp_53_virtual					
😚 dns	Description						
Delivery	State	Enabled \$					
GSLB	Listener: Advanced \$						
Zones	Destination	Type: • Host Network					
Caches	Destination	Address: 10.1.10.53					
Settings	Service Port	DNS \$ 53					
Local Traffic	VLAN Traffic	udp_53_virtual Enabled \$ Type: Host Nos \$ 53 Enabled on \$ Selected Available /Common internal socks-tunnel None \$ Enabled Enabled Enabled Enabled Default \$ None \$ UDP \$ example.com_udp-dns_profile \$ (Use Client Profile) \$ example.com_dns_profile \$					
Acceleration	VLANs and Tunnels	Selected Available /Common /Common external <					
Device Management		>> internal socks-tunnel					
Shared Objects	Source Address Translation	None 🗘					
Network	Address Translation	Enabled					
The System	Port Translation	Enabled					
ST System	Route Advertisement	Enabled					
	Auto Last Hop	Default \$					
	Last Hop Pool	None					
	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	(dns_pool \$					
	Default Persistence Profile	None					
	Fallback Persistence Profile	None \$					

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

TCP Listeners

Next, create the TCP listener

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



Create two TCP listeners according to the table below:

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

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

Main Help About	DNS » Delivery : Listeners : L	stener List » New					
Mage Statistics							
	General						
[] IApps	Name	tcp_53_virtual					
S DNS	Description						
Delivery	State	Enabled \$					
GSLB	Listener: Advanced \$						
Zones > Caches >	Destination	Type: OHost Network Address: 10.1.10.53					
Settings	Service Port	DNS \$ 53					
Local Traffic	VLAN Traffic	Enabled on \$					
Traffic Intelligence	VLANs and Tunnels	Selected Available /Common /Common external <					
Acceleration		>> internal socks-tunnel					
Subscriber Management	Source Address Translation	(None 🛊					
Device Management	Address Translation						
Shared Objects	Port Translation Enabled						
Shared Objects	Route Advertisement	Enabled					
Security	Auto Last Hop	Default \$					
Network	Last Hop Pool	None 🗘					
	Service: Advanced \$						
System	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 dns_pool ¢						
	Default Persistence Profile	None \$					
	Fallback Persistence Profile	None 🗘					

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

Results

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

Repeat some of the same queries multiple times

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

2. Viewing Cache Statistics

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

ſ	Standalone	VE)											
N	lain Help	About	Statistics » Module Statisti	cs:DNS:Ca	ches » Caches								
<u>~</u>	Statistics		🔅 👻 Traffic Summary 👻	DNS	 Local Traffic 	: •	Network	Memory		System			
	Dashboard	_											
	Module Statistics	•	Display Options	_									
	Analytics	÷	Statistics Type	Caches	\checkmark								
	Performance	÷	Data Format	Normaliz	ted 🗸								
	iApps		Auto Refresh	Disabled	Refresh								
Lø			Common/transparent cache		Search Reset Search	h		DNS Quar				Failur	
\bigcirc	DNS		✓ A Name		Partition / Path	Details	¢ Queries	+ Responses	Sync	Async	Resolve	¢ Connect	\$
6	SSL Orchestrator		transparent_cache		Common	View	7	4	4	0	0	0	0
(<u>)</u>	Local Traffic		Reset Clear Cache										
	Acceleration												
	Device Management			Cli	<u>ck Vie</u>	W	/						
	Network												
	System												

Examine the Query, Failure, and Cache details below.

	ONLINE (ACT	TVE)									
M	ain Help	About	Statistics » Module Statistics	: DNS : Caches »	Caches : transparent_cac	he					
M	Statistics		🔅 👻 Summary								
	Dashboard	e.									
	Module Statistics	Þ	Display Options								
	Analytics	Þ	Data Format	Normalized 🗸							
	Performance	Þ	Auto Refresh	Disabled 🗸	Refresh						
	iApps		<< Back Clear Statistics								
	DNS		Query Details								
			Queries	7							
	SSL Orchestrator		Responses	4							
n:n			Synchronous Responses	Synchronous Responses 4							
	A		Asynchronous Responses	Asynchronous Responses 0							
~	Acceleration		Failure Details								
	Device Management		Resolve	0	•						
			Connection	0							
	Network		Server	0							
8 🕈	System		Send	0							
			Cache Details	Hits	Misses	Inserts	Updates	Evictions			
			DNS Message Cache	4	3	0	0	0			
			Resource Record Cache	0	15	0	0	0			

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

the following TMSH command:

TMSH

tmsh show Itm dns cache records rrset cache transparent_cache

root@(ip-10-1-1-4)(cfg-sync St	andalon	e)(Acti	ve)(/Co	mmon)(tmos)# show ltm dns cache records rrset cache transparent_cache				
tm::DNS-Cache/Resolver RR Records								
	TTL	Туре	Class	rdata				
dyna.wikimedia.org.	225	A	IN	198.35.26.96				
www.wikipedia.org.	86025	CNAME	IN	dyna.wikimedia.org.				
wikimedia.org.	86025	NS	IN	ns1.wikimedia.org.				
wikimedia.org.	86025	NS	IN	ns0.wikimedia.org.				
wikimedia.org.	86025	NS	IN	ns2.wikimedia.org.				
dwbfwz8xncgmg.cloudfront.net.	24	A	IN	13.224.29.57				
dwbfwz8xncgmg.cloudfront.net.	24	A	IN	13.224.29.121				
dwbfwz8xncgmg.cloudfront.net.	24	A	IN	13.224.29.79				
dwbfwz8xncgmg.cloudfront.net.	24	A	IN	13.224.29.75				
dwbfwz8xncgmg.cloudfront.net.	1273	NS	IN	ns-1645.awsdns-13.co.uk.				
dwbfwz8xncgmg.cloudfront.net.	1273	NS	IN	ns-111.awsdns-13.com.				
dwbfwz8xncgmg.cloudfront.net.	1273	NS	IN	ns-1438.awsdns-51.org.				
dwbfwz8xncgmg.cloudfront.net.	1273	NS	IN	ns-683.awsdns-21.net.				
Total records returned (tmm2):	13							

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

TMSH

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

4. Back End Visibility

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

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

```
tcpdump -nni eth1 port 53
Hit *Control-C* to exit the *tcpdump*
```

3.1.3 DNS Express with a Hidden Master

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


Name Server

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

Navigate to DNS » Delivery : Nameservers : Nameserver List

	ONLINE (A(CTIVE)							
M	ain Help	About	DNS » Delivery :	Names	ervers : Nameserve	r List			
Statistics			🔅 🗸 Nameserve	r List	Statistics 🛛 🖸	0			
3	iApps		*		×S	earch			
5	DNS		✓ ▲ Name	Address	Port	≑ TSIG			
	Delivery	•	Listeners	+					
	GSLB	+	Profiles	F					
	Zones	+	Load Balancing	Þ					
	Caches	+	iRules	Þ					
	Settings	+	Translation	F					
SSL Orchestrator			Nameservers		Nameserver List	•			
			Keve		Statistics	A			
0-0									

Create a nameserver according to the following table:

Setting	Value
Name	master.example.com
Address	10.1.20.4

	Firew ONLI Stand	all: Cons NE (ACTI Ialone	sistent IVE)							
Ma	in He	elp	About	DNS »	Delivery : Namese	rvers :	Nameserve	r List » Ne	w Nameserver	
s	Statistics			General	Properties					
Lig I	Apps			Name			master.example.com			
S DNS				Addre	SS		10.1.20.4			
	Delivery			Servic	e Port		53	Other:	\$	
	GSLB			Configu	ration					
	Zones			Route	Domain	1	0 🔹			
Caches Settings		TSICK	· · · · · · · · · · · · · · · · · · ·		Nono A					
		1310 K	ISIG Key None ¢							
R-9 1	ocal Traffic			Cancel	Repeat Finishe	be				

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

DNS Express

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

Navigate to DNS >> Zones : Zones : Zone List

ſ	ONLINE (ACT	IVE)											
Ma	ain Help	About	DNS » Zones : Zone List										
- 	Statistics		🔅 👻 Zone List	Statistics									
i 🧓	Apps		*		× Search	Create							
5) I	DNS		Name										
	Delivery	•	No records to display.										
	GSLB		Delete										
	Zones	•	Zones	Zone List	•								
	Caches		NSSEC Zones	Statistics	Ø								
	Settings		ZoneRunne	Þ									
	SSL Orchestrator												
ı 1	ocal Traffic												

Create a DNS Express zone according to the following table:

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

		-								
Ma	ain Help About		DNS » Zones : Zones : Zone List » New Zone							
<u>M</u>	Statistics									
			General Properties							
Lig I	Apps		Name	example.com						
()	DNS		DNS Express							
	Delivery	•	Server	master.example.com						
	GSLB	•	Availability	Unknown						
	Zones	•	State	Enabled \$						
	Caches	•	Notify Action	Consume \$						
	Settings	•		Address: 10.1.20.4 Add						
(<u>)</u>	ocal Traffic			10.1.20.4						
י 🚊	raffic Intelligence									
	Acceleration			Delete						
-			Verify Notify TSIG	0						
2	Subscriber Management		Response Policy							

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

Results

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

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

Ma	in	Help	About		DNS » Zones : Zone List » Properties : example.com								
<u>^</u> s	Statistics			1	¤ -	Properties	Statis	tics 🗵					
1	Apps			G	General Properties								
S .	ONS			1	Name			example.com					
	Deliver	,		F	Partition / Path			Common					
	Delivery		P										
	GSLB			DI	IS E	xpress							
Zones			\$	Serve	r		master.example.com						
Caches			1	Availability			Available (Enabled) - Successful AXFR						
Settings				\$	State			Enabled \$					

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

- The **DB Dump** section of the **dnsxdump** utility output displays the zone information for all configured DNS Express zones.
- The DB Stats section of the dnsxdump utility output displays a cumulative count of records for all configured DNS Express zones.
- 1. From the Web Shell of SSH session to the BIG-IP:

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

#dnsxdump | less

Examine the results

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

#tail -100 /var/log/ltm | grep zxfrd

Database serial	number	1																	
DNS-Express DB [Dump																		
–= Arena Allocat	tor =-																		
-= Region Stats memory: 39 objec 0	=- ts (39 0000 0000 0000	small/0 0 0 0 0 0 0 0 0 0 0 0 0	large), 0000 0000 0000	1448 byt 0 0 0 0 0 0 0 0 0 0 0 0	es all 0 0 0 0 0 0 0 0 0	ocated 0 0 0 0 0 0 0 0 0	(41 000 00 000	waste 000 000 000	d) in 0 0 0 0 0 0 0 0	1 c 0 0 0 0 0 0	hunks 00 000 000	, 0 0 0 0 0 0 0	clea 0 0 0 0 0 0	inups 00 000 000	, 64 0 0 1 0 0 0 0	4 in 0 0 0 0 0 0	rec 00 00	ycleb 00 000 000	oin 0 0 0
-= DB Dump =- Domain: . Domain: com. Domain: example. example.com.	.com. 7200	IN	NS	master.	exampl	e.com													
example.com.	7200	IN	MX	10 mail	.examp	le.com	I												
example.com.	7200	IN	SOA	master.	exampl	e.com	maste	r.exa	mple.	com	20200	2020	0 21	.600	3600	0 60	4800	8640	0
Domain: mail.exa mail.example.com	ample.co n.	m. 7200	IN	A	10.1.	20.25													
Domain: master.e master.example.c	example. com.	com. 7200	IN	A	10.1.	20.4													
-= DB Stats =- RR Count: 5 Name Count: 5 RR Count by Type A: 2 NS: 1 SOA: 1 MX: 1	2:																		

3.1.4 DNSSec

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



Zone Signing Key

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

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

		(ACTIVE) one									
м	ain Help	About	DNS » Zones	DNSSEC	Zones : DNSSEC Z	one Lis	t				
Statistics			DNSSEC Zone List Statistics Click "Create"								
iApps			* Search Create								
S	DNS		Status	▲ Name							
	Delivery	Þ	Listeners	ŀ							
	GSLB		Profiles	, ∍t	e						
	Zones		Load Balancing	÷							
	Caches	Þ	iRules	÷							
	Settings		Translation	Þ							
e	CCI Orahantari		Nameservers	F							
SSL Orchestrator		er en	Keys	×.	TSIG Key List	÷					
(;;)	Local Traffic				DNSSEC Key List	•					
	Acceleration										
	Device Managen	nem									

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

CONLINE (ACTIVE) Standalone							
Main Help About	DNS » Delivery : Keys : DNSSEC Key List » New DNSSEC Key						
Statistics	General Properties						
IApps	Name	example.com_zsk					
🔁 Wizards	Туре	Zone Signing Key 🔻					
	State	Enabled •					
UN3	Hardware Security Module	None T					
Delivery	Algorithm	RSA/SHA1 T					
GSLB	Key Management	Manual 🔻					
Zones >	Key Cettings						
Caches	Cartificate	default ert					
Settings	Drivete Key	default key					
SSL Orchestrator	Cancel Repeat Finished						

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

Key Signing Key

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

ONLINE (ACTIVE) Standalone		
Main Help Abo	DNS » Zones : I	: DNSSEC Zones : DNSSEC Zone List
Statistics	DNSSEC 2	Click "Create"
iApps	*	Search Create
S DNS	Status -	▲ Name
Delivery	Listeners	Þ
GSLB	Profiles	ete
Zones	Load Balancing	b .
Caches	iRules	b .
Settings	Translation	b .
£	Nameservers	b .
SSL Orchestrator	Keys	TSIG Key List
Local Traffic		DNSSEC Key List 💿
Acceleration		
Device Management		

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

ONLINE (ACTIVE) Standalone		
Main Help About	DNS » Delivery : Keys : DNSSE	C Key List » New DNSSEC Key
Magazina Statistics		
_	General Properties	
iApps	Name	example.com_ksk
iii Wizards	Туре	Key Signing Key
S DNS	State	Enabled
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	

TMSH commands for Key Signing key creation:

TMSH

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

Signed Zone

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

	Standalone	CTIVE)	
м	lain Help	About	DNS » Zones : DNSSEC Zones : DNSSEC Zone List
~	Statistics		DNSSEC Zone List Statistics
	iApps		search
	DNS		Status A Name
	Delivery	•	No records to display.
	GSLB		Enable Disable Delete
	Zones	÷	Zones
	Caches	+	DNSSEC Zones DNSSEC Zone List
	Settings	F	ZoheRunner > Statistics >
6	SSL Orchestrator		
C ;1	Local Traffic		
	Acceleration		
	Device Manageme	1	

Create DNS Express zone signed by DNSSEC

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

Standalone	
Main Help About	DNS » Zones : DNSSEC Zones : DNSSEC Zone List » New DNSSEC Zone
Statistics	General Properties: Basic v example.com
iApps	Name example.com
😚 dns	State Enabled V
Delivery	Keys
GSLB	Active Available
Zones >	Zone Signing Key
Caches	
Settings	
SSL Orchestrator	Active Available Key Signing Key /Common example.com_ksk
Local Traffic	>>
Acceleration	Cancel Repeat Finished

TMSH commands for DNSSEC signed zone creation:

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

Results

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

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

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

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



3.1.5 Validating Resolver

Trust Anchors

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

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

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

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

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

Select the validating-resolver_cache and click "Trust Anchors"

C	5	ONLINE (AC Standalone	TIVE)							
N	lain	Help	About	DNS	s » Cach	es : Cache	List			
~	Statisti	cs		÷.	Cache	List	Statistics			
	iApps			*				Search		
53	DNS				Name					Resolve
_	Deliv	ery		, 🗆	validating	-resolver_c	ache			Validating
	GSL	3		Dele	ete					
	Zone	s		Þ						
	Cach	es 🕨		▶ Cache	e List	0	Eliek "	validating	-resolver_e	ache"
	Settir	ngs		> statis	tics	7				
e				1						
	SSL Or	chestrator		/						
2	Acceler	ation	$\mathbf{\lambda}$							
	Dovico	Management	\sim							
-	Device	manayement								
	5	ONLINE (AC Standalone	(TIVE)							
-	Main	Help	About	DN	s » Cach	ies : Cache	e List » Trust An	ichors : validating-re	esolver_cache	
M-	Statisti	cs		\$	- Prope	rties	Trust Anchors	DLV Anchors	Local Zones	Forward 2
	iApps						10			
	-			Trus	t Anchors	;			2	Add
0	DNS				Trust Ar	diaplay				
	Deli	very		Ro	move 1	display				
	GSL	В	Clic			nch	orell			
	Zone	es	CIIC	N 11	ust A	ALCHO	515		Click "Ac	ld"
	Cac	hes		×						
	Sett	ngs		•						

For each DS record, enter them as trust anchors:

DNS » Caches :	Cache List						
Add Trust Anchor							
							_
Trust Anchor		. IN DS 203	326 8 1 AE1EA	B974D4C858B	740BD03E3CED7E	BFCBD1724	<u>ا</u>
Cancel Repeat	Einished						
Cancer Repeat							
DNS » Caches : Cache	List » Trust Ancho	rs : validating-reso	lver_cache				
🔅 🚽 Properties	Trust Anchors	DLV Anchors	Local Zones	Forward Zones	Response Policy Zones	Statistics	⊿
Trust Anchors							
			50001701				
. IN DS 20326 8 1 AE	1EA5B974D4C858B7	40BD03E3CED7EB	FCBD1724				
. IN DS 20326 8 2 E06	5D44B80B8F1D39A9	5C0B0D7C65D084	58E880409BBC6834	57104237C7F8EC8D)		
Remove							

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

Modify DNS Profile

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

ſ	Standalone								
N	Main Help About	18	DNS » Delivery : Profiles : DNS	>>> Properties : example.com_dns_profile					
~	Statistics		🚓 🚽 Properties						
	iApps		General Properties						
Ê	Wizards		Name	example.com_dns_profile					
	DNS		Partition / Path	Common					
			Parent Profile	dns					
	Delivery	<u>}</u>	Denial of Service Protection						
	Zones		Rapid Response Mode	Disabled 🗸					
	Caches	- 	Rapid Response Last Action Drop						
	Settings	F	Hardware Acceleration						
ĥ	SSL Orchestrator		Protocol Validation	Disabled					
-			Response Cache	Disabled 🔽					
<u>(</u>))	Local Traffic		DNS Features	t the "validating-resolver_cache"					
Ê	Traffic Intelligence		DNSSEC	Enabled V					
3	Acceleration		GSLB	Enabled V					
	Access		DNS Express	Enabled 🔽					
			DNS Cache	Enabled 🔽					
=	Device Management		DNS Cache Name	validating-resolver_cache					
	Network		DNS IPv6 to IPv4	Disabled 🔽					

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

Results

Now lets look at results. Tail the Itm log on the BIG-IP

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

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

First, issue a DNS query that returns no response:

dig @10.1.10.53 nope.f5.com

[root@ip-10-1-1-4:Active:Stan	dalone] co	nfig # ta	ail –f /var/log/l	tm grep tmm				
Feb 8 09:49:54 ip-10-1-1-4 i 10.4#44569: view none: query: Feb 8 09:49:54 ip-10-1-1-4 i .4#44569: [NXDOMAIN qr,rd,ra]	nfo tmm[16 nope.f5.c nfo tmm[16 response:	605]: 202 om IN A - 605]: 202 empty	20-02-08 09:49:54 +E (10.1.10.53%0) 20-02-08 09:49:54	ip-10-1-1-4.us-w ip-10-1-1-4.us-w	est-2.compute. est-2.compute.	internal qio internal qio	d 54150 [.] d 54150 [.]	from 10.1. to 10.1.10
root@ip-10-1-1-6:/# dig @10.1	1.10.53 no	pe.f5.com	n					
; <<>> DiG 9.10.3-P4-Ubuntu < ; (1 server found) ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUER' ;; flags: qr rd ra; QUERY: 1	<<>> @10.1 (, status: , ANSWER:	.10.53 nd NXDOMAIN 0, AUTHOP	ope.f5.com N, id: 54150 RITY: 1, ADDITION	AL: 1				
;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; v ;; QUESTION SECTION:	udp: 4096							
(;nope.f5.com.	IN	A						
;; AUTHORITY SECTION: f5.com. 3415	IN	SOA	pdns130.f5.com.	dnsadmin.f5.com.	9964 3600 900	1209600 360	00	
;; Query time: 1 msec ;; SERVER: 10.1.10.53#53(10.1 ;; WHEN: Sat Feb 08 17:49:54 ;; MSG SIZE rcvd: 93	L.10.53) UTC 2020							

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

	dig	@10.1.1	0.53 c	lnssec	-deplc	oyment.org +dnssec	
Feb 8 10.4#4 Feb 8 .4#499 G A 5 au09cx	09:51: 9953: V 09:51: 53: [NC 2 300 2 Ub+yVjr	:45 ip-10- view none: :45 ip-10- DERROR qr, 2020022208 r1pcTaA3T/	1-1-4 in query: 0 1-1-4 in rd,ra,ad 4002 2020 pnacjmmpl	fo tmm[1 dnssec-d fo tmm[1 ,do] res 00208084 N&iPDavt	6605]: 20 eploymen 6605]: 20 ponse: di 002 55518 bKIq8E1re	2020-02-08 09:51:44 ip-10-1-1-4.us-west-2.compute.internal qid 61180 from 10 nt.org IN A +ED (10.1.10.53%0) 2020-02-08 09:51:44 ip-10-1-1-4.us-west-2.compute.internal qid 61180 to 10.1 dnssec-deployment.org. 278 IN A 46.43.37.10; dnssec-deployment.org. 278 IN F 18 dnssec-deployment.org cKJpHV3mR3Q[PV//3L2Bx6BrR+0KDKNAgmln29ZR9A]yq0F9f1 rdCt9taTu1eYAlQUJrS8Dcx9laUrlWB7kJd0wsB2WvQoAhtngo03wB+tawSQYDpMH/RMFj/0=;	0.1. 1.10 RRSI lrPi
root@i ; <<>> ; (1 s ;; glo ;; Got ;; ->>	p-10-1- DiG 9. erver f bal opt answer HEADER<	1-6:/# dig 10.3-P4-Uk ound) (ions: +cmo : <- opcode: rd ra ad:	g @10.1.1 buntu <~> d . QUERY, 1	10.53 dn: >> @10.1 status:	NOERROR,	ployment.org +dnssec dnssec-deployment.org +dnssec R, id: 61180 ITHORITY: 6. ADDITIONAL: 1	
;; OPT ; EDNS ;; QUE ;dnsse	PSEUDO : versi STION S c-deplo	SECTION: on: 0, fla ECTION: oyment.org	ags: do;	udp: 409 IN	96 A		
;; ANS dnssec dnssec QlPV// wsB2Wv	WER SEC -deploy -deploy 3LZBx6B QoAhtng	TION: ment.org. ment.org. rR+OKDKNAG 003wB+taw	278 278 gmlnz9ZR9 SQYDpMH/F	IN IN 9AjyqoF9⊓ MF j/0=	A RRSIG fIlrPiau	46.43.37.10 A 5 2 300 20200222084002 20200208084002 55518 dnssec-deployment.org. ckJp J 09cxUb+yVjr1pcTaA3T/pnacjmmpN8iPDavtbKIq8E1rdCt9taTu1eYA lQUJrS8Dcx9laUrlW	oHV3m √B7kJ
;; AUT dnssec dnssec dnssec dnssec dnssec cCQm2i waexGa ;; Que	HORITY -deploy -deploy -deploy -deploy -deploy 6uCOiyb fsDJnjk ry time	SECTION: ment.org. ment.org. ment.org. ment.org. BNPCe26K+3 suEuCS9ugg : 1 msec	278 278 278 278 278 278 278 3PpKbeIo- glGwfE6c3	IN IN IN IN IN ⊨iLHzlOr Bhqs ZU8:	NS NS NS NS RRSIG FQ7W9WJM	ns1.mia1.afilias-nst.info. ns1.ams1.afilias-nst.info. ns1.yy21.afilias-nst.info. ns1.sea1.afilias-nst.info. ns1.hkg1.afilias-nst.info. NS 5 2 300 20200222084002 20200208084002 55518 dnssec-deployment.org. EMF NS 5 2 300 20200222084002 20200208084002 55518 dnssec-deployment.org. EMF	-blC8 56b9c
;;	VER: 10 N: Sat SIZE	1.10.53#5 Feb 08 17: rcvd: 559	53(10.1.1 :51:44 UT	L0.53) TC 2020			

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

dig @10.1.10.53 www.google.com +dnssec

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

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

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

Navigate to DNS >> Caches : Cache List

ſ	5	ONLINE (ACT Standalone	(IVE)							
N	lain	Help	About		DNS	» Caches	: Cache I	List		
~	Statistic	s			* -	Cache Lis	t	Statistics	-	
	iApps DN S				*	Name			×	Search
	Delive				No ree	ords to dis	play.			
	Delive	ery	►		Delete	e				
	GSLE	•								
	Zones	3	Þ							
	Cache	es 🔺		7	Cache	List	•			
	Settin	gs			Statistic	:S				
6	SSL Orc	hestrator affic								

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

0	ieneral Properties		
	Name	validating-resolver_cache	
	Resolver Type	Validating Resolver 🔽 🗲	
	Route Domain Name		
	Resolver Type Route Domain Name	Validating Resolver	

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 Image: Enabled Use IPv6 Image: Enabled Use UDP Image: Enabled Use TCP Image: 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 Image: Enabled P Address: Add Add Image: Enabled Image: Enabled Benabled Image: Enabled Benabled Image: Enabled Image: Enabled Image: Enabled I		
Use IPv6 Image: Enabled Use UDP Image: Enabled Use TCP Image: 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 Image: Enabled Note Hints (Optional: Leave blank for defaults) Image: Enabled Image: Enabled Image: Enabled Image: Enabled Image: Enabled	Use IPv4	Enabled
Use UDP Image: Construction of the state of the st	Use IPv6	☑ Enabled
Use TCP Image: Concurrent UDP Flows Image: State Stat	Use UDP	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 In P Address: Add Add In P Address: Add In P Address Pelete In P P P P P P P P P P P P P P P P P P P	Use TCP	☑ Enabled
Max. Concurrent TCP Flows 20 Max. Concurrent Queries 1024 Unsolicited Reply Threshold 0 Allowed Query Time 200 Randomize Query Character Case Imabled Imable Provide Provi	Max. Concurrent UDP Flows	8192
Max. Concurrent Queries 1024 Unsolicited Reply Threshold 0 Allowed Query Time 200 Randomize Query Character Case Image: Character Case Image: Provide Address: Add Root Hints (Optional: Leave blank for defaults) Delete Image: Provide Address: Delete Image: Provide Address: 1 Image: Provide Address: 1 <t< td=""><td>Max. Concurrent TCP Flows</td><td>20</td></t<>	Max. Concurrent TCP Flows	20
Unsolicited Reply Threshold 0 Allowed Query Time 200 Randomize Query Character Case Image: Case Image: Case Image: Case Root Hints (Optional: Leave blank for defaults) Image: Case Batter Case Delete Image: Case Image: Case	Max. Concurrent Queries	1024
Allowed Query Time 200 Randomize Query Character Case Image: Case Image: Case <td< td=""><td>Unsolicited Reply Threshold</td><td>0</td></td<>	Unsolicited Reply Threshold	0
Randomize Query Character Case IP Address: Add B.1. Lab Components Image: Case Image: Case <	Allowed Query Time	200
Root Hints (Optional: Leave blank for defaults) IP Address: Add B.1. Lab Components Delete	Randomize Query Character Case	Enabled
3.1. Lab Components	Root Hints (Optional: Leave blank for defaults)	Add
	3.1. Lab Components	Leiete 125

DNSSEC Validator

Profet	ch.	Kow	

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

3.1.6 RPZ

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

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



Zone Runner

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

Navigate to DNS >> Zones : ZoneRunner : Zone List

	ONLINE (ACTIVE) Standalone								
Ma	in Help About	DNS » Zones : ZoneF	Runner : Zone	List					
<u>~</u>	Statistics	🚓 🚽 Resource Recor	d List Zone	List V	'iew List	named Configuration			
i 🔂	Apps	Find Zones							
S	DNS	View Name	A	\checkmark					
	Delivery	Zone Name	*		Search Reset	t Search			
	GSLB >							Create	b
	Zones >	Zones	•			Zone Type	View Name	Resource Records	1
	Caches	DNSSEC Zones	F						1
	Settings	ZoneRunner	Resource	e Record 🔶					
6	SSL Orchestrator		Zone List	•					
	ocal Traffic		View List	÷					
- 1990 ·	our mallio		named C	onfiguration					

Create a new zone according to the following table:

Setting	Value
View Name	external
Zone Name	rpz.example.com
Zone Type	Master
Zone File Name	db.external.rpz.example.com
Options	also-notify { ::1 port 5353; };
TTL	300
Master Server	master.example.com.
Email Contact	hostmaster.master.example.com.
NS Record: TTL	300
NS Record: Nameserver	master.example.com.
Create A Record	Checked - Enabled
A Record: IP Address	10.1.10.53

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

General Properties

View Name	external \$	
Zone Name	rpz.example.com	
Zone Type	Master 🜲	

Configuration

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

Records Creation

	TTL	300	
	Master Server	master.example.com.	
	Email Contact	hostmaster.master.example.com.	
SOA Record	Serial Number	2020020801	
	Refresh Interval	10800	Seconds \$
	Retry Interval	3600	Seconds \$
	Expire	604800	Seconds \$
	Negative TTL	86400	Seconds \$
NS Record	TTL 30	0	
No Necola	Nameserver ma	aster.example.com.	
Create A Record	Enable		
A Record	IP Address 10.1	1.10.53	
Cancel Repeat Finished			

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

	ONLINE (ACTIVE) Standalone					
Ma	in Help About	DNS	» Zones : ZoneRunner	: Resource Record	d List	
1 s	Statistics	* -	Resource Record List	Zone List	View List	named Configuration
i 🧟	Apps	Find F	Records			
S 1	ONS	View	Name	Ali 🔽		
	Delivery	Zone	Name	All Zones (Sele	ect a View to search	a specific zone) 🔽
	GSLB	Туре		All	\checkmark	
	Zones	Nam	e	*		
	Caches	RDA	та			
	Settings	Sear	ch Reset Search Cr	reate		
6 5	SSL Orchestrator					

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

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

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

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

View Name	external \$
Zone Name	rpz.example.com. 🖨
Name	*.fuzzybunnies.com
TTL	60
Туре	
CNAME	•

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

DNS »	DNS » Zones : ZoneRunner : Resource Record List							
⇔ -	Resource Record List	Zone List	View List	named Configuration				
Find Red	Find Records							
View Na	ame	All 💠						
Zone N	lame	All Zones (Sele	ect a View to search	a specific zone) 🛊				
Туре		All	\$					
Name		*						
RDATA								
Search	Search Reset Search Create							
✓ ▲ Name		View Name		Zone Name	\$ TTL	Type	RDATA	
*.fuzzybunnies.com.rpz.example.com.		external		rpz.example.com.	60	CNAME		
rpz.example.com.		external		rpz.example.com.	300	NS	master.example.com.	
rpz.example.com.		external		rpz.example.com.	300	SOA	master.example.com	

Name Server

Navigate to DNS >> Delivery : Nameservers : Nameserver List

ſ	ONLINE (A Standalone	CTIVE)							
N	Main Help	About	DNS » Delivery	: Names	ervers : Nameserve	r List			
<u>~</u>	Statistics		🔅 👻 Nameserve	er List	Statistics [2				
iApps			*		×S	earch			
5	DNS		✓ ▲ Name				Address	Port	≑ TSIG
	Delivery >		Listeners	Þ					
	GSLB		Profiles	Þ					
	Zones	+	Load Balancing	Þ					
	Caches		iRules	Þ					
	Settings	•	Translation	Þ					
SSL Orchestrator			Nameservers	- 2	Nameserver List	•			
			Kevs	•	Statistics	7			
0-0	Less Troffie								

Create a nameserver according to the following table:

Setting	Value
Name	localhost
Address	127.0.0.1

	ONLINE (AC	TIVE)		
Ma	in Help	About	DNS » Delivery : Nameservers	: Nameserver List » New Nameserver
Mage Statistics			General Properties	
i la	Apps		Name	localhost
(S) C)N S		Address	127.0.0.1
	Delivery	×	Service Port	53 Other: 🗸
	GSLB	•	Configuration	
	Zones	+	Route Domain	
	Caches		TSIG Key	None
	Settings	• •		
C			Cancel Repeat Finished	

TMSH

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

DNS Express

Navigate to DNS >> Zones : Zones : Zone List

ONLINE (ACTIVE) Standalone					
Main Help About	DNS » Zones : Zone List				
Statistics	🔅 👻 Zone List Statistics 🔎				
iApps	* Search	Create			
S DNS	✓ ▲ Name	Response Policy			
Delivery	No records to display.				
GSLB	Delete				
Zones >	Zones 🚽 Zone List 💽				
Caches	NSSEC Zones Statistics				
Settings	ZoneRunpa				
SSL Orchestrator					

Create a DNS Express zone according to the following table:

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

ONLINE (ACTIVE) Standalone				
Main Help About	DNS » Zones : Zones : Z	one List » New Zone		
Mage Statistics	General Properties			
iApps	Name	rpz.example.com		
S DNS	DNS Express	DNS Express		
Delivery	Server	localhost		
GSLB	Availability	Unknown		
Zones	State	Enabled V		
Caches	Notify Action	Consume		
Settings SSL Orchestrator SSL Orchestrator Contemporation Acceleration	Allow NOTIFY From	Address: 127.0.0.1 × Add 127.0.0.1 Delete		
	Verify Notify TSIG			
Device Management	Response Policy			
Network	Zone Transfer Clients			
System	Nameservers	Active Available //Common dc01.example.com localhost		
	TSIG			
	Server Key	None		

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

Local Zone

Navigate to: DNS >> Caches : Cache List

ONLINE (ACTIVE) Standalone	
Main Help About	DNS » Caches : Cache List
Magazina Statistics	Cache List Statistics
iApps	* × Search
🕥 dns	✓ ♦ Name
Delivery	transparent_cache
GSLB	validating-resolver_cache
Zones	Delete Click "validating-resolver_cache
Caches >	Cache List 📀
Settings	Statistics
SSL Orchestrator	
Local Traffic	

Select validating-resolver_cache, click "Local Zones", and click "Add"

ONLINE (ACTIVE) Standalone Main Help	DNS » Caches : Cache List » Local Zones : validating-resolver_cache
Statistics	Properties Trust Anchors DLV Anchors Local Zones Forward Z
iApps	Response Policy Zones Statistics
S DNS	Local Zones Add
Delivery	✓ Name
GSLB >	No records to display.
Zones >	Delete Then click "Add"
Caches >	Then click -Add
Settings	

Create a local zone entry according to the following table:

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

Local Zone					
Name	sorry.example.com No "dot" at the end!!				
Туре ———	Static				
Records	sorry.example.com. IN A 10.1.20.252 sorry.example.com. IN A 10.1.20.252 There is a "dot" at the end!! Delete	Add			

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

Walled Garden

Navigate to: DNS >> Caches : Cache List

Click "validating-resolver_cache"

ONLINE (ACTIVE) Standalone	
Main Help About	DNS » Caches : Cache List
Mage Statistics	to v v Cache List Statistics
iApps	* × Search
😚 dns	✓ ◆ Name
Delivery	transparent_cache
GSLB	validating-resolver_cache
Zones	Delete Click "validating-resolver_cache
Caches >	Cache List 📀
Settings	Statistics
SSL Orchestrator	
Local Traffic	

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

	ONLINE (ACTIVE) Standalone						
Ma	in Help About	DNS » Caches : Cache	List » Response P	olicy Zones : resolv	er_cache		
Mage Statistics		🚓 🚽 Properties	Local Zones	Forward Zones	Response Policy Zones		
iApps		Response Policy Zones				s and Stats Only	Add
	Delivery	No records to display.				2 /	
	GSLB >	Delete	lick "Res	oonse Pol	icy Zone"	Click "/	Add"
	Zones				-		
	Caches >						
	Settings >						

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

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

Response Policy Zone

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

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 } }

Results

From a shell on the Ubuntu Client:

First, a query that returns no response:

dig @10.1.10.53 www.fuzzybunnies.com

root@ip-10-1-1-6:/# dig @10.1.10.53 www.fuzzybunnies.com									
<pre><<>> DiG 9.10.3-P4-Ubuntu <<>> @10.1.10.53 www.fuzzybunnies.com (1 server found) ; global options: +cmd ; Got answer: ; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7454 ; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1</pre>									
;; OPT PSEUDOSECTION: ; EDNS: version: 0, fla; :: OUESTION SECTION:	gs:; udp	: 4096							
;www.fuzzybunnies.com.		IN	А						
;; ANSWER SECTION: www.fuzzybunnies.com. sorry.example.com.	300 3600	IN IN	CNAME A	sorry.example.com. 10.1.20.252					
;; AUTHORITY SECTION: rpz.example.com. 800 86400	300	IN	SOA	master.example.com.	hostmaster.master.example.com.	2020020802	10800	3600	604
; Query time: 0 msec ; SERVER: 10.1.10.53#53(10.1.10.53) ; WHEN: Sat Feb 08 19:06:27 UTC 2020 ; MSG SIZE rcvd: 165									

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

3.1.7 URL Categorization

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



Create an iRule

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

ONLINE (ACTIVE) Standalone								
Main Help About DNS » Delivery : iRules : iRule List								
Statistics	🚓 👻 iRule List	Data Group List iFile List	Statistics 🗵					
iApps	*	* × Search						
😚 dns	Name	Verification	I					
Delivery	Listeners	g None						
GSLB	Profiles	eSupport_OA_BasicAuth 🖭 F5 Verifie	d					
Zones	Load Balancing	sSupport_OA_NtImAuth 🛛 F5 Verifie	d					
Caches	iRulas	iRule List	d					
	II y les	F5 Verifie	d					
Settings	I ranslation	Data Group List 📀 F5 Verifie	d					
	Nameservers	iFile List 💮 F5 Verifie	d					
33E Of Chestrator	Keys 🔸	Statistics F5 Verifie	d					
Local Traffic	sys_auth_ldap	🖭 F5 Verifie	F5 Verified					
Acceleration	Sys_auth_radius	s 📑 F5 Verified						
Acceletation		ap 📃 F5 Verifie	d					
Device Management	Sys_auth_ssl_cridp							

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

Setting	Value
Name	DNS-query-filtering

```
when RULE_INIT {
 # Set categories to block for DNS hosts
 set static::blocked_categories {
  /Common/Bot_Networks
   /Common/Spyware
   /Common/Malicious_Web_Sites
   /Common/Adult Content
   /Common/Entertainment
 Ł
  # CONFIGURATION
 # Check all requests by default
 set static::request_check 1
 # If the category returns as blocked, return NXDOMAIN (1)
 # Otherwise if (0), return a statically defined IP address
 set static::request_return_nxdomain 0
 set static::request_redirect_to "10.1.20.252"
 # Toggle for debug logs
 set static::request_debug 1
}
```

(continues on next page)

(continued from previous page)

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

iRule assignment

Assigned the iRule to the DNS Listeners:

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

ONLINE (ACTIVE) Standalone								
Mai	in Help	About	Local Traffic » iRules :	iRule List				
Magazine Statistics			🔅 👻 iRule List	Data Group List	iFile List	Statistics 🗵		
iApps			* Search					
📢 о	NS		Name		Verification			
	Delivery	•	Listeners >	Listener List	F5 Verified			
	GSLB		Profiles	Statistics	F5 Verified			
	Zones	•	Load Balancing	soupport_neiper	F5 Verified			
	Caches	•	iRules	Support_main	F5 Verified			
	Sottings		Translation	j_SAML_BasicAuth	E F5 Verified			
	Settings	· · · · · · · · · · · · · · · · · · ·		c	F5 Verified			
fi s	SL Orchestrator		Nameservers	te	F5 Verified			
			Keys I		E F5 Verified			
Local Traffic			sys_auth_radius		E F5 Verified			
		1/	sys_auth_ssl_cc_ld	ар	F5 Verified			
• A	cceleration	1/	sys_auth_ssl_cridp			F5 Verified		
Device Management			sys_auth_ssl_ocsp		F5 Verified			

Navigate to the *udp_53_virtual* listener:

DNS » Delivery : Listeners : Listener List							
🔅 👻 Listener List	Statistics						
* Coarab							
✓ ♦ State ♦ Name							
Enabled udp_53_virtual							
Enabled tcp_53_virtual							
Enable Disable Delete							

Navigate to the iRules section

DNS » Delivery : Listeners : Listener List » Properties : udp_53_virtual								
🚓 👻 Properties L	oad Balancing	iRules	Statistics					
General								
Name	Name udp_53_virtu			tual				
Partition	Common							
Description								
State	Enabled \$	Enabled \$						

Click Manage button and assign the iRule

DNS » Delivery : Listeners : Listener List » Properties : udp_53_virtual								
roperties	Load Balancing	iRules	Statistics					
iRule Management								
	Selec	ted	Available					
	/Common		/Common					
	DNS-quer	y-filtering	sys_APM_ExchangeSupport_OA_Basi					
iRules			_sys_APM_Exchan	geSupport_OA_NtImAuth				
		>>	_sys_APM_Exchan	geSupport_helper				
			_sys_APM_Exchan	geSupport_main				
	Up	Down						
Update								
Cepterte								

TMSH

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

Results

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

tail -f /var/log/ltm

Now run DNS queries from the Ubuntu Client:

dig @10.1.10.53 www.f5.com

And analyze the results:

Feb 13 14:47:14 ip-10-1-1-4 info tmm[10647]: 2020-02-13 14:47:13 ip-10-1-1-4.us-west-→2.compute.internal qid 29530 from 10.1.10.4#43881: view none: query: www.f5.com IN_ →A +E (10.1.10.53%0) Feb 13 14:47:14 ip-10-1-1-4 info tmm3[10647]: Rule /Common/DNS-query-filtering <DNS_ →REQUEST>: Category /Common/Uncategorized matching www.f5.com is not filtered Feb 13 14:47:14 ip-10-1-1-4 info tmm[10647]: 2020-02-13 14:47:14 ip-10-1-1-4.us-west-→2.compute.internal qid 29530 to 10.1.10.4#43881: [NOERROR qr,rd,ra] response: www. →f5.com. 30 IN CNAME dwbfwz8xncgmg.cloudfront.net; dwbfwz8xncgmg.cloudfront.net. 60 →IN A 99.86.33.52; dwbfwz8xncgmg.cloudfront.net. 60 IN A 99.86.33.5; dwbfwz8xncgmg. →cloudfront.net. 60 IN A 99.86.33.9; dwbfwz8xncgmg.cloudfront.net. 60 IN A 99.86.33.5;

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

dig @10.1.10.53 www.tmz.com

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

```
Feb 13 15:27:37 ip-10-1-1-4 info tmm[10647]: Rule /Common/DNS-query-filtering <DNS_

→REQUEST>: BLOCKED: Category /Common/Entertainment matching www.tmz.com is filtered.

Feb 13 15:27:37 ip-10-1-1-4 info tmm[10647]: 2020-02-13 15:27:36 ip-10-1-1-4.us-west-

→2.compute.internal qid 32427 to 10.1.10.4#55151: [NOERROR qr,rd,ad] response: www.

→tmz.com. 111 IN A 10.1.20.252;
```

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

To list current categories, from the BIG-IP enter the TMSH shell with *tmsh*, then run the following command:
Class 3 - Data Center Availability Services Using BIG-IP DNS

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

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

4



4.1 Network Map













4.2 System

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

1. Create a "Log Publisher"

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

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Time	e: Jul 20, 2017 User: admin P e: 12:39 PM (CDT) Role: Administrator P
ONLINE (ACTIVE) Standalone	
Main Help About	System » Logs : Configuration : Log Publishers
Statistics	System Captured Transactions Packet Filter GSLB Audit
iApps	Click "Create"
S DNS	Anne 5
S and anti-state	default-ipsec-log-publisher
SSL Orchestrator	local-db-publisher
Acceleration	sys-db-access-publisher
	sys-sso-access-publisher
Device Management	Delete
Retwork	
System	
Casting	
Disk Management	lu l
Software Management	
License	
Resource Provisioning	
Platform	
High Availability	
Archives (*) >	Sveten
Services	Cantured Transactions
Preferences	Paska Filter
sFlow	Lease Filter Options
SNMP	COLD Log Filter
Crypto Offloading	GSLB Log Filters
Users	Audit 3 L stinations
Logs	Configuration

Create a local syslog publisher according to the table below:

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

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

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

TMSH

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

2. Create a "Logging Profile"

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

Hostname: gtm1.site1.example.com Dai IP Address: 10.1.10.13 Tin	te: Jul 20, 2017 ne: 12:49 PM (CDT)	User: admin Role: Administrator		
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » Delivery :	: Profiles : Other : DN	IS Logging	
Mage Statistics	₩ - DNS	Protocol	▼ Other ▼	
iApps	*		× Click "Create"	Create
🕥 dns	✓ ♦ Name			¢ Lo
Delivery	Listeners	>		
GSLB 2	Profiles	> DNS	(+)	
Zones	Load Balancing	Protocol	+	
Caches	iRules	Other	DNS Logging	\odot
Settings	Translation	3	4 Persistence	\odot
SSI Orchestrator	Nameservers	•	Statistics	\odot
g sst orchestian	Keys	•		
Acceleration				
Device Management				
Network				
System				

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

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

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Tim	:: Jul 20, 2017 User: admin :: 12:52 PM (CDT) Role: Administr	ator
Standalone		
Main Help About	DNS » Delivery : Profiles : Othe	er : DNS Logging » New
Mage Statistics		
	General Properties	
1Apps	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		
e	Log Fields	
SSL Orchestrator	Include Complete Answer	✓ Enabled
	Include Query ID	Enabled
Accolution	Include Source	C Enabled
Device Management	Include Timestamp	I Enabled
Network	Include View	Enabled
System	Cancel Repeat Finished	

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

TMSH

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

4.3 Settings

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

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

Host came: gtm1.site1.example.com Da P Address: 10.1.10.13 Ti	te: Jul 20, 2017 User: te: 12:19 PM (CDT) Role:	admin Administrator	Par	
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » Settings : GSLE	I : General		
Mage Statistics	🔅 🚽 Delivery	▼ GSLB ▼ Zones Caches		
iApps	Configuration Synchroni	zation		
S DNS	Synchronize			
Delivery	Group Name EXAMPLE_group			
GSLB >	Time Tolerance 10 seconds			
Zones >	Synchronize DNS Zone Files			
Caches	Configuration Save			
Settings >	Delivery	☑ Enabled		
S SSI Orah strator	GSLB	General		
SSL Of Christiator	Zones	Load Balancing		
Acceleration	Caches	Metrics Collection		
	Auto-Discover	Lenabled		
Device Management	Request Interval 30 seconds			
Network	Network Monitoring			
System	Heartbeat Interval	10 seconds		

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

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

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

TMSH

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

4.4 Listeners

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

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



4.4.1 DNS Profile

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

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

Hostname: gtm1.site1.example.com Da	ate: Jul 20, 2017 Use	r. admin	
IP Address: 10.1.10.13	me: 12:57 PM (CDT) Role	: Administrator	
Main Help About	DNS » Delivery : Pro	iiles : DNS	
Statistics	🔅 👻 DNS	Protocol - Othe	k"Croate"
iApps	*	× Search	Create
😚 dns	✓ A Name		4 ÷ Ar
Delivery 1	Listeners	•	
GSLB	Profiles	DNS 💽	
Zones	2 load Balancing	3 otocol	
Caches	iRules	> Other >	
Settings	Translation	►	
SSI Orchostrator	Nameservers	►	
SSE Ofchestra of	Keys	▶	
Acceleration			
Device Management			0
Network			_
Svstem			

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

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

Main Help About	DNS » Delivery : Profiles : D	NS >> Properties : example.com_dns_profile
Mage Statistics	🔅 🚽 Properties	
- iters		
(6) tapps	General Properties	
😚 dns	Name	example.com_dns_profile
Delivery	Partition / Path	Common
GSLB	Parent Profile	dns 🔽
Zones	Denial of Service Protection	Custom 🗆
Caches	Rapid Response Mode	
Settings	Rapid Response Last Action	
Acceleration	Hardware Acceleration	
Device Management	Protocol Validation	Disabled
	Response Cache	
Network	DNS Features	
System	DNSSEC	Disabled
	GSLB	
	DNS Express	
	DNS Cache	Disabled
	DNS Cache Name	Select
	DNS IPv6 to IPv4	
	Unhandled Query Actions	
	Use BIND Server on BIG-IP	
	DNS Traffic	
	Zone Transfer	
	DNS Security	
	DNS Security Profile Name	Select
	Process Recursion Desired	
	Logging and Reporting	
	Logging	
	Logging Profile	example_dns_logging_profile
	AVR Statistics Sample Rate	Enabled 1/ 1 queries sampled

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 logprofile example_dns_logging_profile enable-logging yes avr-dnsstat-sample-rate 1 enable-dns-express no enable-dnssec no

4.4.2 UDP Profile

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

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

Note:	It is required to	complete the	following task on	both gtm1.site1	and gtm1.site2
			0	0	0

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Tin	te: Jul 20, 2017 User: ne: 1:11 PM (CDT) Role:	admin Administrator	
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Delivery : Prof	iles : Protocol : UDP	Click "Create"
Statistics	DNS	Protocol - Other	
iApps	ŀ	× Search	Create
🕥 dns	Aname 🗢		÷.
Delivery	Listeners	>	
GSLB	Profiles	DNS 📀	
Zones	2 Load Balancing	Protocol	UDP 💿
Caches	iRules	3 Other 4	тср 📀
Settings	rranslation		
SSI Orchastrator	Nameservers		
SSE Orchestrator	Keys		
Acceleration			
Device Management			
Retwork			
System			

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

Field	Value
Name	example.com_udp-dns_profile
Parent Profile	udp_gtm_dns

Hostname: gtm1.site1.example.com IP Address: 10.1.10.13	Date: Jul 26, 2018 Time: 8:17 AM (ED	User: admin T) Role: Administrator	Partition: Common	Log out
ONLINE (ACTIVE) Standalone				_
Main Help About	DNS » D	elivery : Profiles : Protoco	ol : UDP » New UDP Profile	
Mage Statistics				
iApps	General Pro	operties	example.com_udp-dns_profile	
😚 dns	Parent Pro	ofile	dp_gtm_dns	
Delivery	Settings			Custom 🗌
GSLB	Proxy Max	timum Segment		
Zones	Idle Timeo	out	pecify 🔽 5	seconds 🗆
Caches	IP ToS	SI	pecify 🗸 0	
Settings	Link QoS	S	pecify 🔽 0	
Acceleration	Datagram	LB	Enabled	
Device Management	Allow No F	Payload		
Device Management	TTL Mode	P	roxy 🗸	
Network	Don't Frag	ment Mode	UTU	
System	Max Buffe	r Bytes	55350	
	Max Buffe	r Packets		

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

4.4.3 TCP Profile

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

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

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Time	:: Jul 20, 2017 User: admin :: 1:19 PM (CDT) Role: Administrator	Partition: Common
Standalone		
Main Help About	DNS » Delivery : Profiles : Protocol : TCP	
Maga Statistics		
iApps	* × Search	Create
S DNS	Applic	ation 🗢 Parent F
Delivery 1 >	Listeners + I-tcp	tcp-legacy
GSLB	Profiles DNS 📀	tcp-legacy
Zones	2 load Balancing Protocol → UDP (+)	top
Caches	iRules 3 Other TCP 📀	tcp
Settings	Translation	tcp
G an a later	Nameservers	tcp-legacy
SSL Orchestrator	Keys p	tcp-wan-op
Acceleration	∷ tcp	(none)
Device Management	tcp-lan-optimized	tcp-legacy
Device munugement	C tcp-legacy	tcp
Network	tcp-mobile-optimized	tcp-legacy
To System	tcp-wan-optimized	tcp-legacy

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

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

Hostname: gtm1.site1.example.com D IP Address: 10.1.10.13 T	ate: Jul 20, 2017 User: admin ime: 1:23 PM (CDT) Role: Administ	rator	Partition: Common
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Delivery : Profiles : Pro	otocol : TCP » New TCP Profile	
Mage Statistics			
iApps	General Properties		
	Name	example.com_tcp-dns_profile	
S DNS	Parent Profile	🗲 f5-tcp-wan	1
Delivery	Timer Management		
GSLB	Close Wait	Specify 🖌 5	seconds
Zones	Fin Wait 1	Specify 🖌 5	seconds
Caches	Fin Wait 2	Specify 🗸 300	seconds
Settings	Idle Timeout	Specify V 300	seconds
SSL Orchestrator	Keep Alive Interval	Specify 🖌 1800	seconds
Acceleration	Minimum RTO	500 milliseconds	
Device Management	Reset On Timeout	Enabled	
	Time Wait	Specify 🔽 2000	milliseconds
Network	Time Stroll way do	wn to find the "Fini	sh"-button
System	Zero Window Timeout	Specify 20000	milliseconds

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

TMSH

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

4.4.4 UDP IP Address

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

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

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Tin	e: Jul 20, 2017 User: a ne: 1:29 PM (CDT) Role: A	i dmin Administrator	Partition: Common
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Delivery : Listen	ers : Listener List	Click "Create"
Magazine Statistics	🛱 👻 Listener List	Statistics 🗷	
iApps	ł	× Search	Create
😚 dns	State 🗢 Name		▲ Destination
Delivery	Listeners	Listener List 📀	
GSLB	Profiles	Statistics 🦻	
Zones	Load salancing		
Caches	iRules >		
Settings	Translation >		
	Nameservers		
SSE OFCINA MALON	Keys >		
Acceleration			
Device Management			
Network			
System			

Create a UDP listener according to the following table:

Field		gtm1.site1	gtm1.site2	
Name		isp1_site1_ns1.example.com_udp_53_	vi ispa l_site2_ns2.example.com_udp_53_v	/irtua
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	

Hostname gtm1.site1.example.com Date: IP Address: 10.1.10.13 Time	Jul 20, 2017 User: admin : 1:32 PM (CDT) Role: Administra	tor Partition: Common
ONLINE (ACTIVE) Standalone Be sur	e to create 20	3.0.113.8 on gtm1.SITE1
Main Help About	DNS » Delivery : Listeners : List	stener List » New
Mage Statistics		
iApps	General	
	Name	isp1_site1_ns1.example.com_udp_53_virtual
S DNS	Description	
Delivery	State	Enabled V
GSLB >	Listener: Advanced V	
Zones >		
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
	Auto Last Hop	Default 🗸
System	Last Hop Pool	None
	Service: Advanced V	
	Protocol	
	Protocol Profile (Client)	example.com_udp-dns_profile
	Protocol Profile (Server)	(Use Client Profile)
	DNS Profile	example.com_dns_profile

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

Hostname gtm1.site2.example.com Date IP Address: 10.1.10.23	: Jul 20, 2017 User: admin :: 1:32 PM (CDT) Role: Administra	ator Partition: Common
Main Help About	o create 198.5 DNS » Delivery : Listeners : Lis	1.100.40 on gtm1.STTE2 stener List » New
Mage Statistics	Conoral	
iApps	Name	isp1_site2_ns2.example.com_udp_53_virtual
S DNS	Description	
Delivery	State	Enabled V
GSLB	Listener: Advanced 🗸	-
Zones	Destination	Type: O Host O Network
Caches		Address: 198.51.100.40
Settings	Service Port	DNS S3
SSL Orchestrator	VLAN Traffic	All VLANS 🔽
Acceleration	Source Address Translation	None
	Address Translation	Enabled
Device Management	Port Translation	Enabled
Network	Route Advertisement	Enabled
	Auto Last Hop	Default 💌
System	Last Hop Pool	None
	Service: Advanced	
	Protocol	
	Protocol Profile (Client)	example.com_udp-dns_profile
	Protocol Profile (Server)	(Use Client Profile)
	DNS Profile	example.com_dns_profile

gtm1.site1 TMSH command:

TMSH

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

gtm1.site2 TMSH command:

TMSH

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

}

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

4.4.5 TCP IP Address

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

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

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Tin	te: Jul 20, 2017 User: ne: 1:29 PM (CDT) Role:	admin Administrator	Partition: Common
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » Delivery : Liste	ners : Listener List	Click"Croate"
Mage Statistics	🔅 👻 Listener List	Statistics 🗵	Click-Create-
iApps	ř	× Search	Create
😚 dns	State 🗢 Name		▲ Destination 💠 F
Delivery	Listeners	Listener List 💽	
GSLB	Profiles	Statistics	
Zones	Load Jalancing		
Caches	iRules		
Settings	Translation		
	Nameservers		
SSL OTCHERGENION	Keys		
Acceleration			
Device Management			
Network			
System			

Create a TCP listener.

Field		gtm1.site1	gtm1.site2]
Name		isp1_site1_ns1.example.com_tcp_53_v	irt spat _site2_ns2.example.com_tcp_53_v	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	1

Hostname gtm1.site1.example.com Date IP Addres: 10.1.10.13 Tim	e: Jul 20, 2017 User: admin e: 2:18 PM (CDT) Role: Administra	ator Partition: Common		
CONLINE (ACTIVE) Standalone	e to create 20	3.0.113.8 on gtm1.SITE1		
Main Help About	DNS » Delivery : Listeners : List	stener List » New		
Statistics	General			
iApps	Name	isp1_site1_ns1.example.com_udp_53		
😚 dns	Description			
Delivery	State	Enabled V		
GSLB →	Listener: Advanced			
Zones > Caches >	Destination	Type: Host O Network Address: 203.0.113.8		
Settings	Service Port	DNS 53		
SSL Orchestrator	VLAN Traffic	Ali VLANs		
	Source Address Translation	None 🔽		
Acceleration	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 V			
	Protocol	TCP		
	Protocol Profile (Client)	example.com_tcp-dns_profile		
	Protocol Profile (Server)	(Use Client Profile)		
	DNS Profile	example.com_dns_profile		
	Load Balancing			
	Default Pool	None		
	Default Persistence Profile	None		
	Fallback Persistence Profile	None		

Be sure to create the 198.51.100.40 address on gtm1.site2

Hostname gtm1.site2.example.com Date IP Addres: 10.1.10.23 Tim	e: Jul 20, 2017 User: admin e: 2:18 PM (CDT) Role: Administr	ator Partition: Common
ONLINE (ACTIVE) Standalone Be sure	to create 198.	51.100.40 on gtm1.SITE2
Main Help About	DNS » Delivery : Listeners : Li	istener List » New
Statistics	General	
iApps	Name	isp1_site2_ns2.example.com_udp_53
😚 dns	Description	
Delivery	State	Enabled V
GSLB	Listener: Advanced	
Zones > Caches >	Destination	Type: Host O Network Address: 198.51.100.40
Settings	Service Port	DNS 🔽 53
SSL Orchestrator	VLAN Traffic	All VLANS 🔽
Acceleration	Source Address Translation	None
Acceleration	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 V	
	Protocol	TCP
	Protocol Profile (Client)	example.com_tcp-dns_profile
	Protocol Profile (Server)	(Use Client Profile)
	DNS Profile	example.com_dns_profile
	Load Balancing	
	Default Pool	None
	Default Persistence Profile	None
	Fallback Persistence Profile	None

gtm1.site1 TMSH command:

TMSH

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 }

4.5 Data Centers

4.5.1 Servers

gtm1.SITE1

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

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

1. Fill in the Name and Datacenter

Hostname: gtm1.site1.example.com IP Address: 10.1.10.13	Date: Jul 20, 2017 Time: 2:29 PM (CDT)	User: admin Role: Administrato		Parti
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » GSL	B : Servers : Server L	ist » New Server	
Magazine Statistics				
iApps	General Prope	rties		
CO athe	Name 💻	\rightarrow	gtm1.site1_server	
S DNS	Product		BIG-IP System	
Delivery	Data Center	\longrightarrow	site1_datacenter	
GSLB	Prober Prefer	ence	Inherit From Data Center 🔽]
Zones	Prober Fallba	ck	Inherit From Data Center 🔽	1
Caches	State		Enabled 🔽	
Settings	Dovicos		Click"Ad	1 4 10
SSL Orchestrator	Devices	al d		
-	-	Devi	ce Name	Address
Acceleration	No	data available in table	•	
Device Management	BIG-IP System Devices			
Retwork				
System	Ed	lit Delete		

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

Hostname: gtm1.site1.example.com D IP Address: 10.1.10.13 T	ate: Jul 20, 2017 ime: 2:36 PM (CD	User: (T) Role:	admin Administrator		Parti
ONLINE (ACTIVE) Standalone					
Main Help About	DNS » G	SLB : Server	s : Server List »	New Server	
Statistics			Add Bl	G-IP System Device	
iApps	General Pr Name	nerties	Device I Address	Name: gtm1.site1.example.com s: 203.0.113.7	
S DNS	Product		Translat	tion:	(Optional)
Delivery	Click"	Add"	Link:	Auto-Select	
GSLB	Prober Pre		Add	3	
Zones	Prober Fal	lback	203.0.1	113.7	
Caches	State				
Settings	-		Delete	. 1	
SEL Orchestrator	Devices		Delete	e	
SSL Orchestrator					OK Cancel
Acceleration	RIG ID.	No data avai	ilable in table		4
Device Management	System				
Network	Devices			Click"OK"	
System		Edit Delete			

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

Hostname: gtm1.site1.example.com Dat IP Address: 10.1.10.13 Tim	e: Jul 20, 2017 User: admin e: 2:43 PM (CDT) Role: Adminis	strator Pi	arti
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » GSLB : Servers : Serv	ver List » New Server	
Statistics	General Properties		
iApps	Name	gtm1.site1_server	
😚 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		
SSL Orchestrator Acceleration Device Management Network Y System	Add BIG-IF System Devices Edit Delete Configuration: Advanced Health Monitors Availability Requirements Limit Settings iQuery Options	Device Name Address com 203.0.113.7 Selected Available /Common gateway_icmp bigip < jtp http http http All Health Monitors Bits: Disabled Current Connections: Disabled Current Connections: Disabled Service Check Path Path SNMP	

TMSH

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

gtm1.SITE2

Continue the same configuration for gtm1.site2.

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Time	: Jul 20, 2017 User: admin 2: 2:47 PM (CDT) Role: Administrate		Р
Standalone			
Main Help About	DNS » GSLB : Servers : Server I	ist	
Statistics	🔅 👻 Server List Trusted	Server Certificates Statistics	
iApps	ŕ	× Search	Create
😚 dns	Status 🔺 Name	Devices Address	Data Center Virtual :
Delivery	gtm1.site1_server	1 203.0.113	site1_datacenter 0
GSLB	Enable Disable Delete		
Zones	Click	"Create" to define	atm1.site2
Caches	C		
Settings			
SSL Orchestrator			
Acceleration			
Device Management			
Retwork			
System			

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

1. Fill in the Name and Datacenter

Hostr IP Ad	name: gtm1.site1.example.com Idress: 10.1.10.13	Date: Jul 20, 2017 Time: 3:18 PM (CI	User: DT) Role:	admin Administrator			Parti
	Standalone						
Ma	ain Help About	DNS » G	SLB : Server	s : Server Lis	st » New Server		
	Statistics	Conoral Dr	anartiaa				
i 🐻	Apps	General Pr	operties		stm1 aita2 aaavar		
		Name			gunn.suez_server		
591	DNS	Product		E	BIG-IP System		
	Delivery	Data Cer	iter	 9	ite2_datacenter		
	GSLB	Prober Pro	eference	Γ	nherit From Data Center 🔽		
	Zones	Prober Fa	llback	Π	nherit From Data Center 🔽		
	Caches	State		E	Enabled 🔽		
	Settings	>					
e		Devices			Click "Add"		
	SSL Orchestrator		Add				
	Acceleration			Devic	e Name	Address	
		BIG-IP	No data avai	lable in table			
	Device Management	System Devices					
	Network						
			Edit Doloto				
89	System		Delete				

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

Hostname: gtm1.site1.example.com D IP Address: 10.1.10.13 T	ate: Jul 20, 2017 ime: 3:30 PM (CDT)	User: admin Role: Administrator	Par
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » GSL	B : Servers : Server List	» New Server
Ma Statistics		Add	BIG-IP System Device
iApps	General Propr	Add	ice Name: gtm1.site2.example.com
S DNS	Product	Trar	nslation: (Optional)
Delivery	Click	"Add" Link	Auto-Select
GSLB >	Prober Prefe	rence A	bb
Zones	Prober Fallba	ack 298	3.51.100.39
Caches	State		
Settings			
SSL Orchestrator	A		3)ete
Acceleration	N	o data available in table	600 0 more
Device Management	BIG-IP System Devices		
Network			
System			

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



TMSH

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

site1_ha-pair

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

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

Hostname: IP Address:	gtm1.site1.example.com : 10.1.10.13	Date: Time:	Jul 20, 2017 3:49 PM (Cl	7 DT)	User: Role:	admin Administrator					P
6	ONLINE (ACTIVE) Standalone										
Main	Help About		DNS » G	SLB :	Server	s : Server List	t				
Mage Statis	tics		🔅 👻 Se	erver Li	ist	Trusted Se	erver Ce	rtificates	Statistics		
iApps	1		*				5	Search		С	reate
😚 dns			🖌 🖛 S	tatus	 Name 	e		Devices	Address	Data Center	Virtual
De	livery	•			gtm1.si	te1_server		1	203.0.113.7	sile1_datacenter	0
GS	LB	•			gtm1.si	te2_server		1	198.51.100.39	site2_datacenter	0
Zor	nes	•	Enable	Disat	ble De	elete					
Ca	ches	•						/			
Set	ttings	÷					Clic	k "Cre	eate"		
SSL C	Orchestrator										
Accel	eration										
Devic	e Management										
Retwo	ork										
Syste	m										

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

1. Fill in the Name and Datacenter



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

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Til	ite: Jul 20, 2017 Us me: 4:33 PM (CDT) Ro	er: admin Pai Pai
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » GSLB: Sen	vers : Server List » New Server
Statistics		Add BIG-IP System Device
iApps	General Properties	Device Name: bigip1.site1.example.com
S DNS	Product	Translation: (Optional)
Delivery	Data Center	Link: Auto-Select
GSLB	Prober Preference	Add 2
Zones	Click "Add	203.0.113.5
Caches	State	
Settings		
SSL Orchestrator	Add	OK Cancel
Acceleration	No data a	vailable in table
Device Management	System Devices	Click"OK"
Network		
System	Edit Del	ite and a second se

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 | : Jul 20, 2017 User: admin
:: 4:38 PM (CDT) Role: Administrat | or Pa |
|--|--|--------------------------|
| CONLINE (ACTIVE)
Standalone | | |
| Main Help About | DNS » GSLB : Servers : Server | List » New Server |
| Statistics | General Properties | |
| iApps | Name | site1_ha-pair |
| 😚 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 | U U |
| Acceleration | BIGJE | m 203.0.113.5 |
| Device Management | System
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 : Server	s : Server List » New	Server	
Statistics			Add BIG-IP	System Device	
iApps	General Pro	operties	Device Nam Address:	e: bigip2.site1.example.com 203.0.113.6	
			Translation:		(Optional)
Delivery	Click "	.	Link:	Auto-Select	
GSLB	Proper Pre	rerence	Add		
Zones	Prober Fal	lback	203.0.113.6	ò	
Caches	> State				
Settings	•				
e	Devices		Delete		
SSL Orchestrator				OK	Cancel
Acceleration		highed sited a			Cancer
	BIG-IP	bigip1.site1.e	example.com	20.0.113.5	
Device Management	System Devices			Click"OK"	
e Network					
System					

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



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

Resource

Virtual Server Discovery Enabled	
Link Discovery Enabled	
Cancel Repeat Finished	

TMSH

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

site2_ha-pair

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



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

1. Fill in the Name and Datacenter

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Time	: Jul 20, 2017 User: admin :: 5:52 PM (CDT) Role: Administra	tor
CONLINE (ACTIVE) Standalone		
Main Help About	DNS » GSLB : Servers : Server	List » New Server
Market Statistics		
_	General Properties	
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	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

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Tim	te: Jul 20, 2017 ne: 5:56 PM (CD1	User: admin) Role: Administrator	P	artition: Common
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » GS	LB : Servers : Server Lis	t » New Server	
Statistics	General Pro	Device N	ame: bigip1.site2.example.com 198.51.100.37	
ONS	Product	Translatio	on: (C	Optional)
Delivery	Data Cente	er Link:	Auto-Select	
GSLB	ick "Add	Page 400	00.27	
Zones	Prober Fall	back	00.57	
Caches	State			
Settings	Devices	Delete]	
SSL Orchestrator		Add		OK Cancel
Acceleration		Device No data available in table	Name Addre:	SS
Device Management	BIG-IP System Devices		Click"OK"	
System				

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

Hostname: gtm1.site1.example.com Da IP Address: 10.1.10.13 Tir	ite: Jul 20, 2017 ne: 6:13 PM (CDT)	User: admin Role: Administrate	or	Partition: Common
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » GSLB	: Servers : Server I	List » New Server	
Marco Statistics				
iAnns	General Proper	ties		
- in the	Name 💻		site2_ha_pair	
S DNS	Product		BIG-IP System	
Delivery	Data Center	\longrightarrow	site2_datacenter	
GSLB >	Prober Prefere	nce	Inherit From Data Center 🗸	
Zones	Prober Fallbac	k	Inherit From Data Center 🔽	
Caches	State		Enabled 🔽	
Settings				
e	Devices	C	lick "Add"	
SSL Orchestrator	Add	1		
		Dev	rice name	Autress
Received	BIG-IP	p1.site2.example.co	m	198.51.100.37
Device Management	System Devices			
Retwork				
System	Edi	Delete		

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

Hostname: gtm1.site1.example.com D IP Address: 10.1.10.13 Ti	ate: Jul 20, 2017 ime: 6:22 PM (CDT)	User: admin Role: Administrator	Partition: Common
ONLINE (ACTIVE) Standalone			
Main Help About	DNS » GSLB:	Servers : Server List » New Serve	r
Statistics	General Propert	Device Name: bigip2.site	2.example.com
iApps	Name	Address: 198.51.10	0.38
🕥 dns	Product	Translation:	(Optional)
Delivery		2 ^{k:} Auto-Sele	
GSLB	Prober Preferen	Ce Add	
Zones	Prober Fallback	190.51.100.56	
Caches	State		
Settings	Devices	Delete	
SSL Orchestrator	Add		3 OK Cancel
Acceleration	bigip	Device Name 1.site2.example.com	Address 198.51.110.37
Device Management	BIG-IP System Devices		Click"OK"
Retwork			
System	Edit	Delete	

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

DNS Documentation

Hostname: gtm1.site1.example.com Dat IP Address: 10.1.10.13 Tim	e: Jul 20, 2017 e: 7:55 PM (CI	'User: admin DT) Role: Administra	ator	Partition: Common
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » G	SLB : Servers : Server	List » New Server	
Statistics	General Pr	operties		
iApps	Name		site2_ha_pair	
😚 dns	Product		BIG-IP System	
Delivery	Data Cer	nter	site2_datacenter	
GSLB	Prober Pro	eference	Inherit From Data Center	2
Zones	Prober Fa	llback	Inherit From Data Center	2
Caches	State		Enabled V	
Settings	Dovicos			
SSL Orchestrator	Devices	Add		
Acceleration		Digip1.site2.example.co	owies Marris om	198.51.100.37
Device Management	BIG-IP System	bigip2.site2.example.co	om	198.51.100.38
Retwork	Devices			
System		Edit Delete		
	Configurat	ion: Advanced 🔽		
	Health Mo	onitors	Selected /Common bigip	Available /Common gateway_icmp gtp http http_head_f5
	Availability	/ Requirements	All Health Monitors 🔽	

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

Resources	
Virtual Server Discovery	Enabled
Link Discovery	Enabled
Cancel Repeat Finished	

TMSH

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

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

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

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



Click the create button and continue to define objects

Hostname: gtm1.site1.example.com Date IP Address: 10.1.10.13 Time	: Jul 20, 2017 User: ad :: 2:00 PM (CDT) Role: A	d min Administrator	Partition: Common
Standalone	_		
Main Help About	DNS » GSLB : Servers :	: Server List	
Statistics	🔅 👻 Server List	Trusted Server Certificates	Statistics 💌
iApps	*	Search	Create
😚 dns	Status A Name	Devices	Address
Delivery	No records to display.		
GSLB	Enable Disable Dele	ete	
Zones >			
Caches	Clic	:k "Create" to d	efine atm1.site1
Settings >			
SSL Orchestrator			
Acceleration			
Device Management			
e Network			
System			

4.5.2 Device Trust

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

Hostname IP Address	s: gtm1.site1.example.com s: 10.1.10.13	Date: Time:	Jul 20, 2 8:05 PM	017 (CDT)	User: ac Role: A	dmin dministrato				Partition: Com	mon
Main	ONLINE (ACTIVE) Standalone		DNS	GSLP	Samore	Server	iet				
A Stati	stics		₩ -	Server L	ist	Trusted	Server C	ertificates Sta	tistics 🔎		
							_				
iApp	5		*					Search			
😚 dns				Status	 Name 		Devices	Address	Data Center	Virtual Servers	Pr
De	elivery	•		0	gtm1.site1	1_server	1	203.0.113.7	site1_datacenter	0	BI
G	SLB	•			gtm1.site2	2_server	1	198.51.100.39	site2_datacenter	0	BI
Zo	ones	•			site1_ha-j	pair	2	203.0.113.5 203.0.113.6	site1_datacenter	0	BIC
Ca	aches	•			site2_ha_	pair	2	198.51.100.37 198.51.100.38	site2_datacenter	0	BIG
Se	ettings	- × -	Enable	Disa	ble Dele	te					-
🔓 SSL	Orchestrator		Th	ree	other	serve	ers n	eed to "	establish	trust"	
🔊 Acce	eleration										
Devi	ce Management										
Netw	vork										
Syste	em										

1. Launch Putty and login to gtm1.SITE1

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

TMSH

bigip_add



2. Observe the exchanged certificates

Hostname: gtm1.site1.exa IP Address: 10.1.10.13	mple.com Da Tin	te: Jun 25, 2017 ne: 3:36 PM (CDT)	User: admi Role: Admi	n nistrator	
ONLINE (A Standalone	CTIVE)				
Main Help	About	DNS » GSLB: S	Servers : Tr	usted Server Certificates	•
Mage Statistics		🔅 🗸 Server List	t T	rusted Server Certificates	Statistics 🔎
iApps		General Properties	s		
S DNS		Name		server	
Delivery	•	Partition / Path			
GSLB	•	Wide IPs	Þ	gtm1.site2.example bigip2.site1.example	.com, MyCompany e.com, MyCompany
Zones	→	Pools	•	bigip1.site2.example	e.com, MyCompany e.com, MyCompany
Caches		iRules	•	gtm1.site1.example	.com, MyCompany
Settings		Data Centers	×		
e	7	Servers	÷ ۹	Server List 🛞	
SSL Orchestrator		Links		Trusted Server	
Acceleration	K	Prober Pools		Certificates	' GMT
		Monitors	0	Statistics	
Device Managemen	it	Topology	•	234963207	
				Common Name: d	m1 site? evample.com

3. Observe the server status

Hos IP A	stname: Address:	gtm1.site1.example.com 10.1.10.13	Date: Time:	Jul 26 3:44 P	5, 2018 PM (EDT)	User: Role:	admin Administrato	or				Partition:	ommor
ſ	5	ONLINE (ACTIVE) Standalone											
N	Main	Help About		DNS	s » GSLB	Server	s : Server l	List					
~	Statis	tics		* •	Server L	ist	Trusted	I Server C	ertificates		stics 🔎		
	iApps			*				×	Search				
53	DNS				▼ Status	A Nam	е	Devices	Address		Data Center	Virtual Serve	rs Pro
_	Del	iverv	•		۲	gtm1.si	te1_server	1	203.0.113	3.7	site1_datacenter	0	BIC
	GS	LB	•		۲	gtm1.si	te2_server	1	198.51.10	0.39	site2_datacenter	0	BIC
	Zor	nes	•		•	site1_h	a-pair	2	203.0.113 203.0.113	3.5 3.6	site1_datacenter	3	BIC
	Ca	ches	•		•	site2_h	a-pair	2	198.51.10 198.51.10	0.37	site2_datacenter	2	BIC
	Set	tings	•	Ena	ble Disal	ble De	elete						
	Accel	eration		C	re	en	G	re	en		Gree	n !	
	Devic	e Management						_					_
	Netwo	ork											
	Syste	m											

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

4.5.3 Sync Group

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

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

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

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

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



TMSH

gtm_add 203.0.113.7

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

please refer to the link below.

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

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

Hostname: gtm1.site1.example.com IP Address: 10.1.10.13	Date: Jul 20, 2017 User: admin Time: 1:45 PM (CDT) Role: Administrator	Partition: Common
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » GSLB : Data Centers : Data Center List	
Mage Statistics		ate"
iApps	* Search	Create
😚 dns	Availability Availability	Location Links
Delivery	No records to display.	
GSLB	Wide IPs ie	
Zones	> Pools >	
Caches	iRules (+)	
Settings	Data Centers Data Center List 📀	
SSL Orchestra or	2 Servers 3 Statistics	
Acceleration	Prober Pools	
Device Management	Monitors 📀	
	Topology	
Network	Distributed Applications	
System		

Create two data centers according to the table below:

Field	Value
Name	site1_datacenter
Name	site2_datacenter

Hostname: gtm1.site1.example.com IP Address: 10.1.10.13	Date: Jul 20, 2017 Time: 1:48 PM (CDT)	User: admin Role: Administrator	Partition: Common
ONLINE (ACTIVE) Standalone		Data Contore - Data (Santar Lint
Main Help About	UNS » GSLB ; I	Data Centers : Data (enter List
Statistics	General Propertie	es	
iApps	Name	sit	e1_datacenter
😚 dns	Description		
Delivery	Location		
GSLB	Contact		
Zones	Prober Preference	e Ins	ide Data Center
Caches	Prober Fallback	An	y Available
Settings	State	En	abled V
SSL Orchestrator	Cancel Repea	t Finished	
Acceleration			
Device Management	Repeat	this step to	o create "site2_datacenter"
Network			
System			

TMSH command for only site1.gtm1:

TMSH

tmsh create gtm datacenter site1_datacenter

TMSH

tmsh create gtm datacenter site2_datacenter

4.6 Pools

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

Hos IP A	tname: g ddress:	gtm1.site1.exan 10.1.10.13	nple.com	Date: Time:	Jul 26, 3:58 Pl	2018 M (EDT)	Partition:	Common	~	Log ou	it
(5	ONLINE (AC Standalone	TIVE)								
N	lain	Help	About		DNS	» GSLB:	Pools : Po	ool List			
M	Statisti	cs			⇔ -	Pool List		Statistics			
	iApps										
0.55					*				× Sear	ch	Create
5	DNS					 Status 	Name	Type	Member	s 🗢 Parti	tion / Path
	Deliv	very		F	No re	cords to di	splay.				
	GSL	B 🚺	4	۶.	Wide IF	°s		te			
	Zone	es			Pools	;	-	Pool List	(•	
	Cach	nes		~	iRule	s	0	Statistics		2	
	Setti	ngs		F	Data O	enters	F				
	Accolor	ration	//		Serve	ers	Þ				
	Accelel				Links		+				
	Device	Management			Probe	er Pools	F				

Field	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

IP Ac	name: gtm1.site1.example.com kdress: 10.1.10.13	Date Time	: Jul 26, 2018 : 4:11 PM (EDT)	User: admin Role: Administra	rator Partition: Common V
	Standalone				
M	ain Help Abo	ut	DNS » GSLB	: Pools : Pool Lis	ist » New Pool
	Statistics		General Propert	ties	
3	iApps		Name		www.example.com_pool ×
5	DNS		State		Enabled V
	Delivery	÷	Continuetion		
	GSLB		Configuration		Onlandar Australia
	Zones				Available //Common
	Caches		Health Monitors	3	gateway_icmp
	Settings	\rightarrow			http v http_head_f5
	Acceleration				Up Down
•••	Acceleration		Availability Req	uirements	All Health Monitors
	Device Management				Bits: Disabled
	Network		Limit Settings		Packets: Disabled V Current Connections: Disabled V
	System		Manual Resum	e	
			TTL		30
			Dynamic Ratio		
			Maximum Ansv	vers Returned	1
			Verify Member	Availability	
			Members		Select two LTM VIP's and click "Add"
			Load Balancing Method	Preferred: Round Alternate: Round Fallback: Return	nd Robin Ind Robin
			Fallback IP	0.0.0.0	
			Member List	Virtual Server: s Ratio: 1 Add //Common/isp1_ //Common/isp2 s Delete Up Dow	Select 1 site1_www.example.com_tcp_https_virtual (/Common/site1_ha-pair) - 203.0.113.9:443, Ratio(1) site2_www.example.com_tcp_https_virtual (/Common/site2_ha-pair) - 198.51.100.41:443, Ratio(1) wm

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 } } }

4.7 FQDN

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



Create an F5 "wide IP" according to the following table:

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

DNS Documentation

Hostname: gtm1.site1.example.com Date: IP Address: 10.1.10.13 Time:	Jul 29, 2018 User: admin 4:13 PM (EDT) Role: Administra	tor Partition: Common V Log out
ONLINE (ACTIVE) Standalone		
Main Help About	DNS » GSLB : Wide IPs : Wide	IP List » New
Statistics		
iAnne	General Properties: Advanced	
interior interior	Name	www.example.com
S DNS	Туре	A
Delivery >	Description	
GSLB		Alias: www.gslb.example.com
Zones		Add
Caches	Alias List	www.gsib.example.com
Settings		
Acceleration		Delete
Device Management	State	Enabled 🔽
	Minimal Response	Enabled 🔽
Network	Return Code On Failure	Disabled
System	Load-Balancing Decision Log	 ✓ Pool Selection ✓ Pool Traversal ✓ Pool Member Selection ✓ Pool Member Traversal
	iRules	
		Selected Available
For trouble	shooting enable	
par poses		
verbose l	ogging	
	iRule List	Selected Available
	Pools	
	Load Balancing Method	Round Robin
	Persistence	Disabled V
200 Chapte	r 4. Class 3 - Data Center	Availability Services Using BIG-IP DNS Pool Select

TMSH command to run on only gtm1.site1:

TMSH

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

Results

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

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

Note: Your result may differ from below



IP Ad	name: ddress:	gtm1.site1.exam 10.1.10.13	nple.com	Date: Time:	Jul 29, 2018 11:11 PM (EDT)	Partition	Common	~	Log	out
	5	ONLINE (ACT Standalone	TIVE)							
Ma	ain	Help	About		DNS » GSLB	: Wide IPs	: Wide IP Li	ist		
<u>~</u>	Statisti	CS			🔅 👻 Wide IP	List	Statistics	Ø		
i	iApps				*	_		× Se	arch	Crea
()	DNS				Status	 Name 		Type	Aliases	
					_					
	Deliv	/ery		×		www.exan	nple.com	A	www.gslb.	exam
	Deliv GSL	very		•	Wide IPs	www.exan	Wide IP Li	A	www.gslb.	exam
	Deliv GSL Zone				Wide IPs 2 Pools	www.exam	Wide IP Li	A	www.gslb.	exam
	Deliv GSL Zone Cach	very B es hes			Wide IPs 2 Pools iRules	www.exan	Wide IP Li	A	www.gslb.	exam
	Deliv GSL Zone Cach Setti	very B es hes ings)))))	Wide IPs 2 Pools IRules Data Centers	www.exan	Wide IP Li Statistics	A	www.gslb.	exam
	Deliv GSL Zone Cacl Setti	very B es nes rus			Wide IPs 2 Pools iRules Data Centers Servers	www.exan	Wide IP Li Statistics	A	www.gslb.	exam

Hos IP A	stname: gtm1.site1.example.com Address: 10.1.10.13	Date: Time:	Jul 29, 2018 User: ad 11:21 PM (EDT) Role: Ad	min ministrator			Partition	n:
(ONLINE (ACTIVE) Standalone							
N	Main Help About		Statistics » Module Statis	tics : DNS : GS	LB			
-	Statistics		🚓 🚽 Traffic Summary 👻	DNS	✓ Subset	riber Management	Network	
	Dashboard	e.						
	Module Statistics	÷	Display Options					
	Analytics	•	Statistics Type	Wide IPs		\checkmark		
	Performance	•	Data Format	Normaliz	ed 🗸			
-	iApps		Auto Refresh	Disabled	Refres	h	Provente	
S	DNS		Status - Wide IP	Туре	Partition / Pat	Details Pools	Total Resolved R	le
	Acceleration		www.example.c	om A	Common	View /iew	44 44 0	
3	Device Management		Reset					
	Network		For mo	re (deta	ails c	lick	
8 🕈	System							

TMSH

tmsh show gtm wideip A www.example.com detail

🚽 gtm1.SITE1	_					_ 0
[root@gtm1:Active:Standal	one] config <mark>#</mark> tm.	sh show gtm	wideip .	A www.exampl	e.com detail	
Gtm::WideIp: <mark>:</mark> A www.exampl						
Status						
Availability : availabl	e					
State : enabled						
Reason . Availabl						
Requests						
Persisted 0						
Resolved 44						
Dropped O						
Load Balancing						
Preferred 44						
Fallback 0						
CNAME Resolutions 0						
Returned from DNS 0 Returned to DNS 0						
Failures with RCODE 0						
Gtm::Pool::A www.exam	ple.com_pool					
Status						
Availability : avai	lable					
State : enab Reason : Avai	lable					
Load Balancing Preferred	44					
Alternate	0					
Fallback	0					
Returned from DNS	0					
Dropped	õ					
Gtm::Pool Member:	www.example.com	pool:A isp1	site1 w	ww.example.c	om top https	virtual:site1 ha-pair
Status	wailable					
State : e	nabled					
Reason : A	vailable					
Load Balancing						
Preferred 35						
Alternate 0						
railback o	, 					
Gtm::Virtual Se	rver: isp1_site1	_www.exampl	e.com_tc	p_https_virt	ual	
l Statua						
Availability	: available					
State						
Reason Destination	: Monitor /Comm : 203.0.113.9:44	on/bigip fr 3		.113.5 : UP		
Up Time	: 10:18					
I fink Mama	203 0 1	13 1				
	203.0.1	10.1				
Global		0.5				
Picks Connections		35				
Virtual Serve	r Score	1				
 Throughput		In Out				
Bits/sec		0 0				
Packets/sec						
Gtm::Pool Member:	www.example.com_	poulth isp2	_tita?_r	na grankşu c	າະຫຼະດກູ∛ລະະຫa	yézturá:mite?_bu-puis
Status						
Availability : a	wailable					
State : e Reason : A	nabled Wailable					

TMSH

tail -f /var/log/ltm

Antm1.STTF1
Front@dtm1.bctive.Standalonel_config # tail_f _n 12 /var/log/ltm
Jul 30 00:19:49 gtml info tmm[1966]: 2018-07-30 00:19:49 gtml.sitel.example.com gid 991 from 198
.51.100.68#64119: view none: query: www.gslb.example.com IN & + (203.0.113.8%0)
Jul 30 00:19:49 gtml info tmm[1966]: 2018-07-30 00:19:49 gtml.site1.example.com gid 991 from 198
.51.100.68#64119 [www.gslb.example.com A] [round robin selected pool (www.example.com pool)] [poo
1 member check succeeded (isp1 site1 www.example.com tcp https virtual:203.0.113.9) - pool member
state is available (green)] [round robin selected pool member (isp1 site1 www.example.com tcp ht
tps virtual:203.0.113.9)]
Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com qid 991 to 198.5
1.100.68#64119: [NOERROR qr,aa,rd] response: www.gslb.example.com. 30 IN & 203.0.113.9;
Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 from 198
.51.100.68#64120: view none: query: www.gslb.example.com IN & + (203.0.113.8%0)
Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 from 198
.51.100.68#64120 [www.gslb.example.com A] [round robin selected pool (www.example.com_pool)] [poo
l member check succeeded (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9) - pool member
state is available (green)] [round robin selected pool member (isp1_site1_www.example.com_tcp_ht
tps_virtual:203.0.113.9)]
Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 to 198.5
1.100.68#64120: [NOERROR qr,aa,rd] response: www.gslb.example.com. 30 IN A 203.0.113.9;
Jul 30 00:23:44 gtml info tmm[11966]: 2018-07-30 00:23:43 gtml.sitel.example.com qid 261 from 203
.0.113.68#64121: view none: query: www.example.com IN & + (203.0.113.8%0)
Jul 30 00:23:44 gtml info tmm[11966]: 2018-07-30 00:23:43 gtml.sitel.example.com qid 261 from 203
.0.113.68#64121 [www.example.com A] [round robin selected pool (www.example.com_pool)] [pool memb
er check succeeded (isp2_site2_www.example.com_tcp_https_virtual:198.51.100.41) - pool member sta
te is available (green)] [round robin selected pool member (isp2_site2_www.example.com_tcp_https_
virtual:198.51.100.41)]
Jul 30 00:33:44 gtml info tmm[11966]: 2018-0/-30 00:23:43 gtml.sitel.example.com qid 261 to 203.0
.113.68#64121: [NOLKKOK dr,aa,rd] response: www.example.com. 30 IN & 198.51.100.41;
Jul 30 00:33:50 gtml info tmm[11966]: 2018-0/-30 00:33:50 gtml.sitel.example.com q1a 97 from 203.
0.113.65764122: view hone: query: www.example.com iN x + (203.0.113.650)
Sui so doississo gumi into unmilipsoj: 2010-00/-so doississo gumi.sitel.example.com qiu 9/ from 20s.
U.113.66#94122 [www.example.com x] [round robin selected poor (www.example.com poor)] [poor membe
is everylated (reprint role and role an
the available (green) [Found form selected poor member (ispi_steel_www.example.com_ttp_nttps_vif
Jul 30 00:23:50 gtml info tmm[11966] · 2018-07-30 00:23:50 gtml_sitel.example.com gid 97 to 203.0

4.8 Delegation

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

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



4.8.1 A Records

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

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

🥠 I	🖫 DEN1 - 10.1.70.200 - Remote Deskto	n Connection		
Postman	Å DI	NS Manager	_	
~	File Action View Help			
a	🗢 🏟 🖄 📅 🗙 🗒 🙆	Click arrows	to expand	
Internet Explorer	🚊 DNS	Name Type	Data	Timestamp
Explored	📕 🖬 🗍 DC01			
100	Forward Lookup Zones			
	🔰 🕛 👌 🛐 _msdaneXAMPLE.CC	tcp		
dig_www-ex	EXAMPLE.COM			
	🕘 þ 🛐 _msdcs	in anch01		
	▷ ites	DomainDnsZones		
	⊳ 🚞 _tcp	EorestDasZones		
DC01	⊳ 🛄 _udp			
DC01	þ 🧰 branch01	ingine site1		
	DomainDnsZones	ite?		
	▷	Site2 (same as narent folder) Start of Authority (SO)	 [637] dc01 example com 	static
	⊳ 🚞 mgmt	(same as parent folder) Start of Additionty (SO.	dc01 overanle com	static
agility_pub-key	⊳ 🚞 site1	(same as parent folder) Name Server (NS)	10.1.70.000	7(20(2010.0)
	⇒ ite2	same as parent roller) Host (A)	10.1.71.100	7/30/2018 8:
	Reverse Lookup Zones	Elentor Host (A)	10.1.71.100	// SU/ 2018 /:
💼 🔁 🛛	▷ Irust Points		10.1.70.200	static
adility prv key	Conditional Forwarders	docs Host (A)	10.1.10.60	static
ogiiicy_prv_koy	Global Logs	sorry Host (A)	10.1.71.21	static
		Www Host (A)	203.0.113.9	
Notopod L L		e	🔺 Þ 🗜 🕼	9:23 AM
Notepau++				7/50/2016
💐 Start 🛛 🧯	🎒 🧬 ᇘ 🖬 🌄 DC01 - 10.1.70.	200 - Re	× P 🛍 📢	🧿 9:23 AM 📃

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



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

Field	Value
ns1	203.0.113.8
ns2	198.51.100.40



Create ns2.example.com

I	👼 DC01 - 10.1.70.200 - Remote	Desktop Connection		
	Å	DNS <u>Mana</u>	iger	
BIG-IP Edge	File Action View Help	New Host 🗙		
Clienc	🗢 🔿 🙍 📰 🗶 🗐 🧔	Name (uses parent domain name if blank):		
	🚊 DNS	ns2	Data	Time:
agility_pub		Fully qualified domain name (FQDN): ns2.EXAMPLE.COM.		
2	▷ □ _msdcs ▷ □ _sites	IP address: 198.51.100.40		
agility_prv	▷ □ _tcp□ _udp□ branch01▷ □ DomainDnsZq	Create associated pointer (PTR) record Allow any authenticated user to update DNS records with the same owner name		
PuTTY (64-bi	▷ ☐ ForestDnsZon ▷ ☐ mgmt ▷ ☐ site1 ▷ ☐ site2		[152], dc01.example.com., dc01.example.com. ns1.branch01.example.com.	static static static
Notepad++	▷ ²¹ Reverse Lookup Zon ▷ ²¹ Trust Points ▷ ²¹ Conditional Forwarde ▷ ¹¹ Global Logs	rs dc01 Host (A)	10.1.70.200 10.1.71.100 10.1.70.200 203.0.113.9	6/26/ 6/26/ static static
Ð	<	ns1 Host (A)	203.0.113.8	
A start		DC01 - 10.1.70.200 - Re		

4.8.2 Sub Domain

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

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

堤 DC01 - 10.1.70.200 - Remote Desktop Connection					
Å.	DNS Manager				
File Action View Help					
🔶 🔶 📶 🗶 🗈 Q 🕞 🗾 🗾 🗄 🖬 🖏					
DNS DC01 Forward Lookup Zones Forward Lookup Zones Condi Con	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	Timestamp static static static 6/26/2017 12:00:00 / 6/26/2017 12:00:00 / static		
ureate a new delegated DNS domain.					

2. Create the "gslb" subdomain.



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



Repeat to add ns2.example.com

- 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 Forward Lookup Zones C02 EXAMPLE.COM C02 EXAMPLE.COM C02 C02 C02 C02 C02 C02 C02 C02	 msdcs sites tcp udp branch01 DomainDnsZones ForestDnsZones mgmt site1 site2 (same as parent folder) ns1 	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. Add Edit Remove Add Edit Remove
III >	ns2	Host (A) 198.51.100.40
2	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	x
b 📰 🗙 🗊 Q 🗟		Name Servers You can select one or more name servers to host the delegated zone.	
>1 Forward Lookup Zones msdcs.EXAMPLE.CC msdcs.EXAMPLE.COM >sites >sites >udp >udp >branch01 >ForestDnsZones >mgmt >site2 Reverse Lookup Zones	<pre>Name _msdcs _sites _tcp _udp branch01 DomainDnsZones ForestDnsZones mgmt site1 site2 (same as parent folder) (same as parent folder) (same as parent folder) (same as parent folder) (same as parent folder)</pre>	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] Add Edt	>
Conditional Forwarders	dc01	<back next=""> Cancel</back>	
Global Logs	ns1 ns2	Host (A) 198.51.100.40	
III >			
			•

6. Click "Finish"



4.8.3 CNAME

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

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

🔚 DC01 - 10.1.70.200 - Remote De	esktop Connection			
å.		DNS Ma	nager	
File Action View Help				
🗢 🏟 🖄 📷 🗶 🖼 🔒	? 🖬 🗂 🖬			
 DNS DC01 Forward Lookup Zones Smsdcs.EXAMPLE.COM Smsdcs 	Name msdcssitestcpudpbranch01DomainDnsZonesForestDnsZonesmgmtsite1site2gslb(same as parent folder)(same as parent folder) Delete Properties	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	Static static static 6/26/2017 12:00:00 Å 6/26/2017 12:00:00 Å static
Right Click - De	Help			
< III >				
Deletes the current selection.				
	A			

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



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

😓 DC01 - 10.1.70.200 - Remote De	sktop Connection			
å		DN	S Manager	
File Action View Help				
🗢 🄿 🙍 📰 🗶 📴 🧟 🖻		(i)		
 DNS DC01 Forward Lookup Zones 	Name Same Market Ma	Туре	Data	Timestamp
msdcs.EXAMPLE.CC	🛄 _tcp	New Re	esource Record	×
b C	udp branch01 DomainDnsZon	Alias (CNAME)	ZLOLL IN	_
▷ 🔜 _tcp ▷ 🚰 _udp ▷ 🦳 branch01	ForestDnsZones	Alias name (uses parent domain i	ir iert blank):	
▷ CompainDesize DomainDesize DomainDesize Desize Desiz	site1	Fully qualified domain name (FQD www.EXAMPLE.COM.	DN):	
p <u> </u>	🔲 (same as parent	Fully qualified domain mane (FQD	DN) for target host:	c
⊳ 🧰 site2	📄 (same as parent	www.gslb.example.com.	Browse	c
 Image: Second Sec	 (same as parent (same as parent client01 dc01 ns1 ns2 	Allow any authenticated user name. This setting applies on	B.example.com to update all DNS records with the sam by to DNS records for a new name.	c /2017 12:00:00 A /2017 12:00:00 A c
			OK Cano	4
			Calif	
< III >				
	.			

4.8.4 Results

From the Jumpbox use "dig" from the CMD prompt

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

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



Hostr IP Ad	name: Idress:	gtm1.site1.exam 10.1.10.13	ple.com	Date: Time:	Jul 29, 2018 11:11 PM (EDT)	Partition	Common	~	L	og out
	5	ONLINE (ACT Standalone	NVE)							
Ma	ain	Help	About		DNS » GSLB	: Wide IPs	: Wide IP Li	st		
<u>~</u>	Statisti	ics			🔅 👻 Wide IP	List	Statistics			
i 🔂	Apps				*	_		× Se	arch	Crea
() I	DNS				Status	 Name 		Type	Aliase	es
	Deli	very		F		www.exan	nple.com	A	www.gs	lb.exan
	GSL	.B		-	Wide IPs	•	Wide IP Li	st	÷	
	Zone	es	/	•	Pools		Statistics			
	Cac	he		F	iRulec	÷	3			
	Setti	ings		Þ	Data Centers	Þ				
	Setti			>	Data Centers Servers	ا ا				

Hos IP A	stname: gtm1.site1.example.com Address: 10.1.10.13	Date: Time:	Jul 29, 2018 U 11:21 PM (EDT) R	lser: admin tole: Administrat	tor				Part	ition:
ſ	ONLINE (ACTIVE) Standalone									
N	Main Help About		Statistics » Module	e Statistics : D	NS:GSL	B				
~	Statistics		🔅 🗸 Traffic Summ	ary v DNS	i	▼ Subscr	iber Managemen	t Netv	vork	
	Dashboard	æ								
	Module Statistics	•	Display Options							
	Analytics	•	Statistics Type		Wide IPs					
	Performance	•	Data Format		Normalized V					
3	iApps		Auto Refresh]	Disabled	Refresh		Re	quests	
5	DNS		Status 🔺 Wide	IP	Туре	Partition / Path	Details Pools	Total	Resolved	Ret
>	Acceleration		www.ex	ample.com	A	Common	View /iew	44	44	0
3	Device Management		Neser							
	Network		For n	nor	e (leta	ils d	li	ck	
0 +	System								<u> </u>	

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

TMSH

tmsh show gtm wideip A www.example.com detail

🚽 gtm1.SITE1						
[root@gtm1:Active:Standald	one] config <mark># tms</mark> h	show gtm w	videip A t	www.example.	com detail	
Gtm::WideIp: <mark>:A www.example</mark>						
Status						
Availability : available	2					
State : enabled						
Acason . Available						
Requests						
Persisted 0						
Resolved 44						
Dropped O						
Load Balancing						
Preferred 44						
Fallback 0						
CNAME Resolutions 0						
Returned from DNS 0						
Failures with RCODE 0						
Gtm::Pool::A www.examp	ple.com_pool					
Status						
Availability : avail	lable					
State : enab. Reason : Avail	led					
Load Balancing	14					
Alternate	0					
Fallback	0					
Returned from DNS	0					
Dropped	0					
Gtm::Pool Member: v	www.example.com po	ol:A isp1 s		.example.com	tep https v	irtual:site1 ha-pair
Status	zailabla					
State : er	habled					
Reason : Av	/ailable					
 Load Balancing						
Preferred 35						
Alternate 0						
Failback U						
Gtm::Virtual Ser	ver: isp1_site1_v	ww.example.	.com_tcp_1	https_virtua	1	
Availability :	available					
State						
Reason	Monitor /Common	/bigip from		13.5 : UP		
Up Time	10:18					
	202 0 112					
Link Name	203.0.113	.1				
Global						
Picks		35				
Virtual Server	Score	1				
		To Out				
Bits/sec		0 0				
Packets/sec						
Gtm::Pool Member: t	www.example.com_po	olth ispl.:	eita2_sm	. อนสมญริก (อเวล)	tap_%strain	studistist ghu-puis
Status						
Availability : av	vailable					
State : er	habled					
Reason : A	allable					

TMSH

tail -f /var/log/ltm

Antm1.STTF1
Front@dtm1.bctive.Standalonel_config # tail_f _n 12 /var/log/ltm
Jul 30 00:19:49 gtml info tmm[1966]: 2018-07-30 00:19:49 gtml.sitel.example.com gid 991 from 198
.51.100.68#64119: view none: query: www.gslb.example.com IN & + (203.0.113.8%0)
Jul 30 00:19:49 gtml info tmm[1966]: 2018-07-30 00:19:49 gtml.site1.example.com gid 991 from 198
.51.100.68#64119 [www.gslb.example.com A] [round robin selected pool (www.example.com pool)] [poo
1 member check succeeded (isp1 site1 www.example.com tcp https virtual:203.0.113.9) - pool member
state is available (green)] [round robin selected pool member (isp1 site1 www.example.com tcp ht
tps virtual:203.0.113.9)]
Jul 30 00:19:49 gtm1 info tmm[11966]: 2018-07-30 00:19:49 gtm1.site1.example.com qid 991 to 198.5
1.100.68#64119: [NOERROR qr,aa,rd] response: www.gslb.example.com. 30 IN & 203.0.113.9;
Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 from 198
.51.100.68#64120: view none: query: www.gslb.example.com IN & + (203.0.113.8%0)
Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 from 198
.51.100.68#64120 [www.gslb.example.com A] [round robin selected pool (www.example.com_pool)] [poo
l member check succeeded (isp1_site1_www.example.com_tcp_https_virtual:203.0.113.9) - pool member
state is available (green)] [round robin selected pool member (isp1_site1_www.example.com_tcp_ht
tps_virtual:203.0.113.9)]
Jul 30 00:19:50 gtm1 info tmm[11966]: 2018-07-30 00:19:50 gtm1.site1.example.com qid 372 to 198.5
1.100.68#64120: [NOERROR qr,aa,rd] response: www.gslb.example.com. 30 IN A 203.0.113.9;
Jul 30 00:23:44 gtml info tmm[11966]: 2018-07-30 00:23:43 gtml.sitel.example.com qid 261 from 203
.0.113.68#64121: view none: query: www.example.com IN & + (203.0.113.8%0)
Jul 30 00:23:44 gtml info tmm[11966]: 2018-07-30 00:23:43 gtml.sitel.example.com qid 261 from 203
.0.113.68#64121 [www.example.com A] [round robin selected pool (www.example.com_pool)] [pool memb
er check succeeded (isp2_site2_www.example.com_tcp_https_virtual:198.51.100.41) - pool member sta
te is available (green)] [round robin selected pool member (isp2_site2_www.example.com_tcp_https_
virtual:198.51.100.41)]
Jul 30 00:33:44 gtml info tmm[11966]: 2018-07-30 00:23:43 gtml.sitel.example.com qid 261 to 203.0
.113.68#64121: [NOLKKOK dr,aa,rd] response: www.example.com. 30 IN & 198.51.100.41;
Jul 30 00:33:50 gtml info tmm[11966]: 2018-0/-30 00:33:50 gtml.sitel.example.com q1a 97 from 203.
0.113.65764122: view hone: query: www.example.com iN x + (203.0.113.650)
Sui so doississo gumi into unmilipsoj: 2010-00/-so doississo gumi.sitel.example.com qiu 9/ from 20s.
0.113.00#07122 [www.example.com x] [round round in Selecced poor [www.example.com poor] [poor member and the selecced poor [www.example.com poor] [poor [www.example.com poor] [www.example.com poor] [poor [www.example.com poor] [www
is even by (creen) [round robin selected not member (ign) site and some of the transformer better vir
is available (green) [Found form selected poor member (ispi_steel_www.example.com_ttp_nttps_vif
Jul 30 00:23:50 gtml info tmm[11966]: 2018-07-30 00:23:50 gtml.site1.example com gid 97 to 203 0

4.9 Failure Condition

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

2	
agility_prv	
_	Command Prompt
PuTTY (64-bit)	;; MSG SIZE rcvd: 72
	C:\Users\user.EXAMPLE>dig www.example.com
.	; <<>> DiG 9.3.2 <<>> www.cwample.com ;; global options: printcmd
Notepad++	;; ->HEADERX<- opcode: QUERY, status: NOERROR, id: 838 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
	;; QUESTION SECTION: ;www.example.com. IN A
1	ANSWER SECTION: www.example.com. 3600 IN CNAME www.gslb.example.com.
viozilia Firero	www.gslb.example.com. 30 IN A 203.0.113.9
5	;; SERUER: 10.1.70.200453(10.1.70.200) ;; WHEN: Sun Jun 25 21:37:31 2017 ;; MSG SIZE rcvd: 72
Google Chrome	C:\Users\user.EX0 IPLE>dig www.example.com
-	
2	
Recycle Bin	
💱 Start 🛛 🏉 Bi	IG-IP® - gtm1.site2.ex 🗦 🖸 💿 📷 Command Prompt 💋 🍢 DC01 - 10.1.70.200 - Re

Log into both the Active and the Standby ADC device in SITE1 and disable all interfaces. https://bigip1.site1.example.com/tmui/Control/jspmap/tmui/locallb/network/interface/list.jsp https://bigip2.site1.example.com/tmui/Control/jspmap/tmui/locallb/network/interface/list.jsp

IP Address: 10.1.10.11 Ti	me: 10:40 PM (EDT) Role	Administrator		
In Sync	·			
Main Help About	Network » Interfaces :	Interface List		
SSL Orchestrator	🚓 🚽 Interface List	Interface Mirroring	LLDP 🔻	Statistics
Statistics				
iApps	🕑 🗢 Status 🔺 Name			
	✓ UP 1.1			
	✓ UP 1.2			
Device Management	✓ UP 1.3			
Network	✓ UP 1.4			
Nework	✓ UP 1.5			
hterfaces	✓ UP 1.6			
Routes	Enable Disable			
Self IPs 📀				
Packet Filters	Clie	/ Uni	sahla	
Trunks			Dane	

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

TMSH

tmsh modify interface all disabled

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

Hostname IP Addres	e: gtm1.site1.example.co ss: 10.1.10.13	m Date: Time:	Aug 9, 20 11:01 PN	018 / (EDT)	User: Role:	admin Administrator				
6	ONLINE (ACTIVE) Standalone									
Main	Help Al	bout	DNS »	GSLB	: Servers	: Server List				
Magazaria	istics		* -	Server L	ist	Trusted Serv	er Certificates	Statistics	۸	
iApp	05		*				Search	,		
S DNS	3		•	Status	 Name 				Devices	A
D	elivery	÷		•	gtm1.site	1_server			1	20
G	SLB	•		0	gtm1.site	2_server			1	19
Z	ones	Þ		•	site1_ha-	pair			2	2(2(
С	aches	•		0	site2_ha-	N ir			2	19 19
S	ettings	•	Enable	Disa	ole Dele	ete				
Acce	eleration									
📄 Devi	ice Management		Si	te:	LH	A pa	ir is	Dow	/n	
🤶 Netv	vork									

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

TMSH

tmsh show gtm server



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

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

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

TMSH

tmsh modify interface all enabled

4.10 Rest API

4.10.1 Authenticate

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

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

1. Reveal the navigation panel in Postman



2. Click on "Authenticate and Obtain Token from gtm1.site1".



3. Click on the "Send" button in the top right.

Get GTM F Create a \	example.com_en	vironment	*	•	*
		\frown	Examp	oles (0)	•
	Params	Send 🝷	s	ave	*
			Coo	kies (Code

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

POST	https://{{gtm1.site1}}/mgmt/shared/authn/login							
Pretty	Raw Preview JSON -							
1 ▼ { 2 3 ▼ 4 5	"username": "admin", "loginReference": { "link": "https://localhost/mgmt/cm/system/authn/providers/local/login" }, "loginDecuiderWare", "logal"							
5 7 - 8 9	"loginProviderName": "local", "token": { "token": "IK54KQEQECEBAS3UHUAOMOW5XV", "name": "IK54KQEQECEBAS3UHUAOMOW5XV",							
10 11 12 - 13	"userName": "admin", "authProviderName": "local", "user": { 							
14 15 16	<pre>}, "groupReferences": [], "timeout": 1200,</pre>							
17 18 19 20	"start/ime": "2018-08-07/11:40:20.671-0400", "address": "10.1.10.100", "partition": "[All]", "generation": 1,							
21 22 23	<pre>"lastUpdateMicros": 1533656420670671, "expirationMicros": 1533657620671000, "kind": "shared:authz:tokens:authtokenitemstate", "kind": "shared:authz:tokens:authtokenitemstate",</pre>							
24	<pre>}, Setternk : netps://iocarnosi/mgme/snared/autnz/tokens/ik54kQEQECEBAS50H0A0MDW5KW* },</pre>							

4.10.2 POST

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

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



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

4.10.3 Results

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

Note: Use FTP credentials admin/admin

🔁 admin@ftp.example.com - FileZilla
File Edit View Transfer Server Bookmarks Help New version available!
🔛 - 🖹 🗂 🚍 😂 比 😣 🛼 🔛 🔳 🍳 🤌 🦚
Host: [ftp.example.com Username: admin Password: ••••• Port: Quickconnect •
Status: Resolving address of ftp.example.com
Status: Connecting to 203.0.113.9:21
Status: Connection established, waiting for welcome message
Status: Insecure server, it does not support FTP over TLS.
Status: Logged in
Status: Retrieving directory listing
Status: Calculating timezone offset of server
Status: Timezone offset of server is 0 seconds.
Status: Directory listing of "/home/admin" successful

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

4.10.4 Active/Standby

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

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

Open Postman and send both of the patch commands below.



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

4.10.5 API Extras (Optional)

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

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

	Ģ
≻ liii	API 7 requests
) Ni	API Extras 3 requests
> Nii	DNS 67 requests
) Ni	DNS: Availabilty 12 requests
≻ hii	F5_Postman_Workflows 42 requests

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

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

update_do	KACVCIA BID				
	<mark>6</mark> Postman File Edit View Help				
Internet Explorer	🕂 New 🔻 Import	Runner 📭 🖛	example.com_workspace	🔹 🌲 Invite 🙆 🐚	e 1
filezilla.exe - Shortcut	Authentic Verify Autors 5	pen tr		steni Ve stma	^{com_e}
	POST - https://	({{etm1.site <mark>}}</mark> /memt/tm/etm	n a a	Params	
Comman	d Prompt	ADD	licatio	n"	
DC01.RE)P				
PuTTY (6	54-bit)	Documents			
Remote I	Desktop Connection	Downloads			
Postman		Percent literar	equest is not inheriting any auth the p	iorization helper at the mom arent's authorization helper.	ent. S
🚄 Wiresho	2	Recencicents •	ure p	arene a bachon control per	
2 Notepad	A Contraction of the second se	Computer			
Notepad OuteETP		Control Panel			
BIG-IP E	dge Client	Devices and Printers			
😪 Snipping	Tool				
		Default Programs			
	1	Administrative Tools			
		Run			
► All Progra	ams	Windows Security	- C =	Duild	Bee
1	rams and files	Log off		Bullo	Bro
Start	🍃 🧉 Rest API — Reference A	C:\Windows\system32\c	💋 Postman	gtm1.SITE1	🛃 user@docker:~/example

4.11 Congratulations

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

Class 4 - EDNS0 client subnet

5

This class covers the following topics:

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

Expected time to complete: 2 hours

5.1 Getting Started

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

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

5.1.1 Lab Topology

The following components have been included in your lab environment:

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

Lab Components

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

Component	VLAN/IP Address(es)	Credentials
bigip-dc1	 Management: 10.0.1.245 External: 10.1.0.245 	admin/f5edns0
bigip-dc2	 Management: 10.0.1.246 External: 10.2.0.245 	admin/f5edns0
bigip-router	• Management: 10.0.1.240	admin/f5edns0
Linux Jumphost	• Management: 10.0.1.50	ubuntu/supernetops
ubuntu server	• Management: 10.0.1.253	ubuntu/ubuntu

Follow these steps to get your lab started:

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



WELCOME TO THE AGILITY 2018 LABS.

Enter your class number and your student number.

	Class #:	Student #:		Submit	
ABOUT F5 Corporate Information Newsroom Investor Relations Careers Contact Information Marketing Guidelines	EDUCATION Training Certification F5 University Free Online Training	F5 SITES F5.com DevCentral Support Portal Partner Central F5 Labs	PREFERENCES Sign Out Update Profile Email Preferences	CONNECT WITH US Twitter in LinkedIn f Facebook YouTube dc DevCentral	
© 2018 F5 Networks, Inc. All rights r	eserved Policies Privacy Trademai	rks			

Welcome									
Welcome to F5's Automation, Orchestration and Programmability Training series. The intended audience for these labs are Super NetOps and DevOps engineers that would like to leverage the various programmability tools offered by the F5 platform. If you require a pre-built lab environment please contact your F5 account team and they can provide access to environments on an as-needed basis.									
The content contained here adheres to a pipeline. All content contained here is so repository:	The content contained here adheres to a DevOps methodology and automation pipeline. All content contained here is sourced from the following GitHub repository:								
https://github.com/f5devcentral/f5-auto	mation-labs/								
Bugs and Requests for enhancements are	e handled in two ways:								
Fork the Github Repo, fix or enhance	as required and submit a Pull	Request							
 https://help.github.com/articles/c 	reating-a-pull-request-from-a	-fork/							
• Open an Tocus shttps://aithub.com/f5dc More •	vcontrol/f5_outomotion_	lobs/issues	within						
O Stopping in: 02:43 (hr:min)				All VMs: Start	/ Stop	Help			
Standard		Charland		Started					
BIG-IP B	BIG-IP B Linux Jumphost		iWorkflow	Started					
SERVICES	SERVICES	MORE -	SERVICES						
тми	RDP		TMUI						
SSH: 129.146.151.219 Port: 22	SSH: 129.146.91.23 Port: 22		SSH: 129.146.147.110 Port: 22						
CONSOLE	CONSOLE		CONSOLE						
INFO	INFO		INFO						

To start your lab you will want to log into the linux jumpbox. From this you can then do all of the exercises in the lab. To log into the jump box for the lab start your session and access the jumpbox via RDP. Once the RDP window is open then just click to log in the "supernetops" user. You should not need a password.



5.2 Module – EDNS0 and client subnet

EDNS0 client subnet - RFC 7871

Problem: With the GSLB solution from f5 it is possible to use DNS to determine the geographical location of the user. We can't use the IP address of the client for this, because it is masked by the DNS resolver, and so the dns engine uses the IP address of the DNS resolver instead. In case of the Google DNS or OpenDNS servers, for many end users those servers are not close to them, simply because these providers don't have servers in every country and every ISP's network. For example, OpenDNS does not have DNS servers in South-America. Someone in Brazil using OpenDNS will likely hit their resolver in Florida. The F5 will then think the user is in Florida and as a result it will serve content to the user from a server far away (Florida, not Brazil) resulting in a slow, high latency experience.

Solution: To mitigate the problem of DNS based geo-targetting, Google proposed a technical solution to the issue in an IETF draft Client subnet information in DNS requests. This is an experimental DNS extension that allows DNS resolvers to pass the client's IP address (or part of) to compatible authoritative DNS servers.

The F5 DNS server can then use this information to better determine where the end user is. Google DNS and OpenDNS implemented this solution as part of the Global Internet Speedup initiative in August 2011.

The drawback is the experimental nature of the spec and limited support in existing DNS server software. Only OpenDNS and Google Public DNS seems to support it on the resolver side, but NOW with v14 of TMOS F5's DNS GSLB solution can use the Client-subnet options for decision making!

5.2.1 Lab – Setup lab and get logged into the components

This lab you will log into the jumpbox and then log into the east and west f5 dns nodes and inspect.

Task – Review basic configurations

In this task you will open a web browser and navigate east and west nodes.

Follow these steps to complete this task:

- 1. Log into the jumphost with the credentials provided in the setup section.
- 2. Open your web browser in the jumphost window.
- 3. Navigate to the east DC F5 and open another tab for the west DC.
- 4. Login with the username and password from the setup section.
- 5. After logging in take a look at the different settings for the interfaces and ip addresses and examine things to become comfortable with the environment and the two devices.

Task – Review the DNS profile

In this task you will review the dns profile used on the listeners and take note of any non-default configuration options. You will see three major changes. One of them is very important to EDNS0 client subnet operation, make sure that you understand that there is no button labeled "EDNS0" of any sort.

- 1. Navigate to "DNS : Delivery : Profiles : DNS "
- 2. Click the dns_nobind_edns0 profile and examine the options set.

Host IP A	tname: gtm_west.f5demo.com ddress: 10.0.1.245	Date: Jun 19, 2018 U Time: 2:58 PM (PDT) F	Jser: admin Role: Administrator		Partition: Common \$	Log out
ſ	Standalone					
M	lain Help About	DNS » Delivery	: Profiles : DNS »	Properties : dns_nobind_edns0		
M	Statistics	🔅 🗸 Properties				
-						
Lø	IApps	General Properties	S			
5	DNS	Name	dr	ns_nobind_edns0		
	Delivery	Partition / Path	Co	ommon		
	GSLB	Parent Profile		dns 🔶		
	Zones	Denial of Service	Protection			Custom 🗹
	Caches	Rapid Response	Mode	Disabled \$		
	Settings	Rapid Response I	Last Action	Drop \$		
	Local Traffic	Hardware Acceler	ation			
	Annalanatian	Protocol Validation	n 🗌	Disabled		
	Acceleration	Response Cache	0	Disabled		
	Device Management	DNS Features				
-	Shared Objects	DNSSEC		Enabled \$		
	Network	GSLB	0	Enabled		
	Network	DNS Express	0	Enabled		
8 🕈	System	DNS Cache		Disabled \$		
		DNS Cache Name	e (Select \$		 ✓
		DNS IPv6 to IPv4	(Disabled		
		Unhandled Query	Actions	Allow 🗘	-	
		Use BIND Server	on BIG-IP	Disabled \$		
		Insert Source Add Client Subnet Opt	Iress into ion	Enabled \$	-	۷
		DNS Traffic				
		Zone Transfer		Disabled \$		
		DNS Security		Disabled		
		DNS Security Pro	file Name	Select ♦		2
		Process Recursio	n Desired	Enabled		
		Logging and Repo	orting			
		Logging	,	Enabled 🛊	-	
		Logging Profile		dnslog_profile 💠		
		AVR Statistics Sa	mple Rate			
		Undate Delete				

Task – Review the DNS Logging profile

- 1. Navigate to "DNS : Delivery : Profiles : Other : DNS Logging "
- 2. Click the dnslog_profile profile and examine the options set.

3. Examine the log publisher by navigating to "System: Logs: Configuration: Log Publishers" and click on "local-log"

Hostname: gtm_west.f5demo.com IP Address: 10.0.1.245	Date: Jun 19, 2018 User: admin Time: 3:04 PM (PDT) Role: Administrato	r	Partition: Common 🛟	Log out
ONLINE (ACTIVE) Standalone				
Main Help About	DNS » Delivery : Profiles : Oth	er : DNS Logging		
Magazine Statistics	DNS Proto	col - Other -		
iApps				
		Search		Create
S DNS	✓ ♦ Name	\$	Log Publisher	Partition / Path
Delivery	dnslog_profile	lo	cal-log C	Common
GSLB	Delete			
Zones	•			
Caches	•			
Settings	•			
IP Address: 10.0.1.245 ONLINE (ACTIVE) Standalone	Time: 3:10 PM (PDT) Role: Administrat	я		
Main Help About	System » Logs : Configuration	: Log Publishers » local-log		
Statistics	roperties			
iApps	General			
S DNS	Name	local-log		
P-9 Local Texture	Partition / Path	Common		
	Description]
Acceleration	Log Destinations			
Device Management	_	Selected Avai	lable	
Shared Objects	Destinations	local-syslog		
Network				
System	Update Delete			

Task - Open a terminal session to view the log output

Follow these steps to complete this task:

- 1. Open the terminal application on the jumphost
- 2. Log into the GTM east and west in different windows via ssh using the admin login and use the following command to tail the log file.

tail -f /var/log/ltm



5.2.2 Lab – Examine GSLB objects

In the previous lab we reviewed the basic config and then set up a couple of terminal sessions to watch the dns logs. In this lab we will move forward and examine the GSLB objects that are set up, inspect listeners pool members and other GSLB objects

Task – Examine the DNS listeners and their profiles

In this task we will examine the listeners set up and make sure the dns profiles are set up correctly.

- 1. On both east and west F5s take a look at the listeners and remember the IPs as you will need them..
- 2. Navigate to DNS >> Delivery: Listeners: Listener List and select the listener your interested in viewing.
- 3. Make sure that the right dns profile is selected for the listeners. Also are there two listeners?

Hostname: gtm_west.f5demo.com Date IP Address: 10.0.1.245 Time	: Jun 19, 2018 User: admin : 3:23 PM (PDT) Role: Admir	Partition: Common 🗘 Log out				
CONLINE (ACTIVE) Standalone						
Main Help About	DNS » Delivery : Listener	s : Listener List » Properties : udp_listener				
Market Statistics	Properties	Load Balancing iRules Statistics				
iApps	General					
S DNS	Name	udp_listener				
Delivery	Partition	Common				
GSLB	Description					
Zones	State	Enabled \$				
Caches	Listener: Basic					
Settings	Destination	Type: O Host Network				
Local Traffic	VLAN Traffic	All VLANs \$				
Acceleration	Service: Basic \$					
Device Management	Protocol					
Shared Objects	DNS Profile	dns_nobind_edns0 \$				
- Network	Update Delete					
System						

Task - Review the DNS GSLB server objects

In this task we will review the servers used in the GSLB configuration.

- 1. Navigate your browser to DNS >> GSLB : Servers
- 2. Inspect the servers. Identify the servers and the underlying objects associated with them.
- 3. What is the state of the servers , green?

Hostn IP Ad	ame: gtm_west.15dem dress: 10.0.1.245	o.com Date: Time:	: Jun 19, 2018 : 3:24 PM (PDT)	User: adm Role: Adn	nin ninistrator			Partition:	Common \$	Log out
ſ	ONLINE (ACTIVE) Standalone									
Ma	in Help	About	DNS » GSI	.B : Servers :	Server List					
100 s	Statistics		🕁 🗸 Serve	er List	Trusted Server Ce	rtificates S	tatistics			
-										
L@ "	Apps		•			Search				Create
S	ONS		🗹 💌 Stat	us 🔺 Name	Devices	Address	Data Center	Virtual Servers	Product	Partition / Path
	Delivery			gtm_east	1	10.2.0.245	east_dc	1	BIG-IP System	Common
	GSLB			gtm_west	: 1	10.1.0.245	west_dc	1	BIG-IP System	Common
Zanas		Enable Di	Enable Disable Delete							
	Zones	P								
	Caches	• •								
	Settings									

Task – Review the DNS GSLB Data Center objects

In this task we will review the data centers used in the GSLB configuration.

Follow these steps to complete this task:

- 1. Navigate your browser to DNS >> GSLB : Data Centers
- 2. Inspect the data centers.
- 3. What is the what happens when you disable a DC? Discuss.

Hostn IP Add	arne: gtm_west.15demo.com dress: 10.0.1.245	Date: Jun 19, 2018 User: admin Time: 3:25 PM (PDT) Role: Administrator Partition:	Common	¢	Log out
ſ	ONLINE (ACTIVE) Standalone				
Ma	in Help About	DNS » GSLB : Data Centers : Data Center List			
100 s	Statistics	🔅 🗸 Data Center List Statistics 🗵			
I	Apps	• Search			Create
S	ONS	Availability Name Location 	Links Se	ervers 🗢	Partition / Path
	Delivery	east_dc	0 1	Co	ommon
		west_dc	0 1	Co	ommon
	GSLB	Enable Disable Delete			
	Zones	→			
	Caches	▶			

Task – Review the DNS Pools and examine the LB algorithm

In this task we will review the pools used in the GSLB configuration.

- 1. Navigate your browser to DNS >> GSLB : Pools
- 2. Inspect the Pools and understand their algorithm.
- 3. What is the what happens If you changed this ? would it make a difference? Discuss.

Hosti IP Ac	name: gtm_west.f5demo.com Dat idress: 10.0.1.245 Tim	e: Jun 19, 2018 User: admin e: 3:28 PM (PDT) Role: Adminis	strator		Partition	Common 🗍		Log out
	ONLINE (ACTIVE) Standalone							
M	ain Help About	DNS » GSLB : Wide IPs : W	/ide IP List » Me	mbers : app.f5dem	io.com : A			
<u>~</u>	Statistics	🚓 🚽 Properties iF	lules	Pools	Statistics -			
Pools								
S	DNS	Load Balancing Method	Load Balancing Method Topology					
	Delivery	Persistence	Disabled \$)				
	GSLB	Last Resort Pool	None	\$				
	Zones	Update			-			
	Caches							
	Settings	Pools					(Manage
		✓ A Order Status ♦	Pool Name			Туре	Ratio	Members
	ocal Traffic	🗆 0 🥥 ea	stpool			Α	1	1
	Acceleration	🗌 1 🥥 we	estpool			А	1	1
		Delete						

Task – Review the GSLB WidelP and its configuration

In this task we will review the WideIP used in the GSLB configuration.

- 1. Navigate your browser to DNS >> GSLB : WidelP
- 2. Inspect the WideIP and understand the configuration settings, LB algorithm, logging settings.
- 3. Do you notice anything new here? Use the built in help for the explination.

DNS Documentation

Hostname: gtm_west.f5demo.com Date: IP Address: 10.0.1.245 Time:	Jun 19, 2018 User: admin 3:28 PM (PDT) Role: Administr	ator	Partition: Common \$				
ONLINE (ACTIVE) Standalone							
	properties iRui	es Pools Statistics	•				
IApps	General Properties: Advanced	1.					
S DNS	Name	app.f5demo.com					
Delivery	Partition / Path	Common					
GSLB	Туре	A					
Zones	Description						
Caches		Alias:					
Settings							
Local Traffic	Alias List						
Acceleration		Delete					
Device Management	Availability	O Available (Enabled) - Available					
	State	Enabled \$					
Shared Objects	Minimal Response	Disabled ¢					
Network	Return Code On Failure	Disabled \$					
System	Prefer Client Subnet						
	Load-Balancing Decision Log	 Pool Selection Pool Traversal Pool Member Selection Pool Member Traversal 					
	Update Delete						

Task – Review the Global GSLB settings for Client Subnet

In this task we will review the Global client subnet settings used in the GSLB configuration. Follow these steps to complete this task:

- 1. Navigate your browser to DNS >> Settings : GSLB: Load Balancing
- 2. Under Topology, take a look at the "Prefer Client Subnet" option...
- 3. Open the help tab and take a look at the included documentation.



Task – Review the GSLB Topology records

In this task we will review the GSLB topology records used in the configuration.

Follow these steps to complete this task:

- 1. Navigate your browser to DNS >> GSLB : Topology: Records
- 2. Review the records and understand their use.

when you check out the topology records you will see that we have created a topology record that matches the local subnet coming from the querier and then another record was added to simulate a different client subnet sent by the dig query with edns0.

Hostname: gtm_west.f5demo.com Da IP Address: 10.0.1.245 Ti	tte: Jun 19, 2018 User: admin ne: 3:37 PM (PDT) Role: Administrator	Partition:	Common 🗘 Log out
ONLINE (ACTIVE) Standatone			
Main Help About	DNS » GSLB : Topology : Records		
Statistics	🔅 👻 Records Regions		
IApps	s	Search	Create Change Order
S DNS	✓ ✓ Order LDNS Request Source Destination	ation	Weight
Delivery	IP Subnet is 10.0.1.0/24 Pool is	eastpool	1
CSLR	2 IP Subnet is 1.2.2.0/24 Pool is	westpool	1
GOLD	Delete		
Zones	▶		
Caches	•		
Settings	•		

5.2.3 Lab – Use DIG command to query with client subnet GSLB objects

In this lab, we will utilize the dig command on a linux machine to query the F5 dns engines and observe the responses sent. We will change the options on the dig command to use the new client subnet option.

We will be using a new version of the dig command. My hope is you should be familiar with the general use of the dig command from your previous work with DNS.

The new version of Dig is version 9.10 and it includes an option called the "edns-client-subnet" which allows us to insert the client subnet in the query.

As the client itself cannot insert the client subnet in the query we use the dig command to simulate a query coming from a LDNS which has already inserted the client subnet.

Due to the restrictions on lab resources we have tried to keep this lab of such a size not to be too large or cumbersome, for this reason we will use the dig command instead of a LDNS.

Task - Log into the linux server and check out the new dig command

In this task you will open a terminal session and ssh to the linux server to use the local new version of dig.

- 1. Log into the linux server at 10.0.1.253 using the user named ubuntu and the password ubuntu
- 2. Once logged into the linux server check out the linux dig command by typing dig $\,-\mathrm{v}$

- 3. Take a look at the following output dig -h | grep subnet
- 4. Now do a simple query for the wideip that is configured on one of the east or west DC listener IPs dig @listener_IP app.f5demo.com

				1	. bill@ubuntu: ~ (ssh)
<pre>bill@ubuntu:~\$ dig -v DiG 9.10.3-P4-Ubuntu bill@ubuntu:~\$ dig -h +subne bill@ubuntu:~\$ dig @10.</pre>	grep sul t=addr 1.0.245	bnet (S app.f5de	iet edns- emo.com	client-subnet opti	.on)
<pre>; <<>> DiG 9.10.3-P4-Ub ; (1 server found) ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: ;; flags: qr aa; QUERY:</pre>	QUERY, S 1, ANSW	> @10.1. status: ER: 1, A	0.245 ap NOERROR, WTHORITY	p.f5demo.com id: 55469 : 0, ADDITIONAL: 1	
;; OPT PSEUDOSECTION: ; EDNS: version: 0, fla ;; QUESTION SECTION: :app.f5demo.com.	ıgs:; udp	: 4096	IN	Δ	
Jupper Bulline Feeline					
;; ANSWER SECTION: app.f5demo.com.	30	IN	A	10.2.0.100	
;; Query time: 9 msec ;; SERVER: 10.1.0.245#53(10.1.0.245) ;; WHEN: Tue Jun 19 17:46:12 CDT 2018 ;; MSG SIZE rcvd: 59					
bill@ubuntu:~\$					

Task – View the query logs and observe the dig query

Now that we have the new dig command we are almost ready to do some querys but it would be nice to see the query and decision logs that we are looking for just to make sure things are going correctly and we see any output that might be different than we might expect.

- 1. Open two new terminal windows if you do not have them open from previous sessions, logging into both the East and West DC BigIPs.
- 2. Once you have logged in as admin you can then tail -f /var/log/ltm in both windows to view the logs for the listeners.

• •	1. gtm_west (ssh)
;; SERVER: 10.1.0.245#53(10.1.0.245)	
;; WHEN: Tue Jun 19 17:46:12 CDT 2018	
;; MSG SIZE rcvd: 59	
bill@ubuntu:~\$ ssh admin@10.1.0.245	
Password:	
Last login: Tue Jun 19 15:15:22 2018 from 10.0.1.253	
<pre>[admin@gtm_west:Active:Standalone] ~ # tail -20 /var/log/ltm</pre>	
Jun 19 13:18:54 gtm_west info audit_forwarder: audit_forward	er started.
Jun 19 15:00:34 gtm_west info tmm[11566]: 2018-06-19 15:00:3	3 gtm_west.f5demo.com qid 57797 from 10.0.1.253#45171: view none: query: app.f5demo.com IN A +E (10.1.0.245%0)
Jun 19 15:00:34 gtm_west info tmm[11566]: 2018-06-19 15:00:3	3 gtm_west.f5demo.com qid 57797 from 10.0.1.253#45171 [app.f5demo.com A] [topology selected pool (eastpool) - topol
ogy score (0) is higher] [topology selected pool (westpool)	- topology score (1) is higher] [topology selected pool (westpool) with the highest topology score (1)] [pool membe
r check succeeded (west_dc_vs:10.1.0.100) - pool member state	e is available (green)] [round robin selected pool member (west_dc_vs:10.1.0.100)]
Jun 19 15:00:34 gtm_west info tmm[11566]: 2018-06-19 15:00:3	3 gtm_west.f5demo.com qid 57797 to 10.0.1.253#45171: [NOERROR qr,aa] response: app.f5demo.com. 30 IN A 10.1.0.100;
Jun 19 15:00:46 gtm_west info tmm[11566]: 2018-06-19 15:00:4	6 gtm_west.f5demo.com qid 12005 from 10.0.1.253#59304: view none: query: app.f5demo.com IN A +E (10.1.0.245%0)
Jun 19 15:00:46 gtm_west info tmm[11566]: 2018-06-19 15:00:4	6 gtm_west.f5demo.com qld 12005 from 10.0.1.253#59304 [app.f5demo.com A] [topology selected pool (eastpool) - topol
ogy score (1) is higher] [topology skipped pool (westpool) -	topology score (0) is not higher] [topology selected pool (eastpool) with the highest topology score (1)] [pool me
mber check succeeded (east_dc_vs:10.2.0.100) - pool member s	tate is available (green)] [round room selected pool member (east_dc_vs:10.2.0.100)]
Jun 19 15:00:46 gtm_west info tmm[11566]: 2018-06-19 15:00:4	$_{0}$ grm_west.rsaemo.com qta 12005 to 10.01.1253#39304: [NUERKUK qr,aa] response: app.rsaemo.com. 30 IN A 10.2.0100;
Jun 19 15:32:05 gtm_west notice mcpd[4509]: 010/1680:5: Inch	emental sync complete: Inis system is updating the configuration on device group /common/gtm device %pigsd-for-lqsy
ncer-::TTTT:10.0.1.240:4/4/8 from commit 10 { 1 050844041239	52286/9 /COmmon/DiglpUL.TSdemo.com } to commit ta { 110 55692/0905/8804119 /Common/DiglpUL.TSdemo.com }.
Jun 19 15:40:12 gtm_west info tmm[11500]: 2010-00-19 15:40:1	I gom_west.rouemo.com qtu bs400 from 10.0.1.250#50516; View none; query; qpp.rouemo.com in A + E (10.1.0.45300)
Jun 19 15:46:12 gtm_west into tmm[11566]: 2018-00-19 15:46:1	I gtm_west.Tsaemo.com qla 55409 Trom 10.0.1.255950516 [gp].Tsaemo.com Aj [topology selected pool (eastpool) - topol
mber check succeeded (east do vs:10.2.0.100) - pool member s	topology scole (e) is not right a consolid consolid consolid with the right of the second second consolid conso
lup 19 15:46:12 gtm west info tmm[11566]: 2018-06-19 15:46:1	a the west folders com aid 5469 to 10 0 1 25%5618. INDEROR ar all response and folders com 30 IN A 10 2 0 100:

Task – Use the +subnet option in dig to change the client subnet

Lets test to see if the client subnet affects the response given by the topology records in our GSLB configuration. To do this we will be using our friend dig.

- 1. Use the dig command to hit your favorite listener and query the wideip app.f5demo.com
- 2. dig @10.1.0.245 app.f5demo.com
- 3. Change the client subnet using dig @10.1.0.245 app.f5demo.com +subnet=9.9.9.0/24
- 4. Examine the response and the logs to see what decision was made ... why?
- 5. Change your query request to include a matching client subnet for a topology record that matches the configuration. dig @10.1.0.245 app.f5demo.com=1.2.2.0/24.
| | | 1. b | ill@ubun | tu: ~ (ssh) |
|---|--|--------------------------------|--------------------------------|---|
| bill@ubuntu:~\$ dig @ | 10.1.0.24 | 5 app.f5 | demo.com | +subnet=1.2.2.0/24 |
| <pre>; <<>> DiG 9.10.3-P4 ; (1 server found) ;; global options: ++ ;; Got answer: ;; ->>HEADER<<- opcod ;; flags: qr aa; QUEN</pre> | -Ubuntu <
cmd
de: QUERY
RY: 1, AN | ↔ @10.
, status
SWER: 1, | 1.0.245
: NOERRO
AUTHORI | app.f5demo.com +subnet=1.2.2.0/24
NR, id: 11666
TTY: 0, ADDITIONAL: 1 |
| <pre>;; OPT PSEUDOSECTION ; EDNS: version: 0, ; CLIENT-SUBNET: 1.2 ;; QUESTION SECTION: ;app.f5demo.com.</pre> | :
flags:; u
.2.0/24/2 | dp: 4096
4 | IN | Α |
| ;; ANSWER SECTION:
app.f5demo.com. | 30 | IN | A | 10.1.0.100 |
| ;; Query time: 3 mse
;; SERVER: 10.1.0.24
;; WHEN: Tue Jun 19 ;
;; MSG SIZE rcvd: 70 | c
5#53(10.1
17:52:42
0 | .0.245)
CDT 2018 | | |
| bill@ubuntu:~\$ | | | | |

5.2.4 Lab – Use TCPdump and Wireshark to analyze DNS ends0 client subnet transactions

In this lab, we will utilize the tcpdump utility to capture DNS queries to the F5 BIGIP DNS listeners.

Next we will use wireshark on the jumphost to examine the queries and responses edns0 information to see the ECS (client subnet) information.

Last, we will change our query to the BIND server and use tcpdump/wireshark to examine the LDNS behavior of BIND.

As in the previous lab, we will be using a new version of the dig command. You should be familiar with the general use of the dig command from your previous labs and work with DNS.

Task – Use tcpdump to capture dns queries from the linux jumphost

Follow these steps to complete this task:

- 1. Log into the BIGIP DNS via ssh admin@10.0.1.245 and use the command tcpdump -nnni 0.0 port 53 -w /tmp/edns0.pcap
- 2. Use the jumphost to query the listener with a edns0 query: dig @10.1.0.245 app.f5demo.com +subnet=9.9.9.0/24
- 3. Once the query and response are complete stop the capture with a ctrl-c.

- 4. Copy the file from the BIGIP to the jumphost using the scp command scp admin@10.1.0.245:/ tmp/edns0.pcap .
- 5. Start wireshark by typing the following into a terminal wireshark &
- 6. Once wireshark is open, choose file->open and open the edns0.pcap file in wireshark.
- 7. Open up the DNS query and examine the ends0 section. It is under the "Additional Records" arrow. What is the client subnet set to?

															edr	ns0.ca	P			
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> aptur	e <u>A</u> na	lyze <u>s</u>	tatistic	5 Te	elephon <u>y</u>	Wir	eless	Tools	<u>H</u> elp							
		6	١	0101 0310 0311		6	۹ <) 🖄	•	₹			Ð	Q	₽,]	•			
	Apply a	displa	y filter	<ctr< td=""><td>-/></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></ctr<>	-/>															
No.	1 2 3 4	Fime 9.0000 9.0049 9.0066 9.0083 9.0119	00 06 08 78 93	Source 10.0 10.0 10.0 10.1 10.0	.1.50 .1.253 .1.253 .0.245 1.253		De 10 10 8. 10 10	estina 0.0.1 0.1.0 8.4. 0.0.1	tion . 253 . 245 4 . 253 50		Pro DN DN DN DN DN	s S S S S S S S	Length 96 85 70 101 312	Info Stan Stan Stan Stan	idard idard idard idard	query query query query	0x505e A 0x0e1a A 0xe312 N response	app.f5 app.f5 S <root 0x0e1a 0x505e</root 	demo.c demo.c > OPT A app A app	com OPT com OPT .f5demo
	6 (9.0146	84	8.8.	4.4		10	.0.1	.253		DN	S	567	Stan	ndard	query	response	0xe312	NS <f< td=""><td>loot> NS</td></f<>	loot> NS
→	7 - 8 - 9 - 10 - 11 - 12 -	41.522 41.526 41.527 41.528 41.530 41.536	261 264 981 879 973 152	10.0 10.0 10.1 10.1 10.0 8.8.	.1.253 .1.253 .0.245 .1.253 .0.245 .1.253 4.4		10 10 8. 10 10 10	0.1.0 0.1.0 8.4. 0.0.1 0.0.1 0.0.1	.253 .245 4 .253 .50 .253		DN DN DN DN DN DN	S S S S S S S	96 85 70 101 312 567	Stan Stan Stan Stan Stan Stan	dard Idard Idard Idard Idard Idard	query query query query query query	0x7581 A 0xe6ab A 0x2ab4 N response response response	app.f5 app.f5 S <root: 0xe6ab 0x7581 0x2ab4</root: 	demo.o demo.o > OPT A app A app NS <f< td=""><td>com OPT com OPT 0.f5demo 0.f5demo Root> NS</td></f<>	com OPT com OPT 0.f5demo 0.f5demo Root> NS
	Answ Auth Addi Quer Addi • C	ver RRs nority tional ies tional Root>: Name Type UDP High EDNS Z: 0 Data Opti	s: 0 RRs: L RRs: L recc type : <ro : OPT paylo er bi 0 ver x0000 leng on: C</ro 	0 1 OPT ot> (41) ad size ts in e sion: 0 th: 11 SUBNET	: 4096 xtende	d RCOD	E: 0x00		1											
000 001 002 003 004 005	2c 00 01 00 01 00 6f 00	c2 60 52 5e fd 87 00 00 03 63 00 00	7c 12 38 00 79 00 00 00 6f 6d 00 0b	63 2c 00 40 35 00 01 03 00 00 00 08	c2 60 11 05 3e 4f 61 70 01 00 00 07) 2b 59 5 35 0a 5 48 75 9 70 06 9 01 00 7 00 01	a5 08 00 01 81 01 66 35 00 29 18 00	00 4 32 0 20 0 64 0 10 0	45 00 0a 00 00 01 05 6d 00 00 02 02	,.` . .R^8. y. o.com	c,. .@ 5.> 0 a p 	+Y2 52 Hu p.f5d).	E. lem							

Task - Use wireshark to view a client dns request from the linux jumphost

This task is pretty simple but looking at the client request should in theory look just like the request captured at the DNS listener.

- 1. Start wireshark and start a new capture on the ethernet interface of the jumphost.
- 2. Filter for DNS packets (port 53)
- 3. Use a terminal window to send a dig @10.1.0.245 app.f5demo.com=9.9.9.0/24
- 4. send a new dig command to 8.8.8 and look at the response... dig @8.8.8.8 www.microsoft. com +subnet=8.7.6.0/24
- 5. Inspect the dns request and the response packets, and look to see if you can see any difference between the last tasks output.
- 6. Notice the difference in the dig output between the query to the BIGIP DNS listener and 8.8.8.8.

FLD-ML-BWESTER1:agility_edns0_docs_18 bwester\$ dig @8.8.8.8 www.microsoft.com +subnet=8.7.6.0/24
; <<>> DiG 9.10.3-P4 <<>> @8.8.8.8 www.microsoft.com +subnet=8.7.6.0/24
; (1 server found)
:: alobal options: +cmd
:: Got gnswer:
:: ->>HEADER<<- opcode: OUERY, status: NOERROR, id: 20923
: flags: an rd ra: OUERY: 1 ANSWER: 4 AUTHORITY: 0 ADDITIONAL: 1
,, reags, qr ra ra, quert, 1, Ansner, 4, Authorit, 0, Abbilionne, 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
; CLIENT-SUBNET: 8.7.6.0/24/0
;; QUESTION SECTION:
;www.microsoft.com. IN A

Class 5 - DNS over HTTPS/DNS over TLS

6.1 Introduction

In this lab, you will see DNS over HTTPS (DoH) and DNS over TLS (DoT) queries proxied in both directions. That is, traditional DNS queries will be proxied to backend DoT/DoH servers, as well as DoH/DoT queries being proxied to traditional DNS servers.

DoT is "simpler" to proxy as the original DNS protocol is simply encapsulated in TLS using client-SSL (DoT-to-DNS) or server-ssl (DNS-to-DoT) profiles.

DoH is a bit more complex as we must take the DNS request and encapsulate it into a binary HTTPS payload (DNS-to-DoH) or extract the binary payload and convert it into a traditional DNS query (DoH-to-DNS).

We will use the power of iRulesLX to handle this advanced task. Native functionality will be available in a near-future release of TMOS so that the iRules will not be necessary.

The lab consists of four sections:

- · Proxying DNS over HTTPS queries to traditional DNS servers
 - In this section, you will use Mozilla Firefox as a DoH client to browse the web using encrypted DNS through the BIG-IP using DNS over HTTPS
- Proxying DNS over TLS queries to traditional DNS servers
 - In this section, you will use the kdig utility as a DoT client to perform queries through the BIG-IP using DNS over TLS
- · Proxying traditional DNS queries to DNS over HTTPS servers
 - In this section, you will use the nslookup/dig utilities to send traditional DNS queries through the BIG-IP to Google's DoH service
- · Proxying traditional DNS queries to DNS over TLS servers
 - In this section, you will use the nslookup/dig utilities to send traditional DNS queries through the BIG-IP to Google's DoT service

6.1.1 Topology

This lab consists of a single BIG-IP that is proxying the various DNS packet types. A single Windows jump host sits in the client segment while an Ubuntu jump server sits in the server segment.



6.1.2 Components

The lab consists of the following items:

- Subnets
 - Management: 10.1.1.0/24
 - DNS VIPs: 10.1.10.0/24
 - DNS Servers: 10.1.20.0/24
- · Hosts
 - Windows Jump Host
 - * Credentials: user / f5agility2020
 - * Management IP: 10.1.1.4

- Ubuntu Jump Host
 - * Credentials: user / f5agility2020
 - * Management IP: 10.1.1.6
- F5 BIG-IP Proxy:
 - * Credentials: admin / f5agility2020 | root / f5agility2020
 - * Management IP: 10.1.1.5
 - * Client Subnet IP: 10.1.10.10
 - * Server Subnet IP: 10.1.20.10
 - * DNS VIPs
 - · DoT-to-DNS: 10.1.10.100 (TCP/853)
 - DoH-to-DNS: 10.1.10.100 (TCP/443)
 - · DNS-to-DoT: 10.1.10.101 (TCP/53 and UDP/53)
 - · DNS-to-DoH: 10.1.10.102 (TCP/53)

6.1.3 BIG-IP Configuration Review

Launch your RDP client and connect to the Windows Jump Host.



Click "No" to close the network discovery prompt.

Click on the Firefox icon to launch the browser.

Three tabs will open up. The first tab is the UI of the BIG-IP. Let's login using **admin** for our username and **f5agility2020** as our password.



You should see the license screen initially. Let's take a look at the configuration before we proceed with testing the proxy.

System Configuration

Resource Provisioning

First, let's look at how the platform's modules are provisioned. Navigate to **System** -> **Resource Provisioning** in the menu. You will see that we have LTM and iRulesLX provisioned. We'll need both of these modules for handling DNS connections and translating between DNS and HTTPS.

🚯 BIG-IP® - ip-10-1-1-5.us-west∘ × 🛛 A	dvanced Preferences X	About Networking	× +				-	٥	×	
← → ♂ ☆	🛛 🖗 https://10.1.1.5/xui/?no	ache=157983235720	50			ତ ☆	lii\ 🖽 🤇	9 1	1	
~	Disk (47GB)	GMT	T							
Local Traffic	Momony (7.20P)	GMT	тим	ШХ	H Y					
Acceleration	menioly (7.5GB)	······			iex.			1		
Device Management	Module	Provisioning		License Status	Required Disk (GB)	Required Memory (MB)		4		
-	Management (MGMT)	Small	\checkmark	N/A	0	1264				
Shared Objects	Local Traffic (LTM)		Nominal	~	Nicensed	0	1504			
Retwork	Application Security (ASM)		None		📰 Unlicensed	20	1492			
System	Fraud Protection Service (FPS)	None		N/A	12	544			
Configuration >	Global Traffic (DNS)		None		n Licensed	0	148		-	
File Management >	Link Controller (LC)		None		🖭 Unlicensed	0	148			
Certificate Management			None		🎫 Limited	12	494		-	
Disk Management	Access Policy (APM)								-	
Software Management	Application Visibility and Repo	rting (AVR)	None		E Licensed	16	576			
License	Policy Enforcement (PEM)		None		🖭 Unlicensed	16	1223			
Resource Provisioning	Advanced Firewall (AFM)		None		📰 Unlicensed	16	1058			
Platform		aar (AAM)	None		🛤 Unlicensed	32	2050		-	
		ger (AAM)			- Unlicensed	24	4006		-	
Archives	Secure Web Gateway (SWG)		L None		E Onicensed	24	4090			
Preferences	iRules Language Extensions	(iRulesLX)	Nominal	~	📷 Licensed	0	748			
sFlow	URLDB Minimal (URLDB)		None		🔚 Unlicensed	36	2048			
SNMP >	SSL Orchestrator (SSLO)		None		🔚 Unlicensed	0	128		-	
Crypto Offloading	Carrier Grade NAT (CGNAT)		None		🖭 Unlicensed	16	336			
Users	Revert Submit								1	
Logs >	out and a second									
Logins										
Support										

NTP

Next, let's look at a few key system settings necessary for overall system health. Navigate to **System** -> **Configuration** -> **Device** -> **NTP**. It's important that NTP is configured and working properly on all BIG-IPs, especially when deployed in a cluster and/or when managed by BIG-IQ.

BIG-IP ◎ - ip-10-1-1-5.us-west- × A	Advanced Preferences	× About Networking	× +					-	٥	×
(←) → ⊂ ŵ	🛈 🔒 https://10.1.1.5/2	kui/?nocache=1579832357260				ເ ☆	li	N	e 1	1 =
		F5 Agility 2020 -	DNS Over HTT	PS/DNS over	TLS Lab					
Hostname ip-10-1-1-5.us-west-2.compute.ii IP Address 10.1.1.5	nternal Date Jan 23, 2020 Time 9:44 PM (EST)	User admin Role Administrator					n: Common	~	Log out	
Main Help About	System » Configuration :	Device : NTP		dire y consideration and	in and the second s					
Mage Statistics	🔅 🚽 Device	 Local Traffic AWS 		App IQ						
iApps	Properties									
S DNS		Address:								
Local Traffic		Add								
Acceleration		1.pool.ntp.org 2.pool.ntp.org	^							
Device Management	Time Server List									
shared Objects										
Network		Edit Delete	~							
System	Undete									_
Configuration >	Opdate									
File Management >										
Certificate Management										
Disk Management										
Software Management >										
License										
Resource Provisioning										
Platform										

DNS

Navigate to System -> Configuration -> Device -> DNS

Because we're using FQDNs in our iRules and DNS pools, we'll need a DNS resolver(s) that the BIG-IP can use to resolve them.

If avoid specifying DNS servers in a your environment, you can simply assign static pool members addresses and specify resolvers by IP address in the iRules to alleviate this requirement. If this doesn't make sense now, it will shortly.

(È) BIG-IP® - ip-10-1-1-5.us-west- × A	dvanced Preferences	K About Networking X +			-	o ×
$\overleftarrow{}$ \rightarrow $\overleftarrow{}$	🔽 🔊 https://10.1.1.5/xui/	?nocache=1579832357260		♡ ☆	lii\ 🖸	III III
		F5 Agility 2020 - DNS Over H	TTPS/DNS over TL	S Lab		
Hostname ip-10-1-1-5.us-west-2.compute.in IP Address 10.1.1.5	ternal Date Jan 23, 2020 Time 9:44 PM (EST)	User admin Role Administrator			Partition: Common 🗸	Log out
ONLINE (ACTIVE) Standalone						
Main Help About	System » Configuration : Dev	rice : DNS				
Mage Statistics	🔅 👻 Device 👻 I		App IQ			
iApps	Properties)			
ONS Local Traffic Acceleration Device Management	DNS Lookup Server List	Address: Add 10.1.255.254				
	BIND Forwarder Server List	Address:				
Certificate Management Disk Management Software Management License Resource Provisioning Platform	DNS Search Domain List	Address: Add us-west-2.compute.internal				

Network Configuration

The BIG-IP sits in two VLANs with self-IPs in each. One side serves up the DNS VIPs and the other is used to reach DNS servers. If you wish to view this portion of the config, you can click on the respective sections under the Network menu. Please do not make any changes.

Network	
Interfaces	F
Routes	(\div)
Self IPs	(\div)
Packet Filters	Þ
Quick Configuration	
Trunks	÷
Tunnels	Þ
Route Domains	(\div)
VLANs) ->

Local Traffic Manager (LTM)

Let's now look at the portion of the configuration that is performing the heavy lifting – the LTM configuration.

Nodes

Navigate to **Local Traffic** -> **Nodes** and look at the node list. Here, we're resolving dns.google and automatically creating pool members based on the records returned.

BIG-IP [®] - ip-10-1-1-5.us-west × A	dvanced Preferences X About Networking X +		– o ×
← → ♂ ଢ	🔞 https://10.1.1.5/xui/?nocache=1579832357260	♡ ☆	II\ 🖸 🛎 👬 Ξ
	F5 Agility 2020 - DNS Over HTTPS/DNS over	TLS Lab	
Hostname ip-10-1-1-5.us-west-2.compute.ir IP Address 10.1.1.5	ernal Date Jan 23, 2020. User admin Time 9:45 PM (EST). Role Administrator	Partition: Common	✓ Log out
I ONLINE (ACTIVE) Standalone			
Main Help About	Local Traffic » Nodes : Node List		
Statistics	☆ → Node List Default Monitor Statistics Image: Comparison of the state of the sta		
i Anne			
To why	* Search		Create
S DNS	V Status Aname		ameral + Partition / Path
Local Traffic	□auto_8.8.4.4	8.8.4.4 dns.google Yes	Common
Network Man	□auto_8.8.8	8.8.8.8 dns.google Yes	Common
Virtual Servere	dns.google	:: dns.google No	Common
Policies	Enable Disable Force Offline Delete		
Profiles			
Ciphers			
iRules			
Pools			
Nodes >			
Monitors 📀			
Traffic Class			
Address Translation >			
Acceleration			
Device Management			
Nared Objects			

Pools

If you'll kindly navigate to **Local Traffic** -> **Pools**, you will see three pools. While the backend nodes are identical between them, the ports used for each are not. You'll see a pool for DNS over HTTPS (doh_dns.google) that uses port 443, a pool for DNS over TLS (dot_dns.google) that utilizes port 853 and finally a pool that uses port 53 for traditional DNS services (traditional_dns.google). If you're not familiar with LTM pools, click through each pool to see how the service ports are specified.

ତ BIG-IP® - ip-10-1-1-5.us-west∘ ×	Adv	vanced Preference	s X	About Networking	×	+						-	0
(←) → C û		🖲 🖗 https:	:// 10.1.1.5 /xui/?nd	ocache=1579832357	7260				⊠ ☆		lii1\		•
				F5 Agility 20	020 - DNS	Over l	HTTPS/DNS over 1	TLS Lab					
Hostname ip-10-1-1-5.us-west-2.comp IP Address 10.1.1.5	ute.inte	ernal Date Ja Time 9:4	in 23, 2020 Use 45 PM (EST) Rol	er admin le Administrator						Partition: Comm	ion 🗸		Log out
ONLINE (ACTIVE) Standalone													
Main Help About		Local Traffic »	> Pools : Pool List					in and the second second					
Mage Statistics		🔅 👻 Pool Lis	st Statist	ics 🗷									
iánna													
Log Mapps		*		Search									Create
S DNS		💌 💌 Status	▲ Name						Description	Application	Members	Partiti	on / Path
Local Traffic			doh_dns.google								3	Commo	n
			dot_dns.google								3	Commo	n
Network Map			traditional_dns.g	oogle							3	Commo	n
Virtual Servers	<u> </u>	Delete											
Policies	<u> </u>												
Profiles	<u>}</u>												
Cipners	<u> </u>												
Rules	<u> </u>												
Pools													
Nodes	<u>,</u>												
Monitors													
I raffic Class	9												
Address translation	-												
Acceleration													
Device Management													
the shared Objects													

iRulesLX

iRulesLX engine based on Node.js is the mechanism that we will leverage to handle DNS over HTTPS translations. DoH requests either arrive at the BIG-IP in an HTTPS POST with a binary payload or a base64url- encoded GET request parameter. We'll need to transpose the data from these requests and translate into a traditional DNS request (DoH-to-DNS). We can also take a traditional DNS request and encapsulate it into a DoH request using iRulesLX.

Workspaces

If you'll navigate to **Local Traffic** -> **iRules** -> **LX Workspaces**, you can see the two rules for handling conversions in their respective direction. Click on the rule titled *DNS_to_DoH_Proxy*.

Hostname ip-10-1-1-5.us-west-2.compute.in IP Address 10.1.1.5	ternal Date Jan 23, 2020 User admin Time 9:43 PM (EST) Role Administrator		Partition: Common 🧹 Log out
ONLINE (ACTIVE) Standalone			
Main Help About	Local Traffic » iRules : LX Workspaces		
Mage Statistics	Image: Ward ward ward ward ward ward ward ward w		
iApps			
	* Search		Import Create
S DNS	✓ ♦ Name	Associated Plugins	Partition / Path
Cocal Traffic	DNS_to_DoH_Proxy	DNS_to_DoH_Proxy	Common
	DoH_to_DNS_Proxy	DoH_to_DNS_Proxy	Common
	Delete Export		
Virtual Servers			
Policies			
Profiles			
Ciphers			
iRules >			
Pools >			
Nodes >			
Monitors 📀			
Traffic Class 📀			
Address Translation			
Acceleration			
Device Management			

DNS to DoH Proxy

Click on the *DNS_to_DoH_Proxy* item under the *rules* section of **Workspace Files**. The first rule, *DNS_to_DoH_Proxy*, has two components. The classic iRule, which is written in TCL, is used to nab data from the incoming payload and pass it off to iRulesLX. The ILX::init function is called and the entire UDP payload is simply passed to iRulesLX using base64 encoding. Once the request is processed, the response will be returned to this iRule, which will be base64 decoded and passed to the client.

🚯 BIG-IP® - ip-10-1-1-5.us-west- 🛛 A	Advanced Preferences	< About Networking	× +		- o ×
(←) → C' ŵ	🖲 🖗 https://10.1.1.5/xui/	nocache=1579832357260?		⊠ ☆	II\ 🖸 🍭 👬 Ξ
Standalone					
Main Help About	Local Traffic » iRules : LX W	orkspaces » DNS_to_DoH_Proxy			
Statistics	General Properties				
	Name	DNS_to_DoH_Proxy			
tapps	Partition / Path	Common			
S DNS	Node.js Version	6.9.1 (default) 🗸			
Local Traffic	Associated Plugin	ONS_to_DoH_Proxy Reload fro	om Workspace		
Network Map .=					
Virtual Servers	Workspace Files	<pre> DNS_to_DoH_Prox </pre>	(y		~
Policies >	Indes	1 * when CLIENT 2 set rpc_h	_DATA { andle [ILX::init DNS_to_DoH_Proxy dns_ov	er_https]	lug
Profiles	Ins_bits_to_bon_rioxy Ins_over_https	3 set rpc_r 4 UDP::resp	esponse [ILX::call <pre>\$rpc_handle query_dns</pre> ond [b64decode <pre>\$rpc_response]</pre>	[b64encode [UDP::payload]]]	n Vie
Ciphers	index.js	5 }			W
iRules >	package.json				
Pools					
Nodes					
Monitors 📀					
Traffic Class 🔄					
Address Translation >					
Device Management					
Shared Objects					
Retwork					
System					
	Add iRule Add Extension	Add Extension File Delete Revert	File Save File		

Click on the *index.js* file under the *dns_over_https* section of **Workspace Files**. The iRulesLX portion takes the DNS packet's payload and sends it to a remote DoH server as a binary payload using the HTTP POST method. The response, which will also be binary, gets base64 encoded and passed back to the TCL portion of the iRule, which then sends the request back to the client.

⑥ BIG-IP [®] - ip-10-1-1-5.us-west [−] ×	Advanced Preferences	× Abo	ut Networking X	+				-	٥	×
$\overleftarrow{\leftarrow}$ \rightarrow \overleftarrow{c}	🗊 🔒 https://10.1.1	.5/xui/?nocache	e=1579832357260			90% … 🛛 🏠	li	N	۲	ú I
Hostname ip-10-1-1-5.us-west-2.compute.in IP Address 10.1.1.5	ternal Date Jan 23, 2020 Time 9:49 PM (EST)	User admin Role Administra	ator				Partition: Common	~	Log o	ut
ONLINE (ACTIVE) Standalone	Local Traffic » iRules : LX W	orkspaces » Di	NS to Doli Proxy							
Ma Statistics	Concert Proportion								_	
	Name	DNS to DoH Pro	'0XV							
iApps	Partition / Path	Common								_
S DNS	Node.js Version	6.9.1 (default)	~							
Local Traffic	Associated Plugin	ONS_to_Do	oH_Proxy Reload from Workspace							
Network Map										
Virtual Servers	Workspace Files		index.js							**
Policies	I TUIES		1 'use strict'; 2						^	lugi
Profiles	Ins_to_bon_rroxy Ins_over_https		<pre>3 var https = require('http 4 var f5 = require('f5-node</pre>	os'); ds');						n Vie
Ciphers	index.js		5 6 var ilx = new f5.ILXServe	en():						ž
iRules	package.json		7 8 - ilx.addMethod('query.dos'	function(reg. res) {						
Pools			9 var dns_query = Buffe	er.from(req.params()[0],'base64');						
Nodes			11 hostname: 'dns.go	oogle',						
Monitors (+)			12 port: 445, 13 path: '/dns-query	('s						
Traffic Class (*)			14 method: 'POST', 15 - headers: {							
Address Translation			16 'Host':'dns.g 17 'Content-Type 18 'Content-Lens	<pre>coogle', ': 'application/dns-message', th': Buffer bytelength(dns query 'bi </pre>	inary')					
Acceleration Device Management Shared Objects			<pre>is contained by contained</pre>	<pre>squest(options, (dohres) => { g('binary'); function (chunk) { nk;</pre>	,					
Network			27 - dohres.on('end', 28 res.reply(But 29 });	<pre>() => { fer.from(output,'binary').toString()</pre>	'base64'));					
📳 System			30 }); 31 - dohreq.on('error', fu 32 console.log('prot 33 }).	unction(e) { lem with request: ' + e.message);					~	
	Add IRule Add Extension	Add Extension File	Delete Revert File Save File							

DoH to DNS Proxy

Navigate back to the iRulesLX Workspace list (Local Traffic -> iRules -> iRulesLX Workspaces) and view the *DoH_to_DNS_Proxy* iRule. Click on the *DoH_to_DNS_Proxy* item under the *rules* section of Workspace Files. This conversion is a more intensive task.

First, POST and GET are both valid DoH request methods, but have different payloads. POST payloads are binary and GET requests are base64url encoded in the URI request, so we need to treat them separately.

Since POST has the request in the actual HTTP payload, we'll have to grab that information, perform base64 encoding and pass it along to iRulesLX to process.

For GET requests, we can simply send the base64url-encoded GET parameter. In both cases, we'll also have to wait for a response from the iRulesLX engine, which is handled in this portion of the iRule as well.

There is a slight distinction between base64 and base64url encoding! For more information, see https: //en.wikipedia.org/wiki/Base64.

🚯 BIG-IP⊗ - ip-10-1-1-5.us-west- ×	Advanced Preferences	× About Netw	iworking x + – ø ×
← → ♂ ☆	🖸 🔏 https://10.1	.1.5/xui/?nocache=157	79832357260 🥨 🐨 🗟 🛍 🖽 🖲
Hostname ip-10-1-1-5.us-west-2.compute.int IP Address 10.1.1.5	ternal Date Jan 23, 2020 Time 9:52 PM (EST)	User admin Role Administrator	Partition: Common 🕠 Log out
ONLINE (ACTIVE) Standalone			
Main Help About	Local Traffic » iRules : LX	Workspaces » DoH_to_C	DNS_Proxy
Mage Statistics	General Properties		
iAnns	Name	DoH_to_DNS_Proxy	
Con white	Partition / Path	Common	
S DNS	Node.js Version	6.9.1 (default) 🗸	
Local Traffic	Associated Plugin	ODH_to_DNS_Prox	xy Reload from Workspace
Network Map -			
Virtual Servers	Workspace Files	« DoH_to	a_DNS_Proxy
Policies	A Crules	1 ~ 2	when HTTP_REQUEST { set iLx::init "DoH_to_DNS_Proxy" "DoH_to_DNS_Proxy"]
Profiles	A DoH_to_DNS_Proxy	3	set dns_timeout 5000 log local0.info "ONSOHTPS: [IP::client_addr] [HTTP::method] [HTTP::uri] Accept: [HTTP::header "accept"] Content-type: [HTTP::header "co
Ciphers	index.js ▷ □ node_modules	5 + 6 +	if { (IMTP::method] equals "GET") and ((IMTP::header "accept"] equals "application/dns-message") or (IMTP::header "content-type"] equ if { (catch { ILx:call SiLx:handle -timeout" "SRASH44 get" [UMT::aquery [MTTP::wi] dns] } result] }
iRules	D package.json	7	log locale.erron "ILX Failure: Sresult" HTTP:/resound 488 content "Request lined out" noserver
Pools >		9 -	} else { set contentlength [lindey Specult 1]
Nodes >		11	set result [Desdecode [Lindex Sresult 0]] Inc locale [index Sresult 0]]
Monitors (*)		13	<pre>ing inclassing one based for information and international internat</pre>
Traffic Class (*)		14	3
Address Translation		16 - 17 - 18	elseit { (([HTTP::netnod) equals "POST") and (([HTTP::neader "accept"] equals "application/ons-message") or ([HTTP::neader "content-type if {[HTTP::header exists "Content-Length"] && [HTTP::header "Content-Length"] <= 65535 { set content length [HTTP::header value "Content-Length"]
Acceleration		19 20 ~ 21	<pre>} else { set content_length 65535</pre>
Device Management		22 23 ~ 24	} if { scontent_length > 0} { HTTP::collect scontent length
🐞 Shared Objects		25 26 ~) else { }relación (record cartact landt)
Retwork		27 28 29	Aug aveaues ennons concern beingen = aconcern_aeingen } }
System		30 - 31 32	else { log local0.info "Bad request from client - HTTP/415"
	Add iRule Add Extension	Add Extension File Delet	ete Revert File Save File

Click on the *index.js* item under *DoH_to_DNS_Proxy* section of **Workspace Files**. For the iRulesLX portion, the script has several steps it must perform.

First, we need to get the DoH request into a traditional DNS request packet. Not only that, but we need check for truncated responses from UDP requests and resend them as TCP requests. Once we have a response from the DNS server, we'll need to encode it to pass back to TCL so the final response can be returned to the server.

The process intensive iRule can take advantage of the BIG-IPs native SSL and TCP protocol accelerations, greatly increasing the volume of requests that can be handled.

ତ BIG-IP® - ip-10-1-1-5.us-west⊂ ×	Advanced Preferences	× About Networki	ng X	+			- o - ×
← → ⊂ ŵ	🛈 🔒 https://10.1.1	.5 /xui/?nocache=157983	2357260		90% 🛛 🕁	lii\ 🗊	: :: =
Hostname ip-10-1-1-5.us-west-2.compute.int IP Address 10.1.1.5	temal Date Jan 23, 2020 Time 9:57 PM (EST)	User admin Role Administrator				Partition: Common 🗸	Log out
Standalone	Plugin is up to date /Common/DoH_to_DNS	_Proxy					
Main Help About	Local Traffic » iRules : LX W	orkspaces » DoH_to_DNS_F	Proxy				
Mage Statistics	General Properties						
iénne.	Name	DoH_to_DNS_Proxy					
100 mappa	Partition / Path	Common					
S DNS	Node.js Version	6.9.1 (default) 🧹					
Local Traffic	Associated Plugin	O DoH_to_DNS_Proxy Rel	oad from Workspace				
Network Map @							
Virtual Servers	Workspace Files	index.js					~
Policies		1 "use 2	strict";				^ Plug
Profiles	A DoH_to_DNS_Proxy	3 var 4	f5 = require('f5-nodej dgram = require('dgram	js'); n'):			in Vi
Ciphers	index.js	5 var l	<pre>base64url = require('b base64url = require('b) base64url = require('b base64url = require('b) base64url = req</pre>	base64url');			øw
iRules >	package.json	7 var i	<pre>net = require('net');</pre>	his-packet);			
Pools		9 var	errMessage = Buffer.fr	<pre>rom('Internal Server Error').toString('base64');</pre>			
Nodes		10 var 11 var	ilx = new f5.ILXServer	le;; *();			
		12 ilx. 13	listen();				
Tatta Class		14 - ilx.	addMethod('RFC8484_get	t', function(req, res) { toBuffer(req.params()[0]):			
		16	fc8484_handler_get(ms	;g, res);			
Address translation		18 19 - ilx. 20 21 22 });	addMethod('RFC8484_pos const msg = Buffer.fro rfc8484_handler_post(m	<pre>st', function(req, res) { m(req.params()[0],'base64'); sg, res);</pre>			
Shared Objects		24 - func 25 26 -	tion rfc8484_handler_g const server = dgram.c server.on('error', (er	<pre>get(msg, res) { reateSocket('udp4'); r) => {</pre>			
Retwork		27 28 29 30	<pre>res.statusCode = 5 res.reply([errMess server.close(); });</pre>	500; age,Buffer.byteLength(errMessage)]);			
System		31 - 32 33	<pre>console.log('DNS A</pre>	<pre>(resp, rinfo) => { answer From ' + rinfo.address + ':' + rinfo.port + 'Le suncated flag</pre>	ength: ' + rinfo.size);		~
	Add iRule Add Extension	Add Extension File Delete	Revert File Save File				

Plugins

Navigate to Local Traffic -> iRules -> LX Plugins. This is where a workspace is mapped to a plug-in. This allows you to make changes to the workspace without committing those changes immediately.

🚯 BIG-IP® - ip-10-1-1-5.us-west- ×	Advanced Preferences X	About Networking X	+	- o ×
← → ♂ ଢ	🔞 https://10.1.1.5/xui/?nd	ocache=1579832357260	90% ··· 🛛 🕁	II\ 🛈 🛎 👬 ≡
		F5 Agility 2020 - DNS	Over HTTPS/DNS over TLS Lab	
Hostname ip-10-1-1-5.us-west-2.compute.i IP Address 10.1.1.5	nternal Date Jan 23, 2020 User av Time 10:01 PM (EST) Role Av	imin dministrator		Partition: Common 🗸 Log out
CONLINE (ACTIVE) Standalone				
Main Help About	Local Traffic » iRules : LX Plugins			
Statistics	🔅 🗸 LX Workspaces 🛛 LX Plugins	Statistics 🔊		
iApps	8	Search		Create
😚 DNS	V Name	State	© From Workspace	Application Partition / Path
I ocal Traffic	DNS_to_DoH_Proxy	enabled	DNS_to_DoH_Proxy	Common
Natural Man	DoH_to_DNS_Proxy	enabled	DoH_to_DNS_Proxy	Common
Virtual Services	Enable Disable Delete			
Dolicies				
Profiles				
Ciphers				
iRules				
Pools				
Nodes				
Monitors 📀				
Traffic Class 📀				
Address Translation				
Acceleration				
Device Management				
🐞 Shared Objects				
Retwork				
System				

Virtual Servers

Finally, let's take a look at the virtual servers handling incoming requests. Navigating to Local Traffic -> Virtual Servers will bring up the list.

Notice that we have 5 scenarios to cover in order to handle DNS translations in either direction.

First, the DNS-to-DoH virtual server handles incoming traditional DNS requests and encapsulates them to a backend DoH server. The next two rules handle DNS-to-DoT for both inbound TCP and UDP requests. An example use case for these proxies would be offering encrypted DNS services to client software/hardware that doesn't support DoH/DoT.

The next two rules handle inbound DoH and DoT requests, respectively. An example use case for these proxies would be for offering DoH/DoT to clients/customers/etc. without the need for modifying existing DNS infrastructure.

🚯 BIG-IP® - ip-10-1-1-5.us-west- ×	Advanced Preferences X	About Networking ×	+						- 0	
← → ♂ ଢ	🖲 🖗 https://10.1.1.5/xui/?r	ocache=1579832357260		909	🛛	☆		III\ 🗉) (2) 👔	: ≡
		F5 Agility 2020 - DNS	Over HTTPS/DNS over TLS	Lab						
Hostname ip-10-1-1-5.us-west-2.compute.in IP Address 10.1.1.5	nternal Date Jan 23, 2020 U∌er a Time 10:02 PM (EST) Role a	idmin Idministrator				Partition	Common	n 🗸	Log out	
I ONLINE (ACTIVE) Standalone										
Main Help About	Local Traffic » Virtual Servers : Virtu	al Server List								
Mage Statistics	🔅 🗸 Virtual Server List Virtual Addres	s List Statistics 👻								
itana										
Les tapps	•	Search							Create.	
S DNS	Status * Name			Description Application	Destination	Service Port	• Туре	Resources	Partition / Pa	th
Local Traffic	dns-to-doh_udp_proxy				10.1.10.102	53	Standard	Edit	Common	_
Network Map	dns-to-dot_tcp_proxy				10.1.10.101	53 :	Standard	Edit	Common	
Virtual Servers	dns-to-dot_udp_proxy				10.1.10.101	53	Standard	Edit	Common	
Policies	doh-to-dns_proxy				10.1.10.100	443 (HTTPS)	Standard	Edit	Common	
Profiles	dot-to-dns_proxy				10.1.10.100	853	Standard	Edit	Common	
Ciphers	Enable Disable Delete									
iRules										
Pools										
Nodes										
Monitors 🔶										
Traffic Class 📀										
Address Translation										
Acceleration										
Device Management										
Nared Objects										
Retwork										
System										

6.1.4 Proxying DNS over HTTPS Queries to Traditional DNS

Certificate Requirements for DoH/DoT Virtual Servers

NOTICE DNS over HTTPS requires a valid server-side certificate. In our lab, we created a selfsigned CA certificate as well as a self-signed certificate for the server. We loaded those certificates in your Firefox browser so that the browser will trust the BIG-IP DoH resolver.

In a real-world scenario, you would need a certificate signed by a well-known certificate authority and loaded into the BIG-IP and attached to the client-ssl profile in use for DoH/DoT listeners. Most DoH clients, including Firefox, will not trust a DoH server if the certificate is not signed by a known certificate authority.

Test Driving DNS over HTTPS to Traditional DNS

Now, let's generate some traffic and see the translations in real-time.

Firefox Configuration

For this test, we're going to use Firefox as our DoH client. Click the second tab in Firefox to view the about:config page. On the top of that page, you'll see a search box. Enter *trr* and press enter to see the DoH (trusted recursive resolver) configuration.

🚯 BIG-IP® - ip-10-1-1-5.us-west- ×	Advanced Preferences	× About Networking	×	+				-	ć	9	\times
← → ⊂ ŵ	Sirefox about:config				679	0 ☆	liiN		۲	÷	Ξ
० ज											_
network.dns.skipTRR-when-parental-con	trol-enabled			false						≠	5
network.trr.allow-rfc1918				false						⇒	
network.trr.blacklist-duration				60						1	
network.trr.bootstrapAddress										1	
network.trr.builtin-excluded-domains				localhost,local						1	
network.trr.clear-cache-on-pref-change				true						⇒	
network.trr.confirmationNS				example.com						1	
network.trr.credentials										1	
network.trr.custom_uri										1	
network.trr.disable-ECS				true						≓	
network.trr.early-AAAA				false						⇒	
network.trr.enable_when_nrpt_detected				false						⇒	
network.trr.enable_when_proxy_detected				false						⇒	
network.trr.enable_when_vpn_detected				false						⇒	
network.trr.excluded-domains										1	
network.trr.max-fails				5						1	
network.trr.mode				3						1	'n
network.trr.request_timeout_mode_trronly_m	15			30000						1	
network.trr.request_timeout_ms				1500						1	
network.trr.resolvers				[{ "name": "Cloudflare", "url": "https://mozilla.cloudflare-	-dns.com/dns-query" }]					1	
network.trr.send_accept-language_headers				false						⇒	
network.trr.skip-AAAA-when-not-supported				true						⇒	
network.trr.uri				https://10.1.10.100/dns-query						1	ĥ
network.trr.useGET				true						⇒	5
network.trr.wait-for-A-and-AAAA				true						⇒	
network.trr.wait-for-portal				false						⇒	
trr				Boolean ONumber OString						+	

We've pre-configured a few things for you. First, we set *network.trr.uri* to our custom virtual server URL. We also enabled *network.trr.useGET* as it's a bit faster than using POST, but you're welcome to test using POST as well. We set *network.trr.mode* to 3, which means we want Firefox to **only** use DoH. This will not be a typical configuration as Firefox defaults to traditional DNS when a DoH request fails. That explains the differing timeout values just below that setting. The *network.dns.skipTRR-when-parental-control-enabled* disables Firefox's feature that disables DoH when parental control via DNS is sensed on the network.

Please keep in mind that these settings are changing as Firefox continues testing DoH. The ink on the RFC is still wet, technically, and those heavily involved in encrypted DNS are still working out the nuances.

Firefox Network Utilities

Clicking on the third tab in Firefox will open the networking tools page within the browser. This is a great way to see if DoH (TRR in Mozilla-speak) is working. Click on *DNS Lookup* to bring up the DNS query tool.

DNS Documentation

🚯 BIG-IP⊗ - ip-10-1-1-5.us-west- ×	Advanced Preferences X	About Networking	× +					-	٥	×
← → C' ŵ	i about:networking#dnsloo	kuptool			••	• ⊠ ☆	lu		3	# ≡
	DNS Lookup					Refresh	Autorefre	sh every	3 seco	nds
НТТР										
Sockets	Domain: www.f5.com	Resolve								
DNS	IPs									
WebSockets										
DNS Lookup										
Logging										
RCWN Stats										
Network ID										

Entering a URL and clicking *Resolve* will show the A/AAAA records returned for that FQDN.

🚯 BIG-IP® - ip-10-1-1-5.us-west- ×	Advanced Preferences X	About Networking	× +		- o ×
\leftrightarrow \rightarrow C \textcircled{a}	i about:networking#dnslooku	ptool		▽ ☆	III\ 🗉 🛎 👬 🗏
	DNS Lookup			Refresh	Autorefresh every 3 seconds
НТТР					
Sockets	Domain: www.f5.com	Resolve			
DNS	IPs				
	13.224.29.75				
WebSockets	13.224.29.79				
	13.224.29.57				
DNS Lookup	13.224.29.121				
	2600:9000:2196:cc00:14:232	e:8a00:93a1			
Logging	2600:9000:2196:d800:14:232	e:8a00:93a1			
	2600:9000:2196:e00:14:232e	:8a00:93a1			
RCWN Stats	2600:9000:2196:8000:14:232	e:8a00:93a1			
	2600:9000:2196:8400:14:232	e:8a00:93a1			
Network ID	2600:9000:2196:d400:14:232	e:8a00:93a1			
	2600:9000:2196:2000:14:232	e:8a00:93a1			
	2600:9000:2196:3200:14:232	e:8a00:93a1			

If you then click on *DNS*, you'll be presented with a table of the current in-browser DNS cache. Click on *Refresh* to update the view. You can see in the output below that TRR was *true* for the queries sent, meaning DoH was used to resolve those hostnames.

DNS Documentation

🔓 BIG-IP⊗ - ip-10-1-1-5.us-west∘ ×	Advanced Preferences	K About Networking		× +		- ø ×
↔ ↔ ↔ ↔	(i) about:networking#dns				☑ ☆	II\ ① ② i =
нттр	DNS				Refresh A	utorefresh every 3 seconds
Sockets DNS	DNS suffix us-west-2.compute.interr us-west-2.ec2-utilities.an	nal nazonaws.com				
WebSockets	us-east-1.ec2-utilities.am us-west-2.compute.interr	nazonaws.com nal				
DNS Lookup	Hostname	Family	TRR	Addresses	Expires (Se	conds)
Logging	ocsp.digicert.com	ipv4	true	72.21.91.29	2051	
	ocsp.digicert.com	ipv4	true	72.21.91.29	2928	
RCWN Stats Network ID	www.f5.com	ipv4	true	13.224.29.75 13.224.29.79 13.224.29.57 13.224.29.121 2600:9000:2196:cc00:14:232e:8a00:93a1 2600:9000:2196:e00:14:232e:8a00:93a1 2600:9000:2196:8000:14:232e:8a00:93a1 2600:9000:2196:8000:14:232e:8a00:93a1 2600:9000:2196:2000:14:232e:8a00:93a1 2600:9000:2196:2000:14:232e:8a00:93a1 2600:9000:2196:3200:14:232e:8a00:93a1	17	

DoH in Action

Open a new tab and browse to a website. Return to the third tab and click *Refresh* to see the updated DNS cache table.

🚯 BIG-IP⊗ - ip-10-1-1-5.us-west- ×	Advanced Preferences X About Networking	🗙 🏳 Send	d Money, Pay Onlin	e or Set × +		- o ×
$\overleftarrow{\bullet}$ \rightarrow $\overleftarrow{\bullet}$	(i) about:networking#dns				♡ ☆	III\ 🗉 🔹 👬 =
	DNS				Refresh	Autorefresh every 3 seconds
НТТР						,
Sockets	DNS suffix					
	us-west-2.compute.internal					
DNS	us-west-2.ec2-utilities.amazonaws.com					
	us-east-1.ec2-utilities.amazonaws.com					
WebSockets	us-west-2.compute.internal					
DNS Lookup	Hostname	Family	TRR	Addresses	Expires (Seconds)	
1	ocsp.digicert.com	ipv4	true	72,21,91,29	1906	
Logging	ocsp.digicert.com	ipv4	true	72.21.91.29	2783	
RCWN Stats	www.paypal.com	ipv4	true	184.26.82.215	52	
	ak1s.abmr.net	ipv4	true	104.81.179.236	54	
Network ID	www.paypalobjects.com	ipv4	true	184.51.50.36	53	

BIG-IP Statistics and Logging

Back in the first tab on the F5 web UI, navigate to **Statistics** -> **Module Statistics** -> **Local Traffic**. Make sure that *Virtual Servers* is selected in the *Statistics Type* drop-down. Observe the traffic statistics on the DoH-to-DNS virtual server.

🚯 BIG-IP® - ip-10-1-1-5.us-west∘. ×	Advanced I	Preferences	× About N	etworking			×	+											-	٥	×
← → ♂ ✿	0	https://10.1.1	.5/xui/?nocache=1	5798323	57260									90%	··· (5	0 ☆		l	N 🖽 🤅	9	≡
			F	5 Agilii	ty 202	20 - D	NS (Over	HTTP	s/DNS	over 1	TLS Lab									
Hostname ip-10-1-1-5.us-west-2.compute.in IP Address 10.1.1.5	ternal Da Tir	e Jan 23, 2020 ne 10:27 PM (EST)	User admin Role Administrator														Partition:	Common	\sim	Logio	ut
ONLINE (ACTIVE) Standalone																					
Main Help About	Statistics	» Module Statistic	s : Local Traffic » V	irtual Serve	ers																
Statistics	🔅 👻 Traf		NS 🕶 L	ocal Traffic	s		Manag														
Dashboard = Module Statistics +	Display Opt Statistics Ty	ons	Virtual Servers	×																	
iApps	Data Forma Auto Refre	t sh	Normalized V 9 seconds V S	top Refres	h																
S DNS	*		Search		В	its	Pac	kets	C	onnection		Requests	CPU	Utilization	Ava.		Me	ssage Roj	uting Frame	work	_
Cocal Traffic	🖌 💌 Sta	tus + Virtual Serve	Partition / Pa	ath Details	≎ In	© Out	≎ In	0 Out	 Current 	Maximur	n 🔍 Total	0 Total	0 5 Sec.	0 1 Min.	0 5 Min.	© Msg. In	Msg. Out	Req. In	Req. Out	Resp. I	n 🛛 F
Acceleration		dns-to-doh_udp	proxy Common	View	0	0	0	0	0	0	0	0	0% 0%	0% 0%	0% 0%	0	0	0	0	0	0
Device Management		dns-to-dot_udp	_proxy Common	View	0	0	0	0	0	0	0	0	0%	0%	0%	0	0	0	0	0	0
Nhared Objects		doh-to-dns_pro	xy Common	View	622.8K	545.9K	707	798	2	3	33	0	0%	0%	0%	0	0	0	0	0	0
Retwork	Reset	dot-to-dns_prox	cy Common	View	0	0	0	0	0	0	0	0	0%	0%	0%	0	0	0	0	0	0
System																					

Change the *Statistics Type* to iRulesLX and you can see how many RPC connections have been made.

😮 BIG-IP® - ip-10-1-1-5.us-west- ×	Advanced Preferences	× About	Networking	× +										٥	
← → ⊂ ŵ	🖲 🔓 https://10.1.1.	5/xui/?nocache=	=157983235726	60					90%	⊌ ☆		1111			* ≡
			F5 Agility 2	2020 <mark>- DNS O</mark> v	er HTTPS/	DNS	over Tl	S Lab							
Hostname ip-10-1-1-5.us-west-2.compute.i IP Address 10.1.1.5	nternal Date Jan 23, 2020 Time 10:29 PM (EST)	User admin Role Administrat	lor								Partition	Common	~	Log	out
ONLINE (ACTIVE) Standalone															
Main Help About	Statistics » Module Statistic:	s : Local Traffic »	iRules LX												
Statistics	🔅 👻 Traffic Summary 💌 DM	is 🝷	Local Traffic	Subscriber Manageme	nt Network	M	lemory	Syster	n						
Dashboard @															
Module Statistics	Display Options														
Performance Reports	Statistics Type	iRules LX	\checkmark												
	Data Format	Normalized 🗸													
iApps	Auto Refresh	1 seconds 🔍	Stop Refresh												
S DNS	*	Search						Dropper		DDC Int	10	Ster	amina	nfo	
The Local Traffic	Status		▲ Plugin : Extensi	ion	Partition / Path	Details	Restarts	¢ CPU (%)	 Total Virtual Siz 	e Total Connections	Total Calls	Clientside To	tal 0 S	erverside	Total
	Carling		DNS_to_DoH_Pro	xy : dns_over_https	Common	View	0	0	1.8G	0	0	0	0		
Acceleration	Carling		DoH_to_DNS_Pro	xy : DoH_to_DNS_Prox	Common	View	0	0	2.1G	54	54	0	0		
Device Management	Reset														
6 Shared Objects															
Retwork															
System															

Change the drop-down to *Pools*. You should notice that the back-end pools show 0 connections. Why? Because iRulesLX is talking to the back-end DoH resolvers directly.

🚯 BIG-IP® - ip-10-1-1-5.us-west- ×	Advanced Preferences	× About Netwo	orking	×	+										-	٥	×
$\overleftarrow{\leftarrow}$ \rightarrow \overleftarrow{c}	🖲 🖗 https://10.1.1	.5/xui/?nocache=1579	832357260							90%	🖂 1	\$		111			i ≡
		F5 /	Agility 2020) - DNS	Over HT	TPS/DN	S over T	LS L	ab								
Hostname ip-10-1-1-5.us-west-2.compute.in IP Address 10.1.1.5	nternal Date Jan 23, 2020 Time 10:30 PM (EST)	User admin Role Administrator											Partition: Cor	mmon	~	Log	out
I ONLINE (ACTIVE) Standalone																	
Main Help About	Statistics » Module Statistic	s : Local Traffic » Pools															
Ma Statistics	🔅 🗸 Traffic Summary 🔻 D	NS 🔫 Local	Traffic Sub	iscriber Mana	igement Netw												
Dashboard 🖝	Display Options		,														
Module Statistics	Statistics Type	Pools															
Performance Reports	Data Format	Normalized	-														
iApps	Auto Refresh	2 seconds V Stop	Refresh														
S DNS	*	Search		Pite	Daakata	6	anastiana		Dogucata	Deg	ant Ourous		Ma		uting Fr		
Ref Local Traffic	V Status + + Pool	Pool Member	Partition / Path		rt ⊜ In ⊕ Out		Maximum	Total	Total	Depth	Maximum Age	0 Msg. In	Msg. Out	Reg. In	Reg.	Out 0	Resp. In
		pogle	Common	0 0	0 0	0	0	0	0	0	0	0	0	0	0	0	
Acceleration		ogle	Common	0 0	0 0	0	0	0	0	0	0	0	0	0	0	0	
Device Management	C C traditional	dns.google	Common	0 0	0 0	0	0	0	0	0	0	0	0	0	0	0	
🐞 Shared Objects	Reset																
Network																	
System																	

Navigate to **System** -> **Logs** -> **Local Traffic**. Notice that some useful information is being logged to help show the parsing and querying that is taking place behind the scenes.

BIG-IP® - ip-10-1-1-5.us-west	× Advanced Preferences	×	About Networking	× +			- 8 ×
$\overleftarrow{\leftarrow}$ \rightarrow \overleftarrow{C}	🛛 🖗 https://10.1	.1.5/xui/?no	cache=1579832357260			90% … 🛛 🕁	′ III\ 🗉 🔹 👬 Ξ
			F5 Agility 2020 -	DNS Over HTTPS	/DNS ove	r TLS Lab	
Hostname ip-10-1-1-5.us-west-2.comp IP Address 10.1.1.5	oute.internal Date Jan 23, 2020 Time 10:36 PM (EST	User ad r) Role Adr	min ministrator				Partition: Common 🗸 Log out
Main Help About	System » Logs : Local Tra	affic					
Mage Statistics	🔅 🗸 System Pa	icket Filter	Local Traffic GSLB	Audit 👻	Configuration	*	
iApps	F		Search				
S DNS	▲ Timestamp	+ Log Level	Host	Service	Status Code	Event	
00	Thu Jan 23 03:09:02 EST 2020) info	ip-10-1-1-5.us-west-2.compute.inte	ernal audit_forwarder[17998]	audit_forwarder started.	
Local Traffic	Thu Jan 23 09:47:43 EST 2020) info	ip-10-1-1-5.us-west-2.compute.inte	ernal soap[3935]		src=127.0.0.1, user=	
Acceleration	Thu Jan 23 09:47:44 EST 2020) info	ip-10-1-1-5.us-west-2.compute.inte	ernal soap[3935]		src=127.0.0.1, user=	
	Thu Jan 23 09:48:34 EST 2020) info	ip-10-1-1-5.us-west-2.compute.inte	ernal soap[3935]		src=127.0.0.1, user=	
Device Management	Thu Jan 23 09:48:34 EST 2020) info	ip-10-1-1-5.us-west-2.compute.inte	ernal soap[3935]		src=127.0.0.1, user=	
🐞 Shared Objects	Thu Jan 23 09:48:34 EST 2020) info	ip-10-1-1-5.us-west-2.compute.inte	ernal soap[3935]		src=127.0.0.1, user=	
	Thu Jan 23 09:48:34 EST 2020) info	ip-10-1-1-5.us-west-2.compute.inte	ernal soap[3935]		src=127.0.0.1, user=	
Network	Thu Jan 23 09:49:54 EST 2020) info	ip-10-1-1-5.us-west-2.compute.inte	ernal soap[3935]		src=127.0.0.1, user=	
System	Thu Jan 23 09:49:54 EST 2020) info	ip-10-1-1-5.us-west-2.compute.inte	ernal soap[3935]		src=127.0.0.1, user=	
Configuration	Thu Jan 23 09:49:54 EST 2020) info	ip-10-1-1-5.us-west-2.compute.inte	ernal soap[3935]		src=127.0.0.1, user=	
File Management	Thu Jan 23 09:49:54 EST 2020) info	ip-10-1-1-5.us-west-2.compute.inte	ernal soap[3935]		src=127.0.0.1, user=	
Cartificate Management	Thu Jan 23 10:07:32 EST 2020) info	ip-10-1-1-5	tmm[18491]		Rule /Common/DoH_to_DNS_Proxy/DoH_to_DNS_Proxy <h auery?dns=AAABAAABAAAAAAABB2V4YW1wbGUDY</h 	ITTP_REQUEST>: DNSoHTTPS: 10.1.1.4 GET /dns- 29tAAACAAEAACkQAAAAAAAAAAAAAAAAAAAAAAAAAAAA
	Thu Jan 23 10:07:32 EST 2020) info	ip-10-1-1-5.us-west-2.compute.inte	ernal sdmd[13620]	018e0017	pid[14179] plugin[/Common/DoH to DNS Proxy.DoH to DN	NS Proxy] DNS Answer From 10.1.20.101:53Length: 196
Disk management	Thu Jan 23 10:07:32 EST 2020) info	ip-10-1-1-5.us-west-2.compute.inte	ernal sdmd[13620]	018e0017	pid[14179] plugin[/Common/DoH_to_DNS_Proxy.DoH_to_DN	NS_Proxy] Answer is NOT truncated. Flag is:0.Returning D
Software Management	Thu Jan 23 10:07:32 EST 2020) info	ip-10-1-1-5	tmm[18491]		Rule /Common/DoH_to_DNS_Proxy/DoH_to_DNS_Proxy <h< th=""><th>ITTP_REQUEST>: DNS answer for 10.1.1.4 (len 196)</th></h<>	ITTP_REQUEST>: DNS answer for 10.1.1.4 (len 196)
License	Thu Jan 23 10:07:32 EST 2020) info	ip-10-1-1-5	tmm[18491]		Rule /Common/DoH_to_DNS_Proxy/DoH_to_DNS_Proxy <h< th=""><th>ITTP_REQUEST>: DNSoHTTPS: 10.1.1.4 GET /dns-</th></h<>	ITTP_REQUEST>: DNSoHTTPS: 10.1.1.4 GET /dns-
Resource Provisioning Platform	-					query?dns=AAABAAABAAAAAAAABCHNuaXBwZXRzA2 Content-type:	:Nkbgdtb3ppbGxhA25ldAAAAQABAAApEAAAAAAAAA
High Availability	Thu Jan 23 10:07:32 EST 2020) info	ip-10-1-1-5	tmm1[18491]		Rule /Common/DoH_to_DNS_Proxy/DoH_to_DNS_Proxy <h query?dns=AAABAAABAAAAAAAABCHNuaXBwZXRzA2</h 	ITTP_REQUEST>: DNSoHTTPS: 10.1.1.4 GET /dns- 2Nkbgdtb3ppbGxhA25IdAAAHAABAAApEAAAAAAAAg
Archives			5 40 4 4 5 m m 1 0 m 1 1 1		010-0017	Content-type:	
Services	Thu Jan 23 10:07:33 EST 2020) into	Ip-10-1-1-5.us-west-2.compute.inte	ernal somo[13620]	018e0017	pid[141/9] piugin[/Common/JoH_to_DNS_Proxy.DoH_to_DN	IS_ProxyJ DNS Answer From 10.1.20.101:53Length: 323
Preferences	Thu Jan 23 10:07:33 EST 2020	J INTO	IP-10-1-1-5.us-west-2.compute.inte	ernai sdmd[13620]	01860017	pia[14179] piugin[/Common/DoH_to_DNS_Proxy.DoH_to_DN	<pre>ISS_Proxy] Answer IS NOT truncated. Flag IS:0.Returning D</pre>

Capturing DNS over HTTPS Queries to Traditional DNS Traffic

Finally, minimize *Firefox* to reveal the CLI shortcuts on the desktop:



Let's open the BIG-IP DNS Proxy link to bring up the BIG-IP's CLI. Once running, let's start a capture that will show us both sides of the DoH proxy:

tcpdump -nni 0.0 (host 10.1.1.4 and host 10.1.10.100 and port 443) or (host 8.8.4.4 or host 8.8.8.8 and port 53)

Once running, maximize *Firefox* and perform another DNS lookup. View the HTTPS and DNS traffic in the packet capture output. The output below shows my queries to f5.com, f5agility.com and disney.com.

2:14:14:2057.2 HP 10.1.20.24:33 > 10.1.20.104:753 LS03F A/G B. 20.05 A

Stop your capture before moving to the next section. This concludes the DoH-to-DNS proxy portion of the lab.

6.1.5 Proxying DNS over TLS Queries to Traditional DNS

DoT-to-DNS is a bit more simplistic. We're simply taking the existing DNS request and encapsulating it in TLS. No iRule magic needed here; just classic BIG-IP high-performance SSL offloading.

The client-SSL profile on this virtual server specifies that SSL/TLS termination should occur on the client side of the connection.

Virtual Server Configuration

Maximize *Firefox*. Click on the first tab to return to the BIG-IP web UI. Navigate to **Local Traffic** -> **Virtual Servers**. If you review the virtual server configuration, you'll notice that we're simply using a client-SSL profile and a backend pool. The client-SSL profile utilizes a self-signed certificate in this lab, you'll need a certificate from a certificate authority that your clients' browsers trust in a production deployment.

General Properties	
Name	dot-to-dns_proxy
Partition / Path	Common
Description	
Туре	Standard
Source Address	Host O Address List 0.0.0/0
Destination Address/Mask	Host O Address List 10.1.10.100
Service Port	Port O Port List 853 Other:
Notify Status to Virtual Address	
Availability	Available (Enabled) - The virtual server is available
Syncookie Status	Inactive
State	Enabled 🗸
Configuration: Basic V	
Protocol	ТСР
Protocol Profile (Client)	f5-tcp-lan 🗸
Protocol Profile (Server)	f5-tcp-wan 🗸
HTTP Profile (Client)	None
HTTP Profile (Server)	(Use Client Profile) 🧹
HTTP Proxy Connect Profile	None
FTP Profile	None 🗸
RTSP Profile	None 🗸
	Selected Available
SSL Profile (Client)	Q Q /Common /Common agility_selfsigned <
278	Chapter 6. Class 5 - DNS over HTTPS/DNS over FLS crypto-server-default-clients splitsession-default-clientssl wom-default-clientssl

Clicking on **Resources** tab on the top navigation bar will show that the virtual server has a simple pool and no iRules attached.

Local Traffic » Virtual Servers : Virtual Server List » dot-to-dns_proxy	Local Traffic 's' Virtual Servers : Virtual Server List >> dot-to-dns_proxy Image: traffic 's' Virtual Servers : Virtual Server List >> dot-to-dns_proxy Image: traffic 's' Virtual Servers : Virtual Server List >> dot-to-dns_proxy Image: traffic 's' Virtual Servers : Virtual Server List >> dot-to-dns_proxy Image: traffic 's' Virtual Servers : Virtual Server List >> dot-to-dns_proxy Image: traffic 's' Virtual Servers : Virtual Server List >> dot-to-dns_proxy Image: traffic 's' Virtual Servers : Virtual Server List >> dot-to-dns_proxy Image: traffic 's' Virtual Servers : Virtual Server List >> dot-to-dns_proxy Image: traffic 's' Virtual Servers : Virtual Server : Virtual Server List >> dot-to-dns_proxy Image: traffic 's' Virtual Server : Virtu								
Properties Resources Statistics Load Balancing Default Pool traditional_dns.google Default Persistence Profile None Fallback Persistence Profile None iRules Name No records to display. Policies	Arrow Properties Resources Statistics Load Balancing Default Pool traditional_dns.google Default Persistence Profile None Fallback Persistence Profile None Update Rules Name Name Name Name No records to display.	Local	Traffic » Virtua	Server	s : Virtual S	erver List »	dot-to-dns	_proxy	
Load Balancing Default Pool traditional_dns.google Default Persistence Profile None Fallback Persistence Profile None Update Image: Comparison of the second	Load Balancing Default Pool Traditional_dns.google Default Persistence Profile None Fallback Persistence Profile None Update Rules Name No records to display. Policies Name No records to display.	* •	Properties	Reso	urces	Statistics			
Load Balancing Default Pool traditional_dns.google Default Persistence Profile None Fallback Persistence Profile None Update IRules Name No records to display. Policies	Load Balancing Default Pool Traditional_dns.google Default Persistence Profile None Fallback Persistence Profile None Update Rules Name No records to display. Policies Name Name No records to display.								
Default Pool traditional_dns.google Default Persistence Profile None Fallback Persistence Profile None Update IRules Name No records to display. Policies	Default Pool traditional_dns.google Default Persistence Profile None Fallback Persistence Profile None Update Rules Name No records to display. Policies Name No records to display.								
Default Pool traditional_dns.google Default Persistence Profile None Fallback Persistence Profile None Update Image: Comparison of the second secon	Default Pool traditional_dns.google Default Persistence Profile None Fallback Persistence Profile None Update Rules Name No records to display. Policies Name No records to display.	Load B	alancing						
Default Persistence Profile Fallback Persistence Profile None Independent of the second s	Default Persistence Profile Fallback Persistence Profile None Update Rules Name No records to display. Policies Name No records to display.	Defau	lt Pool		traditional_	dns.google	\sim		
Fallback Persistence Profile None Update Interview iRules Name Name No records to display. Policies Interview	Fallback Persistence Profile None Update Image: Comparison of the second se	Defau	It Persistence Prof	le	None	\sim			
Update iRules Name No records to display. Policies	Update Rules Name No records to display. Policies Name No records to display.	Fallba	ck Persistence Pro	file	None	\sim			
iRules Name No records to display. Policies	Rules Name No records to display. Policies Name No records to display.	Updat	e						
iRules Name No records to display. Policies	Rules Name No records to display. Policies Name Name No records to display.								
IRules Name No records to display. Policies	Rules Name No records to display. Policies Name No records to display.								
Name No records to display. Policies	Name No records to display. Policies Name No records to display.	iRules							
No records to display. Policies	No records to display. Policies Name No records to display.	Name							
Policies	Policies Name No records to display.	No rec	cords to display.						
	Name No records to display.	Policie	s						
Name	No records to display.	Name							
	No records to display.		and a deadlosed and						
No records to display.		No rec	cords to display.						

Test Driving DNS over TLS to Traditional DNS

Minimize Firefox to view the desktop shortcuts and launch the Lab DNS Server client. You'll be automatically logged in. Let's run a DNS over TLS query:

kdig +tls @10.1.10.100 www.f5.com

You should see a response similar to the output below. Run a few more queries against other domains to generate statistics.

🛃 user@ip-10-1-1-6: ~

u -1					
user@ip-10-1-1-6:~\$ man dig					^
user@ip-10-1-1-6:~\$					
user@ip-10-1-1-6:~\$ kdig +t1:	s @10.1.	10.100 www	.f5.co	m	
;; TLS session (TLS1.2)-(ECD)	HE-RSA-S	ECP256R1)-	(AES-1	28-GCM)	
;; ->>HEADER<<- opcode: QUER	Y; statu	s: NOERROR	; id:	15427	
;; Flags: qr rd ra; QUERY: 1	; ANSWER	: 5; AUTHO	RITY:	0; ADDITIONAL: 1	
;; EDNS PSEUDOSECTION:					
;; Version: 0; flags: ; UDP	size: 51	2 B; ext-r	code:	NOERROR	
;; QUESTION SECTION:					
;; www.f5.com.	IN	A			
;; ANSWER SECTION:					
www.f5.com. 29	IN	CNAME	dwbf	wz8xncgmg.cloudfront.net.	
dwbfwz8xncgmg.cloudfront.net	. 59	IN	A	13.224.2.97	
dwbfwz8xncgmg.cloudfront.net	. 59	IN	A	13.224.2.74	
dwbfwz8xncgmg.cloudfront.net	. 59	IN	A	13.224.2.75	
dwbfwz8xncgmg.cloudfront.net	. 59	IN	A	13.224.2.91	
;; Received 145 B					
;; Time 2020-01-24 03:52:48	UTC				
;; From 10.1.10.100@853(TCP)	in 59.2	ms			
user@ip-10-1-1-6:~\$					~

_

×

Viewing Statistics for DoT-to-DNS

You can then see statistics on the virtual server by navigating to **Statistics** -> **Module Statistics** -> **Local Traffic** and selecting *Virtual Servers* in the drop-down list.

🚯 BIG-IP® - ip-10-1-1-5.us-west⊲ ×	+																		-	٥	×
← → ♂ ଢ	0 🔒	https://10.1.1.5	/xui/?nocache=157	983235	57260									90%	··· 0	פ ל		l	N	9 11	≡
			F5	Agilit	ty 20	20 - D	NS	Over	HTTP	S/DNS (over '	TLS Lab									
Hostname ip-10-1-1-5.us-west-2.compute.in IP Address 10.1.1.5	ternal Date Time	Jan 23, 2020 10:54 PM (EST)	User admin Role Administrator														Partition:	Common	×	Log o	ut
Standalone																					
Main Help About	Statistics »	Module Statistics	: Local Traffic » Virt	ual Serve	ers																
Ma Statistics	🔅 🗸 Traffic		S 🔻 Loc	al Traffic	s			gement													
Dashboard																					
Module Statistics	Display Option	15																			
Performance Reports	Statistics Type Virtual Servers																				
	Data Format		Normalized 🗸																		
iApps	Auto Refresh		9 seconds 🗸 Stop	Refrest	h																
S DNS	*		Search																		
~	V Statur	+ Virtual Server	Bartition / Bath	Detaile	B	its Out	Pac	kets	Current	Maximum	C Total	Requests	CPU	Utilization	Avg.	the Mea In	Meg. Out	Bag In	Reg. Out	Base I	n n P
Local Traffic	I → Status	das to dob udp	Common	View	⇒ in	0 Out	⇒ m	0 Out	o	• Maximum		o lotal		0%	• 5 Min.	o msg. in	⇒ msg. Out	o Req. in	• Req. Ou	• Resp. I	1 • FG
Acceleration		des to det tes e	proxy Common	V IC VV	0	0	0	0	0	0	0	0	0.00	0.70	0.0	0	0	0	0	0	0
		ans-to-aot_tcp_p	roxy Common	view	0	0	0	0	0	U	0	U	0%	0%	0%	0	U	0	0	0	0
Device Management		dns-to-dot_udp_p	oroxy Common	View	0	0	0	0	0	0	0	0	0%	0%	0%	0	0	0	0	0	0
Nared Objects		doh-to-dns_prox	Common	View	793.6K	704.9K	1.0K	1.1K	2	3	33	0	0%	0%	0%	0	0	0	0	0	0
Retwork		dot-to-dns_proxy	Common	View	8.4K	32.2K	10	11	0	1	1	0	0%	0%	0%	0	0	0	0	0	0
िं 🖗 System	Reset																				

Because this virtual server is taking advantage of backend pools, you will see statistics under the *Pools* statistics type as well.

🚯 BIG-IP® - ip-10-1-1-5.us-west⊲ ×	+														٥	
$\overleftarrow{\leftarrow}$ \rightarrow C' $\overleftarrow{0}$	🖸 🔒 https://10.1.	1.5/xui/?nocache=1579832	357260						90%	🛛 1	삶		111\	•	÷,	≡
		F5 Agil	lity 2020 -		ver HT	TPS/DNS	over TLS	Lab								
Hostname ip-10-1-1-5.us-west-2.compute.in IP Address 10.1.1.5	internal Date Jan 23, 2020 Time 10:54 PM (EST)	User admin Role Administrator									F	artition: Com	mon	\mathbf{v}	Log o	ut
ONLINE (ACTIVE) Standalone																
Main Help About	Statistics » Module Statisti	ics : Local Traffic » Pools														
Mage Statistics	🔅 👻 Traffic Summary 👻 I	DNS 👻 Local Traffi	fic Subsci	riber Manage	ment Netw	ork	Memory	System								
Dashboard																
Module Statistics	Display Options															_
Performance Reports	Statistics Type	Statistics Type Pools														
iApps	Data Format Auto Refresh	6 seconds V Stop Refre	esh													-
S DNS	*	Search		814						1.0						
RER Local Traffic	Status + + Pool	Pool Member P	Partition / Path	Bits In ≑Out	o In o Out	© Current	Maximum 0 Tota	Requests	Depth	 Maximum Age 	≑ Msg. In	Me Msg. Out	 Req. In 	 Req. 	Dut 🗢 R	esp. In
	doh_dns.	google Cor	mmon (0 0	0 0	0 0	0	0	0	0	0	0	0	0	0	
Acceleration	dot_dns.g	oogle Cor	mmon (0 0	0 0	0 0	0	0	0	0	0	0	0	0	0	
Device Management	🗌 🥥 🖾 traditional	_dns.google Cor	mmon 3	3.1K 2.9K	54	0 1	1	0	0	0	0	0	0	0	0	
Chared Objects	Reset															
Network																
§♥ System																

Because we don't have any type of logging configured for that virtual server, you won't see any information in **System** -> **Logs** for this traffic. If you'd desire logging in your environment, general LTM F5 logging/statistics practices can be used.

Capturing DNS over TLS to Traditional DNS Traffic

Minimize Firefox and return to the BIG-IP DNS Proxy session from the first section of this lab, or open a new session by clicking on the BIG-IP DNS Proxy icon on the desktop. Execute the follow tcpdump command:

tcpdump -nni 0.0 port 53 or port 853

Pull the Lab DNS Server session window up and re-run the **kdig** command. Observe the front and back-end connections using port 853 and 53, respectively, shown in the packet capture output.

```
23:07:21.434497 IP 10.1.10.100.853 > 10.1.1.6.49992: Flags [P.], seq
is=/Common/dot-to-dns proxy
23:07:21.434520 IP 10.1.20.10.49992 > 8.8.4.4.53: Flags [S], seg 2784
is=/Common/dot-to-dns proxy
23:07:21.434536 IP 10.1.10.100.853 > 10.1.1.6.49992: Flags [P.], seq
lis=/Common/dot-to-dns proxy
23:07:21.434889 IP 10.1.1.6.49992 > 10.1.10.100.853: Flags [P.], seq
is=/Common/dot-to-dns proxy
23:07:21.434913 IP 10.1.10.100.853 > 10.1.1.6.49992: Flags [.], ack 4
o-dns proxy
23:07:21.441472 IP 8.8.4.4.53 > 10.1.20.10.49992: Flags [S.], seq 128
 length 0 in slotl/tmml lis=/Common/dot-to-dns proxy
23:07:21.441494 IP 10.1.20.10.49992 > 8.8.4.4.53: Flags [.], ack 1, w
proxy
23:07:21.441506 IP 10.1.20.10.49992 > 8.8.4.4.53: Flags [P.], seq 1:1
m. (128) out slot1/tmml lis=/Common/dot-to-dns proxy
23:07:21.448194 IP 8.8.4.4.53 > 10.1.20.10.49992: Flags [.], ack 131,
proxy
23:07:21.485209 IP 8.8.4.4.53 > 10.1.20.10.49992: Flags [P.], seq 1:1
8xncgmg.cloudfront.net., A 13.224.2.91, A 13.224.2.97, A 13.224.2.75,
23:07:21.485256 IP 10.1.20.10.49992 > 8.8.4.4.53: Flags [.], ack 148,
s proxy
23:07:21.485373 IP 10.1.10.100.853 > 10.1.1.6.49992: Flags [P.], seq
 lis=/Common/dot-to-dns proxy
23:07:21.488839 IP 10.1.1.6.49992 > 10.1.10.100.853: Flags [P.], seg
```

Stop your capture before moving on to the next section. This concludes the DoT-to-DNS portion of the lab.

6.1.6 Proxying Traditional DNS to DNS over TLS

In this section of the lab, we're going to run DoT in the opposite direction, taking traditional DNS requests and translating them into DoT requests. This is done as simply as the DoT-to-DNS; we simply take the incoming DNS connection (UDP or TCP) and encapsulate it in TLS using a server-side SSL profile.

Test Driving Traditional DNS to DNS over TLS

On the Lab DNS Server, issue the following command:

kdig @10.1.10.101 www.yahoo.com

You should receive a successful response as shown below:

```
user@ip-10-1-1-6:~$ dig @10.1.10.101 www.yahoo.com
; <<>> DiG 9.11.3-lubuntul.11-Ubuntu <<>> @10.1.10.101 www.yahoo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7629
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.yahoo.com.
                                IN
                                        Α
;; ANSWER SECTION:
www.yahoo.com.
                                IN
                                                atsv2-fp-shed.wgl.b.yahoo.com.
                        1185
                                        CNAME
atsv2-fp-shed.wg1.b.yahoo.com. 18 IN
                                                98.137.246.8
                                        А
                                                98.137.246.7
atsv2-fp-shed.wgl.b.yahoo.com. 18 IN
                                        А
;; Query time: 38 msec
;; SERVER: 10.1.10.101#53(10.1.10.101)
;; WHEN: Fri Jan 24 04:12:36 UTC 2020
;; MSG SIZE rcvd: 108
```

Viewing Statistics for DNS-to-DoT

Restore Firefox and click on the first tab to return to the BIG-IP web UI. You can then see statistics on the virtual server by navigating to Statistics -> Module Statistics -> Local Traffic and selecting Virtual Servers in the drop-down list.

BIG-IP [®] - ip-10-1-1-5.us-west ×	+														-	٥	\times
← → C [*] ⁽²⁾	🖸 🔒 https://10.1.	1.5/xui/?nocache=15798	3235726	D						90%	©	7 ☆		10	\	9 ii	≡
		F5 A	gility 20	020 - DI	NS Over	HTTPS/D	NS over	TLS Lab									
Hostname ip-10-1-1-5.us-west-2.compute.in IP Address 10.1.1.5	internal Date Jan 23, 2020 Time 11:14 PM (EST)	User admin Role Administrator											Partition:	Common	×	Log o	ut
Standalone																	
Main Help About	Statistics » Module Statist	ics : Local Traffic » Virtual	Servers														
Mag Statistics	🔅 👻 Traffic Summary 💌 I	DNS 👻 Local T	raffic		Management				n								
Dashboard	Display Options																
Performance Reports	Statistics Type	Virtual Servers]														_
iApps	Data Format Auto Refresh	0 seconds v Stop F	efresh														-
S DNS	*	Search		Bits	Packets	Conne	ctions	Requests	CPU Ut	ilization /	Avg.		Mes	sage Rou	ting Fram	work	
Local Traffic	Status - Virtual Serv	er O Partition / Path D	etails 🗘 In	≎ Out	⇔ In ≑ Out	Current M	aximum 🗘 Total	 Total 	\$ 5 Sec.	0 1 Min.	5 Min.	Msg. In	≑ Msg. Out	Req. In	Req. Out	© Resp. I	e Re
Acceleration	dns-to-doh_ud	lp_proxy Common V	ew 0	0	0 0	0 0	0	0	0% 0	0%	0%	0	0	0	0	0	0
Device Management	dns-to-dot_tcp	p_proxy Common V	ew 0	3.2K	2 2	0 1	2	2	0% (0% (0%	0	0	0	0	0	0
Nhared Objects	doh-to-dns_pr	oxy Common V	ew 832.4	K 742.4K	1.1K 1.2K	0 3	33	0	0% (0%	0%	0	0	0	0	0	0
Retwork	Reset dot-to-dns_pro	xy Common V	ew 39.5k	161.0K	44 55	0 2	5	0	0% (0% (0%	0	0	0	0	0	0
System																	

Back on the Lab DNS Server, issue the same kdig command with the TCP option to increment the counters on the corresponding virtual server:

kdig +tcp @10.1.10.101 www.f5.com

BIG-IP®→ip-10-1-1-5.us-west-×															
← → ♂ ☆	🖲 🖗 https://10.1.1	.5/xui/?nocache=1579832	357260		9	∞ … ⊵ ☆	hi	. ⊡ ⊜ # ≡							
		F5 Agi	lity 2020 - DNS	Over HTTPS/DN	S over TLS Lab										
Hostname ip-10-1-1-5.us-west-2.compute.in IP Address 10.1.1.5	nternal Date Jan 23, 2020 Time 11:21 PM (EST)	User admin Role Administrator					Partition: Common	Log out							
I ONLINE (ACTIVE) Standalone	OKUNE (ACTIVE) Standalone														
Main Help About	Statistics » Module Statisti	cs : Local Traffic » Virtual Se	rvers												
Statistics	🔅 👻 Traffic Summary 💌 🛙	DNS 👻 Local Traff	ic Subscriber Man	nagement Network	Memory System										
Dashboard															
Module Statistics	Display Options														
Performance Reports	Statistics Type	Virtual Servers													
_	Data Format	Normalized 🗸													
iApps	Auto Refresh	5 seconds 🗸 Stop Refre	esh												
S DNS	•	Search	Bits P:	ackets Connectie	ns Requests CPILIItil	ization Avg	Message Rou	ting Framework							
Fin Local Traffic	Status - Virtual Serve	er O Partition / Path Detail	ls ≑ In ≑ Out ≑ Ir	n	num	1 Min. 0 5 Min. 0 Msg.	In 🗢 Msg. Out 🔍 Req. In	Req. Out Resp. In Resp. In							
	dns-to-doh_ud	p_proxy Common View	0 0 0	0 0 0	0 0 0% 0	% 0% 0	0 0	0 0 0							
Acceleration	dns-to-dot_tcp	_proxy Common View	4.8K 5.9K 10	10 0 2	2 2 0% 0	% 0% 0	0 0	0 0 0							
Device Management	dns-to-dot_udp	_proxy Common View	1.8K 4.5K 3	3 0 1	3 3 0% 0	% 0% 0	0 0	0 0 0							
Shared Objects	doh-to-dns_pro	oxy Common View	891.9K 839.5K 1.2I	K 1.3K 2 3	35 0 0% 0	% 0% 0	0 0	0 0 0							
	dot-to-dns_pro	xy Common View	39.5K 161.0K 44	55 0 2	5 0 0% 0	% 0% 0	0 0	0 0 0							
Network	Reset														
System															

Since this is basic LTM functionality, general LTM logging practices can be used if you wish to log traffic in your environment.

Capturing Traditional DNS to DNS over TLS Traffic

On the BIG-IP CLI, we can see the 53/853 exchange on a packet capture using the same **tcpdump** command we used in the DoT-to-DNS section, as the IP/ports are simply being switched around. In the BIG-IP DNS Proxy session, issue the following command:

tcpdump -nni 0.0 (host 10.1.20.10 or 10.1.1.6) and (port 53 or port 853)

When running kdig commands on the Lab DNS Server, you will see the port 53 and port 853 connections in the output, as shown below.

BP BIG-IP DNS Proxy − O ×
length 0 in slot1/tmml lis=/Common/dns-to-dot_tcp_proxy 23:26:41.118037 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [.], ack 1, win 3650, options [nop,nop,TS val 3587003485 ecr 3183768418], length 0 out slot1/tmml lis=/Common/dns-to-dot
_ccp_proxy 23:26:41.18067 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags {P.}, seq 1:163, ack 1, win 3650, options [nop,nop,TS val 3587003485 ecr 3183768418], length 162 out slot1/tmml lis=/Com
mon/dma-to-dot_top_proxy
2016/91/12/94/ 16 0.0.0.003 / 10.1.20.10.35322: Frags [.], ack 105, will 240, options [hop,hop,is val 5103/00406 ecf 530/00405], length 0 in Stol/Lumit 115-/Common/uns-Co-dob Ecp proxy
23:22:41.133447 IP 8.8.8.8.853 > 10.1.20.10.39332: Flags [.], seq 1:1419, ack 163, win 240, options [nop,nop,TS val 3183768433 ecr 3587003485], length 1418 in slot1/tmml lis=/Co
mmon/dns-to-dot_tcp_proxy
23:22:41.133463 IP 8.8.8.8.853 > 10.1.20.10.39332: Flags [.], seq 1419:2837, ack 163, win 240, options [nop,nop,TS val 3183768433 ecr 3587003485], length 1418 in slot1/tmml lis=
Journal, and Conference of the second s
/Common/dns-to-dot_tcp_proxy
23:26:41.133992 IF 10.1.20.10.39332 > 8.8.8.8.853: Flags [.], ack 3098, win 4424, options [nop.nop,TS val 3587003501 ecr 3183768433], length 0 out slot1/tmml lis=/Common/dns-to-
dot top proxy
23/2011/13125 / 10/1/2010/3532 / 0.0.0.0.033: Flags [F.], see 103/211, ack 3050, will 1424, options [hop,hop,15 val 350/003301 et 3103/00533], length to Out Stott/chmmi 115- //common/dhas-to-dot top proxy
23:26:41.134461 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [P.], seq 211:256, ack 3098, win 4424, options [nop,nop,TS val 3587003501 ecr 3183768433], length 45 out slot1/tmml lis=
/Common/dns-to-dot_tcp_proxy
23:26:41.142264 IP 8.8.8.853 > 10.1.20.10.39332: Flags [P.], seq 3098:3149, ack 256, win 240, options [nop,nop,TS val 3183768442 ecr 3587003501], length 51 in slot1/tmml lis=/
Common/dis-to-dot_ccp_proxy 232.6:41.142314 TP 10.1.20.10.120332 > 8.8.8.8.853: Flags [.1. ack 3149. win 4437. options [non.non.TS val 3587003510 ecr 31837684421.]ength 0 out slot]/tmm] lis=/Common/dis-to-
dot tep proxy
23:26:41.142852 IP 10.1.20.10.39332 > 8.8.8.853: Flags [.], ack 3149, win 4437, options [nop,nop,TS val 3587003510 ecr 3183768442], length 0 out slot1/tmml lis=/Common/dns-to-
2012011/14291 12 10.1.20.10.39522 > 0.0.0.0.053: Flags [P.], seq 256:522, ack Sits, win 4457, options [hop,hop,is val 356/005510 ect Si55/05442], length 66 out Si5t//tmml lis- //common/das-to-dot tro provu
23:26:41.153855 IP 6.8.8.8635 > 10.1.20.10.39332: Flags [.], ack 322, win 240, options [nop,nop,TS val 3183768454 ecr 3587003510], length 0 in slot1/tmml lis=/Common/dns-to-dot
_tcp_proxy
23:26:41.262652 IP 8.8.8.853 > 10.1.20.10.39332: Flags [P.], seq 3149:3257, ack 322, win 240, options [nop,nop,TS val 3183768563 ecr 3587003510], length 108 in slot1/tmml lis=
//OMMON/UNE=to-dot_tcp_Droxy 23:06:10 10:00:332 > 8.8.8.8.8.53. Flags []. ack 3257. win 4464. ontions from non TS wal 3587003630 ecc 31837685631. length 0 out slot1/twml liss/Common/dns=to-
dot top proxy
23:26:41.263229 IP 10.1.10.101.53 > 10.1.1.6.39332: Flags [P.], seq 1:80, ack 38, win 12341, options [nop,nop,TS val 3587003630 ecr 1324775930], length 7931166 2/0/0 CNAME redir
ect.f5.com. A 104.219.111.169 (77) out slot1/tmml lis=/Common/dns-to-dot_tcp_proxy
23:22:41.23387 IP 10.1.1.6.39332 > 10.1.10.101.53: Flags [.], ack 80, win 62648, options [nop,nop,TS val 1324776083 ecr 3587003630], length 0 in slot1/tmm1 lis=/Common/dns-to-d
52/26:41.256259 IP 10.1.1.6.39332 > 10.1.10.101.53: Flags [F.], seq 38, ack 80, win 62648, options [nop,nop,TS val 1324776085 ecr 3587003630], length 0 in slot1/tmml lis=/Common
/dns-to-dot_tcp_proxy
23:26:41.265322 IP 10.1.10.101.53 > 10.1.1.6.39332: Flags [.], ack 39, win 12341, options [nop.nop,TS val 3587003633 ecr 1324776085], length 0 out slot1/tmml lis=/Common/dns-to-
400 top proxy 337.2634 TB 10 1 20 10 30332 > 8 8 8 853. Flage (F 1 220 302 302 302 302 302 404 404 Antione from non TS well 3587003533 por 3183768531 langth (out elot1/twm) ligz/Comm
and the body the body the body and the body with the body with the body body body body the body body the body body body body body body body body
23:26:41.273102 IP 8.8.8.8.8.853 > 10.1.20.10.39332: Flags [F.], seq 3257, ack 323, win 240, options [nop,nop,TS val 3183768573 ecr 3587003633], length 0 in slot1/tmml lis=/Common
/dns-to-dot_tcp_proxy
23:22:41.273161 IP 10.1.20.10.39332 > 8.8.8.8.853: Flags [.], ack 3258, win 4464, options [nop.nop.TS val 3587003640 ecr 3183768573], length 0 out slot1/tmml lis=/Common/dns-to- dos ten provi
and popularity and a second se
n/dns-to-dot_tcp_proxy
23:26:41.273546 IP 10.1.1.6.39332 > 10.1.10.101.53: Flags [.], ack 81, win 62648, options [nop.nop,TS val 1324776093 ecr 3587003640], length 0 in slotl/tmml lis=/Common/dns-to-d
or_tep_proxy

Stop your capture before moving on to the next section. This concludes the DNS-to-DoT section.

6.1.7 Proxying Traditional DNS queries to DNS over HTTPS

Finally, let's look at converting a DNS query to a DoH request.

Test Driving Traditional DNS to DNS over HTTPS

Minimize Firefox and bring both CLI session windows up. On the Lab DNS Server, once again use **kdig** to simply generate a traditional DNS request. Notice that this section of the lab uses a different VIP, the 10.1.10.102 address.

kdig @10.1.10.102 www.f5agility.com

You'll get a response as shown below:

user@ip-10-1-1-6:~\$ kdi	g @10.	1.10.102	www.f5agi	lity.com	
;; ->>HEADER<<- opcode:	QUERY	; status:	NOERROR;	id: 25887	
;; Flags: qr rd ra; QUE	RY: 1;	ANSWER:	2; AUTHOR	ITY: 0; ADDITIONAL:	0
;; QUESTION SECTION:					
;; www.f5agility.com.		IN	A		
;; ANSWER SECTION: www.f5agility.com.	299	IN	CNAME	redirect.f5.com.	
redirect.f5.com.	29	IN	A	104.219.111.169	
<pre>;; Received 77 B ;; Time 2020-01-24 04:3</pre>	1:03 U				
;; rrom 10.1.10.102053(UDP) 11	n 134.3 m	IS		

Viewing Statistics for DNS-to-DoH

Back on the BIG-IP, we'll see connections on the DNS-to-DoH virtual server in the Local Traffic module statistics:

BIG-IP [®] - ip-10-1-1-5.us-west ×	+															٥	
↔ → ♂ ŵ	🖲 🖗 https://10.1.	1.5/xui/?nocache=157983	2357260							90%	⊵) ☆		lıl) ii	Ξ
		F5 Ag	ility 202	20 - DN	S Over	HTTPS	/DNS ove	r TLS Lab									
Hostname ip-10-1-1-5.us-west-2.compute.in IP Address 10.1.1.5	internal Date Jan 23, 2020 Time 11:31 PM (EST)	User admin Role Administrator											Partition:	Common	$\mathbf{\mathbf{v}}$	Log ou	4
I ONLINE (ACTIVE) Standalone	Online (Active) Standalone																
Main Help About	Statistics » Module Statist	ics : Local Traffic » Virtual S	ervers														
Mage Statistics	🔅 👻 Traffic Summary 💌	DNS 👻 Local Tra	ffic Su		anagement		Memory										
Dashboard Module Statistics Display Options Statistics True Virtual Sequence																	
Performance Reports	Statistics Type	Statistics Type Virtual Servers															
-	Data Format	Normalized 🗸															
iApps	Auto Refresh	4 seconds 🗸 Stop Re	fresh														
S DNS	*	Search	Bi	its	Packets	Co	nnections	Requests	CPU U	tilization /	Ava.		Mes	sage Rou	ting Frame	work	
Local Traffic	Status A Virtual Serv	er OPartition / Path Det	ails 🗢 In	≎ Out 🗘	In 🗢 Out	• Current	• Maximum 🗘 T	otal 🕕 Total	¢ 5 Sec.	0 1 Min.	• 5 Min.	0 Msg. In	≑ Msg. Out	Req. In	Req. Out	Resp. In	• F
	dns-to-doh_u	dp_proxy Common Vie	v 504	840 1	1	0	1 1	0	0%	0%	0%	0	0)	0	0	0
Acceleration	dns-to-dot_tc;	o_proxy Common Vie	N 14.5K	16.9K 3	0 30	0	2 6	3	0%	0%	0%	0	0)	0	0	0
Device Management	dns-to-dot_ud	p_proxy Common Vie	N 1.8K	4.5K 3	3	0	1 3	3	0%	0%	0%	0	0)	0	0	0
1 Shared Objects	doh-to-dns_pr	oxy Common Vie	v 930.6K	877.3K 1.	.4K 1.4K	2	3 35	0	0%	0%	0%	0	0)	0	0	0
A Natwork	dot-to-dns_pr	oxy Common Vie	N 39.5K	161.0K 4	4 55	0	2 5	0	0%	0%	0%	0	0)	0	0	0
network	Reset																
System																	

If we set the statistics type to *iRulesLX*, we'll see RPC connections on the iRule for this translation:
🚯 BIG-IP® - ip-10-1-1-5.us-west- ×	+													-	٥		×
← → ♂ ☆	🖸 🔒 https://10.1.1.	5/xui/?nocache=	15798323572	260					909		⊠ ☆		111		٢	÷	≡
			F5 Agility	2020 <mark>- DNS O</mark> ve	r HTTPS/	DNS	over TL	S Lab									
Hostname ip-10-1-1-5.us-west-2.compute.ir IP Address 10.1.1.5	nternal Date Jan 23, 2020 Time 11:32 PM (EST)	User admin Role Administrato	or									Partition	Common	$\mathbf{\vee}$.og out	
I ONLINE (ACTIVE) Standalone	Standalone																
Main Help About	Statistics » Module Statistic	s : Local Traffic »	iRules LX										9///				
Mage Statistics	🔅 🗸 Traffic Summary 🔻 DN	vs 🔻	Local Traffic	Subscriber Management			lemory		em								
Dashboard																	
Module Statistics	Display Options																
Performance Reports	Statistics Type	Rules LX	\checkmark														
_	Data Format	Normalized 🗸															
iApps	Auto Refresh	4 seconds 🗸	Stop Refresh														
S DNS	8	Search						Proce			RPC Inf	0	Str	eamin	unfo		5
In Local Traffic	Status		▲ Plugin : Exten	ision	Partition / Path	Details	· Restarts	© CPU (%)	Total Virtual S	ize o T	otal Connections	• Total Calls	Clientside T	otal 0	Servers	ide Tot	al
0	GRunning		DNS_to_DoH_P	roxy : dns_over_https	Common	View	0	0	1.9G	1		1	0	0			1
Acceleration	Running		DoH_to_DNS_P	roxy : DoH_to_DNS_Proxy	Common	View	0	0	2.2G	80		80	0	0			
Device Management	Reset																
📸 Shared Objects																	
Retwork																	
System																	

Capturing Traditional DNS to DNS over HTTPS Traffic

Running a packet capture on the BIG-IP DNS Proxy, we can view the front-end udp/53 requests being translated to DoH requests:

```
tcpdump -nni 0.0 (host 10.1.10.102 and port 53) or (host 8.8.4.4 or host 8.8.
8.8 and port 443)
```

Run kdig queries on the Lab DNS Server to generate traffic.

NOTICE If your packet capture is "noisy," remember that you're also capturing the HTTPS monitor traffic as the "doh_google.dns" pool performing regular queries.

Notice that a port 53 request comes in, a HTTPS connection is set up and the query is passed, then the port 53 response is sent to the client before the HTTPS connection is torn down.

13:24:31.414842 IP	10.1.1.6.44657 > 10.1.10.102.53: 39939+ A? www.f5agility.com. (35) in slot1/tmm0 lis=
13:24:31.492130 IP	10.1.20.10.21881 > 8.8.8.8.443: Flags [S], seq 3145906949, win 29200, options [mss 146
13:24:31.500688 IP	8.8.8.8.443 > 10.1.20.10.21881: Flags [S.], seq 3232513395, ack 3145906950, win 60192,
13:24:31.500967 IP	10.1.20.10.21881 > 8.8.8.8.443: Flags [.], ack 1, win 229, options [nop,nop,TS val 363
13:24:31.501173 IP	10.1.20.10.21881 > 8.8.8.8.443: Flags [P.], seq 1:510, ack 1, win 229, options [nop,no
13:24:31.509805 IP	8.8.8.8.443 > 10.1.20.10.21881: Flags [.], ack 510, win 240, options [nop,nop,TS val 4
13:24:31.510181 IP	8.8.8.8.443 > 10.1.20.10.21881: Flags [P.], seq 1:169, ack 510, win 240, options [nop,
13:24:31.510230 IP	10.1.20.10.21881 > 8.8.8.8.443: Flags [.], ack 169, win 237, options [nop,nop,TS val 3
13:24:31.510516 IP	10.1.20.10.21881 > 8.8.8.8.443: Flags [P.], seq 510:814, ack 169, win 237, options [no
13:24:31.523172 IP	8.8.8.8.443 > 10.1.20.10.21881: Flags [.], ack 814, win 244, options [nop,nop,TS val 4
13:24:31.587284 IP	8.8.8.8.443 > 10.1.20.10.21881: Flags [P.], seq 169:819, ack 814, win 244, options [no
13:24:31.587701 IP	10.1.20.10.21881 > 8.8.8.8.443: Flags [P.], seq 814:845, ack 819, win 247, options [no
13:24:31.587835 IP	10.1.10.102.53 > 10.1.1.6.44657: 39939 2/0/0 CNAME redirect.f5.com., A 104.219.111.169
13:24:31.587902 IP	10.1.20.10.21881 > 8.8.8.8.443: Flags [F.], seq 845, ack 819, win 247, options [nop,no
13:24:31.587917 IP	8.8.8.8.443 > 10.1.20.10.21881: Flags [F.], seq 819, ack 814, win 244, options [nop,no
13:24:31.588120 IP	10.1.20.10.21881 > 8.8.8.8.443: Flags [.], ack 820, win 247, options [nop,nop,TS val 3
13:24:31.596160 IP	8.8.8.8.443 > 10.1.20.10.21881: Flags [.], ack 845, win 244, options [nop,nop,TS val 4
13:24:31.596328 IP	8.8.8.8.443 > 10.1.20.10.21881: Flags [.], ack 846, win 244, options [nop,nop,TS val 4
13:24:31.596546 IP	8.8.8.8.443 > 10.1.20.10.21881: Flags [R.], seq 820, ack 846, win 244, options [nop,no
13:24:31.596562 TP	8.8.8.8.443 > 10.1.20.10.21881; Flags [R], seg 3232514215, win 0, length 0 in slot1/tm

This concludes the hands-on portion of the lab.

6.1.8 Additional Resources

The following resources will allow you to explore DoH and DoT more, and setup this functionality in your own environment.

- RFC8484: DNS over HTTPS: https://tools.ietf.org/html/rfc8484
- RFC7858: DNS over TLS: https://tools.ietf.org/html/rfc7858
- Github repository with iRules and sample configuration: https://github.com/grf5/DoHDotiRulesLX

LAB: F5 DNS Cloud Service & F5 DNS Load Balancer Cloud Service

Table of Contents

- LAB: F5 DNS Cloud Service & F5 DNS Load Balancer Cloud Service
 - Introduction
 - Pre-Requisites
 - Lab Environment Overview
 - * 1. APIs and Services
 - * 2. Application Scenario
 - Lab Environment Setup / Validation
 - * 1. F5 Cloud Services Portal
 - * 2. Opera with VPN to Test Geo Services
 - * 3. Postman Configuration
 - * 4. Zone Name
 - F5 DNS Cloud Service UI
 - * 1. Create Secondary DNS Zone
 - * 2. Query via Browser
 - * 3. Delete Zone
 - F5 DNS Cloud Service API
 - * 1. Create Zone
 - * 2. Get Zone File
 - * 3. Query via Browser
 - * 4. Review the JSON
 - * 5. Delete Zone
 - F5 DNS Load Balancer Cloud Service UI

- * 1. Create F5 DNS Load Balancer Cloud Service
- * 2. Add Single Endpoint, Health Monitor, Pool and Default Geoproximity Rule
- * 3. Add Multiple Ednpoints to Load Balanced Pool & Test
- * 4. Add Europe Region & EU Endpoint with Corresponding Geoproximity Record
- * 5. Duplicate Load Balanced Record using JSON through the UI
- * 6. Delete DNS Load Balancer Service
- F5 DNS Load Balancer Cloud Service API
 - * 1. Create DNS Load Balancer Subscription
 - * 2. Activate DNS Load Balancer Subscription
 - * 3. Test NA Pool
 - * 4. Add Endpoints & Pool Members
 - * 5. Test Round Robin (lab)
 - * 6. Update Proximity Rule
 - * 7. Test Proximity Rules (lab)
 - * 8. Review the JSON
 - * 9. Delete DNS Load Balancer Service
- Clean Up

7.1 Introduction

Welcome to the F5 Cloud Services lab that covers DNS and DNS Load Balancer services. This lab will take you through the setting up, configuration, updates, and removal of the F5 Cloud Services that provide DNS capabilities. You will be using both browser-based UI of the F5 Cloud Services platform, as well as the declarative API, which is available to do all of the things the UI does, and more!

In the process of this lab you will learn how to:

- · Set up a DDoS-protected secondary DNS service
- Retrieve and review the zone file retrieved from the primary DNS (we will provide you with a primary DNS and a zone just for you!)
- · Set up Anycast network-backed load balanced DNS record
- Add and update application endpoints and a load-balancer pool
- · Configure, update, and test geoproximity rules, and
- · Have fun working with UI and APIs!

7.2 Pre-Requisites

- Any modern browser: for working with the UI (and this document)
- · Postman: for working with the API of the F5 Cloud Services

- Opera browser: for simulating geo-location specific traffic
- Any text editor: for duplicating Load Balanced Record

IMPORTANT NOTE: If you originally signed up for F5 Cloud Services through a Limited User invitation (such as an email invite from another lab or from a different account owner), then it is possible that you haven't yet completed a full registration.

You can quickly tell if you have a full account by looking at your account(s) in the F5 Cloud Services Portal. If you do now see any "Accounts you own:" and only see "Accounts you've been granted access to" as a "**Limited User**", then you will need to create a full account / update user info before you can proceed with this lab. You can do so in the step 4(c) below via the F5 Cloud Services API using the Postman request titled "Set User Info (optional)", the details of which are outlined below after the Login.

7.3 Lab Environment Overview

7.3.1 1. APIs and Services

This Lab utilizes standard *F5 Cloud Services API*, as well as a *Lab Service API*, which was custom-built just for executing this lab:

- · F5 Cloud Services API: create, use, and remove the services in the scope of this lab
- Lab service API: facilitates auxiliary functions for the lab only: creating DNS entries, sending targeted requests & traffic to the apps/services, etc.

The following diagram captures the core components of this Lab:



7.3.2 2. Application Scenario

In order to fully explore the capabilities of F5 Cloud Services, you will be able to use an existing application with a set of live instances across different clouds and geographic locations. This app is "BuyTime Auction", a fictitious multi-instance deployment that helps to simulate a globally deployed app topology. Unsurprisingly, performance, global availability, zero downtime, and security are critical for this application, while the app Developers & DevOps are used to consuming app infrastructure as-a-Service.

The following are the demo application instances, some of which will be utilized in the scope of this lab:

Name	Geography	Cloud/Region	IP	URI
NA1	North Amer-	AWS - US East (N. Vir-	34.229.48.248	http://na1-auction.
	ica	ginia)		cloudservicesdemo.net/
NA2	North Amer-	AWS – US East (N. Vir-	318.232.64.254	http://na2-auction.
	ica	ginia)		cloudservicesdemo.net/
NA3	North Amer-	Azure – US East	13.82.106.211	http://na3-auction.
	ica			cloudservicesdemo.net/
EU	Europe	AWS – Europe (Frank-	3.122.191.227	http://eu-auction.
		furt)		cloudservicesdemo.net/

The following diagram is a simplified architecture of the Auction application:



7.4 Lab Environment Setup / Validation

7.4.1 1. F5 Cloud Services Portal

a) Login

In order to use F5 Cloud Services, you need to be logged in with a valid user account. If you need to sign up, or if you already have one, proceed to the F5 Cloud Services portal.

Once you've logged in with an account, you will be using the user name and password values in the lab to authenticate with the F5 Cloud Services and the API.

b) Subscribe to Catalogs

In order to access specific F5 Cloud Services, you need to subscribe to the corresponding service catalogs.

CLOUD SERVICES			Sign Up
	LOG IN		
	Email		
	Password	DELIVER EVERY APP.	
		WITH CONFIDENCE.	
	Don't have en account yet? Circate Onel Or if you prefer to use your XWS account, start at XWS Marketplace		
	Copyright F5 Networks, Inc. All Rights Reserved. F5 Cloud Services Legal Privacy Trademarks		

1. Click on the **Your F5 Cloud** tab in the left navigation panel and you will see the available service catalogs, as well as the services you have subscribed to, if any. For this lab you will need to click **Subscribe** to **DNS** and **DNS Load Balancer** services.

CLOUD SERVICES			() Help
NO SUBSCRIBED SERVICES. To get started, subscribe to one of the available se	vices below.		Vsers A 1 Active in this service
ADD F5 CLOUD SERVICES			NEED SUPPORT?
br May and manage your domains and zone files with secondary authoritative DNS. Bericing information write Subscribe Control Subscribe Control Subscribe Control Subscribe Beacn Ban full visibility and insights across your application landscape. Bericing information	Def Load Balance Ded balance your traffic across servers and regions. See pricing information Available Subscribe Def Content D	Esential App Protect Secure your apps and protect your assets. See pricing information Available Try it free (10 days)	PS Cloud Services Support For technical assistance and other questions please visit our support pages Image: Cloud Services Product Services Productions Image: Cloud Services Productions
Available Subscribe	Available Start free preview		now we can make it better. Start the survey here.

2. For the purposes of the lab you can utilize the Free Tier for both the DNS and DNS Load Balancer services. **NOTE**: you will be asked to add your payment card even for the free tier, however you will not be charged if you follow the Free Tier guidelines outlined here:

- F5 DNS Cloud Service Pricing
- F5 DNS Load Balancer Service Pricing

Should you decide to add additional zones or LBR records beyond the Free Tier, you will only pay for what you use.

You may also choose to not use a credit card, and instead subscribe through AWS Marketplace.

- AWS Marketplace: F5 DNS Cloud Service
- AWS Marketplace: F5 DNS Load Balancer Service

SUBSCRIBE TO DNS SERVICE?	×
 Standard service pricing applies. A valid payment method must be present and will be charged for applicable usage at the end of each billing period Unsubscribe from the service at any time to cancel. 	
Use this payment method: Credit card Subscribe through AWS Marketplace 	
Cancel Yes, subscribe now	

Add payment card to pay by credit card:

Or initiate the subscription from AWS Marketplace to subscribe through it:

After successfully subscribing, your services will appear in the **Your F5 Cloud** tab. You will also see their current status.

If you need to check your payment information, it is available in the **Accounts** tab, **Payment** section.

7.4.2 2. Opera with VPN to Test Geo Services

You will need the Opera browser to test proximity rules we will set later.

Open the Opera browser, click Settings, Advanced, Features and then Enable VPN.

ADD PAYMENT CARD	
Card Type	
Card Number	
Expiration Date (YYYY) - Select One - 🔻 / - Select One -	T
CVV	
Cardholder Name	
Street Address	
City	
State/Province/Region	Zip/Postal Code
Country	
- Select One -	





G	CLOUD SERVICES							() Help
د *	Organization Users	Divisions Paymer	ıts					
<u>_</u>	CREDIT CARDS ON FI	LE			Add	OTHER PAYMENT METHODS		
·@·	₽ Filter All	1 items				🐲 aws marketplace		
8	Card ending in	Card type	Expiration	Services		Account Type	Services	
	Default			∰ Beacon ∰ DNS Load Balancer		View billing dashboard	g DNS	
	CURRENT CREDIT CA \$0.00 usp ①	RD USAGE - Ail Services		ٹ Down	mload			
	□ Date ↓		Statement					
			1000					
			1000					
			1000					



7.4.3 3. Postman Configuration

a) Download Postman here, open it, create a Postman account if you don't have one and choose to do so, and sign in.

b) Clone or download and extract the repository

Search or jump to	Pull requests Issues Marke	tplace Explore	₽ +•					
			×					
Learn (Git and GitHub w	thout any code!						
Using the Hello World guide, you'll start a branch, write comments, and open a pull request.								
	Read the guid							
☐ f5devcentral / f5-cloudservicednslab		👁 Watch 🕶	5 🔂 Star 0 😵 Fork 3					
F5 DNS and DNS Load Balancer Cloud Service Manage topics	es - Lab & API examples with Pc	stman	Edit					
-o- 2 commits 🐉 1 branch	O packages	> 0 releases > 2 contrib	butors 최초 MIT					
Branch: master - New pull request		Create new file Upload file	es Find file Clone or download -					
yoctoalex initial commit (#1)		Clone with HT	Use SSH					
_figures	init	al commit (#1) https://github.	com/f5devce.ral/f5-cloud					
postman	init	al commit (#1)						
DNS & Load Balancer.vsdx	init	al commit (#1) Open in Deskt	top Download ZIP					
	Init	al commit	2 months ago					

c) Import collection – /postman/F5 Cloud Services DNS LAB.postman_collection.json and environment – /postman/F5 Cloud Services DNS LAB.postman_environment.json.

You will now see the imported collection (left side) with the calls that you will be utilizing grouped into several categories, as well as the environment variables (top right) used to store and pass data between Postman and the API.

You are now ready to interface with the F5 Cloud Services using Postman.

7.4.4 4. Zone Name

In order to create secondary DNS zone in the F5 Cloud Services portal, you need to have a zone name. Use Postman and follow the steps below to get the Zone name from the Lab service API.

a) Open the "F5 Cloud Services DNS LAB" environment variables by clicking the "Environment Quick Look", click into the field of the corresponding variable, and type the value of user email in the variable



Hew Import Runner	📮 🔹 My Works	pace 🔻 🗼 Invite	🧿 📽 ঌ 🌢 🎔 🌏 Upgrade 🔻		
Q Filter	GET GET POST C POST C POST A POST	C POST A POST T PUT POST T F	+ ··· F5 Cloud Services DNS LAB 🔻 💿 🔅		
History Collections APIs	▶ Get GSLB JSON		Comments (0) Examples (0) 🔻		
+ New Collection Trash	GET • https://{{HOSTNAME}}//{{API_VERSION}}/svc-	ubscription/subscriptions/{{GSLB_SUBSCRIPTION_ID}}	Send 💌 Save 💌		
21 requests	Params Authorization Headers (9) Body Pre-request Script Tests Settings				
Core Requests DNS	▼ Headers (2)				
 DNS Load Balancer 	KEY	VALUE	DESCRIPTION •••• Bulk Edit Presets 🔻		
🕨 🖿 Clean Up	Content-Type	application/json			
	Authorization	Bearer {{ACCESS_TOKEN}}			

F5 Cloud Services DNS LAB POST A DOST T DUIT F5 Cloud Services DNS LAB Environment quick look VARIABLE INITIAL VALUE CURRENT VALUE HOSTNAME api.cloudservices.f5.com api.cloudservices.f5.com API_VERSION v1 ν1 DNS_WEB_ADMIN 54.211.12.173:10000 54.211.12.173:10000 USER EMAIL user@email.com USER_PASSWORD password ACCOUNT_NAME

"USER_EMAIL" (click Enter after typing the values).

Repeat the same for the "USER_PASSWORD".

b) Select the **Login** request in the sidebar to login to your F5 Cloud Services profile and click **Send** to get the authorization token. More detailed information on this API request can be found here.

History Collections APIs	▶ Login		Examples (0)		
+ New Collection Trash	POST + https://{(HOSTNAME))//(API_VERSION))/svc-a	uth/login	Send - Save -		
21 requests Params Authorization Headers (9) Body • Pre-request Script Tests • Settings					
POST Login GET Get Current User	KEY	VALUE	DESCRIPTION *** Bulk Edit		
GET Get DNS Zone (lab)	Key	Value	Description		
GET Get User Membership	Body Cookies Headers (6) Test Results (1/1)	Stat	us: 200 OK Time: 850ms Size: 3.01 KB Save Response 🔻		

A successful login will result in Postman returning the tokens from the API, shown in the response body below:



These tokens are then stored for subsequent calls using a function inside Postman to set environment variables. You can see the test function in the **Tests** tab:

NOTE: If any of the subsequent Postman calls return a blank response or "**status**": "**unauthorized**" response (see the screenshot below), it means your user token has expired and you will need to re-login. To do that you just need to re-send the **Login** request.

POST	*	https://{	{HOSTNAME}}/{{/	API_VERSION}	}/svc-auth/login			
Params	Author	rization	Headers (9)	Body 鱼	Pre-request S	cript Tests •	Settings	
1 ▼ pm 2 3 i 4 }) 5	.test("Se var jsc pm.envi	:t token onData = ironment.	variable", func pm.response.jsc set("ACCESS_TOK	tion() { n(); EN", jsonDa	ta.access_toke	n);		
Body Co	okies H	eaders (6)	Test Results (1/1)				5
Pretty	Raw	Preview	w Visualize B	JSON	• =			
1 2 3 4	{ "sta "mes }	tus": "un sage": "a	authorized", access denied"					

c) OPTIONAL: Set User ID & Account Info

IMPORTANT NOTE: If you originally signed up for F5 Cloud Services through a Limited User invitation (such as an email invite from another lab or from a different account owner), then it is possible that you haven't yet completed a full registration. You can quickly tell if you have by looking at your account(s) in the F5 Cloud Services Portal If you do now see any "Accounts you own:" and only see "Accounts you've been granted access to" as a "**Limited User**", then you need to create a full account & update user info before you can proceed with this lab.

You can do this by running the following **Set User Info** API call, after you've updated the Body of the request with your own organization & address information:

The response returns the following detail, including your own organization account ID (id):

More information on this API request can be found here.

At this point you should be a full user with an "Owned Account" and a primary organization account id, which can also be confirmed in the F5 Cloud Services Portal in the drop-down under your user name (top right), where you should see "Accounts you own:" and the Organization Account you created with "**Owner**" defined.

d) Retrieve User ID & Account ID

Select the **Get Current User** request and click **Send** to retrieve User ID and Account ID to be used in the further requests.

The response returns the following detail:

The retrieved User ID and Account ID are then stored for subsequent calls.

More detailed information on this API request can be found here.

e) Let's now retrieve DNS Zone Name with the **Get DNS Zone (lab)** API call. Click **Send**. This call will pass your "ACCESS_TOKEN" in the header of the request to the Labs API in order to validate existence of your F5 account & return back a Zone name unique to your lab.

POST	*	https:/	/{{HOSTNAME}}/{{Al	PI_VERSION	}}/svc-acco	ount/accounts			
Params	Author	ization	Headers (10)	Body 鱼	Pre-re	equest Script	Tests 🔵	Setting	35
none	form	m-data	x-www-form-ur	lencoded	🖲 raw	binary	GraphQL	JSON	Ŧ
1 - [{]									
2	"name":	"Demo	Account",						
3 🕶	"addres	s": {							
4	"st	reet_1"	: "801 5th Ave",						
5	"ci	ty": "S	eattle",						
6	"st	ate": "	WA",						
7	"po	stal_co	de": "98104",						
8	"co	untry":	"US"						
9	}								
10 }									

Pretty	Raw Preview Visualize JSON 🔻 异
1	c
2	"id": "a-aaDYQhrBca",
2	Parant account idly UP
4	parent_account_id ;
5	"status": "active",
6	"level": "0",
7	"signup_provider": "standard",
8	"address": {
9	"street_1": "801 5th Ave",
10	"street 2": "",
11	"city": "Seattle".
12	"state": "WA"
12	"country", "US"
15	country : US ,
14	"postal_code": "98104-1663"

GE	Ť	nupsin	(ILOSINAME)////	VEI VEI SIG	my/svc-accountri	1261	
Para	ms Author	ization	Headers (8)	Body	Pre-request Sc	ript Tests • Settings	
v	Headers (1)						
	KEY					VALUE	I
~	Authorization					Bearer {{ACCESS_TOKEN}}	
	Key					Value	
. ·	Tomporany Lloa	dare (7)	•				

Body Co	okies Headers (6) Test Results (1/1)
Pretty	Raw Preview Visualize BETA JSON -
1	K
2	"id": " ",
3	"email": "
4	"first_name": "/ _ ",
5	"last_name": "",
6	"phone": "",
7	"primary_account_id": " " " " " " " " " " " " " " " " " "
8	"status": "active",
9	"email_confirmed": true,
10	"phone_confirmed": false,
11	"unconfirmed_email": "",
12	"time_zone": "",
13	"preferred_language": "",
14	"user_email_history": [],
15	"current_password": "",
16	"create_time": "2019-07-22T14:54:39.9984122",
17	"update_time": "2019-07-22T14:54:39.998412Z",
18	"activate_time": null,
19	"delete_time": null,
20	"reset_password_sent_time": null,
21	"reset_password_time": null,
22	"email_confirmation_sent_time": "2019-07-22T14:54:57.906915Z",
23	"email_confirmation_time": "2019-07-22T14:54:57.906915Z",
24	"phone_confirmation_sent_time": null,
25	"phone confirmation time": null

GET		*	https://	{{HOSTNAME}}/{{	API_VERSIC	N}}/svc-account/user			
Param	15	Author	ization	Headers (8)	Body	Pre-request Script	Tests 🌒	Settings	
1 ▼ 2 3	pm.te	st("Se ar jso m.envi	et accoun onData = ironment.	nt_id and user_ pm.response.js .set("ACCOUNT_I	id variab on(); D", jsonDa	les", function() {	id);		
4	р	m.envi	ironment.	set("USER_ID",	jsonData.	.id);			
i 5 6	})								

Request:

GET		http://	{{DNS_WEB_ADMIN	}}/zone		
Para	ms Auth	orization	Headers (2)	Body	Pre-request Sci	ipt Tests • Settings
	leaders (2)					
	KEY					VALUE
~	Content-Ty	be				application/json
~	Authorizati	on				Bearer {{ACCESS_TOKEN}}

The response will return your test DNS zone name and the status.

Body Cod	okies Headers (6)	Test Results (1/1)			Status: 200 OK
Pretty	Raw Preview	Visualize JSON	• =		
1 2 3 4 5	<pre>status": "ok", "zone": "user-n1 "zone2": "user-r</pre>	lh0si.securelab.online 11h0si-2.securelab.onl:	ine"		

Sending this request will automatically capture of the Zone variables:

GET	Ŧ	http://{	(DNS_WEB_ADMIN	}/zone				
Params	s Author	ization	Headers (9)	Body	Pre-request Script	Tests 🜒	Settings	
1 - 2 3 i 4 5	pm.test("Ge var jsc pm.envi })	et User's onData = ironment.	<pre>> DNS Zone Name" pm.response.jso .set("ZONE_NAME"</pre>	, functio n(); , jsonDat	on() {			

This Zone Name will be used for creating Secondary DNS Zone in the F5 Cloud Services portal, as well as throughout the lab as the domain name for your test applications.

7.5 F5 DNS Cloud Service - UI

7.5.1 1. Create Secondary DNS Zone

Let's now return to the F5 Cloud Services portal and create Secondary DNS Zone using the UI. We will repeat the same flow through the API in the subsequent section.

a) Go to the **DNS** tab and click **Create**.

6	CLOUD SERVICES	⑦ Help	8
C) Xe 1	R DNS		
8	SERVICE HEALTH REQUESTS N/A O 0 Healthy/0 Degraded All zones, past 90 days		
	ZONES		2 Create
	CREATE A ZONE		
	To get started with the DNS service, create some zones!		
**	Copyright FS Networks, Inc. All Rights Reserved. FS Cloud Services Legal Privacy Trademarks		

b) Paste **Zone name** retrieved in step 4.e) above and indicate the following DNS IP: **54.211.12.173** as the DNS Primary Server IP. Other values are optional. Then click **Get Zone File**.

🚯 сі	OUD SERVICES			② Help	8	
0	A UPMIX LLC DNS			CREATE SECONDA	RY DNS ZONE	×
8	R DIRACLEC SERVICE HEALTH N/A 0 Healthy / 0 Degraded ZONES	RECORESTS O All zones, past 90 days To get starte	CREATE A ZONE d with the DNS service, create some zones!	Zane Name User-2442440.securelabor S4211.12.174 Ensue Bris Job DM Mater Ser Alternative IP Octional Division None Description Optional Add Transaction Signatur	Ine Ine Inertifiers from our Ps Iner Alone zone transfers from our Ps Iner Key (TSIG) Cancel Cet Zone File	

c) This will retrieve the zone file from your primary DNS server. Click **Deploy** and then **Done**. This will create Secondary DNS Zone.

7.5.2 2. Query via Browser

Let's now see how the created Secondary DNS works.

a) Click on your zone in the **DNS** tab and scroll down to see **ZONE FILE**, where you need to copy "na1-auction.user-**your_zone_name**".

b) Paste the address into your browser and you'll get to the website:

6	CLOUD SERVICES					Help Alex Shemyakin UPMIX LLC
© %	DNS DECISETE				• Zon • A cop vertic	e File y of the raw zone file is displayed below for your auton
88 ⊕ ∛	HEALTHY 178 2 Healthy / 0 Degraded All zones, past 90 days ZONES				user- n1100 2020 user- ns1.f user- ns2.f	11h0si securelab online. 30 IN SOA ns1.user- is ecurelab online. Info user-n1h0si securelab online. 101011 30 30 30 30 n1h0si securelab online. 30 IN NS 5cloudservices.com. n1h0si securelab online. 30 IN NS 5cloudservices.com.
6	후 Filter All 3 Itams				auctions ns91. eu-au	un.user-n1h0si.securelab.online. 30 IN NS .dns.cloudservices.f5.com. uction.user-n1h0si.securelab.online. 30 IN A
	Zone Name 1	Health	Primary IP	Division	Last Updated 3.122 14.22	191.227 suction.user-n1h0si.securelab.online. 30 IN A
	user-3s95yl.securelab.online	🗢 Healthy	54.211.12.173		Jan 31, 2020 / 10:47 52.22	uction.user-n1h0si.securelab.online. 30 IN A 26.147.184
	user-n1h0sLsecurelab.online	Ø N/A	54.211.12.173		rs1.u Feb 13, 2020 / 10:51 user-	ser-n1n0si.securelab.online. 30 IN A .1.12.173 .n1h0si.securelab.online. 30 IN SOA ns1.user-
	user-z4e2440.securelab.online	🗢 Healthy	54.211.12.173		Feb 7, 2020 / 16:26 0 2020	ui.securelab.online. info.user-n1h0si.securelab.online. 010101 30 30 30 30
>>	Copyright F5 Networks, Inc. All Rights Reserved. F5 Cloud Services Legal Pri	vacy Trademarks			В	lack Cancel Deploy

ONE PROPERTIES		
ame and location of your zone file.		
Zone Name	Description	
user-z4e2440.securelab.online	Optional	
DNS Primary Server IP	Add Transaction Signature Key (TSIG)	
54.211.12.173		
Alternative IP		
Optional -	+ -	
Dhésian		
None	-	
	•	
Interesting the sone file we're using.		
user-z4e2440.securelab.online. 10 IN SOA	8180256742b8. info.user-z4e2440.securelab.online. 2020020537 10 10 10 10	
user-z4e2440 securelab online. 10 IN NS ns1	N COUDENS VIENS COTT.	
user-z4e2440.securelab.online. 10 IN NS ns1 user-z4e2440.securelab.online. 10 IN NS ns2 auction user-z4e2440.securelab.online. 10 IN NS ns2	s. Escludeamides.com. 52. F5cludeamides.com.	
user-z4e2440.securelab.online. 10 IN NS ns1 user-z4e2440.securelab.online. 10 IN NS ns2 auction.user-z4e2440.securelab.online. 10 IN NS au-auction.user-z4e2440.securelab.online. 10 IN ns1 auction.user-z4e2440.securelab.online. 10 IN	2 20-04 and 20 20 20 20 20 20 20 20 20 20 20 20 20	
user-z4e2440 securelab online. 10 IN NS ns: auction user-z4e2440 securelab online. 10 IN NS ns: auction user-z4e2440 securelab online. 10 IN NS au-auction user-z4e2440 securelab online. 10 IN na1-auction user-z4e2440 securelab online. 10 IN na2-aucuor user-z4e2440 securelab online. 10 IN	1 acculation web cont 5 (m2) diversifies a content of the content	
user-z4e2440 securelab online. 10 IN NS m.3 user-z4e2440 securelab online. 10 IN NS m.3 auction user-z4e2440 securelab online. 10 IN NS marticulton user-z4e2440 securelab online. 10 IN marticulton user-z4e2440 securelab online. 10 IN marticulton user-z4e2440 securelab online. 10 IN sub-rz4e2440 securelab online. 10 IN SOA	22 Edolution/veas.com 22 Edolution/cast.com A 3 122 42 101 227 A 3 122 24 24 24 blagb twift prd 5sas.com. A 32 22 44 24 blagb twift prd 5sas.com. A 52 22 147 144 51025572428 blin wear-44244 securitab celline. 2020028537 10 10 10 10	
user-2482440 securalab online 10 IN NS nst user-2482440 securalab online 10 IN NS nst auction user-2482440 securalab online. 10 IN NS naturation user-2482440 securalab online. 10 IN NS naturation user-2482440 securalab online. 10 IN nat-auction user-2482440 securalab online. 10 IN user-2482440 securalab online. 10 IN SOA	22 EStudianticies com SRIS d'as Cydudentices 5 com. A 3122 191227 A 34224 84248 C NVME, war-auSchogt x waf prd ISaas com. A 52 225 11;7 A 52 225 11;7 8 3102557 4206 info user-24r2440 securetab online. 2020020537 10 10 10 10	
user-242424 securitebonine 10 IN NS mi auction user-242244 securitebonine 10 IN NS mi auction user-2422440 securitebonine 10 IN mit auction user-2422440 securitebonine 10 IN mit auction user-24224245 securitebonine 10 IN mit auction user-2422440 securitebonine 10 IN user-2462440 securitebonine 10 IN SOA	22 ESolution-local com 22 ESolution-local-science (5 com. 1 A 3 122 191 227 C CNAME vmFaa53kbagt swaf prd Fsias com. C CNAME vmFaa53kbagt swaf prd Fsias com. A 52 226 1/12 8180256742b8 info user-z4e2440 securelab online. 2020020537 10 10 10 10	
user-z42440 securatiba online 10 IN NS mi seucifio user-z42440 securatiba online 10 IN NS mi seucifio user-z424240 securateba online 10 IN mission mission and the securation of the securation of the securation mission of the securation of the securation mission mission of the securation of the securation of the user-z4ed2440 securateba online 10 IN SOA	22 Edoladan/veas.com R 22 Edoladan/veas.com A 3 122 191 / 221 CANNEZ 24 191 / 221 CANNEZ 24 1927 CANNEZ 24 1927 194 A 52 225 147 154 A 52 225 147 154 S180225574288 info user-z4e2440 securetab online. 2020020537 10 10 10	
user 24240 securab office 10 N N S mi user 24240 securab office 10 N N S mi metanticity of the securation of the securation metantic securation of the securation of the securation securation of the securation of the securation of the securation securation of the securation of the securation of the securation securation of the securation of the securation of the securation of the securation securation of the securation of the securati	22 Edudance/sea com 22 Edudance/sea com 24 A 122 191227 C 1404E _ ver4_adS2 g/s wil prd/Saac com. C 1404E _ ver4_adS2 g/s wil prd/Saac com. 21802255742b8. info user-24e2440 securetab online. 2020020537 10 10 10 10	
user-24244 securation time. 10 IN NS mit wer-24244 securation totime. 10 IN NS mit assumption user-24244 securation totime. 10 NS mit assumption user-24244 securation totime. 10 NS mit = succion user-242444 securation totime. 10 NS mit = succion user-242444 securation totime. 10 NS CA	22 EStudencies com 22 EStudencies 5 com. 1 A 3122 191227 A 34224 8228 C NAME, wir-alsöksgtz wirf prd ISas com. A 52228 1/1, 4 518025574206 info.user-24e2440 securelab online. 202020537 10 10 10 10	
user-24244 securate bontine 10 IN NS mi auction user-242244 securate bontine 10 IN NS mi auction user-2422440 securatebontine 10 IN mis-auction user-2422440 securatebontine 10 IN mit autocom user-24224240 securatebontine 10 IN mit autocom user-2422440 securatebontine 10 IN user-24e2440 securatebontine 10 IN SOA	22 Edoladowices.com I 22 Edoladowices.form. A 3 122 191 227 I 227 191 227 I 227 191 227 I 227 191 227 I 227 191 201 201 201 201 201 201 201 201 201 20	



7.5.3 3. Delete Zone

In case you need to delete the zone, tick your zone, click **Delete** and then confirm your choice.

🕒 CL	OUD SERVICES					⑦ Help	Alex Snemyakin UPMIX LLC
0							
8 ⊈	SERVICE HEALTH REQU HEALTHY 143 2 Healthy / 0 Degraded All zon	ESTS nes, past 90 days					
*	ZONES						2 Create
6	Filter All 2 Itoms						🔟 Delete
	Zone Name ↑	Health	Primary IP	Division	Last Updated	Status	
	1 user-3s95yl.securelab.online	🗢 Healthy	54.211.12.173		Jan 31, 2020 / 10:47 UTC	 Active 	
	user-z4e2440.securelab.online	Itealthy	54.211.12.173		Feb 7, 2020 / 16:26 UTC	 Active 	
			PERMANENTLY DELE Delete trees 20ner?	ter These Zones?			

7.6 F5 DNS Cloud Service - API

In this section we will repeat the flow of the preceding section by using the F5 Cloud Services APIs with the help of Postman.

7.6.1 1. Create Zone

In order to create your zone using API, you will first need to get your account details - membership and catalogs.

a) Get User Membership to F5 Cloud Services accounts

In Postman, send the **Get User Membership** request which returns info on your user's access to Cloud Services accounts.

GET	Г	Ŧ	https://	ttps://{{HOSTNAME}}/{{API_VERSION}}/svc-account/users/{{USER_ID}}/memberships							
Para	ms	Author	ization	Headers (8)	Body	Pre-request Sc	ript Tests • Settings				
* +	leader	rs (1)									
	KEY						VALUE				
\checkmark	Autho	rization					Bearer {{ACCESS_TOKEN}}				
	Key						Value				

You will see account ids, names, roles and other information in the body of response.

Body Cookie	s Headers (6) Test Results (1/1)
Pretty	Raw Preview Visualize BETA JSON -
1 {	
2	"memberships": [
3	< contract of the second secon
4	"account_id": "i",
5	"user_id": " ",
6	"role_id": "
7	"user": {
8	"id": "",
9	"email": "
10	"first_name": "/ :",
11	"last_name": "",
12	"phone": "",
13	"create_time": "2019-07-22T14:54:39.998412Z",
14	"update_time": "2019-07-22T14:54:39.998412Z"
15	},
16	"account_name": "UPMIX LLC",
17	"role_name": "owner",
18	"level": "0",
19	"signup_provider": "standard",
20	"create_time": "2019-07-22T14:54:40.152317Z",
21	"update_time": "2019-07-22T14:54:40.152317Z"
22	},
23	Ę
24	"account_id": "",

Your "account_id" will be retrieved using "account_name" and used for creating user's instances.

More detailed information on this API request can be found here.

b) Retrieve information on available catalogs and their IDs

Select the Get Catalogs request and click Send to retrieve data about the available Catalogs and their IDs.

As you see there are a number of catalogs available:

The retrieved IDs are then stored for subsequent calls using a function inside Postman to set environment variables. You can see the test function in the **Tests** tab:

GET			Ψ.	https://	nttps://{{HOSTNAME}}/{{API_VERSION}}/svc-account/users/{{USER_ID}}/memberships								
Param	IS	Au	thor	ization	Headers (8)	Body	Pre-request Script	Tests 🖲	Settings				
1 - 2 3 - 4 - 5 6 7 <i>i</i> 8	pm.1	test var for }	("Sw jso (var if }	itch ac nData = i=0; i (jsonDa pm.env	count", functior pm.response.jsc (jsonData.member ta.memberships[ironment.set("A(n() { on(); ~ships.ler i].account CCOUNT_ID	ngth; i++) { name === "{{ACCOUN ', jsonData.membersh:	T_NAME}}") ips[i].acco	{ unt_id);				

GE	Г	*	https://	tps://{ <mark>{HOSTNAME}}/{{API_VERSION}</mark> }/svc-catalog/catalogs							
Para	Params Authorization Headers (8) Body Pre-request Script Tests • Settings										
*	leaders	(1)									
	KEY							VALUE			
~	Author	ization						Bearer {{ACCESS_TOKEN}}			
	Key							Value			

Temporary Headers (7)

Body Cod	okies Headers (6) Test Results (1/1)
Pretty	Raw Preview Visualize BETA JSON 🔻 🛱
/1	b
72	"create_time": "2019-07-22T21:21:49.494932Z",
73	"update_time": "2019-07-22T21:21:49.494932Z",
74	"delete_time": null,
75	"preview_end_time": null
76	},
77	< compared with the second sec
78	"catalog_id": "c-aaQnOrPjGu",
79	"name": "DNS Load Balancer",
80	"description": "Load balance your traffic across servers and regions.",
81	"status": "STATUS_ACTIVE",
82	"logo_url": "https://staging-ui.srv.f5aas.com/static/media/logo.6a1ab75a.svg",
83	"info_url": "https://www.f5.com/products/ways-to-deploy/cloud-services/dns-load-balancer-cloud-service
84	"service_type": "gslb",
85	"deleted": false,
86	"preview": false,
87	"providers": [
88	{
89	"name": "aws",
90	"preview": false,
91	"status": "STATUS_ACTIVE",
92	"info_url": "https://aws.amazon.com/marketplace/pp/B07W3P8HM4",

GET	Ψ.	https:/	/{{HOSTNAME}}/{{	API_VERSIO	N}}/svc-catalog/catalo	gs		
Params	Author	rization	Headers (8)	Body	Pre-request Script	Tests 🌒	Settings	
1 -	pm.test()	Set Cata	log variables",	function	() {			
3 -	for(va	ar i=0;	i <jsondata.cata< td=""><th>logs.leng</th><th>th; i++) {</th><th></th><th></th><th></th></jsondata.cata<>	logs.leng	th; i++) {			
4 -	i	f (jsonD	ata.Catalogs[i]. viconment_set("	Service_1	type === "waf") { DG TD" _isonData Ca	talogs[i] cat	talog id):	
6	}	pinten	vironnene.see(Jo_ro , jsonbaca.ca	calo82[1].ca	cuio <u>s_</u> iu/,	
7		(deenD						
9	11	pm.en	vironment.set("[ONS CATAL	DG ID", isonData.Ca	talogs[i].ca	talog id);	
10	}			-		0.1.1	0_ //	
11		- /						
12 -	11	F (jsonD	ata.Catalogs[1]	service_	type === "gslb") {			
14	3	pm.en	vironment.set((JSLD_CATA	.uo_iu , jsonData.c	araiogs[1].C	ataiog_1d);	
15	}							

More detailed information on this API request can be found here.

c) Select the **Create DNS Subscription** request and click **Send** to create a new service instance of Secondary Authoritative DNS using "account_id" and "catalog_id" retrieved a few steps above.

POST	Ŧ	https://	{{HOSTNAME}} / {{A	PI_VERSION}}/s	vc-subs	cription/sub	scriptions	
Param	s Author	rization	Headers (10)	Body 鱼	Pre-rec	quest Script	Tests 🌒	Settings
• no	ne 🔵 forr	m-data	x-www-form-u	rlencoded 🦲	raw	binary	GraphQ	L ^{BETA} JSON 🔻
1 -	ł.							
2	"account_	id": "{{/	ACCOUNT_ID}}",					
3	"catalog_	id": "{{	DNS_CATALOG_ID}}	",				
4	"service_	instance	_name": "{{ZONE_	NAME}}",				
5 🕶	"configur	ation":	{					
6 🕶	"adns_s	ervice":	{					
7	"zone	": "{{ZO	NE_NAME}}",					
8 -	"mast	er_serve	rs": [
9	"54	.211.12.	173"					
10]							
11	}							
12	},							
13	"service_	type": "	adns"					
14	}							

You will see "subscription id" and created "service instance id" in the body.

The retrieved "subscription_id" is then stored for subsequent calls.

You can change its status from "DISABLED" to "ACTIVE" sending the **Activate DNS Subscription** request below. More detailed information on this API request can be found here.

d) Select the **Activate DNS Subscription** request and click **Send**. This will deploy the secondary DNS using "subscription_id" captured in one of the steps above.

You will see "active" subscription status.

Note that it takes some time to deploy the service, so you can just re-send the same request after a few minutes to see "service_state": "DEPLOYED".

More detailed information on this API request can be found here.

Body Cookies Headers (6) Test Results (1/1)
Pretty Raw Preview Visualize BETA JSON -
<pre>1 2 "subscription_id": "", ", 3 "account_id": ", ", 4 "user_id": ", , 5 "catalog_id": "c-aaxBJkfg8u", 6 "service_instance_id": "user-z4e2440.securelab.online", 7 "status": "DISABLED", 8 "service_type": "adns", 1 "configuration": { 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1</pre>
POST
Params Authorization Headers (10) Body • Pre-request Script Tests • Settings
<pre>1 * pm.test("Set DNS subscription id variable", function() { 2 var jsonData = pm.response.json(); 3 pm.environment.set("DNS_SUBSCRIPTION_ID", jsonData.subscription_id); i 4 }) 5</pre>
POST
Params Authorization Headers (10) Body Pre-request Script Tests Settings
none form-data x-www-form-urlencoded raw binary GraphQL ^{BETA} JSON v
<pre>' "subscription_id": "{{DNS_SUBSCRIPTION_ID}}", 3 "omit_config": true 4 }</pre>

Body Cookies Headers (6) Test Results		S
Pretty Raw Preview Visualize	JSON 🔻 🚍	
<pre>1 { 2 "status": "ACTIVE", 3 "service_state": "DEPLOYING", 4 "subscription_id": " 5 }</pre>		
Body Cookies Headers (6) Test Results		
Pretty Raw Preview Visualize	JSON 🔻 🚍	
<pre>1 { 2 "status": "ACTIVE", 3 "service_state": "DEPLOYED", 4 "subscription_id": " 5 }</pre>	1 1	

7.6.2 2. Get Zone File

Send the **Get DNS Subscription Zones** request which uses DNS "subscription_id" created a few steps above. This will retrieve a zone file from your primary DNS server.

POS	ST https://{{HOSTNAME}}/{{API_VERSION}}/svc-subscription/subscriptions/{{DNS_SUBSCRIPTION_ID}}/test										
Parar	ams Authorization Headers (10) Body Pre-request Script Tests Settings										
▼ H	leaders (2)										
	KEY				VALUE						
~	Content-Type				application/json						
~	Authorization				Bearer {{ACCESS_TOKEN}}						
	Key				Value						

As a result, you will get the zone file describing your DNS zone and containing mappings between domain names and IP addresses.

7.6.3 3. Query via Browser

Let's now check the created DNS service via browser.

- a) Copy NA1 address from the Zone file retrieved in the step above:
- b) Paste the copied address into your browser and you will get to the created secondary DNS instance:

Body	Cooki	s Headers (6) Test Results Status: 200 OK Time:	186ms
Pret	ty	Raw Preview Visualize JSON 🔻 🚍	
1	ł		
2		"configuration": {	
3		<pre>"zone_field": "user-n1h0si.securelab.online.\t30\tIN\tSOA\tns1.user-n1h0si.securelab.online. info.use 2020021809 30 30 30 30\nuser-n1h0si.securelab.online.\t30\tIN\tNS\tns1.f5cloudservices.com.\nuser-n1h0si.securelab.on f5cloudservices.com.\nauction.user-n1h0si.securelab.online.\t30\tIN\tNS\tns91.dns.cloudservices. securelab.online.\t30\tIN\tA\t3.122.191.227\nna1-auction.user-n1h0si.securelab.online.\t30\tIN\t user-n1h0si.securelab.online.\t30\tIN\tCNAME\twaf-aaqr4igerk.waf.prd.f5aas.com.\nna3-auction.use \t30\tIN\tA\t52.226.147.184\nns1.user-n1h0si.securelab.online.\t30\tIN\tA\t54.211.12.173\nuser-n \t30\tIN\tSOA\tns1.user-n1h0si.securelab.online. info.user-n1h0si.securelab.online. 2020021809 3</pre>	er-n1h(hline.' F5.com A\t34.: r-n1h0: 1h0si.: 0 30 3(
4		}	
5	}		

Body Cool	ties Headers (6) Test Results		Status: 200 OK	Time: 186ms	
Pretty	Raw Preview Visualize JSON 🔻 🚍				
		na1		Aa Abl	
1 {					
2	"configuration": {				
3	<pre>"zone_field": "user-n1h0si.securelab.online.\t30\tIN\tSOA\tns1.user-n1h0si.securelab.online. info.user-n 2020021809 30 30 30\nuser-n1h0si.securelab.online.\t30\tIN\tNS\tns1.f5cloudservices.com.\nuser-n1h0si.securelab.onlin f5cloudservices.com.\nauction.user-n1h0si.securelab.online.\t30\tIN\tNS\tns1.f5cloudservices.com.\nuser-n1h0si.securelab.online f5cloudservices.com.\nauction.user-n1h0si.securelab.online.\t30\tIN\tNS\tns1.f5cloudservices.com.\nuser-n1h0si.securelab.online f5cloudservices.com.\nauction.user-n1h0si.securelab.online.\t30\tIN\tA\t3.122.191.227\na1-auction.user-n1h0si.securelab.online \t30\tIN\tA\t3.122.191.227\na1-auction.user-n1h0si.securelab.online \t30\tIN\tA\t52.216.177.184\nns1.user-n1h0si.securelab.online.\t30\tIN\tA\t54.211.12.173\nuser-n1h0si (t30\tIN\tS0A\tns1.user-n1h0si.securelab.online. info.user-n1h0si.securelab.online. 2020021809 30 30</pre>				



7.6.4 4. Review the JSON

Let's now see the structure of the JSON. In order to get the JSON, go back to Postman and send the **Get DNS JSON** request which uses your ACCESS_TOKEN to retrieve the JSON:

GET	Г	https://{{HOSTNAME}}/{{API_VERSION}}/svc-subscription/subscriptions/{{DNS_SUBSCRIPTION_ID}}						
Para	ms	Author	ization	Headers (9)	Body	Pre-request S	cript Tests Settings	
v	▼ Headers (2)							
	KEY						VALUE	
~	Conter	nt-Type					application/json	
~	Authorization					Bearer {{ACCESS_TOKEN}}		
	Key						Value	

The response will retrieve the JSON containing all the DNS instance information:

As you can see, the JSON provides some general information on subcription_id, user_id, and instance name, as well as all configuration details (service IP, zone name, etc).

7.6.5 5. Delete Zone

In order to delete your Zone using Postman, send the **Retire DNS Subscription** request which uses the relevant "subscription_id".

You will see "retired" status in the response body which means that it's not available on the F5 Cloud Services portal anymore.

More detailed information on these API requests can be found here.

7.7 F5 DNS Load Balancer Cloud Service - UI

In this section we will use the F5 Cloud Services UI to set up the Load Balancer DNS record, add endpoints for our Auction app, add health checks, load balanced pools, and run through a few configuration options.

7.7.1 1. Create F5 DNS Load Balancer Cloud Service

Let's now create DNS Load Balancer Service to be able to balance loads across multiple clouds (Azure & AWS) and provide global availability and performance with health-check and built-in DDoS protection.

a) Go to the DNS Load Balancer tab and click Create.

b) Enter name of the zone we created before and click Create.

Your DNS Load Balancer instance will appear on the list but in **Inactive** status. You can change the status after creating load balanced record and pool.



G	CLOUD SERVICES	⑦ Help	8
0	A DNS LOAD BALANCER		
÷	SERVICE HEALTH REQUESTS N/A O 0 Healthy / 0 Degraded All services, past 90 days CURRENT LOAD-BALANCING SERVICES		2 Create
8			
	To get started, configure services and get your traffic loads under control.		





7.7.2 2. Add Single Endpoint, Health Monitor, Pool and Default Geoproximity Rule

a) Create a Region

Creating regions will allow grouping incoming requests by geographic areas and directing them to specific pools.

1. Click on DNS Load Balancer instance which we have just created and go to the **Regions** tab. Click **Create**.

CLOUD SERVICES	⑦ Help	8
O DNS Load Balancer > user24e2440.securelab.online •		
Ref SERVICE HEALTH REQUESTS ACTIVE LBRS MONITORED POOL MEMBERS POOLS Image: This service 1 1 0 2 2 Image: This service All services, past 90 days Enabled - balancing traffic 0 Standard / 0 Advanced 2 Enabled / 0 Disabled		
使 Service overview JSON configuration		
COMPONENTS		
Load balanced records IP endpoints Pools Monitors Regions		
Regions		Create
HELLO! To get started, configure some regions.		
>> Copyright F5 Networks, Inc. All Rights Beserved. F5 Cloud Services Legal Physey Tademarks		

2. Fill "usa" as "Region name" and select "North America" in "Include these continents". **Save** the created region.

G	CLOUD SERVICES	(2) Help
0	DNS Load Blatancer > user:24e2440 securelab.online 👻	CREATE REGION ×
8	StRive REQUESTs ACTIVE LBRS MONITORED POOL MEMBERS POOLS HEALTHY 76 1 0 1 This service ALl services, past 90 days Enabled - balancing traffic 0 Standard (0 Advanced 1 Enabled / 0 Diabled	Region name USa
•	Service overviewJSON configuration	Add notes here
	сомронентя	A
	Load balanced records IP endpoints Pools Monitors Regions Regions Regions	Include these continents North America ×
		Include these countries Type to choose countries
		Include these states/provinces Type to choose states/provinces
l	HELLO! To get started, configure some regions.	Save and create another Cancel Save

Now all requests from North America will be covered by the "usa" region.

b) Add A Health Monitor

To distribute the load, DNS Load Balancer will need to monitor health of each IP Endpoint. So, let's create a monitor.

1. C	Go	to	the	Monitors	tab	and	then	click	Create
------	----	----	-----	----------	-----	-----	------	-------	--------

G	CLOUD SERVICES	(?) Help	8
	DNS Load Balancer > user-z42440.securelab.online SERVICE HEALTH HEALTHY This service JSON configuration Service overview JSON configuration ComPONENTS Load balanced records IP endpoints Pools Monitors Monitors		Create
	HELO! To get started, configure some monitors.		

2. Fill in "health-monitor" name, choose "HTTP Standard" protocol, indicate "80" port and click **Save**.

CLOUD SERVICES	() Help
C DNS Load Balancer > user z4e2440.securelab.online +	CREATE MONITOR ×
XR SERVICE HEALTH REQUESTS ACTIVE LERS MONITORED POOL MEMBERS POOLS HEALTHY 76 1<	Name this monitor health-monitor
Service overview JSON configuration	Add notes here
COMPONENTS	A
Load balanced records IP endpoints Pools Monitors Regions Monitors	HEALTH MONITORING OPTIONS Additional charges apply for advanced monitoring
	Choose protocol HTTP Standard
	What's the port? 80
HELLO: To get started, configure some monitors.	Save and create another
	Cdifter

c) Add an IP Endpoint (NA) with Health Check

Let's now create an IP endpoint that will currently service all incoming requests. DNS Load Balancer chooses an IP endpoint based on request origin and configuration of IP endpoints, as well as IP Endpoint health.

1. Go to the **IP endpoints** tab and then click **Create**.

CLOUD SERVICES	? Help	8			
DNS Load Balancer > user-nth0si.securelab.online					
SERVICE HEALTH REQUESTS ACTIVE LBRS MONITORED POOL MEMBERS		POOLS			
N/A O O O This service All services, past 90 days Enabled + balancing traffic 0 Standard / 0 Advanced		0 Enabled / 0 Disabled			
Service overviewISON configuration					
Jervice over view JSON Conniguration					
COMPONENTS					
Load balanced records IP endpoints Pools Monitors Regions					
IP Endpoints		Create			
HELLO! To get started, configure some IP endpoints.					
	CLUUD SERVICES DNS Load Balancer > user-nth05i.securelab.online SERVICE HEALTH N/A O All services, past 90 days ACTIVE LBRS O O Standard / 0 Advanced O Service overview JSON configuration COMPONENTS Load balanced records P endpoints Pools Monitors Regions P Endpoints IP Endpoints Load balanced records IP endpoints D cget started, configure some IP endpoints.	CLUD SERVICE Service > user-nth0si.securelab.online =			

2. Fill in name ("na1-auction"), IP address ("34.229.48.248"), port ("80") and select the monitor we created above.

G	CLOUD SERVICES				CREATE IP ENDPOINT ×
 C) ∞ ⊕ ⊕ ∅ ∅ 	DNS Load Balancer > user-n SERVICE HEALTH N/A This service Service overview JSC COMPONENTS Load balanced records	Ith0si.securelab.online REQUESTS O All services, past 90 days DN configuration IP endpoints Pools Monitors	MONIT O O Stanc	Name the IP endpoint na1-auction What's the IP address of your endpoint? 34.229.48.248 What's the port? 80 What's monitor would you like to use? health-monitor	
	IP Endpoints		HELLO! To get started, configure some IP er	ndpoints.	+ Create monitor Add notes here Save and create another Cancel Save

d) Create a Pool

Let's now create a pool and add a member to it.

- 1. Go to the **Pools** tab and then click **Create**.
- 2. Fill in "america" name, choose "round-robin" method and define TTL "30". Then click Next.
- 3. Click Add Member to add an IP Endpoint to the pool.
- 4. Select the endpoint we've just created, as well as the monitor. Click Add and Create.
- A newly created pool with the one NA endpoint will appear on the list.

e) Add a Load Balanced Record

¢	CLOUD SERVICES				⑦ Help
0	DNS Load Balancer > user-	n1h0si.securelab.online 🔻			
89	SERVICE HEALTH	REQUESTS	ACTIVE LBRS	MONITORED POOL MEMBERS	POOLS
	N/A	0	0	O	0 0 Factorial (0 Disabled
8	This service	All services, past 90 days	Enabled + balancing traffic	U Standard / U Advanced	0 Enabled / 0 Disabled
⊕					
·@-	Service overview JS	ON configuration			
a	COMPONENTS				
•	Load balanced record	IP endpoints Pools Monitors	Regions		
	Pools				Create
			æ		
			HELLO!		
			To get started, configure some	pools.	

G	CLOUD SERVICES		•	CREATE POOL ×
0	DNS Load Balancer > user-r	nh0si.securelab.online 🔻	•	Name this pool
28	SERVICE HEALTH	REQUESTS	ACTIVE LBRS	america
8	N/A This service	All services, past 90 days	Enabled + balancing traffic	What's the resource record type?
●	Service overview JS	ON configuration		A RR types of pools must match those of the LBRs they service.
·@·				Choose a load balancing method
6	Load balanced records	IP endpoints Pools Monitors	Regions	round-robin 👻
	Pools			Define TTL (Time to live)
				(seconds)
				Add notes here
			HELLO	Cancel
			io get started, comgt	

CLOUD SERVICES				CREATE POOL		
0	DNS Load Balancer > user-n	1h0si.securelab.online 🔻	Pool RR Ty			
୧୧		REQUESTS	ACTIVE LBRS	america	Α	
-	This service	All services, past 90 days	Enabled + balancing traffic	LOAD BALANCING SETTINGS		
9				Add at least one pool member to use a pool in an active service. For optimal load		
⊕				balancing, add at least two pool members.		
冻	Service overview JSC	ON configuration		Enabled		
6	COMPONENTS			0 MEMBERS	Add Member	
	Load balanced records	IP endpoints Pools Monitors				
	HELO To get started, configu			MEMBERS APPEAR HERE As you add them above Specify the maximum IP endpoints returned per response		
				1		
				Back	Save and create another Cancel Create	

G	CLOUD SERVICES	ADD MEMBER TO POOL
0	DNS Load Balancer > user-n1h0si.securelab.online -	Pool RR Type america A
Xx	SERVICE HEALTH REQUESTS ACTIVE LBRS	IP endpoint
8	This service All services, past 90 days Enabled + balancing traff	no1-auction (34.229.48.248)
♥	Service overview ISON configuration	+ Create IP endpoint
-@-	Soft Control Soft Control Soft Control	Monitor
a	COMPONENTS	health-monitor 🔹
0	Load balanced records IP endpoints Pools Monitors Regions	+ Create monitor
	Load balanced records in endpoints Pools Pionitors Regions	Save and create another
	Pools	Cancel Add
	HEL	
	To get started, conf	

× RR Type Α

After creating all the components (IP endpoint, Pool, Region and Monitor), we can create a DNS Load Balancer record and its proximity rule.

1. Go to the **Load balanced records** tab and then click **Create**.

G	CLOUD SERVICES				⑦ Help				
0	DNS Load Balancer > user-n1h0si.securelab.online ▼								
ደ	SERVICE HEALTH REQUESTS		ACTIVE LBRS	MONITORED POOL MEMBERS	POOLS				
8	This service All services, pas	90 days	Enabled + balancing traffic	0 Standard / 0 Advanced	1 Enabled / 0 Disabled				
<u>⊕</u> ```@`	Service overview JSON configuration								
6	COMPONENTS Load balanced records IP endpoints Poo	ls Monitors	Regions						
	Load Balanced Records				Create				
	HELLO! To get started, configure some LBRs.								

2. Fill in LBR name "auction", host "auction", select "A" as "Resource Record Type" and set a proximity rule ("Anywhere" -> "america" pool) to direct requests from anywhere to "america" pool with the created NA1 endpoint. Set score of the proximity rule to be "1". This will define the priority of the rule after some more are added.

Click Add Rule, then check *Enabled* tick and Save the record.

3. Go back to the DNS Load Balancer tab, click on your service and activate it.

The DNS Load Balancer service is now setup.

f) Test via Browser

Let's test the created service with the proximity rule via browser.

1. Open FQDN ("auction.{{zone name}}" where {{zone name}} is the value copied from postman in one of the step above) in your browser.

2. You will see that acc to the proximity rule, you joined the endpoint belonging to the "america" pool.

g) Test via Command Prompt

Another way to test the new proximity rule is via Command Prompt.

1. Start Command Prompt.

2. Paste the following command to the **Command Prompt**: **nslookup** "your FQDN name" and press **Enter**.

And you will see **34.229.48.248** IP in the response which belongs to **na1-auction** endpoint from **america** pool.

7.7.3 3. Add Multiple Ednpoints to Load Balanced Pool & Test

a) Add More Endpoints (NA2,3)
Constrained Records 2 unition * Record Status
A cardital conduct of a statution * conduct
Receive Stratus Image: Stratus Image: Stratus
 Center and a construction of the construction of the
PROXIMITY RULES Text Endeures requests across regions and pools For Al Endeures Requests to This Pool Interice Octeate region Outing this Score Interice Create pool Interice Create pool Interice Create pool Interice
If our to belance end-user requests across regions and pools For All End-user Requests Coming From Create region Create region Create Requests to This Pool Immerica Create pool Create Decouptions ODE BALANCED RECORD PROPERTIES Which host to load belance Immerica Immerica ODE SALANCED RECORD PROPERTIES Using this Score Immerica Immerica Immerica Immerica Immerica Immerica Create region Immerica Immerica </th
Porval Induced Records Allaged) Image: Induced Records Allaged) Indition of CIDR masks used to group client Pode Sections Allaged) Indition of CIDR masks used to group client Pode Sections Allaged) Indition of CIDR masks used to group client Pode Sections Allaged) Indition of CIDR masks used to group client Pode Sections Allaged) Indition of CIDR masks used to group client Pode Sections Allaged) Indition of CIDR masks used to group client Pode Sections Allaged) Indition of CIDR masks used to group client Pode Sections Allaged) Indition of CIDR masks used to group client Pod Sections Allaged) Indition of CIDR masks used to group client Indition of CIDR masks used to group client Indition of CIDR masks used to group client
Create region america Create region Create region Create region Create region Cusing this Score Create pool Comparison Create pool Create
Immetica Create pool Using this Score Chad Rule I Chad Rule CAD-BALANCED RECORD PROPERTIES Which host to load belance Immetica Resource Record Type I auction Notes Index State (Instance) Immetica Immutica Immutica Immutica Immutica Immutica Immutica Immutica Immutica </th
Create pool 1 Lobe Sector DECORD PROPERTIES Which host to load belance Using this Score Lobe Sector DECORD PROPERTIES Which host to load belance Leght of CIDR masks used to group client Hosts (Wildcards Alaged) Lots (Wildcards Alaged) L
1 Add Rule LOAD-BALANCED RECORD PROPERTIES Which host to load belance Image: Strate Strat
LAD-BALANCED RECORD PROPERTIES Which host to load belance Image: Image in the second second type in the second secon
LOAD-BALANCED RECORD PROPERTIES Which host to load balance Image: solution of the s
LBR name Resource Record Type auction A Hosts (Wildcards Allayed) Notes auction Pr4 Clients (0-128) auction 2 bit control Frequencies auction Frequencies auction Remember persistence records for (seconds) auction S6 auction S600
auction A 3 Cache responses so that clients receive persistent answers Hosts (Wildcards Aloved) Notes IP-4 Clients (0-32) IP-6 Clients (0-128) auction 2 + - 24 56 Remember persistence records for (seconds) 3600 3600 -
Hosts (Wildcards Alaged) Notes IPv4 Clients (0-32) IPv6 Clients (0-128) auction 24 56 Remember persistence records for (seconds) 3600
Remember persistence records for (seconds) 3600
3600
0
Delete Cancel Sav
SERVICE HEALTH REQUESTS
Image: N/A O 0 Healthy / 0 Degraded All services, past 90 days
Current Load-Balancing SERVICES
Image: Bar Strength and St
Service name Requests (90 days) Division Last Updated Health Status
user-nth0si.securelab.online 0 May 28, 2020 / 17:11 UTC ONA Inactive
× +
x +
 × + ← → C ③ Not secure auction.user-n1h0si.securelab.online
$\begin{array}{c c} \times & + \\ \leftarrow & \rightarrow & \mathbb{C} \\ \hline \end{array} \text{ (i) Not secure } auction.user-n1h0si.securelab.online } \end{array}$
 × + ← → C ③ Not secure auction.user-n1h0si.securelab.online



Let's now add a few more endpoints for load balancing of the application. Note that NA2 endpoint is deployed on Amazon AWS, whereas NA3 is running on Microsoft Azure.

1. Go back to the F5 Cloud Services portal, the **DNS Load Balancer** service, the **IP endpoints** tab and select **Create**.

2. Fill in name ("na2-auction"), IP address ("18.232.64.254"), port ("80") and select the monitor we created above.

Create one more endpoint repeating the step above using the following properties: "na3-auction" for name, "13.82.106.211" for IP address, "80" for port. You will have three endpoints as a result.

b) Add the Endpoints to the Pool

Let's now add the newly created endpoints to the existing pool.

- 1. Go to the **Pools** tab and click on the **america** pool.
- 2. Click Add Member and select the endpoint to be added.

Add one more endpoint and click Save. Now all three endpoints belong to one pool:

c) Test via Default Browser

Let's test the updated pool with the new endpoints via browser.

1. Open FQDN ("auction.{{zone name}}" where {{zone name}} is the value copied from postman in one of the step above) in your browser.

2. You will see that acc to the proximity rule and pool members, you will get to endpoints belonging to the **america** pool in a round-robin manner.

And let's now update the page:





3	DNS Load Balancer > user-n	nh0si.securelab.online 🔻				
я В	SERVICE HEALTH N/A This service	REQUESTS O All services, past 90 days	ACTIVE LBRS 1 Enabled + balancing traffic	MONITORED POOL POOL 0 1 0 Standard / 0 Advanced 1 Enable	s led / 0 Disabled	
⊕ ∛	Service overview JS0	ON configuration				
8	COMPONENTS Load balanced records	IP endpoints Pools Monitors	Regions			
	IP Endpoints				Crea	te
	후 Filter All	3 items			⑪ Delet	te
	IP endpoint nam	ne †	LTM VIP? ()	IP Address	Notes	
	na1-auction			34.229.48.248		
				N 100 P 100		
				100 C		
	Convright F5 Networks Inc. All P	inhis Reserved. ES Cloud Services Legal + Privacy + T	ademarks			

6	LOUD SERVICES					CREATE IP ENDPOINT
0	DNS Load Balancer > user-r	n1h0si.securelab.online 🔻				Name the IP endpoint
28		REQUESTS	ACTIVE LBRS	MONITORED POOL MEMBERS	POOLS	na2-auction
8	This service	All services, past 90 days	Enabled + balancing traffic	1 Standard / 0 Advanced	1 Enabled / 0 Dis	What's the IP address of your endpoint?
۰	Condex average (10					18.232.64.254
·@·	Service overview JS	UN configuration				What's the port?
6	COMPONENTS					80
	Load balanced records	IP endpoints Pools Monitors	Regions			What monitor would you like to use?
	IP Endpoints					+ Create monitor
	Filter All	1 items				Add notes here
	IP endpoint nan	ie †	LTM VIP?	IP Address		
	no1-auction			34.229.48.248		h
						Save and create another

0	DNS Load Balancer > use	-n1h0si.securelab.online 🔻				
% 8	SERVICE HEALTH N/A This service	REQUESTS O All services, past 90 days	ACTIVE LBRS 1 Enabled + balancing traffic	MONITORED POOL MEMBERS 0 0 Standard / 0 Advanced	POOLS 1 1 Enabled / 0 Disabled	
	Service overview J	SON configuration				
÷. اها	COMPONENTS					
	Load balanced record	ls IP endpoints Pools Monitor	s Regions			
	IP Endpoints					Create
	÷ Eilter All	3 items				Tul Delete
	- 11061740					iii Delete
	IP endpoint na	ime †	LTM VIP? ()	IP Addres	i	Notes
	IP endpoint na na1-auction	ime †	LTM VIP? 🕕	IP Addres 34.22948	248	Notes
	IP endpoint n nat-auction na2-auction	me †	LTM VIP? 🕜	IP Addres 34 229 44 18 232 64	s 248 254	Notes
	IP endpoint ni ne1-auction ne3-auction	me †	LTM VIP? ()	IP Addres 34 229 4 18 232 64 52 226 14	: 248 254 7184	Notes
	IP endpoint n nel-auction ne3-auction	me †	LTM VIP? ()	IP Addres 34 229 40 18 232 64 52 226 14 52 226 14	s 248 254 7/84	Notes
	Prezzon Prezzon Pendpoint n not-euction not-euction no3-euction	me †	LTM VIP? ()	IP Addres 34.229.41 18.232.64 52.226.14	: 248 254 7/184	Notes
	Precode P	me †	LTM VIP? ()	IP Addres 34.229.41 18.232.64 52.226.14	5 248 254 2184	Notes
	Preconstruction Perconstruction Perconstruction nat-auction na2-auction na3-auction	me î	LTM VIP? ()	IP Addres 34.229.41 18.232.64 52.226.14	1 248 254 7184	Notes

· ·	CLOUD SERVICES					⑦ Help	8
0	DNS Load Balancer > user-n1h0si.sec	curelab.online 🔻					
*	SERVICE HEALTH HEALTHY This service	REQUESTS 3 All services, past 90 days	ACTIVE LBRS 1 Enabled + balancing traffic	MONITORED POOL MEMBERS 1 1 Standard / 0 Advanced	POOLS 1 1Enabled / 0 Disabled		
<u>●</u> ∻	Service overview JSON confi	iguration					
6	COMPONENTS Load balanced records IP e	endpoints Pools Monitors	Regions				
	Pools						Create
	후 Filter All	1 items				Disable	Delete
	Pool name 1	Pool record type		Pool members Load balancing met	od	Status	
	america	A		1 round-robin		 Enabled 	

POOL STATUS				
At least one pool member is required to enable this pool for use in an	active service.			
Z Enabled				
LOAD BALANCING SETTINGS				
Add at least one pool member to use a pool in an active service. For o	optimal load balancing, add at least two pool members.			
What's the resource record type?	1 MEMBERS		Add Member	
A •	≠ Filter All	1 items	Delete	
RR types of pools must match those of the LBRs they service.				
Choose a load balancing method	IP endpoint T	Health monitor	Member status	
round-robin 👻	na1-auction	health-monitor	N/A	
1 DOD DODEDUES				
Pool name	Notes		TTL (Time to live)	
america			30 (seconds)	

0	DNS Load Balancer > user-nth0si.securelab.online			
<u>8</u> 8	Pools > america 🔻			
	POOL STATUS			
8	At least one pool member is required to enable this pool for use in an active service.			
۲	Enabled			
·@·	LOAD BALANCING SETTINGS			
8	Add at least one pool member to use a pool in an active service. For optimal load bal	lancing, add at least two pool members.		
	What's the resource record type?	3 MEMBERS	Add Member	
	A •		10 Delete	
	RR types of pools must match those of the LBRs they service.	B enchoint t Health monitor	Member status	
	Choose a load balancing method			
	round-robin 👻	nat-auction nealth-monitor	NA	
	Specify the maximum IP endpoints returned per	na2-auction health-monitor	NA	
	response	na3-auction basic option	NA	
	1			
	Pool name america	Notes	TL (Time to live) 30 (seconds)	
	Delete			Cancel Save
		× +		
	← → C ③ Not secur	re auction.user-n1h0si.secu	relab.online	





7.7.4 4. Add Europe Region & EU Endpoint with Corresponding Geoproximity Record

a) Add EU Endpoint

Let's now add a EU endpoint which is deployed on Amazon AWS.

1. Go back to the F5 Cloud Services portal, the **DNS Load Balancer** service, the **IP endpoints** tab and select **Create**.

5	DNS Load Balancer > user-n	1h0si.securelab.online 🔻				
× ∃	SERVICE HEALTH N/A This service	REQUESTS O All services, past 90 days	ACTIVE LBRS 1 Enabled - balancing traffic	MONITORED POOL MEMBERS POOLS 0 1 0 Stenderd / 0 Advanced 1 Enabled / 0 C	isabled	
₽ \$`	Service overview JSC	DN configuration				
8	COMPONENTS Load balanced records	IP endpoints Pools Monitors	Regions			
	IP Endpoints					Create
	Filter All	3 items				🔟 Delete
	IP endpoint nam	e↑	LTM VIP? ()	IP Address	Notes	
	nal-auction			34.229.48.248		
				1.11.1		
»	Copyright F5 Networks, Inc. All R	ights Reserved. F5 Cloud Services Legal Privacy	Trademarks			

2. Fill in name ("eu-auction"), IP address ("3.122.191.227"), port ("80") and select the monitor we've created above.

The new endpoint will appear on the list.

🚯 CLO	UD SERVICES					CREATE IP ENDPOINT
0	DNS Load Balancer > user-n1h0si	.securelab.online 🔻				Name the IP endpoint
22		REQUESTS	ACTIVE LBRS	MONITORED POOL MEMBERS	POOLS	eu-auction
8	This service	All services, past 90 days	Enabled + balancing traffic	3 Standard / 0 Advanced	1 Enabled / 0 Dis	What's the IP address of your endpoint?
						3.122.191.227
*	Service overview JSON of	onfiguration				What's the port?
a	COMPONENTS					80
	Load balanced records	Pendpoints Pools Monitors	Regions			What monitor would you like to use?
	ID Facilitate					health-monitor 👻
		2 30.000				+ Create monitor
	IP endpoint name 1	S NOR	LTM VIP? ()	IP Address		Add notes here
	na1-auction			34.229.48.248		
	na2-auction			18.232.64.254		
	na3-auction			13.82.106.211		Save and create another Cancel Save

b) Add EU Region

Creating EU region will allow grouping requests coming from the European region and directing them to a specific pool.

1. Go to the **Regions** tab and click **Create**.

0	DNS Load Balancer > user-n1h0si.sect	urelab.online 🔻					
**	SERVICE HEALTH N/A This service	REQUESTS O All services, past 90 days	ACTIVE LBRS 1 Enabled + balancing traffic	O Standard / 0 Advanced	ERS POOLS 1 1 Enabled / 0 1	Disabled	
● *	Service overview JSON config	guration					
8	COMPONENTS Load balanced records IP er	ndpoints Pools Monitors Re	gions				
	Regions	_					Create
	Filter All	1 items					🔟 Delete
	□ Region / group name ↑	Includes	s continents Include	es countries In	cludes states/provinces	Mentioned in rules	Mentioned in LBRs
	usa		1	0	0	0	0

2. Fill "europe" as "Region name" and select "Europe" in "Include these continents". Save the created region.

Now you have two regions created.

c) Add EU Pool

Let's now create a pool and add a member to it.

- 1. Go to the **Pools** tab and then click **Create**.
- 2. Fill in "europe" name, choose "round-robin" method and define TTL "30". Then click Next.
- 3. Click Add Member to add an IP Endpoint to the pool.

() c	OUD SERVICES					(2) Help	8
0	DNS Load Balancer 👌 user-n1h0si.sec	urelab.online 🔻				CREATE REGION	×
~	SERVICE HEALTH HEALTHY This service	REQUESTS 9 All services, past 90 days	ACTIVE LBRS 1 Enabled + balancing traffic	MONITORED POOL MEMBERS 3 3 Standard / 0 Advanced	POOLS 1 1 Enabled / 0 Dis	Region name europe	
_ ● ☆	Service overview JSON confi	guration				Add notes here	
6	COMPONENTS Load balanced records IP er	ndpoints Pools Monitors	Regions			Include these continents	
	Regions					Europe ×	•
	Filter All	1 items				Include these countries Type to choose countries	•
	usa	Inci	udes continents include:	o	0	Include these states/provinces	
						Type to choose states/provinces	•
							Save and create another Cancel

Б	CLOUD SERVI	ICES					⑦ Help	8
0	DNS Loa	ad Balancer > user-n1h0si.sec	urelab.online 🔻					
29			REQUESTS	ACTIVE LBRS	MONITORED POOL MEMBERS	POOLS		
8	This serv	vice	All services, past 90 days	Enabled + balancing traffic	3 Standard / 0 Advanced	1 Enabled / 0 Disabled		
<u>_</u>	l Comin	150N6						
•	Service	-e overview	guration					
6	СОМ	IPONENTS						
	Load	d balanced records IP er	ndpoints Pools Monitors	Regions				
	Pools	5						Create
								5 H
	臣	Filter All	1 items				🗌 Disable D	Enable 🔟 Delete
	幸	E Filter All Pool name ↑	Pool record type		Pool members Load balancin	g method	Disable Disable	Enable 🔟 Delete
	#	Filter All Pool name america	1 items Pool record type A		Pool members Load balancin 3 round-robin	g method	Disable Disable Status Enabled	Enable U Delete
	± □	Filter All Pool name america	1 items Pool record type A		Pool members Load balancin 3 round-robin	g method	Disable Status Enabled	Enable U Delete
	÷	Filter All Pool name america	Pool record type		Pool members Load balancin 3 round-robin	g method	Disable Disable Status Enabled	Enable Delete
	÷	Filter All Pool name america	Pool record type A		Pool members Load balancin 3 round-robin	g method	Disable	Enable Delete
	±	Filter All Pool name name name america	Pool record type A		Pool members Load balancin 3 round-robin	g method	Disable	Enalote U Derete

G	CLOUD SERVIC	ES					(?) Help	8
0	DNS Load	d Balancer > user-n1h0si.sed	curelab.online 🔻			•	CREATE POOL	2
<u>8</u> 8			REQUESTS 9 All services past 90 days	ACTIVE LBRS 1 Enabled a balancing traffic	MONITORED POOL MER 3 3 Standard / 0 Advanced	MBERS	Name this pool	
₩ ●	Service	overview ISON conf	inuration				What's the resource record type?	
*	СОМР	PONENTS	iguration				A RR types of pools must match those of the LBRs they service.	•
	Load I Pools	balanced records IP e	endpoints Pools Monitors	Regions			round-robin	•
	ŧ	Filter All	1 items				Define TTL (Time to live) 30	
		america	A A		Pool members	round-robin	Add notes here	J
								h
								Cancel

LOUD SERVICES		CREATE POOL	
DNS Load Balancer > user-nth0si.se SERVICE HEALTH HEALTHY	REQUESTS ACTIVE 179 1	RS MONITORED POOL MEN 3 LOAD BALANCING SETTINGS	RR Type A
Service overview JSON cor	All services, past 90 days Enocied	Add at least one pool members to use a pool in an activ balancing, add at least two pool members.	e service. For optimal load
COMPONENTS		0 MEMBERS	Add Member
Pools ## Filter All Pool name ↑	1 items Pool record type	Pool members Load b	LEDE
america	A	3 round As you add them ab	ove
		Specify the maximum IP endpoints returned per respon	ise
			Save and create another
		Back	Cancel Create

4. Select the endpoint we've just created, as well as the monitor. Click Add and Create.

NS Load Balancer 🤌 user-mth0si.securelab.online 👻
RVICE HEALTH REQUESTS ACTIVE LBRS MONITORED POOL N
IEALTHY 187 1 3
is service All services, past 90 days Enabled + balancing traffic 3 Standard / 0 Advanc
ervice overview JSON configuration
COMPONENTS
Load balanced records IP endpoints Pools Monitors Regions
Pools
후 Filter All 1 Items
Pool name † Pool record type Pool members Load

A newly created pool with one EU endpoint will appear on the list.

d) Update LB Record Europe -> "europe"

Now that we have created EU pool, region and endpoint, we can update load balanced record and add a new proximity rule: to send the traffic originating in Europe to the "europe" pool, utilizing a higher relative score than the previous rule of routing traffic from "Anywhere" to the "america" pool. This type of geoproximity based routing is useful for GDPR compliance.

Go to the **Load balanced records** tab and click on your record. Set a new proximity rule ("europe" -> "europe" pool). Set the score of the proximity rule to be "50".

For All End-user Requests Coming From		1 proximity rules				
europe	•	Filter All	1 items		🔟 Delete	
	+ Create region	Score ↑	Region		Pool	
Route Requests to This Pool		□ 1	Anywhere		america	
europe	•					
	+ Create pool					
Using this Score						
50	Add Rule					
DAD-BALANCED RECORD PROPERTIES						
DAD-BALANCED RECORD PROPERTIES hich host to load balance						
DAD-BALANCED RECORD PROPERTIES hich host to load balance		Resource Record Type				
DAD-BALANCED RECORD PROPERTIES hich host to load balance		Resource Record Type		•	Cache responses so that clients receiv	ve persistent answers
DAD-BALANCED RECORD PROPERTIES hich host to load balance LBR name user-n1h0si.securelab.online		Resource Record Type		•	Cache responses so that clients received of CIDR masks used to group client Cond Client (2.22)	ve persistent answers nt
DAD-BALANCED RECORD PROPERTIES hich host to load balance LBR name user-n1h0ki.securelab.online Hosts (Mickards Allowed)		Resource Record Type		•	Cache responses so that clients receil Length of CIDR masks used to group clien (Pv4 Clients (0-32)	ve persistent answers nt IPv6 Clients (0-128)
DAD-BALANCED RECORD PROPERTIES hich host to load balance LBR name user-n1h0si.securelab.online Hosts (Wildcards Allowed) auction	+ -	Resource Record Type A Notes		•	Cache responses so that clients recei Length of CIDR masks used to group clien IP-4 Clients (0-32) 24	te persistent answers te IPr6 Cilents (0-128) 56
DAD-BALANCED RECORD PROPERTIES hich host to load balance LBR name User-n1h0sl.securelab.online Hosts (Wildcards Allowed) auction	* -	Resource Record Type		•	Cache responses so that clients receiv Length of CIDR masks used to group clien IPv4 Clients (0-32) 24 Remember persistence records for (secon	ve persistent answers nt IP+6 Clients (0-128) 56
DAD-BALANCED RECORD PROPERTIES hich host to load balance LBR name User-nthOsi.securelab.online Hosts (Wildcards Allowed) auction	+ -	Resource Record Type A Notes		•	Cache responses so that clients receit Length of CIDR masks used to group clien (P+4 Clients (0-32) 24 Remember pensistence records for (secon 3600	ve persistent answers nt IPv6 Clients (0-128) 5.6 dds)
DAD-BALANCED RECORD PROPERTIES hich host to load balance LBR name user-n1h0si.securelab.online Hosts (Wildcards Allowed) auction	+ -	Resource Record Type A Notes		•	Cache responses so that clients receil Length of CIDR masks used to group clien IP-4 Clients (0-32) 24 Remember persistence records for (secon 3600	ve persistent answers Nt IP-V6 Clients (0-128) 56
DAD-BALANCED RECORD PROPERTIES hich host to load balance LBR name user-n1h0sl.securelab.online Hosts (Wildcards Allowed) auction	* -	Resource Record Type A Notes		•	Cache responses so that clients receil Length of CIDR masks used to group clien IP-4 Clients (0-32) 24 Remember pensistence records for (secon 3600	ve persistent answers nt IPv6 Clients (0-128) 56

Click **Add Rule** and **Save** the record. The new proximity rule will direct requests from Europe region to **europe** pool.

e) Test using the Opera Browser

Now let's test the new proximity rule. This can be done either via the Opera browser or via your computer's **Command Prompt** (see the next section).

1. Open the Opera browser, copy FQDN name ("auction."your zone name"") in **Load balanced record properties** and paste into your browser. You will get to one of three available IP endpoints of the "america" pool.

2. Let's now test the EU proximity rule. Click **VPN** and select **Europe**. This will simulate your entering BuyTime Website from Europe.

3. Update your "auction." zone name"" page to see that acc to the proximity rule, you switched to the European pool.

f) Test via Command Prompt

Another way to test the new proximity rule is via Command Prompt.

1. Start Command Prompt.

2. Paste the following command to the **Command Prompt**: "nslookup auction.cloudservicesdemo.net 198.6.100.25".

And you will see **34.229.48.248** IP in the response which belongs to **na1-auction** endpoint from **america** pool.

3. Now let's check the **europe** pool. Paste the following command to the **Command Prompt**: **nslookup auction.cloudservicesdemo.net 158.43.240.3**.

And you will see **3.122.191.227** IP in the response which belongs to **eu-auction** endpoint from **europe** pool.

7.7.5 5. Duplicate Load Balanced Record using JSON through the UI

Let's now duplicate a load balanced record and its configuration in the existing Load-balancing service via the F5 Cloud Services portal. To do that, follow the step below:

a) Get JSON

Go to the **DNS Load Balancer** tab in the portal and click on your existing Load-balancing service. Open the **JSON configuration** tab and copy it.











()	CLOUD SERVICES	() Help
0	DNIS Lood Balancer > usternthOsisecurelab.online 👻	
*	SERVICE HEALTH REQUESTS ACTIVE LERS MONITORED POOL MEMBERS POOLS HEALTHY 22 2 0 3 This service All services, past 90 days Enabled - balancing traffic 0 Standard / 0 Advanced 3 Enabled / 0 Disabled	
● *	Service overview JSON configuration.	
6	JSON CONFIGURATION	
	<pre> Toom? 'user-thesis-securelab.olle*, ''ore 'i'''''''''''''''''''''''''''''''''''</pre>	

b) Create New Load Balanced Service

Let's now create a new Load-balancing service via UI to copy the record to. To do that, you will first need to get "zone2".

1. Go back to Postman and open **Get DNS Zone(lab)** request. Copy "zone2" which is returned in its response.

Body	Cooki	kies Headers (6) Test Results (1/1) Stat	us: 200 OK
Prett	Y	Raw Preview Visualize JSON 🔻 🚍	
1 2 3 4 5	{ }	"status": "ok", "zone": "user-nlh0si_securelab_online" "zone2": "user-nlh0si-2.securelab.online"	

2. Open any text editor (say, **Notepad**) and paste the **JSON configuration**. Replace the existing zone name with the "zone2" copied from the Postman in the step above:

A new JSON configuration with the properties copied from the existing zone is ready.

3. Return to the F5 Cloud Services portal and open the DNS Load Balancer tab. Click Create.

Paste "zone2" name which you copied in step 1 above and click Create.

c) Update JSON

?ou have just created a new Load-balancing service. Let's configure it by duplicating the Load balanced record from the existing service.

Click on your newly created service and open the **JSON configuration** tab. Paste the JSON which you created in step b) 2. above and click **Save**.



🚯 CL	OUD SERVI	CES						⑦ Help
C) &	۶	UPMIX LLC DNS LOAD BALANC	ER					
8	SERVIC HEA 3 Health	E HEALTH LTHY y / 0 Degraded	REQUESTS 147 All services, past 90 days					
*	CURRE	NT LOAD-BALANCING	SERVICES					Create
U	幸	Filter All	4 items					Directivate Suspend Delete
		Service name ↑		Requests (90 days)	Division	Last Updated	Health	Status
						Second Sec. 5		
						States and States		1 M M
						Second Second	1.00	8 MIN
						Second Second	1.00	1 (COL)





Go back to the newly created Load-balancing service to see the newly created record which is the copy of the original one.

d) Go back to the DNS Load Balancer tab and activate the new DNS Load Balancer service by selecting **Activate** button:

G	CLOUD SERV	ICES						? Help	Alex She	myakin C
ے ۶۹	۶	UPMIX LLC DNS LOAD BALANCEF	1							
∰ \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	SERVIC N/A 0 Health CURRE	E HEALTH hy / 0 Degraded ENT LOAD-BALANCING S	REQUESTS O All services, past 90	0 days						Create
۵	臣	Filter All	1 selected of 2 items					Activate	Suspend	🔟 Delete
		Service name ↑		Requests (90 days)	Division	Last Updated	Health	Stat	us	
		user-n1h0si-2.securelab.on	line	0		May 28, 2020 / 18:14 UTC	Ø N/A		nactive	
		user-n1h0si.securelab.onlin	e	0		May 28, 2020 / 18:09 UTC	Ø N/A	•	nactive	

Status will be updated a few seconds later.

e) Test via Browser

1. Open FQDN ("auction.{{zone-2 name}}" where {{zone-2 name}} is the value copied from postman in one of the step above) in your browser.



2. You will see that acc to the proximity rule and pool members, you will get to endpoints belonging to the **closest** pool in a round-robin manner.

7.7.6 6. Delete DNS Load Balancer Service

1. Go back to the F5 Cloud Services portal, the **DNS Load Balancer** tab, and click on your load-balancing service.

2. Tick the records and click **Delete**, then confirm your choice.

7.8 F5 DNS Load Balancer Cloud Service - API

7.8.1 1. Create DNS Load Balancer Subscription

Select the **Create GSLB Subscription** request and click **Send** to create a new service instance of DNS Load Balancer using "account_id" and "catalog_id" retrieved a few steps above.



()	LOUD SERVI	CES						⑦ Help	8	-
	SERVICE HEAI 2 Health	JPMIX LLC DNS LOAD BALANCEF E HEALTH LTHY y / 0 Degraded	REQUESTS 325 All services, past 9	90 days						
* * 6	CURRE 幸,	NT LOAD-BALANCING S	2 selected of 2 items					Activate	Suspend	Create
	~	Service name ↑		Requests (90 days)	Division	Last Updated	Health	Sta	tus	
		Service name ↑ user-n1h0si-2.securelab.on	ine	Requests (90 days)	Division	Last Updated May 29, 2020 / 24:15 UTC	Health	Sta	tus Active	
		Service name ↑ user-n1h0si-2.securelab.on user-n1h0si.securelab.onlin	ine e	Requests (90 days) 0 325	Division	Last Updated May 29, 2020 / 24:15 UTC May 28, 2020 / 23:48 UTC	Health C Healthy C Healthy	Sta •	Active Active	
		Service name 1 user-n1h0si-2 securelabion user-n1h0st.securelabionlin	e	Requests (90 days) 0 325	Division	Last Updated May 29, 2020 / 24:15 UTC May 28, 2020 / 23:48 UTC	Health Image: Healthy Healthy Healthy	Sta	Active Active	

All services, pas	t 90 days				
ANCING SERVICES					
2 selected of 2 items	1				Activate Su
r	Reque	Delete these services?		Health	Status
ecurelab.online		Cancel Yes, delete these services) / 24:15 UTC	🎔 Healthy	 Active
urelab.online			,) / 23:48 UTC	🗢 Healthy	Active

POST	Ŧ	https://{{HOSTNAME}}/{{API_VERSION}}/svc-subscription/subscriptions	
Params	Author	prization Headers (10) Body • Pre-request Script Tests • Settings	
none	form	rm-data 🖲 x-www-form-urlencoded 🖲 raw 🔵 binary 🔵 GraphQL BETA JSON 🔻	
1 • { 2 * * 3 * 5 • * 6 • 7 * 10 • 11 12 13 14 15 16 • 17 • 18 19 20	account_ catalog_ service_ configur "gslb_s "zone "lob "lb " "] " " " " " " " " " " "	<pre>_id": "{{ACCOUNT_ID}}",</pre>	

You will see "subscription_id" and created "service_instance_id" in the body. You may also note that this request will create only NA1 endpoint for now. Some more will be created in the subsequent requests.

You may also notice that the current proximity rule is set to send traffic from: Everyone -> Americas pool. This means that only one endpoint (NA1) will be serving all requests now. We will subsequently configure proper load balancing and geoproximity rules.

The retrieved "subscription_id" is then stored for subsequent calls.

You can change its status from "DISABLED" to "ACTIVE" sending the **Activate GSLB Subscription** request below.

More detailed information on this API request can be found here.

7.8.2 2. Activate DNS Load Balancer Subscription

Select the **Activate GSLB Subscription** request and click **Send**. This will deploy DNS Load Balancer using "subscription_id" captured in one of the steps above.

You will see "active" subscription status.

More detailed information on this API request can be found here.

7.8.3 3. Test NA Pool

Send the **Test NA Availability (lab)** request to execute a call against the Lab service API, which in turn uses an external VM (located in the USA) to run a "wget" to retrieve the response from http://auction. cloudservicesdemo.net. This should show the only available instance NA1 in the HTML that is returned.

The response shows that your first instance is available:

Pretty	Raw Preview Visualize BETA JSON 🔻 🛱
1	£
2	"subscription_id": "s-aa2ZnQhKOh",
3	"account_id": "a-aaIQLhugvE",
4	"user_id": "u-aaLHtsH4PJ",
5	"catalog_id": "c-aaQnOrPjGu",
6	"service_instance_id": "gslb-aa79ePk7ri",
7	"status": "DISABLED",
8	"service_instance_name": "user-z4e2440.securelab.online",
9	"deleted": false,
10	"service_type": "gslb",
11	"configuration": {
12	mgslp_service: {
10	Toad_paranced_records:: {
15	IDFS_dUCION: {
15	allases: [
17	
18	"display name": "auction user-742/440 securelah online".
19	"enable": true
20	"persistence": false.
21	"proximity rules": [
22	
23	"pool": "pools usa",
24	"region": "regions usa",
25	"score": 1
26	
27	
28	"rr_type": "A"
29	

POST	Ŧ	https://	ttps://{{HOSTNAME}}/{{API_VERSION}}/svc-subscription/subscriptions									
Params	Author	ization	Headers (10)	Body 🖲	Pre-request Script	Tests 🌒	Settings					
1 • 2 3 1 4 5	om.test("Se var jso pm.envi })	et GSLB s onData = ronment.	subscription id v pm.response.jsor .set("GSLB_SUBSCR	variable", f ((); MIPTION_ID",	Function() {	ion_id);						

POST	Ŧ	https:/	nttps://{{HOSTNAME}}/{{API_VERSION}}/svc-subscription/subscriptions/{{GSLB_SUBSCRIPTION_ID}}/activate									
Params	Author	rization	Headers (10)	Body 鱼	Pre-re	equest Script	Tests	Settings				
none	form	m-data	x-www-form-ur	lencoded	🖲 raw	binary	GraphQl	BETA JSON	*			
1 - {												
2 "sr 3 "or 4 }	ubscript mit_conf	ion_id": ig": tru	: "{{GSLB_SUBSCRI	PTION_ID}}	",							

Body Co	ookies	; Hea	ders (6)	Test Results					
Pretty	R	aw	Preview	Visualize BETA	JSON	Ŧ	₽		
1	{	"statu	IS" . "ACTT\	/F"					
3	3 "service_state": "DEPLOYING", 4 "subscription_id": "								
5	}								





7.8.4 4. Add Endpoints & Pool Members

Send the **Add Endpoint & Pool Members** request to add a few more endpoints for load balancing of the application. Note that three of the new endpoints (EU and NA2) are deployed on Amazon AWS, and one (NA3) is running on Microsoft Azure. NA1, NA2, and NA3 endpoints are aggregated into a pool "usa", which demonstrates multi-cloud load balancing.

PUT	*	https://{{HOSTNAME}}/{{API_VERSION}}/svc-subscription/subscriptions/{{GSLB_SUBSCRIPTION_ID}}								
Params	Author	rization Headers (10) Body • Pre-request Script Tests Settings								
none	form	m-data 🜑 x-www-form-urlencoded 💿 raw 🌑 binary 🜑 GraphQL BETA JSON 🔻								
1 - {										
2	"subscrip	ption_id": "{{GSLB_SUBSCRIPTION_ID}}",								
3	"account	_id": "{{ACCOUNT_ID}}",								
4	"catalog	_id": "{{GSLB_CATALOG_ID}}",								
5	"service	_instance_name": "{{ZONE_NAME}}",								
6 -	"configur	ration": {								
7 -	"gslb_s	service": {								
8	"zone	e": "{{ZONE_NAME}}",								
9 -	"load	d_balanced_records": {								
10 -	"11	brs_auction": {								
11 -	"aliases": [
12	"auction"									
13	1,									
14	"display_name": "auction.{{ZONE_NAME}}",									
15	"enable": true,									
16		"persistence": false,								
17 -	"proximity rules": [

You will see all the information on the added endpoints:

7.8.5 5. Test Round Robin (lab)

Run the **Test Round Robin (lab)** request to check the response from the Lab service API to test what instance is now being returned. This should show a result different from the previous due to the newly-configured round-robin load balancing.

NOTE: it's possible that you will still get the same endpoint in the response due to either DNS caching or 1/3 chance of the same endpoint to be pulled from the load-balance pool. Let's try:

And check the response:

You can send the same request to check other instances.

7.8.6 6. Update Proximity Rule

Run the **Update Proximity Rules & Regions**. This adds a new region "europe", and assigns a EU endpoint to it. It also updates the DNS Load Balancer with new proximity rules: to send the traffic originating in Europe to the "europe" pool, utilizing a higher relative score than the previous rule of routing traffic from "Anywhere" to the "usa" pool. This type of geo-proximity based routing is useful for GDPR compliance.

And you will see all the information on available pools and regions:

7.8.7 7. Test Proximity Rules (lab)

Send the **Test Proximity Rules (lab)** request, which uses an external VM (located in Europe) to run a "wget" to retrieve the response from http://auction.cloudservicesdemo.net. This simulates what an EU-

Pretty	Raw	Preview	Visualize BETA	JSON	*	₽	
24 25 26 27 28 29 30 31		} }, "pools":	"score": }], "rr_type": "A"	: giobal 1	.,		
32		"noo	ls europe": {				
33			"display name":	"europe".			
34			"enable": true,				
35			"load_balancing_	mode": "r	round	robin	",
36			"max_answers": 1	,			
37			"members": [
38			{				
39			"final":	null,			
40			"monitor	": "basid	c",		
41			"virtual	_server":	: "ipB	Indpoi	nt_eu_auction
42			}				
43			ь				
44			"remark": "",				
45			"rr_type": "A",				
46			"ttl": 30				
47		},					
48		"poo	ls_usa": {				
49			"display_name":	"usa",			
50			"enable": true,				
51			"load_balancing_	mode": "r	round	robin	",
52			"max_answers": 1	,			
53			"members": [
5/			5				





PUT	Ψ.	https:/	//{{HOSTNAME	}}/{{API_VERSIO	N}}/svc-su	bscription/sul	oscriptions/ <mark>{{G</mark>	SLB_SUBSCRIPT	TION_ID}}		
Params	Author	ization	Headers ('	0) Body	Pre-	request Script	Tests	Settings			
none	none 🔵 form-data 🌑 x-www-form-urlencoded 💿 raw 🜑 binary 🜑 GraphQL ^{BETA} JSON 🔻										
1 - {											
2	"subscri	ption_i	d": "{{GSLB_9	UBSCRIPTION_I	[D}}",						
3	"account	_1d": "	{{ACCOUNT_ID	()", NG TD11"							
5	"service	instan	((USED_CATAL)	70NE NAME33".							
6 -	"configu	ration"	: {								
7 -	"gslb	service	": {								
8	"zon	e": "{{}	ZONE_NAME}}"								
9 🕶	"loa	d_balan	ced_records"	{							
10 -	"1	brs_auct	tion": {								
11 -		"aliase	s": [
12		"auct:	ion"								
13],									
14		"display_name": "auction.{{ZONE_NAME}}",									
15	"enable": true,										
16	"persistence": false,										
10		proxim:	ity_rules":								
10											
19		"pool": "pools_usa",									
20		re	gion : regi	ms usa ,							



based customer would see when opening this URL in their browser. NOTE: you can also test this in your Opera browser (using EU proxy), the way you've done it previously with the UI.

POST		http://	:p://{{DNS_WEB_ADMIN}}/proxy/europe									
Params	Author	ization	Headers (10)	Body Pre	e-request Script	Tests	Settings					
none	form	n-data	• x-www-form-ur	lencoded 🛛 🖲 rav	w 🌒 binary	GraphQl	IL BETA JSON V					
1 • { 2 3 }	"domain"	: "auct	ion.{{ZONE_NAME}}	8								

Here's what you should see in the response:

7.8.8 8. Review the JSON

Let's now see the structure of the JSON. In order to get the JSON, send the **Get GSLB JSON** request which uses your ACCESS_TOKEN to retrieve the JSON:

The response will retrieve the JSON containing all the DNS Load Balancer instance information:

As you can see, the JSON provides some general information on subcription_id, user_id, and instance name, as well as all configuration details. The configuration section "details" includes information on "pools_health":



GET		https://{{HOSTNAME}}/{{API_VERSION}}/svc-subscription/subscriptions/{{GSLB_SUBSCRIPTION_ID}}									
Para	Params Authorization Headers (9) Body Pre-request Script Tests Settings										
▼	▼ Headers (2)										
	KEY VALUE										
\checkmark	Content-Type				application/json						
~	Authorization				Bearer {{ACCESS_TOKEN}}						
	Key Value										
▶ 1	Temporary Headers (7)										

Pretty	Raw Preview Visualize JSON 🔻 🚍										
1	a contraction of the second seco										
2	"subscription_id": "s-aa6JL5ezUP",										
3	"account_id": "a-aaIQLhugvE",										
4	"user_id": "u-aaLHtsH4PJ",										
5	"catalog_id": "c-aaQnOrPjGu",										
6	"service_instance_id": "gslb-aaiI_uof5Q",										
7	"status": "ACTIVE",										
8	"service_instance_name": "user-n1h0si.securelab.online",										
9	"deleted": false,										
10	"service_type": "gslb",										
11	"configuration": {										
12	"details": {										
13	"lbr_metadata": {										
14	"active_lbr_count": 1,										
15	"active_pool_member_advanced_monitor_count": 0,										
16	"active_pool_member_standard_monitor_count": 0										
17											
18	"pools_nealth": {										
19	"pools_australia": {										
20	"members_nealth": [
21											
22	uetalls: [],										
25	"mealing", "pape"										
24	"virtual server": "inEndpoint au auction"										
26	3										
27											
28											
29	"pools europe": {										
30	"members health": [
31											
32	"details": [],										
33	"health": "GREEN",										
34	"monitor": "none",										
35	"virtual_server": "ipEndpoint_eu_auction"										
36											
37											
38	5 F										
39	"pools_usa": {										



The next configuration section is "gslb_service" which contains "load_balanced_records" with their "name" and "proximity_rules":

It also includes "pools" section with their "name", "load_balancing_mode" and "members":

One more section is "regions" which includes information on region "names" and "sectors":

And another section provides information on "virtual_servers": their IP endpoints, addresses, names, monitors and ports:

7.8.9 9. Delete DNS Load Balancer Service

Send the Retire GSLB Subscription request which uses the relevant "subscription_id".

You will see "retired" status in the response body which means that it's not available on the F5 Cloud Services portal anymore.

7.9 Clean Up

Send the Retire DNS Zone to remove or reset zone file. You will get response with status code "200 OK".

We recommend that you clear your tokens from the Lab Service API for security purposes. In order to do that, send the **Logout** request, which uses your **ACCESS_TOKEN**:

You will get the following response with the status showing "200 OK":

Your ACCESS_TOKEN will be considered invalid:









▶ Retire DNS Zon	ie (lab)	Comments 0 Ex
POST 🔻	http://{{DNS_WEB_ADMIN}}/zone/retire	Send 🔻
Body Cookies H	Headers (6) Test Results	Status: 200 OK Time: Size: 226 B Save
1 { 2 "s 3 }	status": "ok"	

POST	Ŧ	https:/	tps://{{HOSTNAME}}/{{API_VERSION}}/svc-auth/logout									
Params	Author	ization	Headers (9)	Body 🔵	Pre-rec	quest Script	Tests 🔵	Settings				
none	form	n-data	• x-www-form-u	urlencoded	🖲 raw	binary	GraphQL	JSON 🔻				
1 • { 2 · · 3 }	"access_	token":	"{{ACCESS_TOKEN	}}"								
4												

(Iooki	ies He	aders (6)	Test Results (1 /	(1)		Status: 200 OK 1
etty	/	Raw	Preview	Visualize	JSON 🔻	₽	
ı	{}						

POST	Ŧ	https://{{HOSTNAME}}/{{API_VERSION}}/svc-auth/logout								
Params	Author	rization	Headers (9)	Body 鱼	Pre-request Script	Tests 🌒	Settings			
1 - pm. 2 i 3 }) 4	.test("Re pm.envi	eset toke ironment.	en variable", fu .set("ACCESS_TOK	unction() { (EN", "");						
Credits

• Agility 2020:

Bill Wester Brandon Burns Dave Doucette

Pat Fiorino

Matt Harmon

Bret Pleines

Nick Stathakis

Brian Van Lieu

Greg Robinson

Fred Wittenberg









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.