Global Server Load Balancing
Contents

Global Server Load Balancing ............................................................... 5
  Global Server Load Balancing .......................................................... 6
  How GSLB Works ............................................................................. 7
    GSLB Sites .................................................................................. 8
    GSLB Services ............................................................................. 9
    GSLB Virtual Servers .................................................................. 10
  Load Balancing or Content Switching Virtual Servers ...................... 11
  ADNS Services ............................................................................... 12
  DNS VIPs ...................................................................................... 13
Configuring Global Server Load Balancing (GSLB) ......................... 14
  Configuring a Standard Load Balancing Setup ................................. 15
  Configuring an Authoritative DNS Service ..................................... 16
  Configuring a Basic GSLB Site ........................................................ 19
  Configuring a GSLB Service ............................................................ 22
  Configuring a GSLB Virtual Server ................................................ 26
  Binding GSLB Services to a GSLB Virtual Server ......................... 30
  Binding a Domain to a GSLB Virtual Server ................................... 32
  Synchronizing a Configuration in a GSLB Setup .............................. 35
Viewing and Configuring a GSLB Setup by Using the GSLB Visualizer 39
Configuring the Metrics Exchange Protocol (MEP) ......................... 43
  Configuring Site Metric Exchange .................................................. 44
  Configuring Network Metric Information Exchange ........................ 45
  Configuring Persistence Information Exchange .............................. 46
Configuring Site-to-Site Communication ........................................... 47
  Changing the Password of an RPC Node ........................................ 48
  Encrypting the Exchange of Site Metrics ....................................... 50
  Configuring the Source IP Address for an RPC Node ..................... 52
Customizing Your GSLB Configuration .............................................. 54
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modifying Maximum Connections or Maximum Bandwidth for a GSLB Service</td>
<td>55</td>
</tr>
<tr>
<td>Creating CNAME-Based GSLB Services</td>
<td>57</td>
</tr>
<tr>
<td>Changing the GSLB Method</td>
<td>60</td>
</tr>
<tr>
<td>Specifying a GSLB Method Other than Static Proximity or Dynamic (RTT)</td>
<td>61</td>
</tr>
<tr>
<td>Configuring Static Proximity</td>
<td>62</td>
</tr>
<tr>
<td>Adding a Location File to Create a Static Proximity Database</td>
<td>63</td>
</tr>
<tr>
<td>Adding Custom Entries to a Static Proximity Database</td>
<td>66</td>
</tr>
<tr>
<td>Setting the Location Qualifiers</td>
<td>68</td>
</tr>
<tr>
<td>Specifying the Proximity Method</td>
<td>71</td>
</tr>
<tr>
<td>Configuring the Dynamic Method (RTT)</td>
<td>72</td>
</tr>
<tr>
<td>Configuring a GSLB Virtual Server for Dynamic RTT</td>
<td>74</td>
</tr>
<tr>
<td>Setting the Probing Interval of Local DNS Servers</td>
<td>76</td>
</tr>
<tr>
<td>Configuring Persistent Connections</td>
<td>78</td>
</tr>
<tr>
<td>Configuring Persistence Based on Source IP Address</td>
<td>79</td>
</tr>
<tr>
<td>Configuring Persistence Based on HTTP Cookies</td>
<td>81</td>
</tr>
<tr>
<td>Configuring Transition Out-Of-Service State (TROFS) in GSLB</td>
<td>84</td>
</tr>
<tr>
<td>Configuring Dynamic Weights for Services</td>
<td>85</td>
</tr>
<tr>
<td>Monitoring GSLB Services</td>
<td>87</td>
</tr>
<tr>
<td>Adding or Removing Monitors</td>
<td>88</td>
</tr>
<tr>
<td>Binding Monitors to a GSLB Service</td>
<td>90</td>
</tr>
<tr>
<td>Monitoring GSLB Sites</td>
<td>92</td>
</tr>
<tr>
<td>Protecting the GSLB Setup Against Failure</td>
<td>93</td>
</tr>
<tr>
<td>Configuring a Backup GSLB Virtual Server</td>
<td>94</td>
</tr>
<tr>
<td>Configuring a GSLB Setup to Respond with Multiple IP Addresses</td>
<td>96</td>
</tr>
<tr>
<td>Configuring a GSLB Virtual Server to Respond with an Empty Address</td>
<td>97</td>
</tr>
<tr>
<td>Configuring a Backup IP Address for a GSLB Domain</td>
<td>99</td>
</tr>
<tr>
<td>Diverting Excess Traffic to a Backup Virtual Server</td>
<td>101</td>
</tr>
<tr>
<td>Managing Client Connections</td>
<td>105</td>
</tr>
<tr>
<td>Enabling Delayed Cleanup of Virtual Server Connections</td>
<td>106</td>
</tr>
<tr>
<td>Managing Local DNS Traffic by Using DNS Policies</td>
<td>108</td>
</tr>
<tr>
<td>DNS Expressions</td>
<td>109</td>
</tr>
<tr>
<td>Configuring DNS Policies</td>
<td>111</td>
</tr>
<tr>
<td>Binding DNS Policies</td>
<td>115</td>
</tr>
<tr>
<td>Adding DNS Views</td>
<td>117</td>
</tr>
<tr>
<td>Configuring GSLB for Commonly Used Deployment Scenarios</td>
<td>119</td>
</tr>
<tr>
<td>Configuring GSLB for Disaster Recovery</td>
<td>120</td>
</tr>
</tbody>
</table>
Global Server Load Balancing

NetScaler appliances configured for global server load balancing (GSLB) provide for disaster recovery and ensure continuous availability of applications by protecting against points of failure in a wide area network (WAN). GSLB can balance the load across data centers by directing client requests to the closest or best performing data center, or to surviving data centers in case of an outage.

Following are some typical GSLB configurations:

- **Active-active data center setup.** Consists of multiple active data centers. Client requests are load balanced across active data centers.

- **Active-standby data center setup.** Consists of an active and a standby data center. When a failover occurs as a result of a disaster event, the standby data center becomes operational.

- **Proximity setup.** Directs client requests to the data center that is closest in geographical distance or network distance.

In a typical configuration, a local DNS server sends client requests to a GSLB virtual server, to which are bound GSLB services. A GSLB service identifies a load balancing or content switching virtual server, which can be at the local site or a remote site. If the GSLB virtual server selects a load balancing or content switching virtual server at a remote site, it sends the virtual server’s IP address to the DNS server, which sends it to the client. The client then resends the request to the new virtual server at the new IP.

The GSLB entities that you must configure are the GSLB sites, the GSLB services, the GSLB virtual servers, load balancing or content switching virtual servers, and authoritative DNS (ADNS) services. You must also configure MEP. You can also configure DNS views to expose different parts of your network to clients accessing the network from different locations.

**Note:** To take full advantage of the NetScaler GSLB features, you should use NetScaler appliances for load balancing or content switching at each data center, so that your GSLB configuration can use the proprietary Metric Exchange Protocol (MEP) to exchange site metrics.
How GSLB Works

With ordinary DNS, when a client sends a domain name system (DNS) request, it receives a list of IP addresses of the domain or service. Generally, the client chooses the first IP address in the list and initiates a connection with that server. The DNS server uses a technique called DNS round robin to rotate through the IPs on the list, sending the first IP address to the end of the list and promoting the others after it responds to each DNS request. This technique ensures equal distribution of the load, but it does not support disaster recovery, load balancing based on load or proximity of servers, or persistence.

When you configure GSLB on NetScaler appliances and enable Metric Exchange Protocol ( MEP), the appliances use the DNS infrastructure to connect the client to the data center that best meets the criteria that you set. The criteria can designate the least loaded data center, the closest data center, the data center that responds most quickly to requests from the client’s location, a combination of those metrics, and SNMP metrics. An appliance keeps track of the location, performance, load, and availability of each data center and uses these factors to select the data center to which to send a client request.

A GSLB configuration consists of a group of GSLB entities on each appliance in the configuration. These entities include GSLB sites, GSLB services, GSLB virtual servers, load balancing and/or content switching servers, and ADNS services.
How GSLB Works

With ordinary DNS, when a client sends a domain name system (DNS) request, it receives a list of IP addresses of the domain or service. Generally, the client chooses the first IP address in the list and initiates a connection with that server. The DNS server uses a technique called DNS round robin to rotate through the IPs on the list, sending the first IP address to the end of the list and promoting the others after it responds to each DNS request. This technique ensures equal distribution of the load, but it does not support disaster recovery, load balancing based on load or proximity of servers, or persistence.

When you configure GSLB on NetScaler appliances and enable Metric Exchange Protocol (MEP), the appliances use the DNS infrastructure to connect the client to the data center that best meets the criteria that you set. The criteria can designate the least loaded data center, the closest data center, the data center that responds most quickly to requests from the client’s location, a combination of those metrics, and SNMP metrics. An appliance keeps track of the location, performance, load, and availability of each data center and uses these factors to select the data center to which to send a client request.

A GSLB configuration consists of a group of GSLB entities on each appliance in the configuration. These entities include GSLB sites, GSLB services, GSLB virtual servers, load balancing and/or content switching servers, and ADNS services.
GSLB Sites

A typical GSLB setup consists of data centers, each of which has various network appliances that may or may not be NetScaler appliances. The data centers are called GSLB sites. Each GSLB site is managed by a NetScaler appliance that is local to that site. Each of these appliances treats its own site as the local site and all other sites, managed by other appliances, as remote sites.

If the appliance that manages a site is the only NetScaler appliance in that data center, the GSLB site hosted on that appliance acts as a bookkeeping placeholder for auditing purposes, because no metrics can be collected. Typically, this happens when the appliance is used only for GSLB, and other products in the data center are used for load balancing or content switching.
GSLB Services

A GSLB service is usually a representation of a load balancing or content switching virtual server, although it can represent any type of virtual server. The GSLB service identifies the virtual server’s IP address, port number, and service type. GSLB services are bound to GSLB virtual servers on the NetScaler appliances managing the GSLB sites. A GSLB service bound to a GSLB virtual server in the same data center is local to the GSLB virtual server. A GSLB service bound to a GSLB virtual server in a different data center is remote from that GSLB virtual server.
GSLB Virtual Servers

A GSLB virtual server has one or more GSLB services bound to it, and load balances traffic among those services. It evaluates the configured GSLB methods (algorithms) to select the appropriate service to which to send a client request. Because the GSLB services can represent either local or remote servers, selecting the optimal GSLB service for a request has the effect of selecting the data center that should serve the client request.

The domain for which global server load balancing is configured must be bound to the GSLB virtual server, because one or more services bound to the virtual server will serve requests made for that domain.

Unlike other virtual servers configured on a NetScaler appliance, a GSLB virtual server does not have its own virtual IP address (VIP).
Load Balancing or Content Switching Virtual Servers

A load balancing or content switching virtual server represents one or many physical servers on the local network. Clients send their requests to the load balancing or content switching virtual server’s virtual IP (VIP) address, and the virtual server balances the load across the physical servers. After a GSLB virtual server selects a GSLB service representing either a local or a remote load balancing or content switching virtual server, the client sends the request to that virtual server’s VIP address.

For more information about load balancing or content switching virtual servers and services, see Load Balancing, or Content Switching.
ADNS Services

An ADNS service is a special kind of service that responds only to DNS requests for domains for which the NetScaler appliance is authoritative. When an ADNS service is configured, the appliance owns that IP address and advertises it. Upon reception of a DNS request by an ADNS service, the appliance checks for a GSLB virtual server bound to that domain. If a GSLB virtual server is bound to the domain, it is queried for the best IP address to which to send the DNS response.
DNS VIPs

A DNS virtual IP is a virtual IP (VIP) address that represents a load balancing DNS virtual server on the NetScaler appliance. DNS requests for domains for which the NetScaler appliance is authoritative can be sent to a DNS VIP.
Configuring Global Server Load Balancing (GSLB)

Global server load balancing is used to manage traffic flow to a web site hosted on two separate server farms that ideally are in different geographic locations. For example, consider a Web site, www.mycompany.com, which is hosted on two geographically separated server farms or data centers. Both server farms use NetScaler appliances. The NetScaler appliances in these server farms are set up in one-arm mode and function as authoritative DNS servers for the www.mycompany.com domain. The following figure illustrates this configuration.

Figure 1. Basic GSLB Topology

To configure such a GSLB setup, you must first configure a standard load balancing setup for each server farm or data center. This enables you to balance load across the different servers in each server farm. Then, configure both NetScaler appliances as authoritative DNS (ADNS) servers. Next, create a GSLB site for each server farm, configure GSLB virtual servers for each site, create GLSB services, and bind the GSLB services to the GSLB virtual servers. Finally, bind the domain to the GSLB virtual servers. The GSLB configurations on the two appliances at the two different sites are identical, although the load-balancing configurations for each site is specific to that site.

Note: To configure a GSLB site in a NetScaler cluster setup, see Setting Up GSLB in a Cluster.
Configuring a Standard Load Balancing Setup

A load balancing virtual server balances the load across different physical servers in the data center. These servers are represented as services on the NetScaler appliance, and the services are bound to the load balancing virtual server.

For details on configuring a basic load balancing setup, see Load Balancing.
Configuring an Authoritative DNS Service

When you configure the NetScaler appliance as an authoritative DNS server, it accepts DNS requests from the client and responds with the IP address of the data center to which the client should send requests.

**Note:** For the NetScaler to be authoritative, you must also create SOA and NS records. For more information about SOA and NS records, see "Domain Name System".

**To create an ADNS service by using the command line interface**

At the command prompt, type the following commands to create an ADNS service and verify the configuration:

- `add service <name> <IP>@ ADNS <port>`
- `show service <name>`

**Example**

```
add service Service-ADNS-1 10.14.39.21 ADNS 53
show service Service-ADNS-1
```

**To modify an ADNS service by using the command line interface**

At the command prompt, type the following command:

```
set service <name> <IPAddress> ADNS <port>
```

**Example**

```
set service Service-ADNS-1 10.14.39.21 ADNS 53
```

**To remove an ADNS service by using the command line interface**

At the command prompt, type the following command:
Parameters for configuring an ADNS service

name

The name of the ADNS service you are creating. This alphanumeric string is required and cannot be changed after the service is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

IPAddress

The IP address of the server that the ADNS service represents. You can configure the ADNS service to use a mapped IP address (MIP), subnet IP address (SNIP), or any new NetScaler-owned IP address.

Port

The port on which the service communicates with the application on the server. This number must correspond to the protocol that the application supports. The port number must always be a positive number not exceeding 65535.

To configure an ADNS service by using the configuration utility

1. In the navigation pane, expand Load Balancing and click Services.

2. In the details pane, do one of the following:
   - To create a new service, click Add.
   - To modify an existing service, select the service, and then click Open.

3. In the Create Service or Configure Service dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring an ADNS service” as shown:
   - Service Name*—name
   - Protocol*—(Select ADNS as the protocol.)
   - Port*—port

4. Click Create or OK, and then click Close. The server that you created appears in the GSLB Services pane.
Configuring a Basic GSLB Site

A GSLB site is a representation of a data center in your network and is a logical grouping of GSLB virtual servers, services, and other network entities. Typically, in a GSLB set up, there are many GSLB sites that are equipped to serve the same content to a client. These are usually geographically separated to ensure that the domain is active even if one site goes down completely. All of the sites in the GSLB configuration must be configured on every NetScaler appliance hosting a GSLB site. In other words, at each site, you configure the local GSLB site and each remote GSLB site.

Once GSLB sites are created for a domain, the NetScaler appliance sends client requests to the appropriate GSLB site as determined by the GSLB algorithms configured.

To create a GSLB site by using the command line interface

At the command prompt, type the following commands to create a GSLB site and verify the configuration:

- add gslb site <siteName> <siteIPAddress>
- show gslb site <siteName>

Example

add gslb site Site-GSLB-East-Coast 10.14.39.21
show gslb site Site-GSLB-East-Coast

To modify or remove a GSLB Site by using the command line interface

- To modify a GSLB site, use the set gslb site command, which is just like using the add gslb site command, except that you enter the name of an existing GSLB Site.

- To unset a site parameter, use the unset gslb site command, followed by the siteName value and the name of the parameter to be reset to its default value.

- To remove a GSLB site, use the rm gslb site command, which accepts only the <name> argument.
Parameters for configuring a GSLB site

siteName

A name for the data center you are adding as a GSLB site. This alphanumeric string is required and cannot be changed after the site is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

siteIPAddress

The IP address of the GSLB site. This IP address is a system-owned IP address. You can use any IP address configured as a SNIP, MIP, or GSLB site IP address. This is a mandatory parameter.

Note: To avoid a site going down during an HA failover event in a GSLB setup with an independent network configuration high availability deployment, the GSLB site IP address must be on the same subnet as the virtual IP (VIP) address of the load balancing or content switching virtual server that is bound to the service(s) provided by that GSLB site. In an independent network configuration high availability deployment, two nodes do not share the same subnet IPs (SNIPs) or mapped IPs (MIPs), but they have common VIPs.

To configure a basic GSLB site by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Sites.

2. In the details pane, do one of the following:

   · To create a new site, click Add.

   · To modify an existing site, select the site, and then click Open.

3. In the Create GSLB Site or Configure GSLB Site dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a GSLB site” as shown:

   · Name*—siteName

   · Site IP Address*—siteIPAddress

* A required parameter

4. Click Create or OK, and then click Close. The GSLB site you created appears in the GSLB Sites pane.

To view the statistics of a GSLB site by using the command line interface

At the command prompt, type:

```
stat gslb site <siteName>
```
Example

stat gslb site Site-GSLB-East-Coast

To view the statistics of a GSLB site by using the configuration utility

1. In the navigation pane, expand GSLB and click Sites.

2. In the GSLB Sites pane, select the GSLB site whose statistics you want to view.

3. Click Statistics.
Configuring a GSLB Service

A GSLB service is a representation of a load balancing or content switching virtual server. A local GSLB service represents a local load balancing or content switching virtual server. A remote GSLB service represents a load balancing or content switching virtual server configured at one of the other sites in the GSLB setup. At each site in the GSLB setup, you can create one local GSLB service and any number of remote GSLB services.

Creating GSLB Services

To create a GSLB service by using the command line interface

At the command prompt, type the following commands to create a GSLB service and verify the configuration:

- add gslb service <serviceName> <serverName | IP> <serviceType> <port>-siteName <string>
- show gslb service <serviceName>

Example

add gslb service Service-GSLB-1 10.14.39.14 HTTP 80 -siteName Site-GSLB-East-Coast
show gslb service Service-GSLB-1
To modify or remove a GSLB service by using the command line interface

- To modify a GSLB service, use the `set gslb service <serviceName>` command. For this command, specify the name of the GSLB service whose configuration you want to modify. You can change the existing values of the parameters either specified by you or set by default. You can change the value of more than one parameter in the same command. Refer to the `add gslb service` command for details about the parameters. Example

  ```
  > set gslb service SKP_GSLB_NOTCNAME_SVC2 -maxBandWidth 25 -maxClient 8
  Done
  > sh gslb service SKP_GSLB_NOTCNAME_SVC2
  SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
  ...
  Max Conn: 8  Max Bandwidth: 25 kbits
  ```

- To reset a parameter to its default value, you can use the `unset gslb service <serviceName>` command and the parameters to be unset. Example

  ```
  > unset gslb service SKP_GSLB_NOTCNAME_SVC2 maxBandWidth
  Done
  > sh gslb service SKP_GSLB_NOTCNAME_SVC2
  SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
  ...
  Max Conn: 8  Max Bandwidth: 0 kbits
  ```

- To remove a GSLB service, use the `rm gslb service <serviceName>` command.

Parameters for configuring a GSLB service

**serviceName** (Service Name)

The name of the service being configured. This alphanumeric string is required. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ . (period) : (colon) # and space ( ).

**siteName** (Site Name)

The name of the GSLB site that this service represents.

**serviceType** (Service Type)

The type of service or protocol used in client requests. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, MSSQL, MYSQL, RADIUS, RDP, SIP_UDP, RTSP.

**port** (Port)

Port number on which the service runs.

**serverName or ipAddress** (Server IP)
The server name or IP address of the GSLB service being configured. Must be the same as the virtual IP (VIP) address of a local or remote load balancing or content switching virtual server.

**publicIP (Public IP)**

The public IP address of the NAT translator for a GSLB service that is on a private network.

### To create a GSLB service by using the configuration utility

1. In the navigation pane, expand GSLB and click Services.

2. In the details pane, do one of the following:
   - To create a new service, click Add.
   - To modify an existing service, select the service, and then click Open.

3. In the Create GSLB Service or Configure GSLB Service dialog box, set the following parameters:
   - Service Name*
   - Site Name*
   - Server Name - The servers added to the NetScaler configuration are displayed in a dropdown list. If you want to add a new server, click New..., and then in the Create Server dialog box, type the necessary details. For more information about creating servers, see “Adding a Server.”
   - Service Type
   - Port

   **Note:** In the Site Name and Server Name lists, the most recently used value is displayed as selected. Make sure that you select the site and server you want to specify.

4. Click Create, and then click Close. The GSLB service you created appears in the GSLB Services pane.

### To view the statistics of a GSLB service by using the command line interface

At the command prompt, type:

```
stat gslb service <serviceName>
```

**Example**

```
stat gslb service Service-GSLB-1
```
To view the statistics of a GSLB service by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the GSLB Services pane, select the GSLB Service whose statistics you want to view.
3. Click Statistics.

Enabling and Disabling GSLB Services

Before you use a GSLB service for load balancing, it must be enabled. If the service is disabled, it is not included in load balancing even though it exists on the NetScaler appliance.

To enable or disable a GSLB service by using the command line interface

At the command prompt, type one of the following commands:

- enable service <name>
- disable service <name>

Example

> enable service Service-GSLB-1
Done
> disable service Service-GSLB-1
Done

To enable or disable a GSLB service by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Services.
2. In the GSLB Services pane, select the GSLB service which you want to enable or disable.
3. Click enable or disable.
Configuring a GSLB Virtual Server

A GSLB virtual server is an entity that represents one or more GSLB services and balances traffic between them. It evaluates the configured GSLB methods or algorithms to select a GSLB service to which to send the client request.

Creating GSLB Virtual Servers

To create a GSLB virtual server by using the command line interface

At the command prompt, type the following commands to add a GSLB virtual server and verify the configuration:

- add gslb vserver <name> <serviceType> -ipType (IPv4 | IPv6)
- show gslb vserver <name>

Example

add gslb vserver Vserver-GSLB-1 HTTP -ipType IPv4
add gslb vserver Vserver-GSLB-2 HTTP -ipType IPv6
show gslb vserver Vserver-GSLB-1
show gslb vserver Vserver-GSLB-2

To modify or remove a GSLB virtual server by using the command line interface

- To modify a GSLB virtual server, use the set gslb vserver command, which is just like using the add gslb vserver command, except that you enter the name of an existing GSLB virtual server.

- To reset a parameter to its default value, you can use the unset gslb vserver command followed by the vserverName value and the name of the parameter to be unset.

- To remove a GSLB virtual server, use the rm gslb vserver command, which accepts only the <name> argument.

Parameters for configuring a GSLB server

name
The name of the GSLB virtual server. This alphanumeric string is required and cannot be changed after the virtual server is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

serviceType

The service type of the virtual server, that is, the type of content in the processed requests. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RDP, ANY.

ipType

Specifies whether this virtual server supports services that use the IPv4 or IPv6 protocol for IP addresses. Possible values: IPv4, IPv6. Default: IPv4.

To create a GSLB virtual server by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.

2. In the details pane, do one of the following:
   · To create a new GSLB virtual server, click Add.
   · To modify an existing GSLB virtual server, select the service, and then click Open.

3. In the Create GSLB Virtual Server or Configure GSLB Virtual Server dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a GSLB virtual server” as shown:
   · Name*—name
   · Service Type*—serviceType
   · IPv6—ipType (To specify IPv6, select the check box. For IPv4, clear the check box.) *

4. Click Create or OK, and then click Close. The GSLB virtual server that you created appears in the GSLB Virtual Servers pane.

To view the statistics of a GSLB virtual server by using the command line interface

At the command prompt, type:

```
stat gslb vserver <name>
```

Example

```
stat gslb vserver Vserver-GSLB-1
```
To view the statistics of a GSLB virtual server by using the
configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the details pane, select the GSLB virtual server whose statistics you want to view.
3. Click Statistics.

Statistics of a GSLB service

When you run the stat gslb service command from the command line or click on the
Statistics link from the configuration utility, the following details of the service will be
displayed:

- **Request bytes.** Total number of request bytes received on this service or virtual server.
- **Response bytes.** Number of response bytes received by this service or virtual server.
- **Current client established connections.** Number of client connections in ESTABLISHED
  state.
- **Current load on the service.** Load on the service (Calculated from the load monitor
  bound to the service).

The data of number of requests and responses, and the number of current client and server
connections may not be displayed or may not be synchronized with the data of the
 corresponding load balancing virtual server.

Enabling and Disabling GSLB Virtual Servers

When you create a GSLB virtual server, it is enabled by default. If you disable it, it cannot
process traffic. A disabled GSLB virtual server is not included in GSLB configuration but is
not removed from the NetScaler appliance.

To enable or disable a GSLB virtual server by using the
command line interface

At the command prompt, type one of the following commands:

- `enable gslb vserver <name>`
- `disable gslb vserver <name>`

Example

```
enable gslb vserver Vserver-GSLB-1
disable gslb vserver Vserver-GSLB-1
```
To enable or disable a GSLB virtual server by using the configuration utility

1. Select a virtual server and, from the Action list, select enable or disable.
Binding GSLB Services to a GSLB Virtual Server

Once the GSLB services and virtual server are configured, relevant GSLB services must be bound to the GSLB virtual server to activate the configuration.

To bind a GSLB service to a GSLB virtual server by using the command line interface

At the command prompt, type the following commands to bind a GSLB service to a GSLB virtual server and verify the configuration:

- `bind gslb vserver <name> -serviceName <string>`
- `show gslb vserver <name>`

Example

```
bind gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1
show gslb vserver Vserver-GSLB-1
```

To unbind a GSLB service from a GSLB virtual server by using the command line interface

At the command prompt, type:

```
unbind gslb vserver <name> -serviceName <string>
```
To bind GSLB services by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.

2. In the details pane, select the GSLB Virtual Server to which you want to bind the services (for example, Vserver-GSLB-1).

3. Click Open.

4. On the Services tab, in the Active column, select the check boxes next to the GSLB services that you want to bind to the GSLB virtual server.

5. Click OK.
To make a NetScaler appliance the authoritative DNS server for a domain, you must bind the domain to the GSLB virtual server. When you bind a domain to a GSLB virtual server, the NetScaler adds an address record for the domain, containing the name of the GSLB virtual server. The start of authority (SOA) and name server (NS) records for the GSLB domain must be added manually.

For details on configuring SOA and NS records, see “Domain Name System”.

To bind a domain to a GSLB virtual server by using the command line interface

At the command prompt, type the following commands to bind a domain to a GSLB virtual server and verify the configuration:

- `bind gslb vserver <name> -domainName <string>`
- `show gslb vserver <name>`

Example

```bash
bind gslb vserver Vserver-GSLB-1 -domainName www.mycompany.com
show gslb vserver Vserver-GSLB-1
```

To unbind a GSLB domain from a GSLB virtual server by using the command line interface

At the command prompt, type:

`unbind gslb vserver <name> -domainName <string>`
To bind a domain to a GSLB virtual server by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.

2. In GSLB Virtual Servers pane, select the GSLB Virtual Server to which you want to bind the domain (for example, Vserver-GSLB-1) and click Open.

3. In the Configure GSLB Virtual Server dialog box, on the Domains tab, do one of the following:
   · To create a new Domain, click Add.
   · To modify an existing Domain, select the domain, and then click Open.

4. In the Create GSLB Domain or Configure GSLB Domain dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for Binding or Unbinding a Domain to a GSLB Virtual Server” as shown:
   · Domain Name*—domainName (for example, www.mycompany.com)
     * A required parameter

5. Click Create.

6. Click OK.

To view the statistics of a domain by using the command line interface

At the command prompt, type:

stat gslb domain <name>

Example

stat gslb domain www.mycompany.com

Note: To view statistics for a particular GSLB domain, enter the name of the domain exactly as it was added to the NetScaler appliance. If you do not specify the domain name, or if you specify an incorrect domain name, statistics for all configured GSLB domains are displayed.
To view the statistics of a domain by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.

2. In GSLB Virtual Servers pane, select the GSLB Virtual Server (for example, Vserver-GSLB-1) and click Open.

3. In the Configure GSLB Virtual Server dialog box, on the Domains tab, select the domain, and then click Statistics.
Synchronizing a Configuration in a GSLB Setup

Typically, a GSLB setup has a few data centers with a GSLB site configured for each data center. In each NetScaler, participating in GSLB, configure one GSLB site as a local site and the others as remote sites. When you add another GSLB site at a later point of time, ensure that all the GSLB sites have the same configuration. To have the same configuration on all the GSLB sites, you can use the NetScaler appliance’s GSLB configuration synchronization option.

The NetScaler appliance from which you use the synchronization option is referred to as the ‘master node’ and the GSLB sites on which the configuration is copied as ‘slave nodes’. When you synchronize a GSLB configuration, the configurations on all the GSLB sites participating in the GSLB setup are made similar to that on the master node.

Synchronization (may also be referred to as ‘auto sync’) is carried out in the following manner:

- The master node finds the differences between the configuration of the master node and slave node, and changes the configuration of the slave node to make it similar to the master node.

  If you force a synchronization (use the ‘force sync’ option), the NetScaler deletes the GSLB configuration from the slave node and then configures the slave to make it similar to the master node.

- During synchronization, if a command fails, synchronization is not aborted.

- Synchronization is done only on the parent sites. If a GSLB site is configured as a child site, its configuration is not affected by synchronization.

Note: On the remote GSLB site RPC node, configure the firewall to accept auto-sync connections by specifying the remote site IP (cluster IP address for cluster setup) and port (3010 for RPC and 3008 for secure RPC). The source IP address that will be used for auto-sync is the NSIP of the master node (NSIP of the configuration coordinator in a cluster setup).

Limitations of synchronization:

- On the master node, the names of the remote GSLB sites must be identical to the names of sites configured on the NetScaler appliances hosting those sites.

- During the synchronization, traffic disruptions may occur.

- NetScaler can synchronize only up to 80000 lines of the configuration.

- Synchronization may fail:
  - If the spill over method is changed from CONNECTION to DYNAMIC CONNECTION.
Synchronizing a Configuration in a GSLB Setup

- If you interchange the site prefix of the GSLB services bound to a GSLB virtual server on the master node and then try to synchronize.

- If the RPC node passwords are different for NetScaler IP address (NSIP) and GSLB Site IP address.

- If the RPC node passwords are different for NetScaler IP address (NSIP) and loopback IP address.

- If you have configured the GSLB sites as High Availability (HA) pairs, the RPC node passwords of primary and secondary nodes should be same.

- If you rename any GLSB entity that are part of your GSLB configuration (use “show gslb runningConfig” command to display the GSLB configuration). You need to use the force sync option to synchronize the configuration to other GSLB sites.

**Note:** To overcome the limitations due to some settings in the GSLB configuration, you can use the force sync option. But, if you use the force sync option the GSLB entities are removed and re-added to the configuration and the GSLB statistics are reset to zero. Hence the traffic is disrupted during the configuration change.

Before you start the synchronization of a GSLB setup, make sure that:

- On all the GSLB sites including the master node, management access should be enabled for the IP address of the corresponding GSLB site. The IP address of a GSLB site must be an IP address owned by the NetScaler.

  For more information about adding the GSLB site IP addresses and enabling Management Access, see "Configuring a Basic GSLB Site" and "Configuring NetScaler-Owned IP Addresses".

- The GSLB configuration on the NetScaler appliance that is considered as the master node is complete and appropriate to be copied on all the sites.

- If you are synchronizing the GSLB configuration for the first time, all the sites participating in GSLB need to have the GSLB site entity of their respective local sites.

- You are not synchronizing sites that, by design, do not have the same configuration.

**Important:** After a GSLB configuration is synchronized, the configuration cannot be rolled back on any of the GSLB sites. Run the `sync gslb config` command only if you are sure that the synchronization process will not overwrite the configuration on the remote site. Site synchronization is undesirable when the local and remote sites have different configurations by design, and can lead to site outage. If some commands fail and some commands succeed, the successful commands cannot be rolled back. Also, the NetScaler configuration is not saved automatically after a GSLB configuration is synchronized. After synchronization, you must run the `save ns config` command explicitly at all sites.

To synchronize a GSLB configuration by using the command line interface

At the command prompt, type the following commands to synchronize GSLB sites and verify the configuration:
Synchronizing a Configuration in a GSLB Setup

- `sync gslb config [-preview | -forceSync <string> | -nowarn] [-debug]`
- `show gslb syncStatus`

**Example**

```
> sync gslb config
[WARNING]: Syncing config may cause configuration loss on other site.
Please confirm whether you want to sync-config (Y/N)? [N]:y
Sync Time: Dec 9 2011 10:56:9
Retrieving local site info: ok
Retrieving all participating gslb sites info: ok
Gslb_site1[Master]:
  Getting Config: ok
Gslb_site2[Slave]:
  Getting Config: ok
  Comparing config: ok
  Applying changes: ok
Done
```

**Parameters for synchronizing a GSLB configuration**

- `<no option>`
  If no option is passed to this command, synchronization happens on all the GSLB sites in the auto sync method.

- `preview (Preview)`
  Do not synchronize the GSLB sites, but only display the commands that would be applied on the slave node upon synchronization.

- `forceSync <string> (Force Sync)`
  Forcibly synchronize the specified site even if a dependent configuration on the remote site is preventing synchronization or if one or more GSLB entities on the remote site have the same name but are of a different type. Possible values:

  - The name of the remote site that you want to synchronize with the local site.

  - The string `all-sites`. If you specify `all-sites`, all the sites in the GSLB setup are synchronized with the site on the master node.

  **Note:** If you select the force sync option, the synchronization starts without displaying the commands that are going to be executed.
Suppress the warning and the confirmation prompt that are displayed before site synchronization begins. This option can be used in automation scripts that must not be interrupted by a prompt. Appears only if you use the `forceSync` and `debug` options.

**debug (Debug)**

Generate verbose output when synchronizing the GSLB sites. The `debug` option generates more verbose output than a `sync gslb config` command in which the option is not used, and is useful when you want to analyze synchronization issues.

---

**To synchronize a GSLB configuration by using the configuration utility**

1. In the navigation pane, click GSLB.

2. In the GSLB pane, under GSLB Configuration, click Synchronize configuration on remote sites.

3. In the Synchronize GSLB Configuration dialog box, select one of the following settings from the Synchronization Option list:
   - Preview
   - Force Sync
   - Debug

4. If you select Force Sync as the synchronization option, in the GSLB Site Name text box, type the name of the remote site that you want to synchronize with the local site, or type `all-sites`.

5. Click Run.

6. If you want to save the output of the Run command to your local system, click Save output text to a file.

7. Click Close.
Viewing and Configuring a GSLB Setup by Using the GSLB Visualizer

The configuration utility includes a GSLB Visualizer tool, which provides an alternative way to view and configure entities in a GSLB configuration. The visualizer displays all configured GSLB domains, GSLB services, GSLB sites, ADNS services, and any monitors that are bound to the services. It also displays all the load balancing, content switching, cache redirection, and Access Gateway virtual servers that the GSLB services represent.

If you want to view the configurations of remote GSLB sites, you must configure the sites with public IP addresses and enable management access for each of them.

You can use the GSLB Visualizer to perform the following GSLB configuration tasks:

- Add, view, and configure GSLB domains and GSLB services.
- View and configure GSLB sites and ADNS services for each site.
- View and configure any monitors that are bound to the services.
- View and configure the content switching, load balancing, cache redirection, or Access Gateway virtual server that each GSLB service represents.
- View statistics for GSLB domains, sites, ADNS services, and virtual servers.
- View configuration details of any displayed entity.
- View load balancing and content switching virtual servers.
- View bindings for GSLB services, ADNS services, monitors, and virtual servers.
- Enable and disable GSLB services, ADNS services, monitors, and virtual servers.
- Copy the properties of any displayed entity to a document or spreadsheet.
- Remove a domain from the GSLB setup.
- Save the visual representation of the GSLB setup as an image.
To open the Visualizer and locate an entity

1. In the navigation pane, click GSLB.

2. In the details pane, under Getting Started, click GSLB Visualizer, and then do the following.
   - To pan the view of the displayed image, click an empty area of the image, hold down the mouse button, and drag the image.
   - To adjust the viewable area, click Zoom In to increase or Zoom Out to decrease the size of the objects. You can readjust the viewable area by clicking Best Fit.
   - To locate a specific item, begin typing the item’s name in the Search field. Entities whose names match the typed characters are highlighted. Continue typing until the item is uniquely identified. To clear the Search field, click the x adjacent to the field.

To add a GSLB domain and/or configure GSLB services and sites for the domain

1. Open the GSLB Visualizer and click Domain. Alternatively, if domains already exist in the GSLB setup, click the name of an existing domain.

2. Under Related Tasks, click Add.

3. Follow the instructions in the GSLB Wizard to add a GSLB domain and configure GSLB services and sites for the domain.

To view the configuration details of an entity

Open the GSLB Visualizer and do one of the following:

- To view a brief summary of an entity, place the pointer on the entity. A brief summary of the entity appears at the bottom of the viewable area.
- To view the detailed configuration information of the entity, click the entity. The configuration details for that entity appear in the Details area.

To modify a GSLB domain, site, service, monitor, or ADNS service

Open the GSLB Visualizer and do one of the following:

- Click the entity that you want to modify. Then, under Related Tasks, click Open.
- Double-click the entity that you want to modify.
• Right-click the entity that you want to modify, and then click Open. (This option is not available for GSLB sites.)

To view the entities to which a GSLB service, ADNS service, monitor, or virtual server is bound

Open the GSLB Visualizer and do one of the following:

• Click the entity whose binding information you want to view, and then, under Related Tasks, click Show Bindings.

• Right-click the entity, and then click Show Bindings.

To view the Visualizer for load balancing and content switching virtual servers from the GSLB Visualizer

Open the GSLB Visualizer and do one of the following:

• Click the load balancing or content switching virtual server whose Visualizer you want to view, and then, under Related Tasks, click Visualizer.

• Right-click the virtual server, and then click Visualizer.

To view statistics for a GSLB service, site, ADNS service, or virtual server

Open the GSLB Visualizer and do one of the following:

• Click the entity whose statistics you want to view, and then, under Related Tasks, click Statistics.

• Right-click the entity whose statistics you want to view, and then click Statistics. (This option is not available for GSLB sites.)

To enable or disable a GSLB service, ADNS service, monitor, or virtual server

Open the GSLB Visualizer and do one of the following to enable or disable the entity:

• To enable the entity, click the entity and, under Related Tasks, click Enable. Alternatively, right-click the entity that you want to enable, and then click Enable.

• To disable the entity, click the entity and, under Related Tasks, click Disable. Alternatively, right-click the entity that you want to disable, and then click Disable.
To copy the properties of an entity to a document or spreadsheet

Open the GSLB Visualizer and do one of the following:

- Click the entity whose properties you want to copy, and then, under Related Tasks, click Copy Properties.
- Right-click the entity, and then click Copy. (This option is not available for GSLB sites.)

To save the visual representation of the GSLB setup as an image

1. Open the GSLB Visualizer.
2. If necessary, adjust the viewable area by using the Best Fit, Zoom In, and Zoom Out buttons.
3. Click Save Image.
4. In the Save Graph Image dialog box, browse to the folder in which you want to save the image.
5. In File Name text box, type the name, and then click Save.

To remove a domain from the GSLB setup

1. Open the GSLB Visualizer and do one of the following:
   - Click the domain that you want to remove, and then, under Related Tasks, click Remove.
   - Right-click the domain, and then click Remove.
2. Under Remove?, click Yes.
Configuring the Metrics Exchange Protocol (MEP)

The data centers in a GSLB setup exchange metrics with each other through the metrics exchange protocol (MEP), which is a proprietary protocol for the Citrix NetScaler. The exchange of the metric information begins when you create a GSLB site. These metrics comprise load, network, and persistence information.

MEP is required for health checking of data centers to ensure their availability. A connection for exchanging network metrics can be initiated by either of the data centers involved in the exchange, but a connection for exchanging site metrics is always initiated by the data center with the lower IP address. By default, the data center uses a subnet IP address (SNIP) or a mapped IP address (MIP) to establish a connection to the IP address of a different data center. However, you can configure a specific SNIP, MIP, the NetScaler IP address (NSIP), or a virtual IP address (VIP) as the source IP address for metrics exchange. The communication process between GSLB sites uses TCP port 3011 or 3009, so this port must be open on firewalls that are between the NetScaler appliances.

**Note:** You cannot configure a GSLB site IP address as the source IP address for site metrics exchange.

If the source and target sites for a MEP connection (the site that initiates a MEP connection and the site that receives the connection request, respectively) have both private and public IP addresses configured, the sites exchange MEP information by using the public IP addresses.

You can also bind monitors to check the health of remote services. When monitors are bound, metric exchange does not control the state of the remote service. If a monitor is bound to a remote service and metrics exchange is enabled, the monitor controls the health status. Binding the monitors to the remote service allows the NetScaler to interact with a non-NetScaler load balancing device. The NetScaler can monitor non-NetScaler devices but cannot perform load balancing on them. The NetScaler can monitor non-NetScaler devices, and can perform load balancing on them if monitors are bound to all GSLB services and only static load balancing methods (such as the round robin, static proximity, or hash-based methods) are used.
Configuring Site Metric Exchange

Site metrics exchanged between the GSLB sites include the status of each load balancing and content switching virtual server, the current number of connections, the current packet rate, and current bandwidth usage information.

The NetScaler appliance needs this information to perform load balancing between the sites. The site metric exchange interval is 1 second. A remote GSLB service must be bound to a local GSLB virtual server to enable the exchange of site metrics with the remote service.

To enable or disable site metric exchange by using the command line interface

At a command prompt, type the following commands to enable or disable site metric exchange and verify the configuration:

- `set gslb site <siteName> -metricExchange(ENABLED|DISABLED)`
- `show gslb site <siteName>

Example

```
set gslb site Site-GSLB-East-Coast -metricExchange ENABLED
set gslb site Site-GSLB-East-Coast -metricExchange DISABLED
show gslb site Site-GSLB-East-Coast
```

To enable or disable site metric exchange by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Sites.
2. In the details pane, select the site, and then click Open.
3. In the Configure GSLB Site dialog box, select or clear the check box next to the Metric Exchange and click OK.
Configuring Network Metric Information Exchange

You can enable or disable the exchange of round trip time (RTT) information about the client’s local DNS when the GSLB dynamic method (RTT) is enabled. This information is exchanged every 5 seconds.

For details about changing the GSLB method to a method based on RTT, see Changing the GSLB Method.

To enable or disable network metric information exchange by using the command line interface

At the command prompt, type the following commands to enable or disable network metric information exchange and verify the configuration:

- `set gslb site <siteName> -nwmetricExchange (ENABLED|DISABLED)`
- `show gslb site <<siteName>`

Example

```
set gslb site Site-GSLB-East-Coast -nwmetricExchange ENABLED
set gslb site Site-GSLB-East-Coast -nwmetricExchange DISABLED
show gslb site Site-GSLB-East-Coast
```

To enable or disable network metric information exchange by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Sites.
2. In the details pane, select the site, and then click Open.
3. In the Configure GSLB Site dialog box, select or clear the check box next to the Network Metric Exchange and click OK.
Configuring Persistence Information Exchange

You can enable or disable the exchange of persistence information at each site. This information is exchanged every 5 seconds between NetScaler appliances participating in GSLB.

For details about configuring persistence, see "Configuring Persistent Connections".

To enable/disable persistence information exchange by using the command line interface

At the command prompt, type the following commands to enable or disable persistence information exchange and verify the configuration:

- `set gslb site <siteName> -sessionExchange (ENABLED|DISABLED)`
- `show gslb site <siteName>`

Example

```
set gslb site Site-GSLB-East-Coast -sessionExchange ENABLED
set gslb site Site-GSLB-East-Coast -sessionExchange DISABLED
show gslb site Site-GSLB-East-Coast
```

To enable/disable persistence information exchange by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Sites.
2. In the details pane, select the site, and then click Open.
3. In the Configure GSLB Site dialog box, select or clear the check box next to the Persistence Session Entry Exchange and click OK.
GSLB site-to-site communication is between the remote procedure call (RPC) nodes that are associated with the communicating sites. A master GSLB site establishes connections with slave sites to synchronize GSLB configuration information and to exchange site metrics.

An RPC node is created automatically when a GSLB site is created, and is assigned an internally generated user name and password. The NetScaler appliance uses this user name and password to authenticate itself to remote GSLB sites during connection establishment. No configuration steps are necessary for an RPC node, but you can specify a password of your choice, enhance security by encrypting the information that GSLB sites exchange, and specify a source IP address for the RPC node.

The appliance needs a NetScaler-owned IP address to use as the source IP address when communicating with other GSLB sites. By default, the RPC nodes use either a subnet IP (SNIP) address or a mapped IP (MIP) address, but you might want to specify an IP address of your choice.
Changing the Password of an RPC Node

You can secure the communication between sites in your GSLB setup by changing the password of each RPC node. After you change the password for the RPC node of the local site, you must manually propagate the change to the RPC node at each of the remote sites.

The password is stored in encrypted form. You can verify that the password has changed by using the show rpcNode command to compare the encrypted form of the password before and after the change.

To change the password of an RPC node by using the command line interface

At the command line, type the following commands to change the password of an RPC node:

- `set ns rpcNode <IPAddress> {-password}`
- `show ns rpcNode`

Example

```
> set rpcNode 192.0.2.4 -password mypassword
Done
> show rpcNode
.
.
.
2) IPAddress: 192.0.2.4 Password: d336004164d4352ce39e
   SrcIP: *       Secure: OFF
Done
> 
```

To unset the password of an RPC node by using the command line interface

The unset rpcNode command does not accept the IP address of an RPC node as an argument. When you use the unset rpcNode command, the appliance always modifies the RPC node of the NSIP address.

To unset the password of an RPC node by using the NetScaler command line, type the unset rpcNode command and the password parameter, without a value.
Parameters for changing the password of an RPC node

**IPAddress**

The IP address of the GSLB site to which the RPC node belongs. This is the value of the IPAddress field in the output of the show rpcNode CLI command.

**password**

The password that the RPC node must use to authenticate itself to other nodes in the GSLB configuration. By default, a password is configured for all RPC nodes. If you change the password for an RPC node, make sure you propagate that change to the RPC node at each of the other sites. Maximum length: 31 characters.

To change the password of an RPC node by using the configuration utility

1. In the navigation pane, expand Network, and then click RPC.

2. In the details pane, click the RPC node for which you want to change the password, and then click Open.

3. In the Configure RPC Node dialog box, in Password and Confirm Password, specify the password that you want the RPC node to use.
Encrypting the Exchange of Site Metrics

You can secure the information that is exchanged between GSLB sites by setting the secure option for the RPC nodes in the GSLB setup. With the secure option set, the NetScaler appliance encrypts all communication sent from the node to other RPC nodes.

To encrypt the exchange of site metrics by using the command line interface

At the command prompt, type the following commands to encrypt the exchange of site metrics and verify the configuration:

- set ns rpcNode <IPAddress> [-secure { YES | NO }]
- show rpcNode

Example

> set rpcNode 192.0.2.4 -secure YES
Done
> show rpcNode
3) IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e SrcIP:  192.0.2.3 Secure:  ON
Done
>

To unset the secure parameter by using the command line interface

The unset rpcNode command does not accept the IP address of an RPC node as an argument. When you use the unset rpcNode command, the appliance always modifies the RPC node of the NSIP address.

To unset the secure parameter by using the NetScaler command line, type the unset rpcNode command and the secure parameter, without a value.
Parameters for encrypting the exchange of site metrics

**IPAddress**

The IP address of the GSLB site to which the RPC node belongs. This is the value of the IPAddress field in the output of the show rpcNode CLI command.

**secure (Secure)**

Encrypt all communication sent from the RPC node. Possible values: YES, NO. Default: NO.

To encrypt the exchange of site metrics by using the NetScaler configuration utility

1. In the navigation pane, expand Network, and then click RPC.

2. In the details pane, click the RPC node whose communication you want to encrypt, and then click Open.

3. In the Configure RPC Node dialog box, click Secure.

4. Click OK.
Configuring the Source IP Address for an RPC Node

By default, the NetScaler appliance uses a NetScaler-owned subnet IP (SNIP) address or mapped IP (MIP) address as the source IP address for an RPC node, but you can configure the appliance to use a specific SNIP address or MIP address. If neither a SNIP address nor a MIP address is available, the GSLB site cannot communicate with other sites. In such a scenario, you must configure either the NetScaler IP (NSIP) address or a virtual IP (VIP) address as the source IP address for an RPC node. A VIP address can be used as the source IP address of an RPC node only if the RPC node is a remote node. If you configure a VIP address as the source IP address and remove the VIP address, the appliance uses a SNIP address or a MIP address.

To specify a source IP address for an RPC node by using the command line interface

At the command prompt, type the following commands to change the source IP address for an RPC node and verify the configuration:

- `set ns rpcNode <IPAddress> [-srcIP <ip_addr|ipv6_addr|*>]`
- `show ns rpcNode`

Example

```
> set rpcNode 192.0.2.4 -srcIP 192.0.2.3
Done
> show rpcNode
.
.
.
2) IPAddress: 192.0.2.4 Password: d336004164d4352ce39e SrcIP: 192.0.2.3 Secure: OFF
Done
> 
```

To unset the source IP address parameter by using the command line interface

The unset rpcNode command does not accept the IP address of an RPC node as an argument. When you use the unset rpcNode command, the appliance always modifies the RPC node of the NSIP address.
To unset the source IP address parameter by using the NetScaler command line, type the unset rpcNode command and the srcIP parameter, without a value.

**Parameters for specifying a source IP address of an RPC node**

**IPAddress**

The IP address of the GSLB site to which the RPC node belongs. This is the value of the IPAddress field in the output of the show rpcNode CLI command.

**srcIP**

The subnet IP (SNIP) address, mapped IP (MIP) address, NetScaler IP (NSIP) address, or virtual IP (VIP) address that you want the appliance to use as the source IP address for exchanging site metrics. By default, the appliance uses a SNIP address or a MIP address, but you can configure the node to use a SNIP address or MIP address of your choice, or the NSIP address. For a remote node, you also have the option of configuring a VIP address as the source IP address. If neither a SNIP address nor a MIP address is available, and you have not configured a source IP address, a GSLB site cannot exchange site metrics with other sites. The default setting is an asterisk (*), which indicates that the default setting (SNIP address or MIP address) is being used.

**To specify a source IP address for an RPC node by using the NetScaler configuration utility**

1. In the navigation pane, expand Network, and then click RPC.
2. In the details pane, click the RPC node for which you want to assign a specific source IP address for site metrics exchange, and then click Open.
3. In the Configure RPC Node dialog box, in Source IP Address, enter the IP address that you want the RPC node to use as the source IP address.
Customizing Your GSLB Configuration

Once your basic GSLB configuration is operational, you can customize it by modifying the bandwidth of a GSLB service, configuring CNAME based GSLB services, static proximity, dynamic RTT, persistent connections, or dynamic weights for services, or changing the GSLB Method.

You can also configure monitoring for GSLB services to determine their states.

These settings depend on your network deployment and the types of clients you expect to connect to your servers.
Modifying Maximum Connections or Maximum Bandwidth for a GSLB Service

You can restrict the number of new clients that can simultaneously connect to a load balancing or content switching virtual server by configuring the maximum number of clients and/or the maximum bandwidth for the GSLB service that represents the virtual server.

To modify the maximum clients or bandwidth of a GSLB service by using the command line interface

At the command prompt, type the following command to modify the maximum number of client connections or the maximum bandwidth of a GSLB service and verify the configuration:

- set gslb service <serviceName> [-maxClients <positive_integer>] [-maxBandwidth <positive_integer>]
- show gslb service <serviceName>

Example

set gslb service Service-GSLB-1 -maxBandwidth 100 -maxClients 100
show gslb service Service-GSLB-1

Parameters for modifying the maximum clients or bandwidth of a GSLB service

maxClients

The maximum number of simultaneous client connections that the GSLB service can handle.

maxBandwidth

The maximum bandwidth, in kbps, that a GSLB service can handle.
To modify the maximum clients or bandwidth of a GSLB service by using the configuration utility

1. In the navigation pane, expand GSLB and click Services.

2. In the details pane, select the service to be modified and click Open.

3. In the Configure GSLB Service dialog box specify values for one or both of the following parameters, which correspond to parameters described in “Parameters for modifying the maximum clients or bandwidth for a service” as shown:
   
   - Max Clients—maxClients
   - Max Bandwidth—maxBandwidth

4. Click OK.

5. Verify that the Details area displays the values that you entered.
Creating CNAME-Based GSLB Services

To configure a GSLB service, you can use the IP address of the server or a canonical name of the server. If you want to run multiple services (like an FTP and a Web server, each running on different ports) from a single IP address or run multiple HTTP services on the same port, with different names, on the same physical host, you can use canonical names (CNAMEs) for the services.

For example, you can have two entries in DNS as ftp.example.com and www.example.com for FTP services and HTTP services on the same domain, example.com. CNAME-based GSLB services are useful in a multilevel domain resolver configuration or in multilevel domain load balancing. Configuring a CNAME-based GSLB service can also help if the IP address of the physical server is likely to change.

If you configure CNAME-based GSLB services for a GSLB domain, when a query is sent for the GSLB domain, the NetScaler appliance provides a CNAME instead of an IP address. If the A record for this CNAME record is not configured, the client must query the CNAME domain for the IP address. If the A record for this CNAME record is configured, the NetScaler provides the CNAME with the corresponding A record (IP address). The NetScaler appliance handles the final resolution of the DNS query, as determined by the GSLB method. The CNAME records can be maintained on a different NetScaler appliance or on a third-party system.

In an IP-address-based GSLB service, the state of a service is determined by the state of the server that it represents. However, a CNAME-based GSLB service has its state set to UP by default; the virtual server IP (VIP) address or metric exchange protocol (MEP) are not used for determining its state. If a desktop-based monitor is bound to a CNAME-based GSLB service, the state of the service is determined according to the result of the monitor probes.

You can bind a CNAME-based GSLB service only to a GSLB virtual server that has the DNS Record Type as CNAME. Also, a NetScaler appliance can contain at most one GSLB service with a given CNAME entry.

The following are some of the features supported for a CNAME-based GSLB service:

- GSLB-policy based site affinity is supported, with the CNAME as the preferred location.
- Source IP persistence is supported. The persistency entry contains the CNAME information instead of the IP address and port of the selected service.

The following are the limitations of CNAME-based GSLB services:

- Site persistence is not supported, because the service referenced by a CNAME can be present at any third-party location.
- Multiple-IP-address response is not supported because one domain cannot have multiple CNAME entries.
- Source IP Hash and Round Robin are the only load balancing methods supported. The Static Proximity method is not supported because a CNAME is not associated with an IP address and static proximity can be maintained only according to the IP addresses.
Note: The Empty-Down-Response feature should be enabled on the GSLB virtual server to which you bind the CNAME-based GSLB service. If you enable the Empty-Down-Response feature, when a GSLB virtual server is DOWN or disabled, the response to a DNS query, for the domains bound to this virtual server, contains an empty record without any IP addresses, instead of an error code.

To create a CNAME-based GSLB service by using the command line interface

At the command prompt, type:

```
add gslb service <serviceName> -cnameEntry <string> -siteName <string>
```

**Example**

```
add gslb service Service-GSLB-1 -cnameEntry transport.mycompany.com -siteName Site-GSLB-East-Coast
add gslb service Service-GSLB-2 -cnameEntry finance.mycompany.com -siteName Site-GSLB-West-Coast
```

**Parameters for creating a CNAME based GSLB service**

- **serviceName (Service Name)**
  The name of the CNAME-based GSLB service being configured.

- **cnameEntry (DNS Canonical Name)**
  The canonical name of the GSLB domain that the GSLB service will handle.

- **siteName (Site Name)**
  The name of the GSLB site that the GSLB service represents.
Creating CNAME-Based GSLB Services

To create a CNAME-based GSLB service by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Services.

2. In the details pane, click Add.

3. In the Create GSLB Service dialog box, set the following parameters:
   - Service Name*
   - Site Name*
   - Type should be Canonical name based.
   - DNS Canonical name*  
     * A required parameter

4. Click Create, and then click Close.
Changing the GSLB Method

Unlike traditional DNS servers that simply respond with the IP addresses of the configured servers, a NetScaler appliance configured for GSLB responds with the IP addresses of the services, as determined by the configured GSLB method. By default, the GSLB virtual server is set to the least connection method. If all GSLB services are down, the NetScaler responds with the IP addresses of all the configured GSLB services.

GSLB methods are algorithms that the GSLB virtual server uses to select the best-performing GSLB service. After the host name in the Web address is resolved, the client sends traffic directly to the resolved service IP address.

The NetScaler appliance provides the following GSLB methods:

- Round Robin
- Least Connections
- Least Response Time
- Least Bandwidth
- Least Packets
- Source IP Hash
- Custom Load
- Round Trip Time (RTT)
- Static Proximity

For GSLB methods to work with a remote site, either MEP must be enabled or explicit monitors must be bound to the remote services. If MEP is disabled, RTT, Least Connections, Least Bandwidth, Least Packets and Least Response Time methods default to Round Robin.

The Static Proximity and RTT load balancing methods are specific to GSLB.
Specifying a GSLB Method Other than Static Proximity or Dynamic (RTT)

For information about the Round Robin, Least Connections, Least Response Time, Least Bandwidth, Least Packets, Source IP Hash, or Custom Load method, see "Load Balancing."

To change the GSLB method by using the command line interface

At the command prompt, type:

```
set gslb vserver <name> -lbMethod GSLBMethod
```

Example

```
set gslb vserver Vserver-GSLB-1 -lbMethod ROUNDROBIN
```

To change the GSLB method by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the details pane, select a GSLB virtual server and click Open.
3. In the Configure GSLB Virtual Server dialog box, on the Method and Persistence tab, under Method, select a method from the Choose Method list.
4. Click OK, and verify that the method you selected appears under Details at the bottom of the screen.
Configuring Static Proximity

The static proximity method for GSLB uses an IP-address based static proximity database to determine the proximity between the client’s local DNS server and the GSLB sites. The NetScaler appliance responds with the IP address of a site that best matches the proximity criteria.

If two or more GSLB sites at different geographic locations serve the same content, the NetScaler appliance maintains a database of IP address ranges and uses the database for decisions about the GSLB sites to which to direct incoming client requests.

For the static proximity method to work, you must either configure the NetScaler appliance to use an existing static proximity database populated through a location file or add custom entries to the static proximity database. After adding custom entries, you can set their location qualifiers. After configuring the database, you are ready to specify static proximity as the GSLB method.
Adding a Location File to Create a Static Proximity Database

A static proximity database is a UNIX-based ASCII file. Entries added to this database from a location file are called static entries. Only one location file can be loaded on a NetScaler appliance. Adding a new location file overrides the existing file. The number of entries in the static proximity database is limited by the configured memory in the NetScaler appliance.

The static proximity database can be created in the default format or in a format derived from commercially configured third party databases (such as www.maxmind.com and www.ip2location.com).

These databases vary in the details they provide. There is no strict enforcement of the database file format, except that the default file has format tags. The database files are ASCII files that use a comma as the field delimiter. There are differences in the structure of fields and the representation of IP addresses in the locations.

The format parameter describes the structure of the file to the NetScaler appliance. Specifying an incorrect value for the format option can corrupt the internal data.

**Note:** The default location of the database file is /var/netscaler/locdb, and on a high availability (HA) setup, an identical copy of the file must be present in the same location on both NetScaler appliances.

The following abbreviations are used in this section:

- **CSHN.** Short name of a country based on the country code standard of ISO-3166.
- **LCN.** Long name of the country.
- **RC.** Region code based on ISO-3166-2 (for US and Canada). The region code “FIPS-10-4” is used for the other regions.

**Note:** Some databases provide short country names according to ISO-3166 and long country names as well. The NetScaler uses short names when storing and matching qualifiers.

To create a static proximity database, log on to the UNIX shell of the NetScaler appliance and use an editor to create a file with the location details in one of the NetScaler-supported formats.

**To add a static location file by using the command line interface**

At the command prompt, type:

```
add locationFile <locationFile> [-format <format>]
```
Example

> add locationFile /var/nsmapi/locdb/nsgeo1.0 -format netscaler
Done
> show locationFile
Location File: /var/nsmapi/locdb/nsgeo1.0
Format: netscaler
Done
>

Parameters for adding a static location file

locationFile

The name of the location file. Must include the absolute path to the file. If the full path
is not given, the default path /var/netscaler/locdb is assumed. In a high availability
setup, the static database must be stored in the same location on both systems.

format

The format of the location file. Possible values: netscaler, ip-country, ip-country-isp,
ip-country-region-city, ip-country-region-city-isp, geoip-country, geoip-region,

To add a static location file by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Location.
2. In the details pane, click the Static Database tab, and then click Add.
3. In the Create Location File dialog box, in the Location Filename text box, type the
   name of the location file, or click Browse to select the location file (for example, type
   or select /var/nsmapi/locdb/nsgeo1.0).

   Note: The location file must be existing on the NetScaler appliance.
4. In the Location Format box, select the format of the location (for example, netscaler).
5. Click Create and click Close.

You can view an imported location file database by using the View Database dialog box in
the configuration utility. There is no NetScaler command line equivalent.
To view a static location file by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Location.

2. On the Static Database tab, select the location file, and then click View Database.

3. In the View Database dialog box, and click Find to use the following controls to filter and sort the database information.
   a. **Search In.** Choose the field to search from the drop-down list.
   b. **Criterion.** Choose the search criterion from the drop-down list. The list contains a standard set of search criteria. "Contains" is the default choice.
   c. **Look For.** Type the text or number to search for.
   d. **Find Now.** Click this button to perform the search.
   e. **Clear.** Click this button to reset the search controls to their initial state.
4. Click Close to close the View Database dialog box and return to the Static Database tab.

To convert a location file into the netscaler format

By default, when you add a location file, it is saved in the netscaler format. You can convert a location file of other formats into the netscaler format. See the list of supported formats in the table, *Parameters for adding a static location file*.

**Note:** The nsmap option can be accessed only from the command line interface. The conversion is possible only into the netscaler format.

To convert the static database format, at the NetScaler command prompt, type the following command:

```
nsmmap -f <inputFileFormat> -o <outputFileName> <inputFileName>
```

**Example**

```
nsmmap -f ip-country-region-city -o nsfile.ns ip-country-region-city.cvs
```
Adding Custom Entries to a Static Proximity Database

Custom entries take precedence over static entries in the proximity database. You can add a maximum of 50 custom entries. For a custom entry, denote all omitted qualifiers with an asterisk (*) and, if qualifiers have a period or space in the name, enclose the parameter in double quotation marks. The first 31 characters are evaluated for each qualifier. You can also provide the longitude and latitude of the geographical location of the IP address-range for selecting a service with the static proximity GSLB method.

To add custom entries by using the command line interface

At the command prompt, type the following commands to add a custom entry to the static proximity database and verify the configuration:

- add location <IPfrom> <IPto> <preferredLocation> [-longitude <integer>[-latitude <integer>]]
- show location

Example

>add location 192.168.100.1 192.168.100.100 *.us.ca.mycity

>show location
To add custom entries by using the configuration utility

1. Navigate to GSLB > Location.

2. On the Custom Entries tab, click Add.

3. Specify values for the following parameters, which correspond to parameters described in “Parameters for adding custom entries” as shown:
   
   - From IP Address*—IPfrom
   - To IP Address*—IPto
   - Location Name*—preferredLocation
   * A required parameter

4. Click Create, and then click Close. The custom entry that you have created appears on the Custom Entries tab.
Setting the Location Qualifiers

The database used to implement static proximity contains the location of the GSLB sites. Each location contains an IP address range and up to six qualifiers for that range. The qualifiers are literal strings and are compared in a prescribed order at run time. Every location must have at least one qualifier. The meaning of the qualifiers (context) is defined by the qualifier labels, which are user defined. The NetScaler has two built-in contexts:

Geographic context, which has the following qualifier labels:

- Qualifier 1 - “Continent”
- Qualifier 2 - “Country”
- Qualifier 3 - “State”
- Qualifier 4 - “City”
- Qualifier 5 - “ISP”
- Qualifier 6 - “Organization”

Custom entries, which have the following qualifier labels:

- Qualifier 1 - “Qualifier 1”
- Qualifier 2 - “Qualifier 2”
- Qualifier 3 - “Qualifier 3”
- Qualifier 4 - “Qualifier 4”
- Qualifier 5 - “Qualifier 5”
- Qualifier 6 - “Qualifier 6”

If the geographic context is set with no Continent qualifier, Continent is derived from Country. Even the built-in qualifier labels are based on the context, and the labels can be changed. These qualifier labels specify the locations mapped with the IP addresses used to make static proximity decisions.

To perform a static proximity-based decision, the NetScaler appliance compares the location attributes (qualifiers) derived from the IP address of the local DNS server resolver with the location attributes of the participating sites. If only one site matches, the appliance returns the IP address of that site. If there are multiple matches, the site selected is the result of a round robin on the matching GSLB sites. If there is no match, the site selected is a result of a round robin on all configured sites. A site that does not have any qualifiers is considered a match.
To set the location qualifiers by using the command line interface

At the command prompt, type:

```
set locationparameter -context <context> -q1label <string> [-q2label <string>] [-q3label <string>] [-q4label <string>] [-q5label <string>] [-q6label <string>]
```

Example

```
set locationparameter -context custom -q1label asia
```

Parameters for setting the location qualifiers

- **context**
  
The context in which a static proximity decision is made. Possible Values: geographic, custom.

- **q1label**
  
The label for the 1st qualifier.

- **q2label**
  
The label for the 2nd qualifier.

- **q3label**
  
The label for the 3rd qualifier.

- **q4label**
  
The label for the 4th qualifier.

- **q5label**
  
The label for the 5th qualifier.

- **q6label**
  
The label for the 6th qualifier.
To set the location qualifiers by using the configuration utility

1. In the navigation pane, expand GSLB and click Location.
2. Click Location Parameters.
3. In the Context drop-down list, select the appropriate context (for example, Custom).
4. In the Qualifier Label -1 text box, type the qualifier (for example asia).
5. Click OK.
Specifying the Proximity Method

When you have configured the static proximity database, you are ready to specify static proximity as the GLSB method.

To specify static proximity by using the command line interface

At the command prompt, type the following commands to configure static proximity and verify the configuration:

- `set gslb vserver <name> -lbMethod STATICPROXIMITY`
- `show gslb vserver <name>`

Example

```
set gslb vserver Vserver-GSLB-1 -lbMethod STATICPROXIMITY
show gslb vserver
```

To specify static proximity by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. In the GSLB Virtual Servers pane, select the GSLB Virtual Server that you want to set to static proximity (for example, vserver-GSLB-1).
3. Click Open.
4. On the Method and Persistence tab, under Method, select Static Proximity from the Choose Method list.
5. Click OK.
6. Verify that the Details pane shows static proximity as the GSLB method.
Dynamic round trip time (RTT) is a measure of time or delay in the network between the client’s local DNS server and a data resource. To measure dynamic RTT, the NetScaler appliance probes the client’s local DNS server and gathers RTT metric information. The appliance then uses this metric to make its load balancing decision. Global server load balancing monitors the real-time status of the network and dynamically directs the client request to the data center with the lowest RTT value.

When a client’s DNS request for a domain comes to the NetScaler appliance configured as the authoritative DNS for that domain, the appliance uses the RTT value to select the IP address of the best performing site to send it as a response to the DNS request.

The NetScaler appliance uses different mechanisms, such as ICMP echo request / reply (PING), UDP, and TCP to gather the RTT metrics for connections between the local DNS server and participating sites. The appliance first sends a ping probe to determine the RTT. If the ping probe fails, a DNS UDP probe is used. If that probe also fails, the appliance uses a DNS TCP probe.

These mechanisms are represented on the NetScaler appliance as Load Balancing Monitors and are easily identified due to their use of the “ldns” prefix. The three monitors, in their default order, are:

- ldns-ping
- ldns-dns
- ldns-tcp

These monitors are built into the appliance and are set to safe defaults, but may be customized just like any other monitor on the appliance.

The default order may also be changed by setting it explicitly as a GSLB parameter. For example, to set the order to be the DNS UDP query followed by the PING and then TCP, type the following command:

```
set gslb parameter -ldnsprobeOrder DNS PING TCP
```

Unless they have been customized, the NetScaler appliance performs UDP and TCP probing on port 53, however unlike regular load balancing monitors the probes need not be successful in order to provide valid RTT information. ICMP port unavailable messages, TCP Resets and DNS error responses, which would usually constitute a failure are all acceptable for calculating the RTT value.

Once the RTT data has been compiled, the NetScaler uses the proprietary metrics exchange protocol (MEP) to exchange RTT values between participating sites. After calculating RTT metrics, the appliance sorts the RTT values to identify the data center with the best (smallest) RTT metric.

If RTT information is not available (for example, when a client’s local DNS server accesses the site for the first time), the NetScaler appliance selects a site by using the round robin
method and directs the client to the site.

To configure the dynamic method, you configure the site's GSLB virtual server for dynamic RTT. You can also set the interval at which local DNS servers are probed to a value other than the default.
Configuring a GSLB Virtual Server for Dynamic RTT

To configure a GSLB virtual server for dynamic RTT, you specify the RTT load balancing method.

The NetScaler appliance regularly validates the timing information for a given local server. If a change in latency exceeds the configured tolerance factor, the appliance updates its database with the new timing information and sends the new value to other GSLB sites by performing a MEP exchange. The default tolerance factor is 5 milliseconds (ms).

The RTT tolerance factor must be the same throughout the GSLB domain. If you change it for a site, you must configure identical RTT tolerance factors on all NetScaler appliances deployed in the GSLB domain.

To configure a GSLB virtual server for dynamic RTT by using the command line interface

At the command prompt, type:

```
set gslb vserver <name> -lbMethod RTT -tolerance <value>
```

**Example**

```
set gslb vserver Vserver-GSLB-1 -lbMethod RTT -tolerance 10
```

Parameters for configuring the dynamic RTT load balancing method

**name**

The name of the GSLB virtual server for which you are configuring the load balancing method.

**lbMethod**

The load balancing method being configured for the GSLB virtual server. For the dynamic method, specify RTT.

**tolerance**
The minimum number of milliseconds by which the RTT metric must change to trigger an update of this metric in the database.

**To configure a GSLB virtual server for dynamic RTT by using the configuration utility**

1. In the navigation pane, expand GSLB and click Virtual Servers.

2. In the GSLB Virtual Servers pane, select the GSLB Virtual server that you want to set to dynamic RTT (for example, vserver-GSLB-1).

3. Click Open.

4. On the Method and Persistence tab, under Method, select Dynamic Method (RTT) from the Choose Method list.

5. To change the tolerance factor, type the new value in the Tolerance (ms) text box. (For a description of the tolerance factor, see “Parameters for configuring the dynamic RTT load balancing method.”)

6. Click OK.
Setting the Probing Interval of Local DNS Servers

The NetScaler appliance uses different mechanisms, such as ICMP echo request / reply (PING), TCP, and UDP to obtain RTT metrics for connections between the local DNS server and participating GSLB sites. By default, the appliance uses a ping monitor and probes the local DNS server every 5 seconds. The appliance then waits 2 seconds for the response and, if a response is not received in that time, it uses the TCP DNS monitor for probing.

However, you can modify the time interval for probing the local DNS server to accommodate your configuration.

To modify the probing interval by using the command line interface

At the command prompt, type:

```
set lb monitor <monitorName> <type> -interval <integer> <units> -resptimeout <integer> <units>
```

Example

```
set lb monitor monitor-HTTP-1 HTTP -interval 10 sec -resptimeout 5 sec
```

Parameters for modifying the probing interval

- **interval**
  
  Interval at which probes should be sent.

- **units**
  
  Monitor-interval/resptimeout units. Possible values are SEC, MSEC, and MIN. Default value is NSTMUNT_SEC.

- **type**
  
  The type of monitor being configured. The following are valid monitor types:
  
  - **TCP** - The NetScaler appliance establishes a TCP connection with the monitor destination and then closes the connection. If the NetScaler observes TCP traffic to the destination, it does not send TCP monitoring requests. This occurs if LRTM is
disabled. By default, LRTM is disabled on this monitor. This is done only for UDP, and the service goes down immediately.

- **TCP-ECV** - The NetScaler appliance establishes a TCP connection with the monitor destination. When the connection is established, the appliance sends specific data to the service by using the -send parameter, and the appliance and expects a specific response through the receive parameter.

- **HTTP** - the NetScaler establishes a TCP connection with the monitor destination. After the connection is established, the NetScaler sends HTTP requests and compares the response code, in the response from the service, with the configured set of response codes.

- **HTTP-ECV** - the NetScaler establishes a TCP connection with the monitor destination. When the connection is established, the NetScaler sends the HTTP data specified by the -send parameter to the service and expects the HTTP response that the -receive parameter specifies. (HTTP body part, not including HTTP headers.) Empty response data matches any response. Expected data may be anywhere in the first 24K bytes of the HTTP body of the response.

- **PING** - the NetScaler sends an ICMP echo request to the destination of the monitor and expects an ICMP echo response.

**Note:** The NetScaler also supports FTP, UDP, DNS, UDP-ECV, TCPS, HTTPS, TCPS-ECV, HTTPS-ECV, LDNS-PING, LDNS-TCP, and LDNS-DNS monitors.

For more information about monitors, see Load Balancing.

**resptimeout**

Interval after which probe should be marked as FAILED.

---

**To modify the probing interval by using the configuration utility**

- In the navigation pane, expand Load Balancing and click Monitors.

- Select the monitor that you want to modify (for example, ping).

- Click Open.

- In the Configure Monitor dialog box, on the Standard Parameters tab, specify values for the following parameters, which correspond to parameters described in “Parameters for modifying the probing interval” as shown:

  - Interval—interval

  - Response Time-out—resptimeout (type the interval after which the probe should be marked as FAILED. Specify whether the value represents minutes, milliseconds, or seconds by selecting a value from the adjacent list)

- Click OK.
Configuring Persistent Connections

Persistence ensures that a series of client requests for a particular domain name is sent to the same data center instead of being load balanced. If persistence is configured for a particular domain, it takes precedence over the configured GSLB method. Persistence is useful for deployments that deal with e-commerce, such as shopping card usage, where the server needs to maintain the state of the connection to track the transaction. To maintain the state of connection, you must configure persistence on a virtual server. With persistence configured, NetScaler selects a data center to process a client request and forwards the IP address of the selected data center for all subsequent DNS requests. If the configured persistence applies to a site that is down, the NetScaler appliance uses a GSLB method to select a new site, and the new site becomes persistent for subsequent requests from the client.

The GSLB virtual server is responsible for DNS-based site persistence, and it controls the site persistence for a remote GSLB service. The NetScaler appliance supports persistence based on the source IP address or on HTTP cookies.

When you bring a physical service DOWN with a delay time, the physical service goes into the transition out of service (TROFS) state. Site persistence is supported as long as the service is in the TROFS state. That is, if the same client sends a request for the same service within the specified delay time after a service is marked TROFS, the same GSLB site (data center) services the request.

**Note:** If connection proxy is specified as the site persistence method and if you also want to configure persistence of the physical servers, do not configure SOURCEIP persistence. When the connection is proxied, an IP address owned by the NetScaler is used, and not the actual IP address of the client. Configure methods such as cookie persistence or rule-based persistence on the load balancing virtual server.
Configuring Persistence Based on Source IP Address

With source-IP persistence, when a DNS request is received at a data center, the NetScaler appliance first looks for an entry in the persistence table and, if an entry for the local DNS server exists and the server mentioned in the entry is configured, the IP address of that server is sent as the DNS response.

For the first request from a particular client, the NetScaler appliance selects the best GSLB site for the request and sends its IP address to the client. Since persistence is configured for the source IP address of the client, all subsequent requests by that client or another local DNS server in the same IP subnet are sent the IP address of the GSLB site that was selected for the first request.

For source-IP address based persistence, the same set of persistence identifiers must be configured on the GSLB virtual servers in all data centers. A persistence identifier is a number used by the data centers to identify a particular GSLB virtual server. A cookie transmits the persistence identifier, enabling the NetScaler appliance to identify the domain so that it can forward all appropriate requests to the same domain. When persistence is enabled, the persistence information is also exchanged as part of metrics exchange.

For the NetScaler appliance to support persistence across sites, persistence must be enabled on the GSLB virtual servers of all participating sites. When you use source IP address persistence on the network identifier, you must configure a subnet mask. For any domain, persistence takes precedence over any other configured GSLB method.

To configure persistence based on source IP address by using the command line interface

At the command prompt, type:

```
set gslb vserver <name> -persistenceType (SOURCEIP|NONE) -persistenceId <positive_integer> [-persistMask <netmask>] -[timeout <mins>]
```

Example

```
set gslb vserver vserver-GSLB-1 -persistenceType SOURCEIP -persistenceId 23 -persistMask 255.255.255.255 -timeout 2
```
Parameters for configuring persistence based on source IP address

name

The name of the GSLB virtual server for which you are configuring source IP address based persistence.

persistenceType

The type of persistence being configured for the GSLB virtual server. Possible Values: SOURCEIP, None.

persistenceID

A positive integer used to identify the GSLB virtual server on all sites. Minimum value: 1. Maximum value: 65535.

persistMask

The subnet mask used when SOURCEIP based persistence is enabled. Minimum Value: 128.0.0.0. Default: 0xFFFFFFFF.

timeout

The time, in minutes, for which persistence should be in effect for the GSLB virtual server. Minimum value: 2. Maximum value: 1440. Default: 2.

To configure persistence based on source IP address by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.

2. In the GSLB Virtual Servers pane, select the GSLB virtual server whose method you want to change (for example, vserver-GSLB-1).

3. Click Open.

4. On the Method and Persistence tab, under Persistence, select SOURCEIP from the Persistence list and specify values for the following parameters, which correspond to parameters described in “Parameters for configuring persistence based on source IP address” as shown:

   - Time-out—timeout
   - Persistence Id—persistenceID
   - IPv4 Netmask or IPv6 Mask length—persistMask

5. Click OK.
Configuring Persistence Based on HTTP Cookies

The NetScaler appliance provides persistence at the HTTP-request level by using connection proxy and HTTP redirect. With these persistence methods, the appliance uses an HTTP cookie (known as a “site cookie”) to reconnect the client to the same server. The NetScaler inserts the site cookie in the first HTTP response.

The site cookie contains information about the selected GSLB service on which the client has a persistent connection. The cookie expiration is based on the cookie timeout configured on the NetScaler appliance. If the virtual server names are not identical on all the sites, you must use the persistence identifier. Cookies inserted are compliant with RFC 2109.

When the NetScaler appliance responds to a client DNS request by sending the IP address of the selected GSLB site, the client sends an HTTP request to that GSLB site. The physical server in that GSLB site adds a site cookie to the HTTP header, and connection persistence is in effect.

If the DNS entry in the client cache expires, and then the client sends another DNS query and is directed to a different GSLB site, the new GSLB site uses the site cookie present in the client request header to implement persistence. If the GSLB configuration at the new site uses connection-proxy persistence, the new site creates a connection to the GSLB site that inserted the site cookie, proxies the client request to the original site, receives a response from the original GSLB site, relays that response back to the client, and closes the connection. If the GSLB configuration uses HTTP redirect persistence, the new site redirects the request to the site that originally inserted the cookie.

**Note:** Connection proxy persistence can be configured only for local services. However, connection proxy persistence must be enabled on both local and remote GSLB services that are configured for the GSLB virtual server.

Connection proxy occurs when the following conditions are satisfied:

- Requests are sent from a domain participating in GSLB. The domain is obtained from the URL/Host header.
- Requests are sent from a local GSLB service whose public IP address matches the public IP address of an active service bound to the GSLB virtual server.
- The local GSLB service has connection proxy enabled.
- The request includes a valid cookie that contains the IP address of an active remote GSLB service.

If one of the conditions is not met, connection proxy does not occur, but a site cookie is added if the local GSLB service has connection proxy enabled AND:

- No site cookie is supplied; OR,
Configuring Persistence Based on HTTP Cookies

- The site cookie refers to an IP address that is not an active GSLB remote service; OR,
- The cookie refers to the IP address of the virtual server on which the request is received.

The following are the limitations of using connection proxy site cookies:

- Site cookies do not work for non-HTTP(S) protocols.
- If an HTTP request is sent to a back-up virtual server, the virtual server does not add a cookie.
- Site cookies do not work if SSL client authentication is required.
- At the local site, the statistics for a GSLB service on a remote site are not the same as the statistics recorded for that service at the remote site. At the local site, the statistics for a remote GSLB service are slightly higher than the statistics that the remote site records for that same service.

Redirect persistence can be used only:

- For HTTP or HTTPS protocols.
- If the domain name is present in the request (either in the URL or in the HOST header), and the domain is a GSLB domain.
- When the request is received on a backup VIP or a GSLB local service that is in the down state.

To set persistence based on HTTP cookies by using the command line interface

At the command prompt, type:

```
set gslb service <serviceName> -sitePersistence (ConnectionProxy [-sitePrefix <prefix>] | HTTPredirect -sitePrefix <prefix>)
```

Example

```
set gslb service service-GSLB-1 -sitePersistence ConnectionProxy
set gslb service service-GSLB-1 -sitePersistence HTTPredirect -sitePrefix vserver-GSLB-1
```

Parameters for setting persistence based on HTTP cookies

```
serviceName
```
The name of the GSLB service for which connection proxy based cookie persistence is
being configured.

**sitePersistence**

The type of persistence. Possible Values: connectionProxy, HTTPRedirect, None.

**sitePrefix**

This is a mandatory parameter when you configure HTTP redirect based persistence on a
GSLB service. When the service is bound to a GSLB virtual server, for each bound
service-domain pair, a GSLB site domain is generated internally by concatenating the
service's siteprefix and the domain's name. If a special string "NONE" is specified, the
siteprefix string is not set.

**To set persistence based on cookies by using the configuration utility**

1. In the navigation pane, expand GSLB and click Services.

2. In the GSLB Services pane, select the service that you want to configure for site
   persistence (for example, service-GSLB-1).

3. Click Open.

4. On the Advanced tab, under Site Persistence type, specify values for the following
   parameters, which correspond to parameters described in “Parameters for setting
   persistence based on HTTP cookies” as shown:

   - Site Persistence type—sitePersistence

   - Site Prefix—sitePrefix

5. Click OK.
Configuring Transition Out-Of-Service State (TROFS) in GSLB

When you configure persistence on a GSLB virtual server to which a service is bound, the service continues to serve requests from the client even after it is disabled, accepting new requests or connections only to honor persistence. After a configured period of time, known as the graceful shutdown period, no new requests or connections are directed to the service, and all of the existing connections are closed.

When disabling a service, you can specify a graceful shutdown period, in seconds, by using the delay argument. During the graceful shutdown period, if the service is bound to a virtual server, its state appears as Out of Service.
In a typical network, there are servers that have a higher capacity for traffic than others. However, with a regular load balancing configuration, the load is evenly distributed across all services even though different services represent servers with different capacities.

To optimize your GSLB resources, you can configure dynamic weights on a GSLB virtual server. The dynamic weights can be based on either the total number of services bound to the virtual server or the sum of the weights of the individual services bound to the virtual server. Traffic distribution is then based on the weights configured for the services.

When dynamic weights are configured on the GSLB virtual server, requests are distributed according to the load balancing method, the weight of the GSLB service, and the dynamic weight. The product of the weight of the GSLB service and the dynamic weight is known as the cumulative weight. Therefore, when dynamic weight is configured on the GSLB virtual server, requests are distributed on the basis of the load balancing method and the cumulative weight.

When dynamic weight for a virtual server is disabled, the numerical value is set to 1. This ensures that the cumulative weight is a non-zero integer at all times.

Dynamic weight can be based on the total number of active services bound to load balancing virtual servers or on the weights assigned to the services.

Consider a configuration with two GSLB sites configured for a domain and each site has two services that can serve the client. If a service at either site goes down, the other server in that site has to handle twice as much traffic as a service at the other site. If dynamic weight is based on the number of active services, the site with both services active has twice the weight of the site with one service down and therefore receives twice as much traffic.

Alternatively, consider a configuration in which the services at the first site represent servers that are twice as powerful as servers at the second site. If dynamic weight is based on the weights assigned to the services, twice as much traffic can be sent to the first site as to the second.

**Note:** For details on assigning weights to load balancing services, see "Assigning Weights to Services".

As an illustration of how dynamic weight is calculated, consider a GSLB virtual server that has a GSLB service bound to it. The GSLB service represents a load balancing virtual server that in turn has two services bound to it. The weight assigned to the GSLB service is 3. The weights assigned to the two services are 1 and 2 respectively. In this example, when dynamic weight is set to:

- **Disabled:** The cumulative weight of the GSLB virtual server is the product of the dynamic weight (disabled = 1) and the weight of the GSLB service (3), so the cumulative weight is 3.
Configuring Dynamic Weights for Services

- **SERVICECOUNT**: The count is the sum of the number of services bound to the load balancing virtual servers corresponding to the GSLB service (2), and the cumulative weight is the product of the dynamic weight (2) and the weight of the GSLB service (3), which is 6.

- **SERVICEWEIGHT**: The dynamic weight is the sum of the number of services bound to the GSLB service (2), and the cumulative weight is the product of the dynamic weight (2) and the weight of the GSLB service (3), which is 6.

**Note**: Dynamic weights are not applicable when content switching virtual servers are configured.

**To configure a GSLB virtual server to use dynamic weights by using the command line interface**

At the command prompt, type:

```bash
set gslb vserver <name> -dynamicWeight SERVICECOUNT | SERVICEWEIGHT
```

**Example**

```bash
set gslb vserver vserver-GSLB-1 -dynamicWeight SERVICECOUNT
```

**To set GSLB virtual server to use dynamic weights by using the configuration utility**

1. In the navigation pane, expand GSLB and click Virtual Servers.

2. In the GSLB Virtual Servers pane, select the GSLB virtual server for which you want to set dynamic weights (for example, vserver-GSLB-1).

3. Click Open.

4. On the Method and Persistence tab, under Method, select SERVICECOUNT or SERVICEWEIGHT from the Dynamic Weight list.

5. Click OK.
Monitoring GSLB Services

When you bind a remote service to a GSLB virtual server, the GSLB sites exchange metric information, including network metric information, which is the round-trip-time and persistence information.

If a metric exchange connection is momentarily lost between any of the participating sites, the remote site is marked as DOWN and load balancing is performed on the remaining sites that are UP. When metric exchange for a site is DOWN, the remote services belonging to the site are marked DOWN as well.

The NetScaler appliance periodically evaluates the state of the remote GSLB services by using either MEP or monitors that are explicitly bound to the remote services. Binding explicit monitors to local services is not required, because the state of the local GSLB service is updated by default using the MEP. However, you can bind explicit monitors to a remote service. When monitors are explicitly bound, the state of the remote service is not controlled by the metric exchange.

By default, when you bind a monitor to a remote GSLB service, the NetScaler appliance uses the state of the service reported by the monitor. However, you can configure the NetScaler appliance to use monitors to evaluate services in the following situations:

- Always use monitors (default setting).
- Use monitors when MEP is DOWN.
- Use monitors when remote services and MEP are DOWN.

The second and third of the above settings enable the NetScaler to stop monitoring when MEP is UP. For example, in a hierarchical GSLB setup, a GSLB site provides the MEP information about its child sites to its parent site. Such an intermediate site may evaluate the state of the child site as DOWN because of network issues, though the actual state of the site is UP. In this case, you can bind monitors to the services of the parent site and disable MEP to determine the actual state of the remote service. This option enables you to control the manner in which the states of the remote services are determined.

To use monitors, first create them, and then bind them to GSLB services.
Adding or Removing Monitors

To add a monitor, you specify the type and the port. You cannot remove a monitor that is bound to a service. You must first unbind the monitor from the service.

To add a monitor by using the command line interface

At the command prompt, type the following commands to create a monitor and verify the configuration:

- `add lb monitor <monitorName> -type <monitorType> -destPort <portNumber>`
- `show lb monitor <monitorName>`

Example

```
add lb monitor monitor-HTTP-1 -type HTTP -destPort 80
show lb monitor monitor-HTTP-1
```

To remove a monitor by using the command line interface

At the command prompt, type:

```
rm lb monitor <monitorName>
```

Parameters for adding a monitor

**name**

The name of the monitor being created. This alphanumeric string is required and cannot be changed after the monitor is created. The name must not exceed 31 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ . (period) : (colon) # and space ( ).

**type**

The type of monitor being configured. The following are valid monitor types:

- **TCP** - The NetScaler appliance establishes a TCP connection with the monitor destination and then closes the connection. If the NetScaler observes TCP traffic to the destination, it does not send TCP monitoring requests. This occurs if LRTM is disabled. By default, LRTM is disabled on this monitor. This is done only for UDP, and the service goes down immediately.
TCP-ECV - The NetScaler appliance establishes a TCP connection with the monitor destination. When the connection is established, the appliance sends specific data to the service by using the -send parameter, and the appliance and expects a specific response through the -receive parameter.

HTTP - the NetScaler establishes a TCP connection with the monitor destination. After the connection is established, the NetScaler sends HTTP requests and compares the response code, in the response from the service, with the configured set of response codes.

HTTP-ECV - the NetScaler establishes a TCP connection with the monitor destination. When the connection is established, the NetScaler sends the HTTP data specified by the -send parameter to the service and expects the HTTP response that the -receive parameter specifies. (HTTP body part, not including HTTP headers.) Empty response data matches any response. Expected data may be anywhere in the first 24K bytes of the HTTP body of the response.

PING - the NetScaler sends an ICMP echo request to the destination of the monitor and expects an ICMP echo response.

Note: The NetScaler also supports FTP, UDP, DNS, UDP-ECV, TCPS, HTTPS, TCPS-ECV, HTTPS-ECV, LDNS-PING, LDNS-TCP, and LDNS-DNS monitors.

For more information about monitors, see Load Balancing.

destPort

Destination TCP/UDP port of the probe (the port of the dispatcher to which the probe is sent). The port can be different from the server port to which the monitor is bound. The value 0 (zero) directs the probes to the bound server’s port. This parameter has no effect on PING type monitors.

To add a monitor by using the configuration utility

1. In the navigation pane, expand Load Balancing and click Monitors.

2. In the details pane, click Add.

3. In the Create Monitor dialog box, specify values for the following parameters, which correspond to parameters described in “Parameters for adding a monitor” as shown:

   · Name*—name
   
   · Type*—type
   * A required parameter

4. On the Standard Parameters tab, in the Destination Port text box, type the destination port number (see “destPort” in the above parameter list).

5. Click Create, and then click Close.
Binding Monitors to a GSLB Service

Once you create monitors, you must bind them to GSLB services. When binding monitors to the services, you can specify a weight for the monitor. After binding one or more weighted monitors, you can configure a monitor threshold for the service. This threshold takes the service down if the sum of the bound monitor weights falls below the threshold value.

**Note:** In the configuration utility, you can set both the weight and the monitoring threshold at the same time that you bind the monitor. When using the command line, you must issue a separate command to set the service’s monitoring threshold.

**To bind the monitor to the GSLB service by using the command line interface**

At the command prompt, type:

`bind monitor <name> <serviceName> [ -state (Enabled | Disabled) ] -weight <positiveInteger>`

**Example**

`bind monitor monitor-HTTP-1 service-GSLB-1 -state enabled -weight 2`

**To set the monitoring threshold for a GSLB service by using the command line interface**

At the command prompt, type:

`set gslb service <ServiceName> -monThreshold <PositiveInteger>`

**Example**

`set gslb service service-GSLB-1 -monThreshold 9`

**Parameters for binding a monitor to a GSLB service**

- **name**
  - The name of the monitor to be bound to the service.
- **serviceName**
The name of the service to which to bind the monitor.

**weight**


**monThreshold**

The monitoring threshold for the service. Minimum value: 0. Maximum value: 65535.

---

**To bind the monitor to the GSLB service by using the configuration utility**

1. In the navigation pane, expand GSLB and click Services.

2. The details pane, select the service to which you want to bind the monitor (for example, select service-GSLB-1).

3. Click Open.

4. In the Configure GSLB Service dialog box, on the Monitors tab, select the monitor that you want to bind to the service (for example, monitor-HTTP-1).

5. Click Add.

6. In the Configured table, you can select the newly assigned monitor and enter a new weight value.

7. To enable the monitor, make sure the State check box is selected.

8. Repeat the preceding steps to add additional monitors.

9. In the Monitor Threshold text box, you can enter a threshold value.

10. Click OK.
Monitoring GSLB Sites

The NetScaler appliance uses MEP or monitors to determine the state of the GSLB sites. You can configure a GSLB site to always use monitors (the default), use monitors when MEP is down, or use monitors when both the remote service and MEP are down. In the latter two cases, the NetScaler appliance stops monitoring when MEP returns to the UP state.

To configure monitor triggering by using the command line interface

At the command prompt, type:

```
set gslb site <siteName> -triggerMonitor (ALWAYS | MEPDOWN | MEPDOWN_SVCDOWN)
```

Example

```
> set gslb site Site-GSLB-North-America -triggerMonitor Always
Done
```

To configure monitor triggering by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Sites.
2. In the details pane, select the site, and then click Open.
3. In the Configure GSLB Site dialog box, in the Trigger Monitors drop-down list, select an option for when to trigger monitoring.
4. Click OK.
Protecting the GSLB Setup Against Failure

You can protect your GSLB setup against failure of a GSLB site or a GSLB virtual server by configuring a backup GSLB virtual server, configuring the NetScaler appliance to respond with multiple IP addresses, or configuring a Backup IP address for a GSLB domain. You can also divert excess traffic to a backup virtual server by using spillover.
Configuring a Backup GSLB Virtual Server

Configuring a backup entity for a GSLB virtual server ensures that DNS traffic to a site is not interrupted if the GSLB virtual server goes down. The backup entity can be another GSLB virtual server, or it can be a backup IP address. With a backup entity configured, if the primary GSLB virtual server goes down, the backup entity handles DNS requests. To specify what should happen when the primary GSLB virtual server comes back up again, you can configure the backup entity to continue handling traffic until you manually enable the primary virtual server to take over (using the disablePrimaryOnDown option), or you can configure a timeout period after which the primary takes over.

If you configure both the timeout and the disablePrimaryOnDown option for the backup entity, the backup session time-out takes precedence over the disablePrimaryOnDown setting.

To configure a backup GSLB virtual server by using the command line interface

At the command prompt, type the following commands to configure a GSLB virtual server as a backup virtual server and verify the configuration:

- set gslb vserver <name> -backupVServer <name> [-backupSessionTimeout <timeoutValue>] [-disablePrimaryOnDown (ENABLED | DISABLED)]
- show gslb vserver <name>

Example

set gslb vserver vserver-GSLB-1 -backupVServer vserver-GSLB-2 -backupSessionTimeout 3 -disablePrimaryOnDown
show gslb vserver vserver-GSLB-1

Parameters for configuring a backup GSLB virtual server

name

The name of the GSLB virtual server for which you are configuring a backup.

backupVServer
The name of the GSLB virtual server being configured as a backup.

**backupSessionTimeout**

The time, in minutes, after which the former primary GSLB virtual becomes primary again after returning to the UP state.

**disablePrimaryOnDown**

Require manual intervention to return the former primary GSLB virtual server to primary status.

**To set GSLB virtual server as a backup virtual server by using the configuration utility**

1. In the navigation pane, expand GSLB and click Virtual Servers.

2. In the GSLB Virtual Servers pane, select the GSLB virtual server for which you want to configure a backup virtual server (for example, vserver-GSLB-1).

3. Click Open.

4. On the Advanced tab, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a backup GSLB virtual server” as shown:
   - Backup VServer—backupVServer
   - Backup Session Time-out (mins)—backupSessionTimeout
   - Disable Primary When Down—disablePrimaryOnDown

5. Click OK.
Configuring a GSLB Setup to Respond with Multiple IP Addresses

A typical DNS response contains the IP address of the best performing GSLB service. However, if you enable multiple IP response (MIR), the NetScaler appliance sends the best GSLB service as the first record in the response and adds the remaining active services as additional records. If MIR is disabled (the default), the NetScaler appliance sends the best service as the only record in the response.

To configure a GSLB virtual server for multiple IP responses by using the command line interface

At the command prompt, type the following commands to configure a GSLB virtual server for multiple IP responses and verify the configuration:

- set gslb vserver <name> -MIR (ENABLED | DISABLED)
- show gslb vserver <name>

Example

set gslb vserver vserver-GSLB-1 -MIR ENABLED
show gslb vserver <vserverName>

To set a GSLB virtual server for multiple IP responses by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.

2. In the GSLB Virtual Servers pane, select the GSLB virtual server for which you want to configure a backup virtual server (for example, vserver-GSLB-1).

3. Click Open.

4. On the Advanced tab, under When this VServer is “UP,” select the Send all “active” service IP in response (MIR) check box.

5. Click OK.
Configuring a GSLB Virtual Server to Respond with an Empty Address Record When DOWN

A DNS response can contain either the IP address of the requested domain or an answer stating that the IP address for the domain is not known by the DNS server, in which case the query is forwarded to another name server. These are the only possible responses to a DNS query.

When a GSLB virtual server is disabled or in a DOWN state, the response to a DNS query for the GSLB domain bound to that virtual server contains the IP addresses of all the services bound to the virtual server. However, you can configure the GSLB virtual server to in this case send an empty down response (EDR). When this option is set, a DNS response from a GSLB virtual server that is in a DOWN state does not contain IP address records, but the response code is successful. This prevents clients from attempting to connect to GSLB sites that are down.

Note: You must configure this setting for each virtual server to which you want it to apply.

To configure a GSLB virtual server for empty down responses by using the command line interface

At the command prompt, type:

```
set gslb vserver <name> -EDR (ENABLED | DISABLED)
```

Example

```
> set gslb vserver vserver-GSLB-1 -EDR ENABLED
Done
```
To set a GSLB virtual server for empty down responses by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.

2. In the GSLB Virtual Servers pane, select the GSLB virtual server for which you want to configure a backup virtual server (for example, vserver-GSLB-1).

3. Click Open.

4. On the Advanced tab, under When this VServer is “Down,” select the Do not send any service’s IP address in response (EDR) check box.

5. Click OK.
Configuring a Backup IP Address for a GSLB Domain

You can configure a backup site for your GSLB configuration. With this configuration in place, if all of the primary sites go DOWN, the IP address of the backup site is provided in the DNS response.

Typically, if a GSLB virtual server is active, that virtual server sends a DNS response with one of the active site IP addresses as selected by the configured GSLB method. If all the configured primary sites in the GSLB virtual server are inactive (in the DOWN state), the authoritative domain name system (ADNS) server or DNS server sends a DNS response with the backup site’s IP address.

**Note:** When a backup IP address is sent, persistence is not honored.

To set a backup IP address for a domain by using the command line interface

At the command prompt, type the following commands to set a backup IP address and verify the configuration:

- `set gslb vserver <name> -domainName <string> -backupIP <IPAddress>`
- `show gslb vserver <name>`

**Example**

```
set gslb vserver vserver-GSLB-1 -domainName www.abc.com -backupIP 10.102.29.66
show gslb vserver vserver-GSLB-1
```

Parameters for configuring a backup IP address for a domain

- **vserverName**
  
  The name of the GSLB virtual server to which the domain you are configuring a backup IP address for is bound.

- **domainName**
  
  The name of the domain for which a backup IP address is being configured.

- **backupIP**
The IP address of the backup service. This IP address is used when all services bound to the domain are down, or when the backup chain is down.

To set a backup IP address for a domain by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.

2. In the GSLB Virtual Servers pane, select the GSLB virtual server to which you want to bind the backup domain (for example, vserver-GSLB-1).

3. Click Open.

4. On the Domains tab, select a domain and click Open.

5. In the Configure GSLB Domain dialog box, in the Backup IP text box, type the IP address of the backup domain.

6. Click OK.
Diverting Excess Traffic to a Backup Virtual Server

Once the number of connections to a primary GSLB virtual server exceeds the configured threshold value, you can use the spillover option to divert new connections to a backup GSLB virtual server. This threshold value can be calculated dynamically or set manually. Once the number of connections to the primary virtual server drops below the threshold, the primary GSLB virtual server resumes serving client requests.

You can configure persistence with spillover. When persistence is configured, new clients are diverted to the backup virtual server if that client is not already connected to a primary virtual server. When persistence is configured, connections that were diverted to the backup virtual server are not moved back to the primary virtual server after the number of connections to the primary virtual server drops below the threshold. Instead, the backup virtual server continues to process those connections until they are terminated by the user. Meanwhile, the primary virtual server accepts new clients.

The threshold can be measured either by the number of connections or by the bandwidth.

If the backup virtual server reaches the configured threshold and is unable to take any additional load, the primary virtual server diverts all requests to the designated redirect URL. If a redirect URL is not configured on the primary virtual server, subsequent requests are dropped.

The spillover feature prevents the remote backup GSLB service (backup GSLB site) from getting flooded with client requests when the primary GSLB virtual server fails. This occurs when a monitor is bound to a remote GSLB service, and the service experiences a failure that causes its state to go DOWN. The monitor continues to keep the state of the remote GSLB service UP, however, because of the spillover feature.

As part of the resolution to this problem, two states are maintained for a GSLB service, the primary state and effective state. The primary state is the state of the primary virtual server and the effective state is the cumulative state of the virtual servers (primary and backup chain). The effective state is set to UP if any of the virtual servers in the chain of virtual servers is UP. A flag that indicates that the primary VIP has reached the threshold is also provided. The threshold can be measured by either the number of connections or the bandwidth.

A service is considered for GSLB only if its primary state is UP. Traffic is directed to the backup GSLB service only when all the primary virtual servers are DOWN. Typically, such deployments will have only one backup GSLB service.

Adding primary and effective states to a GSLB service has the following effects:

- When source IP persistence is configured, the local DNS is directed to the previously selected site only if the primary virtual server on the selected site is UP and below threshold. Persistence can be ignored in the round robin mode.

- If cookie-based persistence is configured, client requests are redirected only when the primary virtual server on the selected site is UP.
If the primary virtual server has reached its saturation and the backup VIP(s) is absent or down, the effective state is set to DOWN.

If external monitors are bound to an HTTP-HTTPS virtual server, the monitor decides the primary state.

If there is no backup virtual server to the primary virtual server and the primary virtual server has reached its threshold, the effective state is set to DOWN.

To configure a backup GSLB virtual server by using the command line interface

At the command prompt, type the following commands to configure a backup GSLB virtual server and verify the configuration:

- set gslb vserver <name> -soMethod <method> -soThreshold <threshold> -soPersistence (ENABLED | DISABLED) -soPersistenceTimeout <timeout>
- show gslb vserver <name>

Example

set gslb vserver Vserver-GSLB-1 -soMethod CONNECTION -soThreshold 1000 -soPersistence ENABLED -soPersistenceTimeout 2
show gslb vserver Vserver-GSLB-1

Parameters for configuring a backup GSLB virtual server

name

The name of the GSLB virtual server for which a backup virtual server is being configured.

soMethod

The type of spillover used to divert traffic to the backup GSLB virtual server when the primary virtual server reaches the threshold. Possible values:

- CONNECTION. Spillover based on number of connections exceeding the threshold.
- DYNAMICCONNECTION. Spillover based on the combined number of connections exceeding the threshold.
- BANDWIDTH. Spillover based on combined incoming and outgoing bandwidth.
- HEALTH. Spillover occurs if bound and active services and service groups fall below a threshold relative to all bound elements.
- NONE.
Diverting Excess Traffic to a Backup Virtual Server

**soThreshold**

The threshold value that decides when traffic must spill over to the backup virtual server. The following threshold values are supported:

- For the **CONNECTION** (or) **DYNAMICCONNECTION** spillover type, the threshold value is the maximum number of connections that the sites under the primary GSLB virtual server will handle before spillover occurs.

- For the **BANDWIDTH** spillover type, the threshold value is the amount of incoming and outgoing traffic (in kilobits per second) that the GSLB virtual server will handle before spillover occurs. Minimum value: 1. Maximum value: 4,294,967,294.

- For **HEALTH**, the threshold value is a positive integer from 1 through 99. This integer represents a percentage of the sum of the binding weights of all of the enabled, bound, and active GSLB services and service groups relative to the sum of the binding weights of all enabled and bound services and service groups (active and inactive).

**soPersistence**

The configured spillover persistence state. If you enable spillover persistence, the NetScaler appliance maintains source-IP based persistence over the primary virtual server and backup virtual servers. Possible values: ENABLED, DISABLED. Default: DISABLED.

**soPersistenceTimeout**


**backupVServer**

The name of the GSLB virtual server being configured as a backup.

**backupSessionTimeout**

The time, in minutes, after which the former primary GSLB virtual becomes primary again after returning to the UP state.
To configure a backup GSLB virtual server by using the configuration utility

1. In the navigation pane, expand GSLB, and then click Virtual Servers.

2. In the details pane, select the virtual server that you want to configure as a backup (for example, Vserver-LB-1), and then click Open.

3. On the Advanced tab, under Spillover, specify values for the following parameters, which correspond to parameters described in “Parameters for configuring a backup GSLB virtual server” as shown:
   
   - Method— soMethod
   - Threshold— soThreshold
   - Persistence Time-out (min) — soPersistenceTimeout

4. Select the Persistence check box.

5. Click OK.
Managing Client Connections

To facilitate management of client connections, you can enable delayed cleanup of connections to the virtual server. You can then manage local DNS traffic by configuring DNS policies.
Enabling Delayed Cleanup of Virtual Server Connections

The state of a virtual server depends on the states of the services bound to it, and the state of each service depends on the monitors bound to it. If a server is slow or down, the monitoring probes time out and the service that represents the server is marked as DOWN. A virtual server is marked as DOWN only when all services bound to it are marked as DOWN. You can configure services and virtual servers to either terminate all connections when they go down, or allow the connections to go through. The latter setting is for situations in which a service is marked as DOWN because of a slow server.

When you configure the down state flush option, the NetScaler appliance performs a delayed cleanup of connections to a GSLB service that is down.

To enable delayed cleanup of virtual server connections by using the command line interface

At the command prompt, type the following commands to configure delayed connection cleanup and verify the configuration:

- set gslb service <name> -downStateFlush (ENABLED | DISABLED)
- show gslb service <name>

Example

> set gslb service Service-GSLB-1 -downStateFlush ENABLED
Done
> show gslb service Service-GSLB-1
Done

Parameters for delayed connection cleanup

name

The name of the GSLB service for which delayed connection cleanup is being configured.

downStateFlush

Enables or disables delayed cleanup of connections to the GSLB service. Possible Values: ENABLED or DISABLED.
To enable delayed cleanup of virtual server connections by using the configuration utility

1. In the navigation pane, expand GSLB and click Services.
2. In the GSLB Services pane, select the service (for example, service-GSLB-1), and then click Open.
3. On the Advanced tab, select the Down state flush check box.
4. Click OK.
Managing Local DNS Traffic by Using DNS Policies

You can use DNS policies to implement site affinity by directing traffic from the IP address of a local DNS resolver or network to a predefined target GSLB site. This is configured by creating DNS policies with DNS expressions and binding the policies globally on the NetScaler appliance.
The NetScaler appliance provides certain predefined DNS expressions that can be used for configuring actions specific to a domain. Such actions can, for example, drop certain requests, select a specific view for a specific domain, or redirect certain requests to a specific location.

These DNS expressions (also called rules) are combined to create DNS policies that are then bound globally on the NetScaler appliance.

Following is the list of predefined DNS qualifiers available on the NetScaler appliance:

- CLIENT.UDP.DNS.DOMAIN.EQ("domainname")
- CLIENT.UDP.DNS.IS_AREC
- CLIENT.UDP.DNS.IS_AAAAREC
- CLIENT.UDP.DNS.IS_SRVREC
- CLIENT.UDP.DNS.IS_MXREC
- CLIENT.UDP.DNS.IS_SOAREC
- CLIENT.UDP.DNS.IS_PTRREC
- CLIENT.UDP.DNS.IS_CNAME
- CLIENT.UDP.DNS.IS_NSREC
- CLIENT.UDP.DNS.IS_ANYREC

The CLIENT.UDP.DNS.DOMAIN DNS expression can be used with string expressions. If you are using domain names as part of the expression, they must end with a period (.). For example, CLIENT.UDP.DNS.DOMAIN.ENDSWITH("abc.com.")
To create an expression by using the configuration utility

1. Click the icon next to the Expression text box. Click Add. (Leave the Flow Type and Protocol drop-down list boxes empty.) Follow these steps to create a rule.

2. In the Qualifier box, select a qualifier (for example, LOCATION).

3. In the Operator box, select an operator (for example, ==).

4. In the Value box, type a value (for example, Asia, Japan....).

5. Click OK. Click Create and click Close. The rule is created.

6. Click OK.
Configuring DNS Policies

DNS policies operate on a location database that uses static and custom IP addresses. The attributes of the incoming local DNS request are defined as part of an expression, and the target site is defined as part of a DNS policy. While defining actions and expressions, you can use a pair of single quotation marks (‘’’) as a wildcard qualifier to specify more than one location. When a DNS policy is configured and a GSLB request is received, the custom IP address database is first queried for an entry that defines the location attributes for the source:

- When a DNS query comes from an LDNS, the characteristics of the LDNS are evaluated against the configured policies. If they match, an appropriate action (site affinity) is executed. If the LDNS characteristics match more than one site, the request is load balanced between the sites that match the LDNS characteristics.
- If the entry is not found in the custom database, the static IP address database is queried for an entry, and if there is a match, the above policy evaluation is repeated.
- If the entry is not found in either the custom or static databases, the best site is selected and sent in the DNS response on the basis of the configured load balancing method.

The following restrictions apply to DNS policies created on the NetScaler appliance.

- A maximum of 64 policies are supported.
- DNS policies are global to the NetScaler and cannot be applied to a specific virtual server or domain.
- Domain or virtual server specific binding of policy is not supported.

You can use DNS policies to direct clients that match a certain IP address range to a specific site. For example, if you have a GSLB setup with multiple GSLB sites that are separated geographically, you can direct all clients whose IP address is within a specific range to a particular data center.

To add a DNS policy by using the command line interface

At the command prompt, type the following commands to create a DNS policy and verify the configuration:

- add dns policy <name> <rule> -viewName <string>
- show dns policy <name>

Example
To remove a configured DNS policy by using the command line interface

At the command prompt, type:

```
rm dns policy <name>
```

Parameters for configuring a DNS policy

- **name**
  
The name of the DNS policy being created.

- **rule**
  
Expression to be used by the dns policy.

- **viewName**
  
The name of the DNS view to be associated with the DNS policy.

For details on DNS views, see Adding DNS Views.
To configure a DNS policy by using the NetScaler configuration utility

1. In the navigation pane, expand DNS, and then click Policies.
2. In the details pane, do one of the following:
   - To create a DNS policy, click Add.
   - To modify a DNS policy, select the DNS policy, and then click OK.
3. In the Create DNS Policy or Configure DNS Policy dialog box, set the following parameters:
   - Policy Name (cannot be changed for an existing policy)
   - Action
   - Expression
   To specify an expression, do the following:
   a. Click Add, and then, in the drop-down box that appears, select the expression element with which you want to begin the expression. A second list appears. The list contains a set of expression elements that you can use immediately after the first expression element.
   b. In the second list, select the expression element that you want, and then enter a period.
   c. After each selection, if you enter a period, the next set of valid expression elements appear in a list. Select expression elements and fill in arguments to functions until you have the expression you want.
4. Click Create or OK, and then click Close.
To add a DNS policy by using the configuration utility

1. In the navigation pane, expand DNS and click Policies.

2. In the details pane, click Add.

3. In the Policy Name box, type a name for the DNS policy (for example, policy-GSLB-1).

4. Select View Name radio button and, select the view in the View Name drop down list, or click New to create a view.

5. Under Expression, click Add... and in the Add Expression dialog box, do the following:
   a. In the first drop-down box, select CLIENT.
   b. In the second drop-down list box, select UDP.
   c. In the next drop-down list box, select DNS.
   d. In the next drop-down list box, select DOMAIN.
   e. In the next drop-down list box, select EQ(String).
   f. In the next text box, type the domain name (for example, abc.com).

6. Click OK and click Close. The expression is displayed under Expression in the Create DNS Policy dialog box.

7. Click Create, and then click Close.
DNS policies are bound globally on the NetScaler appliance and are available for all configured GSLB virtual servers. Even though DNS policies are globally bound, policy execution can be limited to a specific GSLB virtual server by specifying the domain in the expression.

To bind a DNS policy globally by using the command line interface

At the command prompt, type the following commands to bind a DNS policy globally and verify the configuration:

- bind dns global <policyName> <priority> [-gotoPriorityExpression <string>]
- show dns global

Example

> bind dns global policy-GSLB-1 10 -gotoPriorityExpression END
Done
> show dns global -type REQ_DEFAULT
1) Policy Name: policy-GSLB-1
   Priority: 10
   GotoPriorityExpression: END

Done
To bind a DNS policy globally by using the configuration utility

1. In the navigation pane, expand DNS and click Policies.

2. In the details pane, click Global Bindings.

3. In the Bind/Unbind DNS Policy(s) to Global dialog box, click Insert Policy.

4. In the Policy Name column, select, from the list, the policy that you want to bind. Alternatively, in the list, click New Policy, and then create a DNS policy by setting parameters in the Create DNS Policy dialog box.

5. To modify a policy that is already bound globally, click the name of the policy, and then click Modify Policy. Then, in the Configure DNS Policy dialog box, modify the policy, and then click OK.

6. To unbind a policy, click the name of the policy, and then click Unbind Policy.

7. To modify the priority assigned to a policy, double-click the priority value, and then enter a new value.

8. To regenerate assigned priorities, click Regenerate Priorities. The priority values are modified to begin at 100, with increments of 10, without affecting the order of evaluation.

9. Click OK.

To view the global bindings of a DNS policy by using the command line interface

At the command prompt, type:

show dns global

To view the global bindings of a DNS policy by using the configuration utility

1. In the navigation pane, expand DNS and click Policies.

2. In the details pane, click Global Bindings. The global bindings of all DNS policies appear in this dialog box.
Adding DNS Views

You can configure DNS views to identify various types of clients and provide an appropriate IP address to a group of clients who query for the same GSLB domain. DNS views are configured by using DNS policies that select the IP addresses sent back to the client.

For example, if you have configured GSLB for your company’s domain and have the server hosted in your company’s network, clients querying for the domain from within your company’s internal network can be provided with the server’s internal IP address instead of the public IP address. Clients that query DNS for the domain from the Internet, on the other hand, can be provided the domain's public IP address.

To add a DNS view, you assign it a name of up to 31 characters. The leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ). After adding the view, you configure a policy to associate it with clients and a part of the network, and you bind the policy globally. To configure and bind a DNS policy, see Configuring DNS Policies and Binding DNS Policies.

To add a DNS view by using the command line interface

At the command prompt, type the following commands to create a DNS view and verify the configuration:

- add dns view <viewName>
- show dns view <viewName>

Example

add dns view PrivateSubnet
show dns view PrivateSubnet

To remove a DNS view by using the command line interface

At the command prompt, type:

rm dns view <viewName>
To add a DNS view by using the configuration utility

1. In the navigation pane, expand DNS and click Views.

2. In the details pane, click Add.

3. In the Create DNS view dialog box, in the Name text box, enter the name of the DNS view.

4. Click Create, and then click Close. The DNS view that you created appears in the Views pane.

For details on how to create a DNS policy, see Configuring DNS Policies and for details on how to bind DNS policies globally, see Binding DNS Policies.
Configuring GSLB for Commonly Used Deployment Scenarios

GSLB is commonly used in the following deployment scenarios:

- GSLB for disaster recovery
- GSLB based on proximity
- GSLB based on scalability
- GSLB based on the number of Access Gateway users
- GSLB for XenDesktop
Configuring GSLB for Disaster Recovery

Disaster recovery capability is critical, because downtime is costly. A NetScaler appliance configured for GSLB forwards traffic to the least-loaded or the best-performing data center. This configuration, referred to as an active-active setup, not only improves performance, but also provides immediate disaster recovery by routing traffic to other data centers if a data center that is part of the setup goes down. Alternatively, you can configure an active-standby GSLB setup for disaster recovery only.
Configuring GSLB for Disaster Recovery in an Active-Standby Data Center Setup

A conventional disaster recovery setup includes an active data center and a standby data center. The standby data center is a remote site. When a failover occurs as a result of a disaster event that causes the primary active data center to be inactive, the standby data center becomes operational.

Configuring disaster recovery in an active-standby data-center setup consists of the following tasks.

- Create the active data center.
  - Add a local GSLB site.
  - Add a GSLB vserver, which represents the active data center.
  - Bind the domain to the GSLB virtual server.
  - Add gslb services and bind the services to active GSLB virtual server.
- Create the standby data center.
  - Add a remote gslb site.
  - Add a gslb vserver, which represents standby data center.
  - Add gslb services which represents standby data center and bind the services to the standby gslb vserver.
  - Designate the standby data center by configuring the standby GSLB virtual server as the backup virtual server for the active GSLB virtual server.

Once you have configured the primary data center, replicate the configuration for the backup data center and designate it as the standby GSLB site by designating a GSLB virtual server at that site as the backup virtual server.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).

To designate the standby GSLB site by using the command line interface

At both the active site and the remote site, at the command prompt, type:

```
set gslb vserver <name> -backupVserver <string>
```

Example
To configure the standby site by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.

2. Select the GSLB virtual server for the primary site and click Open.

3. In the Configure GSLB Virtual Server dialog box, on the Advanced tab, in the Backup VServer drop-down list box, select a backup virtual server.

4. Click OK.

By default, once the primary virtual server becomes active, it starts receiving traffic. However, if you want the traffic to be directed to the backup virtual server even after the primary virtual server becomes active, use the ‘disable primary on down’ option.
Configuring for Disaster Recovery in an Active-Active Data Center Setup

An active-active GSLB deployment, in which both GSLB sites are active, removes any risk that may arise in having a standby data center. With such a setup, web or application content can be mirrored in geographically separate locations. This ensures that data is consistently available at each distributed data center.

To configure GSLB for disaster recovery in an active-active data center set up, you must first configure the basic GSLB setup on the first data center and then configure all other data centers.

First create at least two GSLB sites. Then, for the local site, create GSLB a virtual server and GSLB services and bind the services to the virtual servers. Then create ADNS services and bind the domain for which you are configuring GSLB to the GSLB virtual server in the local site. Finally, at the local site, create a load balancing virtual server with the same virtual server IP address as the GSLB service.

Once you have configured the first data center, replicate the configuration for other data centers part of the setup.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).
Configuring for Disaster Recovery with Weighted Round Robin

When you configure GSLB to use the weighted round robin method, weights are added to the GSLB services and the configured percentage of incoming traffic is sent to each GSLB site. For example, you can configure your GSLB setup to forward 80 percent of the traffic to one site and 20 percent of the traffic to another. After you do this, the NetScaler appliance will send four requests to the first site for each request that it sends to the second.

To set up the weighted round robin method, first create two GSLB sites, local and remote. Next, for the local site create a GSLB virtual server and GSLB services, and bind the services to the virtual servers. Configure the GSLB method as round robin. Next, create ADNS services and bind the domain for which you are configuring GSLB to the GSLB virtual server. Finally, create a load balancing virtual server with the same virtual server IP address as the GSLB service.

Each service that represents a physical server in the network has weights associated with it. Therefore the GSLB service is assigned a dynamic weight that is the sum of weights of all services bound to it. Traffic is then split between the GSLB services based on the ratio of the dynamic weight of the particular service to the total weight. You can also configure individual weights for each GSLB service instead of the dynamic weight.

If the services do not have weights associated with them, you can configure the GSLB virtual server to use the number of services bound to it to calculate the weight dynamically.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).

Once you configure a basic GSLB setup, you must configure the weighted round robin method such that the traffic is split between the configured GSLB sites according to the weights configured for the individual services.

To configure a virtual server to assign weights to services by using the command line interface

At the command prompt, type one of the following commands, depending upon whether you want to create a new load balancing virtual server or configure an existing one:

- `add lb vserver <name>@ -weight <WeightValue> <ServiceName>`
- `set lb vserver <name>@ -weight <WeightValue> <ServiceName>`

Example
add lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1
set lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1

To set dynamic weight by using the command line interface

At the command prompt, type:

set gslb vserver <name> -dynamicWeight DynamicWeightType

Example

set gslb vserver Vserver-GSLB-1 -dynamicWeight ServiceWeight

To add weights to the GSLB services by using the command line interface

At the command prompt, type:

set gslb vserver <name> -serviceName GSLBServiceName -weight WeightValue

Example

set gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1 -weight 1

Parameters for configuring a backup GSLB virtual server

lbVserverName

The name of the load balancing virtual server whose services you are configuring weights for.

serviceName

The name of the service whose weights you are configuring.

weight

The weight associated with the service. Minimum Value: 1, Maximum Value: 100.
Configuring for Disaster Recovery with Weighted Round Robin

dynamicWeight

Configures the GSLB virtual server to use either the service count or the cumulative service weights as its dynamic weight. Possible Values: SERVICECOUNT, SERVICEWEIGHT, DISABLED Default Value: DISABLED.

To configure a virtual server to assign weights to services by using the configuration utility

1. In the navigation pane, expand Load Balancing and click Virtual Servers.
2. Select the virtual server (for example, Vserver-LB-1) and click Open.
3. On the Services tab, in the Weights spin box, type or select the weight of a service (for example, 4) next to Service-HTTP-1).
4. Click OK.

To add weights to the GSLB services by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. Select the virtual server (for example vserver-GSLB-1) and click Open.
3. On the Services tab, in the Weight spin box, type or select the weight of a service (for example, next to service-GSLB-1, type 1).
4. Click OK.

To set dynamic weight by using the configuration utility

1. In the navigation pane, expand GSLB and click Virtual Servers.
2. Select the virtual server (for example vserver-GSLB-1) and click Open.
3. On the Method and Persistence tab, under Method, in Dynamic Weight drop-down list, select SERVICEWEIGHT.
4. Click OK.
Configuring for Disaster Recovery with Data Center Persistence

Data center persistence is required for web applications that require maintaining a connection with the same server instead of having the requests load balanced. For example, in an e-commerce portal, maintaining a connection between the client and the same server is critical. For such applications, HTTP redirect persistence can be configured in an active-active setup.

To configure GSLB for disaster recovery with data center persistence, you must first configure the basic GSLB setup and then configure HTTP redirect persistence.

First create two GSLB sites, local and remote. Next, for the local site, create a GSLB virtual server and GSLB services and bind the services to the virtual server. Next, create ADNS services and bind the domain for which you are configuring GSLB to the GSLB virtual server at the local site. Next, create a load balancing virtual server with the same virtual server IP address as the GSLB service. Finally, duplicate the previous steps for the remote configuration, or configure the NetScaler appliance to autosynchronize your GSLB configuration.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).

Once you have configured a basic GSLB setup, configure HTTP redirect precedence to enable data center persistence.

To configure HTTP redirect by using the command line interface

At the command prompt, type the following commands to configure HTTP redirect and verify the configuration:

- set gslb service <serviceName> -sitePersistence <sitePersistence> -sitePrefix <string>
- show gslb service <serviceName>

Example

```
set gslb service Service-GSLB-1 -sitePersistence HTTPRedirect -sitePrefix vserver-GSLB-1
show gslb service Service-GSLB-1
```
Parameters for configuring HTTP redirect

serviceName

The name of the GSLB service for which you are configuring site persistence.

sitePersistence

The type of site persistence being configured. Possible Values: ConnectionProxy, HTTPRedirect, None.

sitePrefix

When a service is bound to a GSLB virtual server, for each bound service-domain pair, a GSLB site domain is generated internally by concatenating the service's siteprefix and the domain name. If a special string, "NONE," is specified, the siteprefix string is not set.

To configure HTTP redirect by using the configuration utility

1. In the navigation pane, expand GSLB and click Services.
2. Select the GSLB service to be configured and click Open.
3. On the Advanced tab, under Site Persistence options, select the HTTPRedirect option.
4. In the Site Prefix text box, enter the site prefix (for example, vserver-GSLB-1).
5. Click OK.
Configuring GSLB for Proximity

When you configure GSLB for proximity, client requests are forwarded to the closest data center. The main benefit of the proximity-based GSLB method is faster response times resulting from the selection of the closest available data center. Such a deployment is critical for applications that require fast access to large volumes of data.

You can configure GSLB for proximity based on the round trip time (RTT), static proximity, or a combination of the two.

Configuring Dynamic Method (RTT)

Dynamic round trip time (RTT) is a measure of time or delay in the network between the client’s local DNS server and a data resource. To measure dynamic RTT, the NetScaler appliance probes the client’s local DNS server and gathers RTT metric information. The NetScaler then uses this metric to make its load balancing decision. Global server load balancing monitors the real-time status of the network and dynamically directs the client request to the data center with the lowest RTT value.

To configure GSLB for proximity with dynamic method, you must first configure the basic GSLB set up and then configure dynamic RTT.

First create two GSLB sites, local and remote. Then, for the local site, create a GSLB virtual server and GSLB services and bind the services to the virtual server. Then create ADNS services and bind the domain for which you are configuring GSLB to the GSLB virtual server at the local site. Finally, create a load balancing virtual server with the same virtual server IP address as the GSLB service.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).

Once you have configured a basic GSLB setup, configure the dynamic RTT method.

For details on how to configure the GSLB virtual server to use the dynamic RTT method for load balancing, see Configuring Dynamic RTT.

Configuring Static Proximity

The static proximity method for GSLB uses an IP address-based static proximity database to determine the proximity between the client’s local DNS server and the GSLB sites. The NetScaler appliance responds with the IP address of a site that best matches the proximity criteria.

If two or more GSLB sites at different geographic locations serve the same content, the NetScaler appliance maintains a database of IP address ranges and uses the database for decisions about the GSLB sites to which to direct incoming client requests.
To configure GSLB for proximity with static proximity, you must first configure the basic GSLB setup and then configure static proximity.

First create two GSLB sites, local and remote. Then, for the local site, create a GSLB virtual server and GSLB services and bind the services to the virtual server. Then create ADNS services and bind the domain for which you are configuring GSLB to the GSLB virtual server at the local site. Finally, create a load balancing virtual server with the same virtual server IP address as the GSLB service.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).

Once you have configured a basic GSLB setup, configure static proximity.

For details on how to configure the GSLB virtual server to use static proximity for load balancing, see Configuring Static Proximity.

### Configuring Static Proximity and Dynamic RTT

You can configure the GSLB virtual server to use a combination of static proximity and dynamic RTT when you have some clients coming from an internal network like a branch office. You can configure GSLB such that the clients coming from the branch office or any other internal network are directed to a particular GSLB site that is geographically close to the client network. For all other requests, you can use dynamic RTT.

First create two GSLB sites, local and remote. Then, for the local site, create a GSLB virtual server and GSLB services and bind the services to the virtual server. Then create ADNS services and bind the domain for which you are configuring GSLB to the GSLB virtual server at the local site. Finally, create a load balancing virtual server with the same virtual server IP address as the GSLB service.

For details on how to configure a basic GSLB setup, see Configuring Global Server Load Balancing (GSLB).

Once you have configured a basic GSLB setup, configure the GSLB virtual server to use static proximity for all traffic originating from an internal network and then use dynamic RTT for all other traffic.

For details on how to configure static proximity, see Configuring Static Proximity and for details on how to configure dynamic RTT, see Configuring Dynamic RTT.