An Oracle White Paper
December, 2012

Enterprise Manager 12c Cloud Control: Configuring OMS Disaster Recovery with F5 BIG-IP Global Traffic Manager

Contents

Executive Overview

Oracle Enterprise Manager is Oracle's integrated enterprise IT management product line and provides the industry's first complete cloud lifecycle management solution. Oracle Enterprise Manager's Business-Driven IT Management capabilities allow you to quickly set up, manage and support enterprise clouds and traditional Oracle IT environments from applications to disk. Enterprise Manager allows customers to achieve:

- *Best service levels for traditional and cloud applications* through management from a business perspective including Oracle Fusion Applications

- *Maximum return on IT management* investment through the best solutions for intelligent management of the Oracle stack and engineered systems

- *Unmatched customer support experience* through real-time integration of Oracle's knowledgebase with each customer environment

Oracle Maximum Availability Architecture (MAA) is the Oracle best practices blueprint for implementing Oracle high-availability technologies. Oracle Enterprise Manager is the management platform for Oracle solutions.

This white paper has been jointly written by Oracle Corporation and F5 Networks and provides the detailed steps for configuring an F5 BIG-IP Global Traffic Manager (GTM) as the front end for Primary and Standby site Oracle Enterprise Manager Cloud Control deployments as part of an Oracle MAA Disaster Recovery (DR) solution

The paper is designed to provide the Cloud Control Administrator with an introduction to the disaster recovery features available with F5 solutions. Step-by-step configuration instructions and screen shots are provided to make it easier to understand and implement BIG-IP as a critical component of the Cloud Control architecture. In general, assume that the following software versions are used in this white paper:

- BIG-IP Version 11.1.0, Build 2268.0 Hotfix HF5

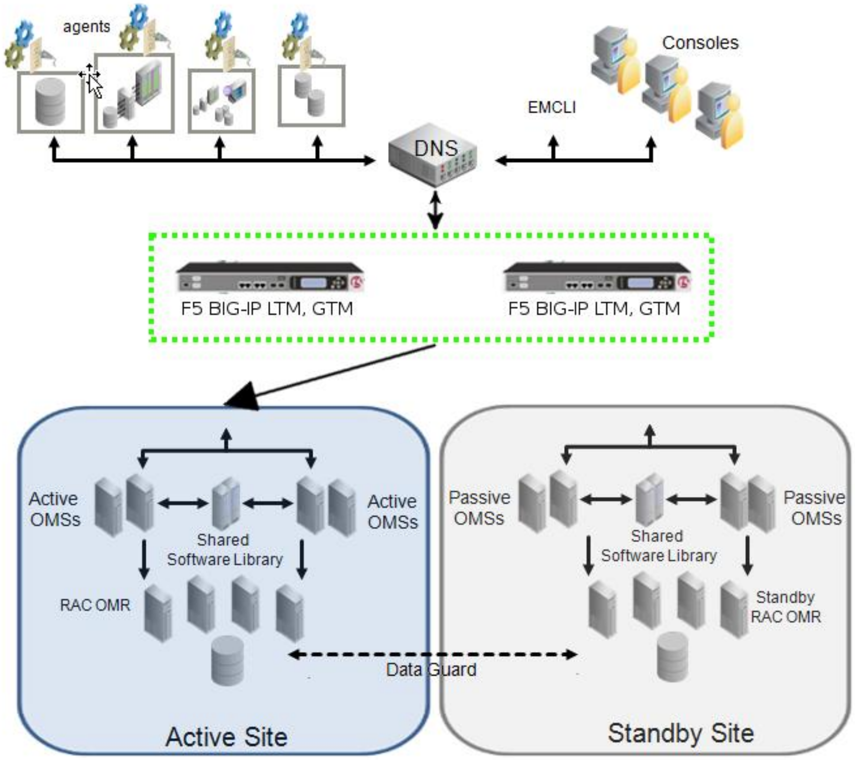
- Cloud Control Release 12.1.0.1.0, 12.1.0.2.0

Any distinction in release numbers is noted within the relevant discussions of this paper.

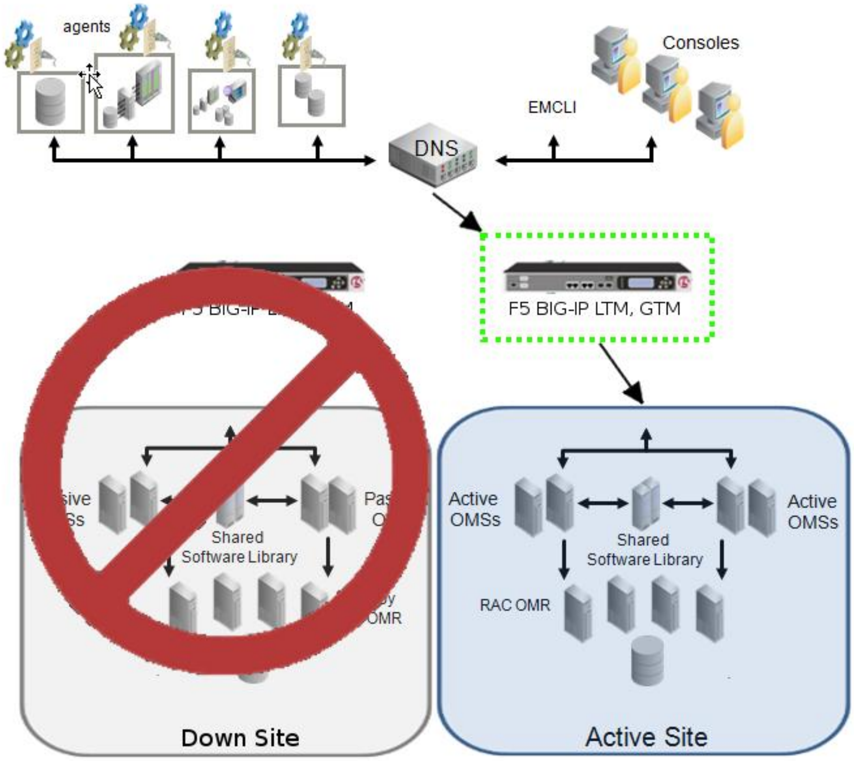
Note: This white paper assumes that you have followed the steps in the paper . Enterprise Manager 12c Cloud Control: Configuring OMS High Availability with F5 BIG-IP Local Traffic Manager to configure BIG-IP Local Traffic Managers (LTMs) for Local Traffic Management on both Primary and Standby sites and understand the concepts of Oracle Enterprise Manager Cloud Control High Availability Levels as described in the Oracle® Enterprise Manager Cloud Control Administrator's Guide.

Disaster Recovery for Oracle Enterprise Manager Cloud Control using F5 GTM

The diagram below shows a Level 4 deployment of Oracle Enterprise Manager Cloud Control with both an Active and Standby site each served by their own BIG-IP LTM and GTM configuration. Disaster recovery is instrumented by GTM directing all OMS client traffic (from agents, consoles and emcli) to the currently Active site.



When failover or switchover is required, the GTM seamlessly directs traffic to the newly Active site.



Configuring a Pool of F5 GTMs for Oracle Enterprise Manager Cloud Control Disaster Recovery.

The steps detailed below describe a basic configuration that meets the requirements of providing DR for an Oracle Enterprise Manager Cloud Control deployment. In our simple example we have a single BigIP on each site, running both LTM and GTM services. In such a simple deployment, when one site goes down the remaining GTM is effectively a single point of failure. To avoid this, multiple GTMs can be configured on each site or GTMs can be configured on other sites that are not necessarily hosting an Enterprise Manager deployment, providing redundancy. See F5 Documentation: Setting Up a Global Traffic Manager Redundant System Configuration for details of how to configure GTM redundancy.

For our example, we move from a configuration where em.example.com is the virtual hostname, fronting the active site only, to em.example.com fronting both an active and standby site. The Active site is in New York and uses the DNS alias em.example.com to point to the IP address 150.10.10.10, which is an IP address allocated to the LTM virtual server that load balances EM traffic for the Active site. The Standby site is in Los Angeles and has the IP address 200.10.10.10 allocated to its LTM virtual server. Without GTM, failover or switchover would rely on the manual process of updating DNS to point em.example.com to the Los Angeles IP address, 200.10.10.10. With GTM, em.example.com resolves automatically to the site that is currently active without any need for manual intervention.

GTM accomplishes this task automatically, by being aware of the current state of the GTMs, the LTMs and the Virtual Servers hosted by the LTMs. Any change in state, such as a failure or manual switchover, is instantly communicated between the GTMs. DNS resolution is then instantly changed to send agents and admins to the Active site. For more information on the details of how GTMs works, start with the F5 GTM Datasheet.

Overview of steps

Prerequisites.

- All GTM units MUST be running the same version of BIG-IP software, including any patches or hotfixes, prior to configuration. For software upgrade procedures, please consult the F5 documentation.
- All GTM units MUST have access to an NTP time server. As the status of network and services can change second by second, it is a requirement that all GTMs have access to an NTP server in order to establish a common singular time reference. If the GTM system clock varies between systems by more than 10 seconds, the synchronization processes will be unstable and unpredictable.
- All Firewalls between GTMs and LTMs MUST be configured to allow TCP ports 22 and 4353 to pass bi-directionally through the firewall. TCP port 22 is used to exchange configuration data securely, and port 4353 is used by the F5 iQuery protocol to exchanges state, status, and synchronization data between GTMs and LTMs.
- Root level access to the GTM SSH or serial console is required for initial configuration.

See AskF5 Knowledge Base article SOL13734: BIG-IP GTM synchronization group requirements for more details of prerequisites.

Configure DNS to add GTM as an authoritative child domain

The fundamental principle of this configuration is that the F5 BIG-IP GTM will be responsible for directing network requests for the virtual hostname that fronts the Oracle

Enterprise Manager Cloud Control services. For this to be possible, the corporate DNS infrastructure needs to be configured to pass any requests for that virtual hostname to the GTM. In our example, we are deploying GTMs as authoritative name servers for a DNS sub-domain.

If the virtual hostname used for the Oracle Enterprise Manager Cloud Control services is em.example.com then a sub domain, for example, gtm.example.com would be created that would result in a virtual hostname of em.gtm.example.com being able to be resolved by each of the GTMs. NOTE: Both GTMs are active for resolving requests, even if one of the sites is in Standby, thereby providing an additional layer of redundancy at the GTM and DNS level.

Once all configuration is completed, the corporate DNS would be updated to replace the A record for em.example.com with a CNAME that points em.example.com to em.gtm.example.com (see Configure DNS to forward requests for the EM hostname to the GTM)

In our example, before configuring DNS to hand off requests to the GTM, DNS would have one A record relevant to the Oracle Enterprise Manager Deployment:

em.example.com.	IN	A	150.10.10.10

The record points to the IP address that is assigned to the BIG-IP LTM virtual servers for the primary site.

After configuring DNS to hand-off requests for the gtm.example.com domain, DNS would have the following extra records relevant to the Oracle Enterprise Manager Deployment:

gtm.example.com.	IN	NS	bigip1-ny.example.com.
gtm.example.com.	IN	NS	bigip1-la.example.com.
bigip1-ny.example.com.	IN	A	150.10.10.53
bigip1-la.example.com.	IN	A	200.10.10.54

The NS records tell DNS to forward requests for the domain gtm.example.com to bigip1-ny.example.com and bigip1-la.example.com, the GTM servers in the two sites, New York and Los Angeles, respectively. In other words, a request to resolve the hostname em.gtm.example.com is passed to one of the GTMs bigip1-ny.example.com or bigip1-la.example.com. At this stage, such a request would not return an IP address since we need to configure the GTMs themselves.

The A records tell DNS the IP address that the GTM servers are listening on.

Configure DNS to use a CNAME record to associate the Virtual hostname used by EM with the Virtual IP served by the F5 BIG-IP LTM

We want the Virtual hostname used by Enterprise Manager to be portable, breaking the link between the Virtual hostname and the IP address served by the Primary site's LTM.

One way of achieving this without creating an outage on the currently live system is to modify the A record for the IP address so that it has a name that is relative to the BIG-IP it is associated with. For example, if the BIG-IP that serves the Virtual Server with the IP address 150.10.10.10 is bigip1-ny.example.com, a good A record would be bigip1-ny_vip1.example.com. As part of the same update, a CNAME can then be used to associate the application/service specific hostname, e.g. em.example.com, with the new alias, maintaining the link between the EM virtual hostname and the IP address that is currently active for the Enterprise Manager services. The following DNS records would implement this step in our example:

bigip1-ny-vip1.example.com.	IN	A	150.10.10.10.
bigip1-la-vip1.example.com.	IN	A	200.10.10.10.
em.example.com.	IN	CNAME	bigip1-ny.vip1.example.com.

Configure a Listener on each BIG-IP GTM

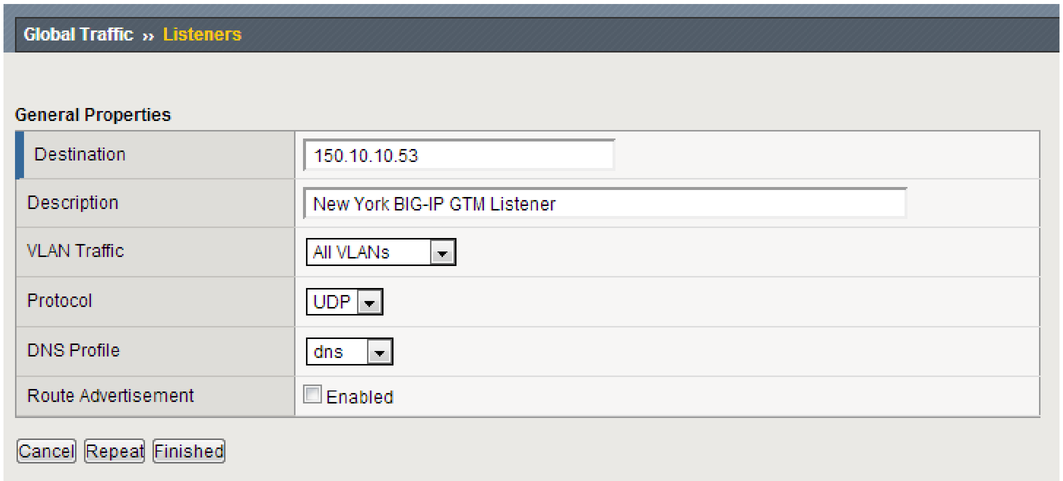
A GTM Listener is a specialized resource that is assigned a specific IP address and listens on port 53, the DNS query port. When traffic is sent to that IP address, the listener alerts the Global Traffic Manager, allowing it to handle the traffic locally or forward the traffic to the appropriate resource, based on the virtual server status and load balancing configuration of the WideIP.

Before syncing a GTM with any other GTMs it is necessary to first configure a Listener for the GTM, because this listener configuration is not synchronized with the GTM configuration.

Repeat the following steps for all GTMs that will be part of the DR setup. In our example we would perform these steps for both the New York and Los Angeles GTMs.

1. On the Main tab of the navigation pane, expand **Global Traffic** and click **Listeners**. The main screen for Listeners opens.

2. Click the **Create** button. The New Listener page appears.
3. In the **Destination** box, type the IP address on which the Global Traffic Manager listens for network traffic. When employing only a single GTM per site, the IP address that you add is the self IP address of the BIG-IP system running the GTM service. In the case of a redundant system configuration, the shared floating IP address that corresponds to both GTM systems should be provided.
4. From the **VLAN Traffic** list, select All VLANS.
5. The default values for all other settings are appropriate. For additional assistance with these settings, see the online help.
6. Click the **Finished** button to save the new listener.



General Properties

Destination	150.10.10.53
Description	New York BIG-IP GTM Listener
VLAN Traffic	All VLANs
Protocol	UDP
DNS Profile	dns
Route Advertisement	□ Enabled

For more information on Listeners, see F5 Documention: Working with Listeners.

Configure Data Centers, a BIG-IP Monitor and Servers on the 'configuration master' GTM

There are F5 GTM components that need to be configured and synchronized between all GTMs. We first configure those GTM components on one GTM, which we will call the 'configuration master', and then create a sync group that includes all of the GTMs. When the other GTMs are added to the sync group they sync with the 'configuration master' and receive all of the GTM components that were configured on that GTM.

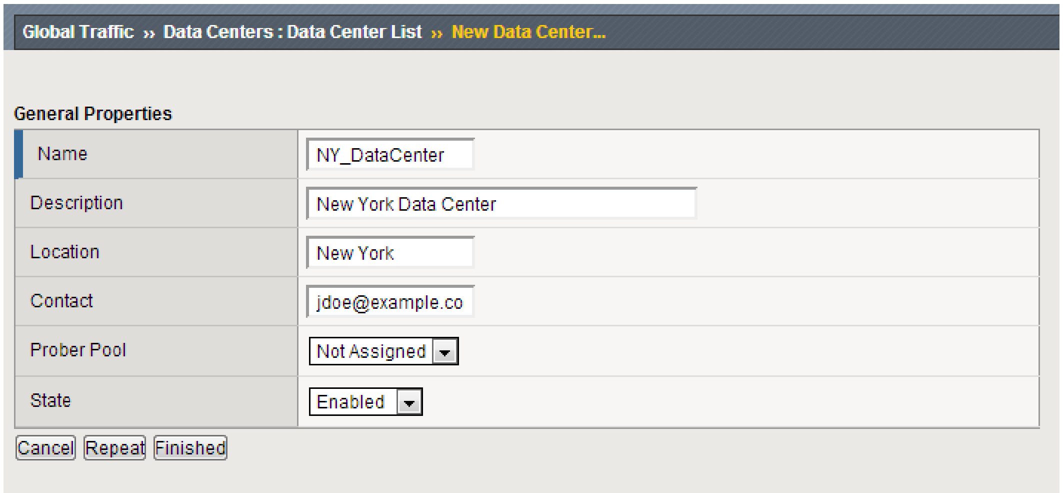
Configure a GTM Data Center

A Data Center is a logical container or collection of the servers and network elements that share common infrastructure on the network. All resources on your network, whether physical or logical, are associated in some way with a Data Center. The GTM consolidates the paths and metrics data collected from servers, virtual servers and links into the Data Center, and uses that data to conduct load balancing operations.

When you create a Data Center on the GTM, you must add at least one Server before it can be used. You must, however, configure at least one Data Center before you can add Servers to the GTM system configuration. Additionally, each Server can belong to one, and only one, Data Center.

Perform the following steps once for each site. In our example we would create Data Centers for New York and Los Angeles

1. On the Main tab of the navigation pane, expand **Global Traffic** and click **Data Centers**. The Data Center List page opens.
2. Click the **Create** button. The New Data Center page appears.
3. Fill in the **Name**, **Description**, **Location**, and **Contact** boxes.
4. The default values for all other settings are appropriate. For additional assistance with these settings, see the online help.
5. Click the **Finished** button.


Global Traffic » Data Centers : Data Center List » New Data Center...
Cancel
Repeat
Finished

General Properties

Name	NY_DataCenter
Description	New York Data Center
Location	New York
Contact	jdoe@example.co
Prober Pool	Not Assigned
State	Enabled

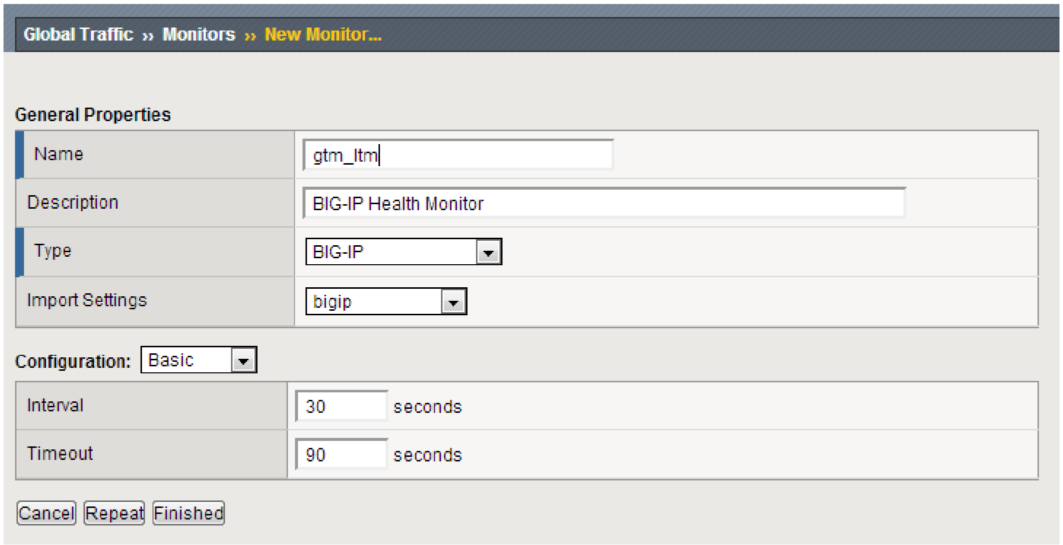
For more information, see F5 Documentation: Managing data centers.

Configure a GTM Monitor

Monitors verify connections on pools and virtual servers and are designed to check the status of a pool or virtual server on an ongoing basis, at a set interval. If a pool or virtual server being checked does not respond within a specified timeout period, or the status of a pool or virtual server indicates that performance is degraded, then the GTM can redirect the traffic to another resource. In our example, we create a BIG-IP monitor to ensure that the BIG-IP LTM virtual servers, which contain the server pools, are available.

1. On the Main tab of the navigation pane, expand **Global Traffic** and then click **Monitors**. The Monitors List page opens.
2. Click the **Create** button. The New Monitor page appears.
3. In the **Name** box, type a name for the monitor. In our example, we give the name gtm_ltm
4. From the **Type** list, select BIG-IP.
5. The default values for all other settings are appropriate. For additional assistance with these settings, see the online help.
6. Click the **Finished** button.

The new monitor is added to the list.



Global Traffic » Monitors » New Monitor...

General Properties

Name	gtm_ltm
Description	BIG-IP Health Monitor
Type	BIG-IP
Import Settings	bigip

Configuration: Basic

Interval	30 seconds
Timeout	90 seconds

For more information, see F5 Documentation: Configuring Monitors.

Configure a GTM Server

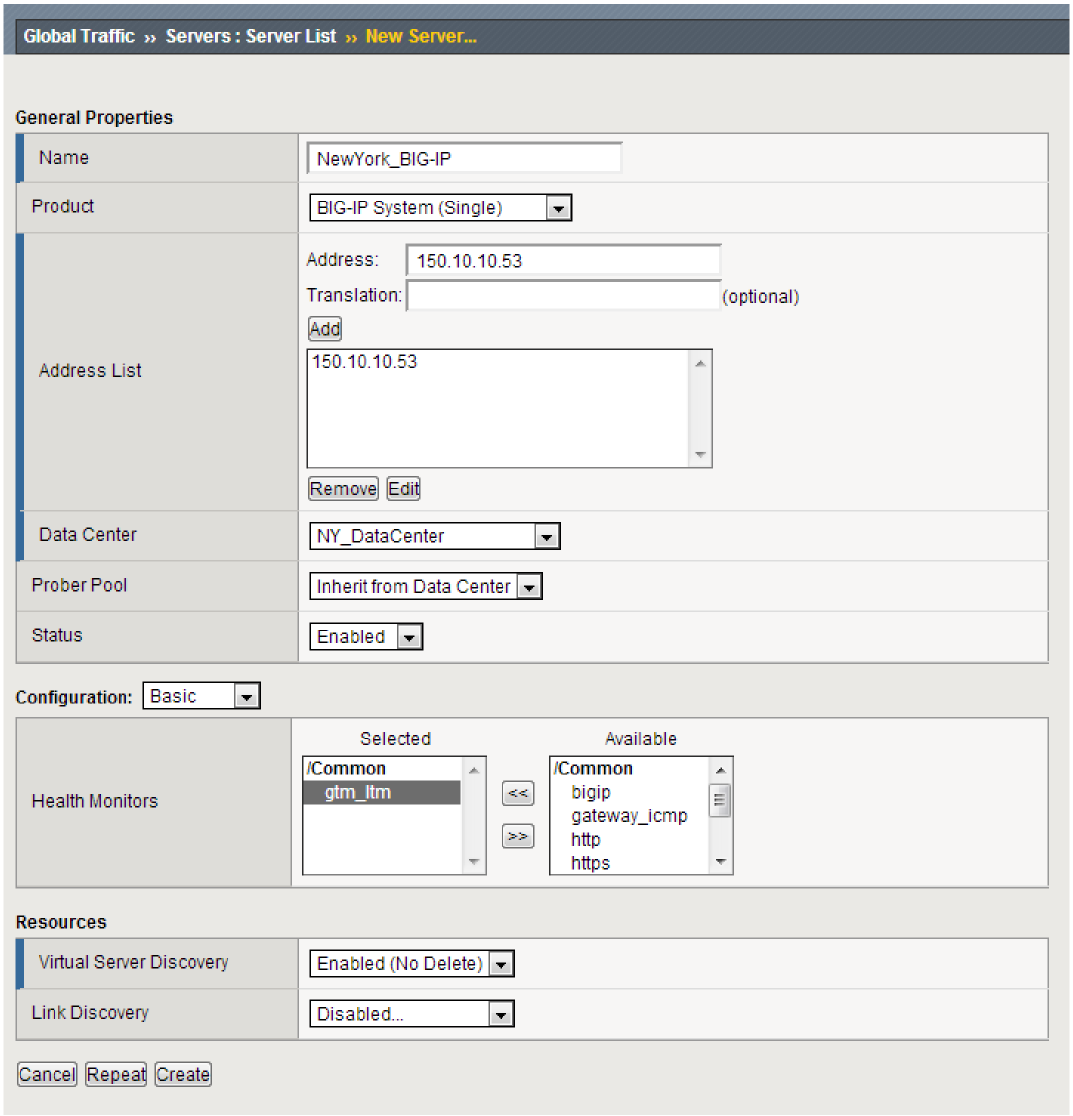
A server defines a specific system on the network. In this deployment, the Servers map to the BIG-IP LTM systems that serve the Enterprise Manager Virtual Servers. In or simple example deployment, both the GTM and LTM services are provided by the same BIG-IP so we create one Server for each LTM that basically points back to itself. In more advanced deployments the GTM could serve a number of LTMs running on a number of separate BIG-IP systems. In the latter case, a Server would be created for each LTM that provided the EM Virtual Servers in the GTM's Data Center.

Perform the following steps once for each LTM. In our example, since the GTMs and LTMs are running on the same BIG-IPs we would create one Server for the New York BIG-IP LTM and one server for the Los Angeles BIG-IP LTM

1. On the Main tab of the navigation pane, expand **Global Traffic** and click **Servers**, (located under Data Centers). The Servers List page opens.
2. Click the **Create** button. The New Server page appears.
3. In the **Name** box, type a name that identifies the BIG-IP. In our example, we type **NewYork_BIG-IP**.
4. From the Product list, select either **BIG-IP System (Single)** or **BIG-IP System (Redundant)** depending on your configuration. In our example, we select **BIG-IP System (Single)**.
5. From the Address List section, in the **Address** box, type the self IP address of the BIG-IP device, and then click the **Add** button. In our example, we provide the self IP address of the New York BIG-IP **150.10.10.53.**
6. If you selected BIG-IP System (Redundant) in Step 4, from the Peer Address List section, in the **Address** box, type the self IP address of the redundant BIG-IP LTM device, and then click the **Add** button.

Note: *Do not use a floating IP address of the redundant pair. Do not use the out of band administrative interface of either member of a redundant pair.*

7. From the **Data Center** list, select the name of the data center you created in the *Configure a GTM Data Center* step. In our example, we select **NY_DataCenter**.
8. In the Health Monitors section, from the Available list, select the name of the monitor you created in the *Configure a GTM monitor* section, and click the Add (**<<**) button. In our example, we select **gtm_ltm**.
9. In the Resources section, from the Virtual Server Discovery list, choose an option. We recommend **Enabled (No Delete)**. With this option, the GTM will discover all the virtual servers you have configured on the LTM(s) via iQuery, and will update the list, but not delete them.
10. Click the **Create** button.



Global Traffic » Servers : Server List » New Server...

General Properties

Name	NewYork_BIG-IP
Product	BIG-IP System (Single)
Address List	Address: 150.10.10.53 Translation: (optional) Add 150.10.10.53 Remove Edit
Data Center	NY_DataCenter
Prober Pool	Inherit from Data Center
Status	Enabled

Configuration: Basic

	Selected	Available
Health Monitors	/Common gtm_ltm	/Common bigip gateway_icmp http https

Resources

Virtual Server Discovery	Enabled (No Delete)
Link Discovery	Disabled...

For more information, see F5 Documentation: Managing Servers.

Configure a GTM Sync group containing the GTMs for each site

The next step is to add the GTMs to a Sync group. This results in all GTMs obtaining the components configured on the 'configuration master' GTM.

The process is broken down into four steps:

1. Ensure all BIG-IP GTMs that will be added to the sync group have accurate date and time settings that are within 10 seconds of each other

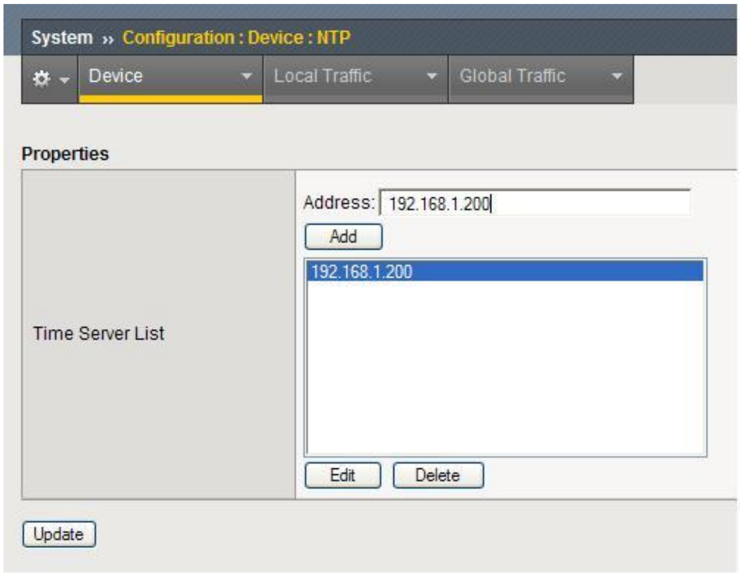
2. Ensure the device SSL certificates for all BIG-IP GTMs are valid. The device SSL certificate is used to encrypt iQuery traffic between the GTMs and LTMs.
3. Use the gtm_add utility to exchange device certificates between BIG-IP GTMS and import the GTM configuration from the 'configuration master' GTM to each of the other GTMs
4. Initialize each GTM's Global Traffic Manager synchronization settings.

On each BIG-IP GTM server, ensure the date and time are within 10 seconds of each other BIG-IP GTM server that will be part of the sync group.

Configure NTP

IMPORTANT NOTE: All BIG-IP GTM systems must have access to an NTP server in order to maintain proper time clock and configuration synchronization.

1. On the Main tab of the navigation pane, expand **System** and click **Configuration > Device > NTP**
2. In the **Address** Box, enter the IP address of the NTP server.
3. Click the **Add** button.
4. Click the **Update** button.



Address: 192.168.1.200

192.168.1.200

For more information on setting the clock on BIG-IP systems, see F5 Support page: SOL3381: Setting the time and date on the BIG-IP system.

For more information on NTP, see F5 Support Page: SOL3122: Configuring the BIG-IP system to use an NTP server.

To verify the BIG-IP systems are properly using the NTP service, see F5 Support Page: SOL10240: Verifying Network Time Protocol peer server communications.

Ensure the TZ is correctly specified

1. On the Main tab of the navigation pane, expand **System** and click **Platform**
2. In the **Time Zone** Box, select the correct Time Zone for the location of the BIG-IP server
3. Click the **Update** button.

On each GTM BIG-IP server, ensure the Device Certificate has not expired.

1. On the Main tab of the navigation pane, expand **System and** click **Device Certificates > Device Certificate**
2. Ensure the Device Certificate has not expired. If necessary, Renew the certificate, extending the Expiration date beyond 1 year, an expiration date of at least 5 years or longer should be considered. The device SSL certificates expiration date should exceed the expected service life of the sync group. Creating a device certificate that will expire in 10 years will be a safe assumption, however, this may need to be adjusted to support a particular network.

On each GTM BIG-IP server other than the configuration master GTM, run gtm_add, with the configuration master GTM's self-ip

The gtm_add utility performs the following operations:

1. Adds the calling GTM's Device Certificate to the Trusted Device Certificates list of the GTM whose self-ip is passed as a parameter to gtm_add
2. Imports the GTM configuration, including the DataCenters, Servers, Wide-IPs and list of Trusted Devices Certificates, from the GTM whose self-ip is passed as a parameter to the calling GTM's configuration, replacing any previous GTM configuration.

In our example we would run gtm_add once on the Los Angeles BIG-IP to import the GTM configuration from the New York BIG-IP. The New York GTM is our 'configuration master' in this example. For example:

```
[admin@bigip1-la.example.com:Active] ~ # gtm_add
150.10.10.53
WARNING: Running this script will wipe out the current
configuration
```

```
files (bigip_gtm.conf, named.conf and named zone files) on
the BIG-IP GTM
Controller on which this script is run.  The configuration
will be
replaced with the configuration of the remote BIG-IP GTM
Controller
in the specified sync group
The local BIG-IP GTM MUST already be added in the
configuration of the
other GTM.

Are you absolutely sure you want to do this? [y/n] y

==> Running 'bigstart shutdown gtmd' on the local system
==> Running 'bigstart shutdown zrd' on the local system
==> Running 'bigstart shutdown named' on the local system
    Retrieving remote and installing local BIG-IP's SSL
certs ...
Enter root password if prompted
Password:
Rekeying Master Key...
Verifying iQuery connection to 150.10.10.53. This may take
up to 30 seconds

Retrieving remote GTM configuration...

Retrieving remote DNS/named configuration...

Restarting gtmd
Restarting named
Restarting zrd

==> Done <==
```

After running gtm_add, each GTM will have the same GTM configuration and Trusted Device Certificates. To verify this step, go to the GUI console of the BIG-IP that ran gtm_add and navigate to the **Global Traffic > Data Centers**, **Global Traffic > Servers** and **Global Traffic > Pools** pages. Those pages should now list the same configuration objects that are listed on the ‘configuration master’ GTM.

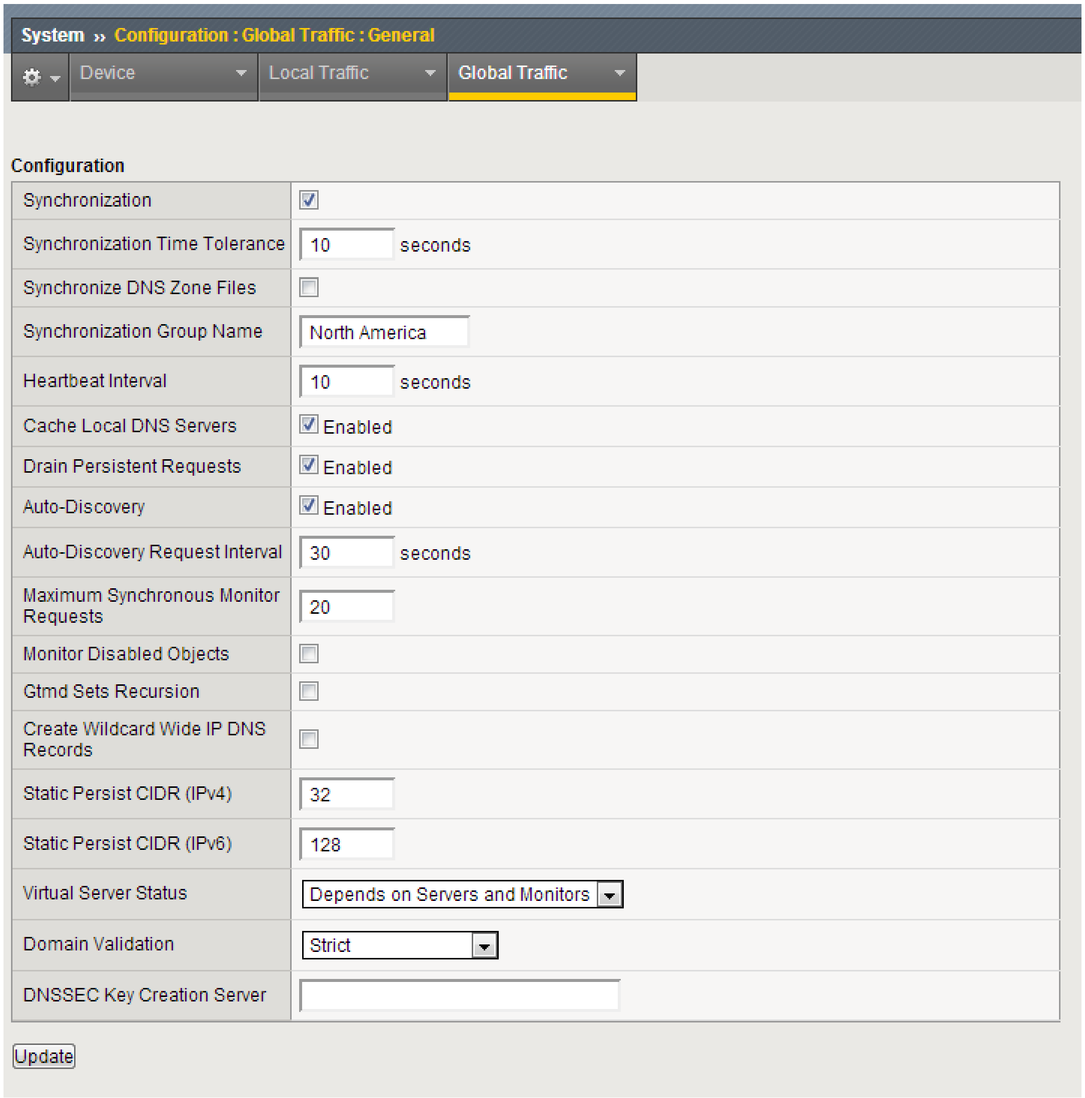
*Note: We have not created any pools in our configuration yet so if none already exist on the 'configuration master' GTM, no pools should be displayed under **Global Traffic > Pools** on the newly added GTM.*

On each GTM, enable Synchronization

Now that each GTM has been synchronized with the 'configuration master' GTM the final step is to configure each of the GTM's Global Traffic Manager Synchronization settings, ensuring each GTM is a member of the same Synchronization Group and has Synchronization enabled. Once this is the case, all modifications to the GTM configuration from any GTM will be propagated to the other GTMs automatically.

Perform the following steps on each BIG-IP GTM:

1. On the Main tab of the navigation pane, expand **System** and then click **Configuration**. The general properties screen opens.
2. From the **Global Traffic** menu, choose General. The General Global Traffic properties screen opens.
3. Ensure the **Synchronization** checkbox is **checked**.
4. In the **Synchronization Group Name** box, type a name of a new group. In our example, the name will be **North America**.
5. Click the **Update** button to save your changes



Configuration

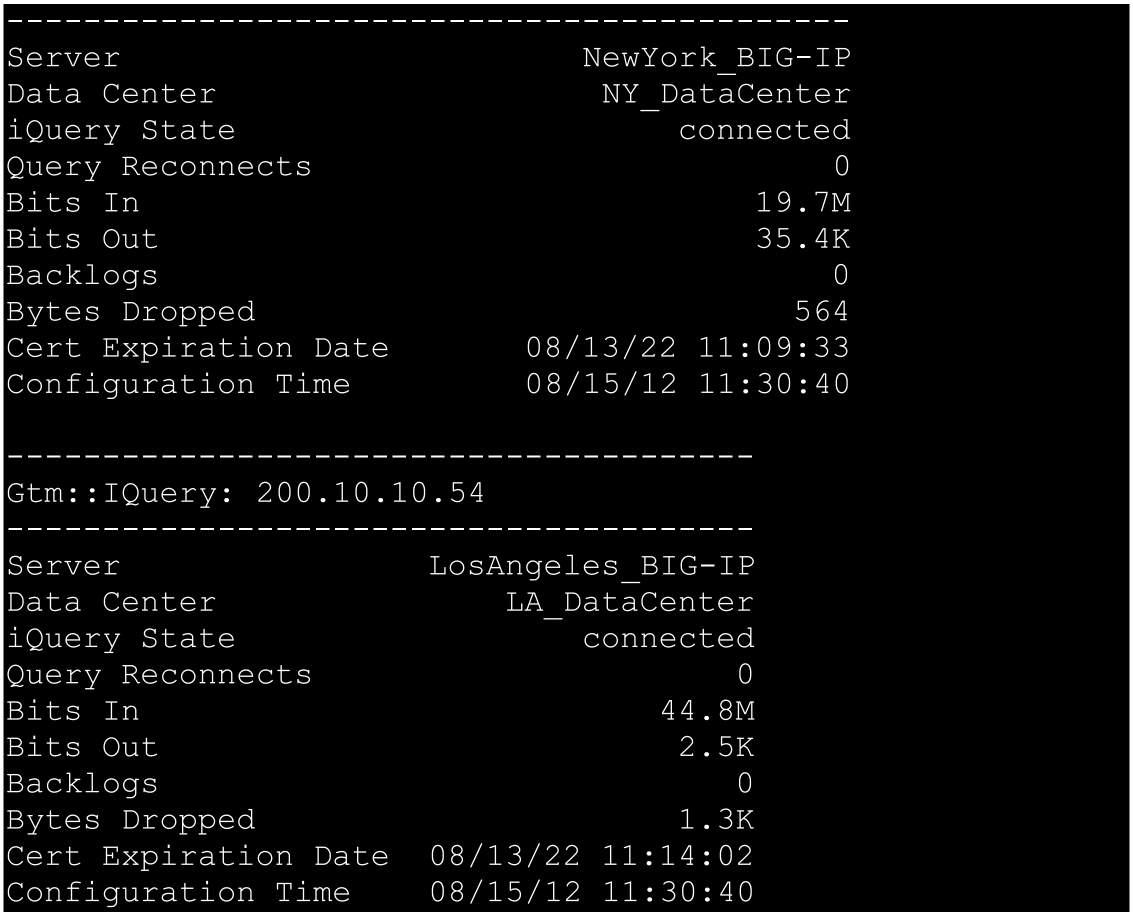
Synchronization	☑
Synchronization Time Tolerance	10 seconds
Synchronize DNS Zone Files	□
Synchronization Group Name	North America
Heartbeat Interval	10 seconds
Cache Local DNS Servers	☑ Enabled
Drain Persistent Requests	☑ Enabled
Auto-Discovery	☑ Enabled
Auto-Discovery Request Interval	30 seconds
Maximum Synchronous Monitor Requests	20
Monitor Disabled Objects	□
Gtmd Sets Recursion	□
Create Wildcard Wide IP DNS Records	□
Static Persist CIDR (IPv4)	32
Static Persist CIDR (IPv6)	128
Virtual Server Status	Depends on Servers and Monitors
Domain Validation	Strict
DNSSEC Key Creation Server	

The GTM systems in the network should now all be configured to pass traffic securely, be synchronized, and share configuration and load data between each unit.

To verify this step, go to the command line for each of the BIG-IP GTM servers and run the command 'tmsh show gtm iquery all'. The output should contain a section for each GTM in the sync group with the iQuery state 'connected' and evidence of incrementing values for Bits In and Bits Out over time. For example:

```
[admin@bigip1-la.example.com:Active] ~ # tmsh show gtm
iquery all

---------------------------------------------
Gtm::IQuery: 150.10.10.53
```



```
--------------------------------------------
Server                        NewYork_BIG-IP
Data Center                    NY_DataCenter
iQuery State                       connected
Query Reconnects                           0
Bits In                                19.7M
Bits Out                               35.4K
Backlogs                                   0
Bytes Dropped                            564
Cert Expiration Date       08/13/22 11:09:33
Configuration Time         08/15/12 11:30:40

---------------------------------------
Gtm::IQuery: 200.10.10.54
---------------------------------------
Server                LosAngeles_BIG-IP
Data Center               LA_DataCenter
iQuery State                  connected
Query Reconnects                      0
Bits In                           44.8M
Bits Out                           2.5K
Backlogs                              0
Bytes Dropped                      1.3K
Cert Expiration Date  08/13/22 11:14:02
Configuration Time    08/15/12 11:30:40
```

For troubleshooting issues with iQuery, please see the appropriate F5 Solution Article:

https://support.f5.com/kb/en-us/solutions/public/13000/600/sol13690.html?sr=25026005

Configure a GTM Pool for each site.

A pool defines the set of BIG-IP LTM virtual servers that are available on each site for Enterprise Manager. In our example we only have one Enterprise Manager deployment, per site so we create a GTM Pool that has only one member.

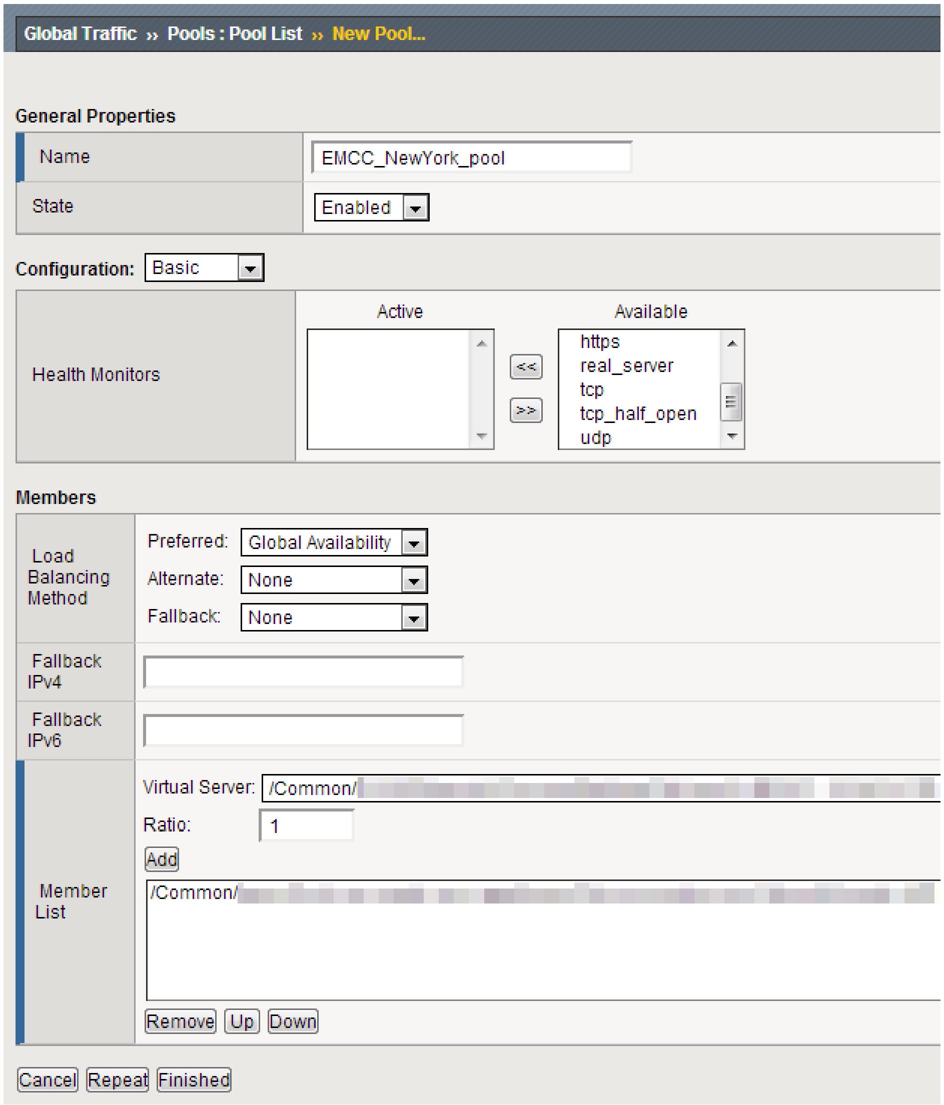
On **one of the GTMs** that is part of the GTM sync group, **perform the following steps once for each site**

NOTE: Remember, now that the GTMs are part of a sync group, we only need to configure the Pools on one GTM and the configuration will be automatically pushed to all other GTMs in the sync group. We need to perform the steps once for each site, creating a pool of LTM servers for each GTM. In our example we would create two Pools, one for New York and one for Los Angeles.

1. On the Main tab of the navigation pane, expand **Global Traffic** and click **Pools** (located under Wide IPs). The Pool List page opens.
2. Click the **Create** button. The General Properties screen for the new Pool appears.
3. In the **Name** box, type a name for the pool. In our example, we provide the name EMCC_ NewYork_pool.
4. Leave the list of **Health Monitors** empty.
5. In the **Load Balancing Method** section, select the value 'Global Availability' for **Preferred** and 'None' for **Alternate** and **Fallback**. Global Availability mode results in traffic being routed to only one site at a time. Traffic is only routed to a different site when the original site is not available.
6. In our example we leave the Fallback IPv4 and Fallback IPv6 boxes blank.
7. In the **Member List** section, from the Virtual Server list, select the secure console virtual server from the LTM for this site, and click the Add button.

   Note: You must select the virtual server by IP Address and port number combination. In our example, we select 150.10.10.53:443.

8. Click the **Finished** button.



Global Traffic » Pools : Pool List » New Pool...

General Properties

Name	EMCC_NewYork_pool
State	Enabled

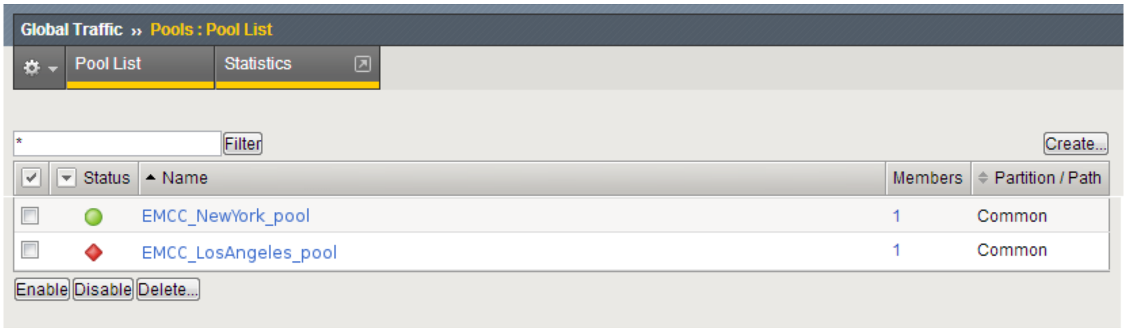
Configuration: Basic

	Active	Available
Health Monitors		https real_server tcp tcp_half_open udp

Members

Load Balancing Method	Preferred: Global Availability Alternate: None Fallback: None
Fallback IPv4	
Fallback IPv6	
Member List	Virtual Server: /Common/[redacted] Ratio: 1 /Common/[redacted]

The new Pool is added to the list. Since the pool for the primary site is the only one whose services are 'up', expect only that pool to show up (green) and the other pool(s) to show as down (red). In our example, the New York pool would be displayed as up and Los Angeles pool would be shown as down, because the LA site is in Standby mode.



☑	Status	Name	Members	Partition / Path
□	●	EMCC_NewYork_pool	1	Common
□	◆	EMCC_LosAngeles_pool	1	Common

For more information, see F5 Documentation: Setting up GTM pools.

Configure a Wide-IP to serve as the Oracle Enterprise Manager virtual hostname

A Wide IP is a mapping of a fully-qualified domain name (FQDN) to a set of virtual servers that host the domain's content. For our purposes, those virtual servers are those defined for Oracle Enterprise Manager. In our example we are mapping the FQDN em.gtm.example.com to Pools that contain the virtual servers that serve Oracle Enterprise Manager on both the Active and Standby sites. When a request is made to resolve the Wide IP em.gtm.example.com, the request is handled by one of the GTMs in the sync group which resolves the request with the IP address of the currently active Virtual server from the list of pools allocated to the Wide IP. Since there is only ever one active pool in an Oracle Enterprise Manager DR setup, the GTM will resolve the Wide IP hostname to the IP address of the Active site consistently until there is a need to switch over to the Standby site.

To create a Wide IP on the GTM system

The following step need only be performed on one of the GTMs. Now that the GTMs are part of a sync group, the Wide-IP definition will be automatically propagated to all GTMs.

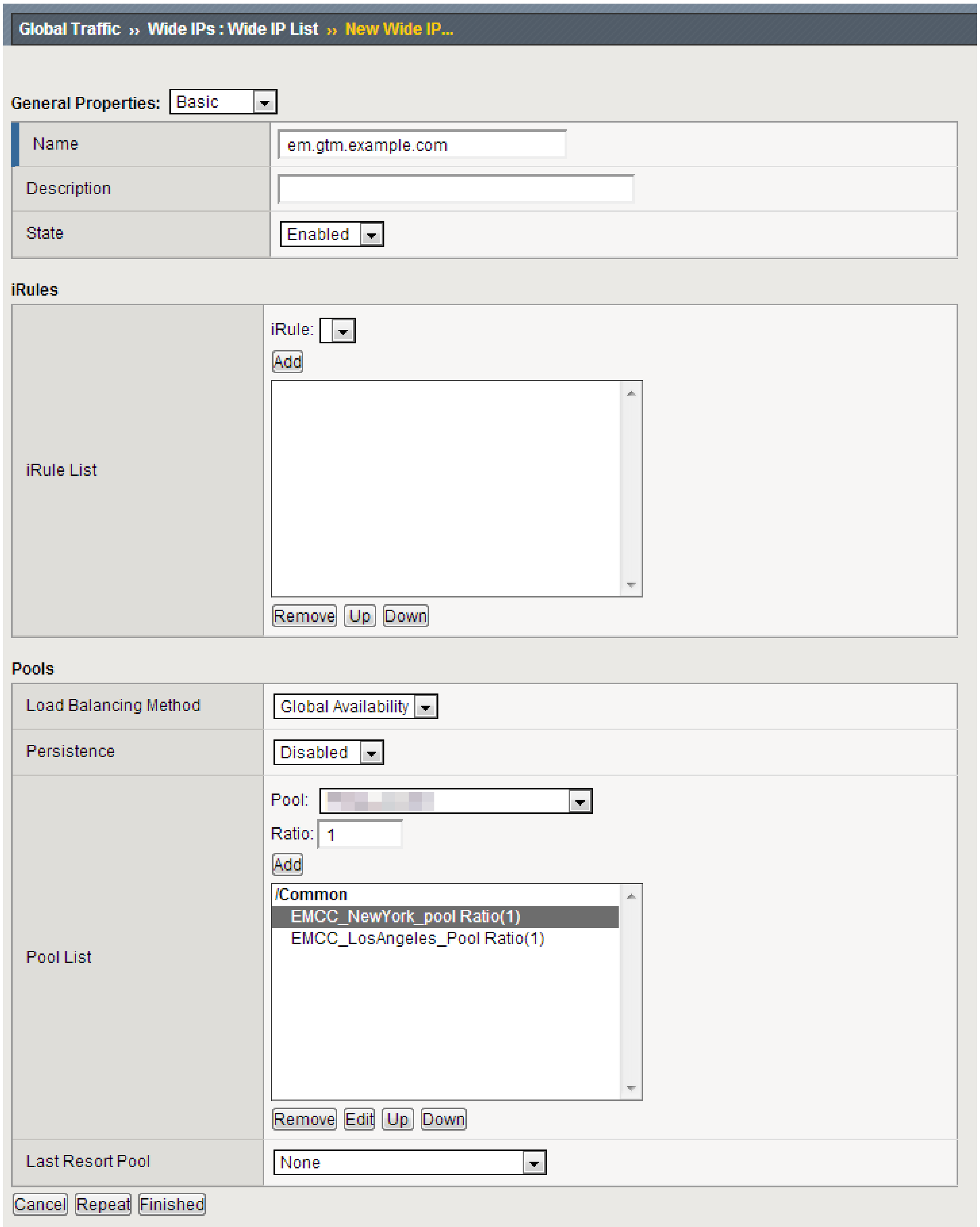
1. On the Main tab of the navigation pane, expand **Global Traffic** and click **Wide IPs**. The Wide IPs list page opens.
2. Click the **Create** button. The New Wide IP screen opens.
3. In the **Name** box, type a name for the Wide IP. In our example, we type **em.gtm.example.com**.
4. In our example, we are not using any iRules, so we skip the iRule section. Configure as appropriate for your deployment, see F5 Documentation: Managing iRules
5. In the Pools section, from the **Load Balancing Method** list, select a load balancing method. In our example, we select **Global Availability**. Global Availability instructs the GTM to select the first pool in the wide IP until it becomes unavailable, at which point it selects the next pool until the first pool

becomes available again. In our example, the GTM sends all incoming EM requests to the first-listed pool, **EMCC_NewYork_pool**. If that pool is unavailable, all incoming requests are sent to the next-listed pool, **EMCC_LosAngeles_pool**.

6. From the Pool List section, from the Pool list, select the name of the pool you created in the *Configure a GTM pool* section, and then click the **Add** button. In our example, we select **EMCC_NewYork_pool.**

   Repeat this step for any additional pools. In our example, we repeat one time for the **EMCC_LosAngeles_pool**.

7. All other settings are optional, configure as appropriate for your deployment.
8. Click the **Finished** button.



Global Traffic » Wide IPs : Wide IP List » New Wide IP...

General Properties: Basic

Name	em.gtm.example.com
Description	
State	Enabled

iRules

iRule List	iRule:

Pools

Load Balancing Method	Global Availability
Persistence	Disabled
Pool List	Pool: [redacted] Ratio: 1 /Common EMCC_NewYork_pool Ratio(1) EMCC_LosAngeles_Pool Ratio(1)
Last Resort Pool	None

For more information, see F5 Documentation: Managing wide IPs.

Validate GTM configuration of Wide IP for Enterprise Manager

To validate that the GTM configuration of the Wide IP is working use a tool like dig to try to resolve the Wide IP FQDN.

dig output should list the GTM servers that we added to the corporate DNS system using NS records and should correctly resolve the Wide IP address to the IP address of the currently Active Oracle Enterprise Manager Virtual server.

For example:

```
$ dig em.gtm.example.com

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-20.P1.el5
<<>>em.gtm.example.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1901
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2,
ADDITIONAL: 2

;; QUESTION SECTION:
; em.gtm.example.com.    IN   A

;; ANSWER SECTION:
em.gtm.example.com. 30   IN   A    150.10.10.10

;; AUTHORITY SECTION:
gtm.example.com.    10800     IN   NS   bigip1-
ny.example.com.
gtm.example.com.    10800     IN   NS   bigip1-
la.example.com.

;; ADDITIONAL SECTION:
bigip1-ny.example.com. 10800 IN A  150.10.10.53
bigip1-la.example.com. 10800 IN A  200.10.10.54

;; Query time: 1 msec
;; SERVER: 70.10.10.10#53(10.10.10.70)
;; WHEN: Fri Aug 24 12:38:50 2012
;; MSG SIZE  rcvd: 220
```

Configure DNS to forward requests for the EM hostname to the GTM

Once we have validated that the GTM configuration is correct and successfully forwards requests for the Wide IP for the Oracle Enterprise Manager services, the final step is to modify the DNS record for the virtual hostname for the Enterprise Manager deployment so that the virtual hostname is a CNAME for the Wide IP.

For example:

em.example.com.	IN	CNAME	em.gtm.example.com

Once this update to DNS is made, all requests for the hostname em.example.com will be translated to requests for em.gtm.example.com. Since em.gtm.example.com has the domain 'gtm.example.com', all those requests will be forwarded to the GTM servers (because of the NS records we added in step Configure DNS to hand off requests to the GTM). The GTM servers will return the IP address of the currently active EM Virtual Servers. When failover/switchover occurs, GTM will transparently start to return the IP address of the newly active EM Virtual Servers.

Summary

After performing the above configuration steps you should have a basic working DR configuration for Enterprise Manager Cloud Control. The FQDN for the EM deployment, e.g. em.example.com, is routed to the currently active EM site, transparently switching between sites when switchover/failover occurs.

Once a basic configuration is in place and the concepts are understood it is recommended to revisit the F5 documentation referenced throughout this document to extend the configuration to meet the HA requirements of your company. Specifically, consider implementing redundancy for both LTM and GTM services.

Related links

BIG-IP GTM / VE 11.1.0 Documentation

Troubleshooting iQuery GTM synchronization

Oracle is committed to developing practices and products that help protect the environment

Enterprise Manager 12c Cloud Control:

Configuring OMS Disaster Recovery with F5 BIG-IP Global Traffic Manager
September, 2012
Author: David Parker-Bastable (Oracle)

Contributing Authors: James Viscusi (Oracle), Chris Akker (F5 Networks)

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Hardware and Software, Engineered to Work Together