## Contents

- Introduction .................................................................................................................. 3
- Prerequisites .................................................................................................................. 3
- Limitations .................................................................................................................... 3
- DTC Workflow ............................................................................................................. 3
  - Best Practices ............................................................................................................ 3
- NIOS DTC Objects ....................................................................................................... 4
  - DTC Servers .............................................................................................................. 4
  - Load Balancing Methods .......................................................................................... 4
    - Global Availability .................................................................................................. 4
    - Ratio ....................................................................................................................... 4
    - Round Robin ........................................................................................................... 4
    - Topology ............................................................................................................... 5
  - DTC Pools .................................................................................................................. 5
    - Topology Ruleset ................................................................................................... 6
  - DTC Load Balanced Domain Name ........................................................................... 6
  - DTC Health Monitors ............................................................................................... 6
- DTC Use Cases ............................................................................................................ 6
  - Load Balancing Internet Applications ........................................................................ 6
  - Load Balancing Internal/Intranet Applications .......................................................... 6
  - The DR Use case ...................................................................................................... 7
- Deploying DTC ............................................................................................................. 7
  - Assign Extensible Attributes to Networks in IPAM .................................................... 8
  - Configure DTC Servers ............................................................................................ 10
  - Configure Server Ruleset for DTC Pools .................................................................. 11
    - Configure DTC Pools ............................................................................................ 15
  - Configure Pool Topology Ruleset for LBDN ............................................................ 19
  - Configure LBDN ...................................................................................................... 21
- DTC LBDN Visualization ........................................................................................... 23
- Test DTC LBDN .......................................................................................................... 24
Introduction

DNS Traffic control (DTC) load balances user’s application traffic based on the Client’s location, the server’s location and the server’s availability. Through DNS Traffic Control, IT administrators can set up multiple sites and direct clients to the best available servers. DTC monitors application availability using various types of health checks to make sure the Clients are sent to servers that are available.

Prerequisites

The following are prerequisites for Infoblox DNS Traffic Control:

- Functional Infoblox Grid with a Grid Master. Several features described in this paper were introduced in 8.0 including Extensible Attributes for location and the HTTP/S Content Check.
- Active Grid with DNS license.
- DNS Traffic Control license.
- At least one NIOS appliance acting as an authoritative DNS Server (Primary).

Limitations

Following general limitations apply:

- Active Grid with DNS license.
- GSLB results are returned only if the query resolves to an authoritative zone to which an LBDN is explicitly linked.
- No authentication support in HTTP or HTTP/S monitor.
- No Automatic MaxMind updates. A single MaxMind DB per grid and only gets updated when a new version is manually uploaded. Please note- this does not need to be updated very often.
- The SIP monitor does not support SCTP transport.
- Only objects in the default DNS view of the default network view are considered.
- DNS Traffic Control license cannot be installed on the Infoblox 4030 appliance as it is intended as a caching only appliance.
- DTC health monitoring does not monitor dual stack servers (supporting IPv4 and IPv6 interfaces) if the Infoblox appliance health monitoring interface does not also have IPv4 and IPv6 IP stacks.

DTC Query Workflow

- A client sends a DNS request to a NIOS Grid Member where the DNS server processes it.
- If the final query name belongs to a zone for which the server is authoritative and matches an LBDN linked to that zone, then DTC handles the response. Otherwise normal DNS processing occurs.
- If the cache contains a previous answer to the same request for the same client and that server is still available, it is selected. Otherwise, based on current availability and configured topology rules, the GSLB algorithm selects first a Pool and then a specific server from that Pool (configuration dependent).
- A DNS record is synthesized from the address of the selected server and returned to the client.

Best Practices

To get the most from Infoblox DTC, Infoblox recommends the following best practices:

- A new DTC configuration should always be tested using the built-in LBDN test tool.
- For web application servers, HTTP and HTTP/S health monitors should be used to verify application level availability i.e. test for a specific string being returned rather than simply port 80 availability.
- Always view the traffic management structures through the built in hierarchical map view that can be used to quickly view the overall traffic management structure of a selected DNS Traffic Control Object.
- Use a naming convention for LBDN’s, and their associated Pools, Servers, and Topology rules. These naming conventions can be used for filtering within the GUI table views (they can be saved) and to identify a Server vs. Pool Topology rule.

**NIOS DTC Objects**

Before implementing DTC on a NIOS appliance, an administrator must understand different objects related to the DTC feature in NIOS. The following are the NIOS DTC objects.

**DTC Servers**

DTC Servers are objects that are associated with synthesized A, AAA, NAPTR, and/or CNAME records. The IP addresses of these Servers are sent back in DNS query-responses from DTC. The Servers can be actual physical servers, or local Server Load Balancer VIPs, or really anything with an IP address. Servers may be used by multiple Pools and topology rules. The Servers can also be disabled affecting all Pools using them. A Server may not be disabled if it is the last, non-disabled Server in any Pool that is used by an LBDN. The Servers that do not belong to any Pool or only belong to Pools that aren’t used by an LBDN may be disabled. Servers cannot be deleted while in use and must first be removed from every Pool and topology rule using them.

**Load Balancing Methods**

**Global Availability**

The Global Availability Load Balancing method always returns the first available Server that is in the list of Servers (obviously order is important). Availability is based on Health Monitor(s) used. It is an excellent load balancing method for DR. There is no weight configuration as part of this load balancing method. An example is shown in table below:

<table>
<thead>
<tr>
<th>Order</th>
<th>Weight</th>
<th>Server</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>n/a</td>
<td>1.1.1.1</td>
<td>down</td>
</tr>
<tr>
<td>2</td>
<td>n/a</td>
<td>2::2</td>
<td>up</td>
</tr>
<tr>
<td>3</td>
<td>n/a</td>
<td>3.3.3.3</td>
<td>up</td>
</tr>
<tr>
<td>4</td>
<td>n/a</td>
<td>4::4</td>
<td>down</td>
</tr>
</tbody>
</table>

With the Pool configuration shown in table above, queries for A records would result in a response of 3.3.3.3 and queries for AAAA records being returned 2::2.

**Ratio**

For the ratio method, the results’ distribution over time matches their weights but there is no expectation for sequential results. Responses are randomized, with each available option assigned a probability equal to its weight divided by the total weight of all available options. An example is shown in table below:

<table>
<thead>
<tr>
<th>Order</th>
<th>Weight</th>
<th>Server</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1.1.1.1</td>
<td>down</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2::2</td>
<td>up</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>3.3.3.3</td>
<td>up</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>4::4</td>
<td>up</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>5.5.5.5</td>
<td>up</td>
</tr>
</tbody>
</table>

With this Pool configuration and state, un-cached queries for A address is going to return 66% 3.3.3.3 and 33% 5.5.5.5 while un-cached queries for AAAA will return 50% 2::2 and 50% 4::4. Responses are going to exhibit no particular order.
Round Robin

In Round Robin method, the appliance returns servers sequentially and cyclically. Consider the following example where a Pool has three servers listed below:

- 10.10.1.1
- 10.10.2.2
- 10.10.3.3

Responses to DNS queries will be sequential in the following order,
10.10.1.1, 10.10.2.2, 10.10.3.3, 10.10.1.1, 10.10.2.2, 10.10.3.3……..

Topology

Topology Rules are configured globally and can be reused. Topology rules map a source IP to a destination Pool or Server. There are three types of Topology Rules:

1. Subnet – most often used with internal authoritative DNS
2. Geography- uses the MaxMind database to identify the location of the Client IP, typically used with external authoritative DNS as the MaxMind database contains public IP addresses.
3. Extensible Attribute- uses the Extensible Attributes (EAs) associated with the Client IP’s subnet to identify the location of the Client IP.

When GSLB processing evaluates a Topology Ruleset, it logically walks the list of Topology Rules in order and uses the first match with an available destination. Topology Rulesets can contain any combination of Subnet, Geography and Extensible Attribute Rules.

A Subnet Rule matches if the subnet contains the client IP.

To use Extensible Attribute Rules, the Admin specifies up to 4 Extensible Attributes to use for matching. The EAs selected are presumed to have a hierarchy based on geography, for example Continent/Country/Subdivision/City, though it is not enforced. A client IP matches an Extensible-Attribute Rule if the Extensible Attributes of the Client subnet match the values specified in the Extensible Attribute Rule.

A client IP matches a Geography rule if the MaxMind values selected matches the location of the Client IP.

As an example, assume that the following set of custom topology rules is configured and linked to an LBDN:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Source Conditions</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CONTINENT IS &quot;North America&quot;</td>
<td>Pool Non_US_Pool</td>
</tr>
<tr>
<td></td>
<td>COUNTRY IS_NOT &quot;United States&quot;</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>COUNTRY IS &quot;United States&quot;</td>
<td>Pool US_Pool</td>
</tr>
<tr>
<td>3</td>
<td>CONTINENT IS &quot;North America&quot;</td>
<td>Pool NA_Pool</td>
</tr>
<tr>
<td>4</td>
<td>SUBNET IS_NOT 173.194.33.0/24</td>
<td>Pool DEFAULT_Pool</td>
</tr>
</tbody>
</table>

- A rule matches only if all source conditions match, so the US won't match rule #1 despite being in North America.
- Rules are matched in order, so rule #3 will never be used.
- Subnet rules ignore the GeoIP database, so any other traffic that isn't from the 173.194.33.0/24 network will be directed to the default Pool.

If no rules are match then either the alternate LB method is used, if any, or a response is based on content from DNS that is not an LBDN. NXDOMAIN is one possible response.

DTC Pools

DTC Pools contain one or more Servers. All of the Servers in a Pool are typically in the same geographical location, but that is not a requirement. Clients are directed to a Pool using the selected Load Balancing Method.
Pools may be used by multiple LBDNs. Pools can be disabled and this affects all LBDNs using them. A Pool cannot be disabled if it is the last non-disabled Pool for any LBDN using it. A Pool cannot be deleted while in use. A Pool must be removed from every LBDN using it before it can be deleted. Pools in use must contain at least one enabled Server. The primary and alternate load-balancing methods of a Pool may not be the same, though load balancing method TOPOLOGY can be used as primary and alternate with different rulesets. Pools can be configured without health monitors.

**DTC Load Balanced Domain Name (LBDN)**

A DTC LBDN is a DTC object that is used by DNS Traffic Control to process DNS queries for load-balanced resources. Multiple LBDNs can be defined on the NIOS appliance and multiple patterns can be defined per LBDN. Permissions and extensible attributes can be configured for the LBDNs for administrative purposes. Multiple Pools and a single load balancing method for Pools can be assigned to an LBDN. For example, two LBDNs can co-exist such as [www.xyzcorp.com](http://www.xyzcorp.com) and [ftp.xyzcorp.com](http://ftp.xyzcorp.com) and can have their own Pools and load balancing methods. So when a dns query is received by NIOS for [www.xyzcorp.com](http://www.xyzcorp.com) or [ftp.xyzcorp.com](http://ftp.xyzcorp.com), the load balancing method for the LBDN is checked and a response formulated based on their respective rule sets. The load balancing method for the Pool is again checked and the query is then directed to the appropriate Server based on the assigned ruleset.

**DTC Health Monitors**

Health monitors determine the availability of DTC Servers and help route application traffic to the best available Servers. Health monitors are associated with Pools and not Servers. Every health monitor checks each Server that is associated with the Pool. NIOS supports pre-defined monitors and new custom health monitors can be created.

**DTC Use Cases**

The following two use cases are the most common:

a. Load balancing Internet applications
b. Load balancing internal/Intranet

**Load Balancing Internet applications**

In this use case, we use the built-in MaxMind database support, which contains information about which IP address blocks belong to which Geographical area of the world. The built-in Maxmind Database support is used to identify a query source IP address at the Continent, Country, City and Subdivision levels. Geography Rules use the Maxmind database to identify the location of the source of the DNS query, and select the appropriate Pool. Pools also use Geography Rules to further direct the DNS query to appropriate DTC Servers.

For example, an Admin can configure an LBDN to use a Geography Ruleset, which directs DNS queries to either a Europe Pool or a North America Pool. The Maxmind database will be used in determining the origin of the DNS query. If the DNS query originates from within Europe, it is directed to Europe Pool. For all queries originated from North America, the destination Pool is going to be North-America Pool.

Both the Europe and North America Pools can be configured to further direct queries to the appropriate Server based on the Client’s location. For example, if the query originated from the UK, the DTC configuration can direct it to the UK Datacenter Server and if it originated from any European country other than UK it is directed to the Paris Datacenter server. It boils down to what a user wants to achieve in terms of load balancing an application.

**Load Balancing Internal/Intranet Applications**

Traffic can be load balanced using DTC based on the querying client’s subnet or the Extensible Attributes of the client’s subnet.
A simple example of this use case is two subnet rules as follows:

- Subnet Rule-1. If the DNS query originates from subnet1, it is directed to Pool1. Then Pool1 directs DNS queries to appropriate DTC servers based on load balancing method configured (Ratio, Round Robin or Global Availability)

- Subnet Rule-2. If the dns query originates from subnet2, it is directed to Pool2. Then Pool2 directs DNS queries to appropriate DTC servers based on load balancing method configured (Ratio, Round Robin or Global Availability)

The Extensible Attribute use case example is provided as a step by step procedure under section “Deploying DTC”.

The Disaster Recovery Use case

This use case is based on availability to provide continuity of service for applications. For example, if Servers at a Primary Datacenter re unavailable, the application traffic can be directed to Servers at a Backup Datacenter. The load balancing method configured in this use case is Global Availability. The idea is to have all traffic go to the Primary Datacenter as long as it is available. If the Primary Datacenter ever goes down, then all traffic will be directed to the Backup Datacenter. When the Primary Datacenter comes back online, all traffic will again be directed to the Primary Datacenter.

It is possible to combine topology and availability rules for services.

Deploying DTC

We are going to use “Load balancing DNS resources for the internal enterprise network” as an example. In this use case there are four Data Center Servers:

- dtc-2-199 (London)
- dtc-2-129 (Paris)
- dtc-2-53 (Chicago)
- dtc-2-141 (Vancouver)

The two DTC Servers in London and Paris are going to be part of Europe Pool and Chicago and Vancouver DTC Servers are going to be part of North-America Pool.

The Pools are given names as follows:

- EMEA_POOL (For Europe and Middle East Region)
- NAM_POOL (For North America Region)

The LBDN is going to be configured for FQDN [www.xyzcorp.com](http://www.xyzcorp.com) and named as LBDN_xyzcorp.com,

The topology is built using Extensible Attributes that are already in use or can be configured for building an internal MaxMind style Geo-IP database. The extensible attributes used in this use-case are:

- Corp.Region (EMEA/NAM)
- Corp.Country (France/UK/USA/Canada)
- Corp.City (Paris/London/Chicago/Vancouver)
- Corp.Building (HQ/BO)

The following steps are required to bring up this DTC use case:

- Assign Extensible Attributes to the networks from where the DNS queries originate
- Configure DTC Servers
- Configure Server Topology Rulesets for DTC Pools
- Configure DTC Pools
- Configure Pool Topology Ruleset for LBDN
Configure LBDN

Assign Extensible Attributes to IPAM networks

In an enterprise environment with internal IP ranges (without a GeoIP database), EAs can be used to build a manual internal GeoIP database by mapping EAs to networks in IPAM.

In our example we are using networks,

- 10.61.3.0/24
- 10.61.4.0/24
- 10.61.5.0/24
- 10.61.6.0/24

1. Click Data Management > IPAM and navigate to networks 10.61.3.0/24.

2. Click Gear next to 10.61.3.0/24 network.

3. Select Extensible Attributes as shown above.
4. Click +.
5. Select Corp-Region under Attribute Name column and select EMEA from drop-down list in Value column.
6. Click +.
7. Select Corp-Country under Attribute Name column and select France from drop-down list in Value Column.
8. Click +.
9. Select Corp-City under Attribute Name column and select Paris from drop-down list in Value column.
10. Click +.
11. Select Corp-Building under Attribute Name column and select HQ from drop-down list in Value column.
12. Click Save & Close.
12. Repeat steps 2 to 11 for the following networks:

   - **10.61.4.0/24**
     - Corp-Region (EMEA)
     - Corp-Country (UK)
     - Corp-City (London)
     - Corp-Building (BranchOffice)
   
   - **10.61.5.0/24**
     - Corp-Region (NAM)
     - Corp-Country (Canada)
     - Corp-City (Vancouver)
     - Corp-Building (BranchOffice)
   
   - **10.61.6.0/24**
     - Corp-Region (NAM)
     - Corp-Country (USA)
     - Corp-City (Chicago)
     - Corp-Building (BranchOffice)

13. Once all networks are assigned EAs, the IPAM screen must look like the screenshot below.

14. Click Grid DNS Properties from Toolbar under Data Management > DNS.
15. Click Traffic Control.
16. Click External Attributes 1 drop down menu and select Corp-Region.
17. Click + to add External Attribute 2.
19. Click + to add External Attribute 3.
20. Select Corp-City.
22. Select Corp-Building.
23. Click Save & Close.
24. Click Rebuild.

**Configure DTC Servers**

In our example we are going to add four DTC Servers with the following names and IP addresses.

dtc-2-53 – 10.61.2.53  (Chicago Datacenter)
dtc-2-129 – 10.61.2.129 (Paris Datacenter)
dtc-2-141 – 10.61.2.141 (Vancouver Datacenter)
dtc-2-199 – 10.61.2.199 (London Datacenter)

The steps below are going to add dtc-2-53 DTC server directly through IPAM assuming that there is a DNS record entry for the DTC server in IPAM. If none, then user must create a DNS record entry, such as an A record. Note: there are other ways to add DTC servers such as using the Toolbar. In NIOS 8.0 functionality has been added to directly create DTC servers from discovered data using IPAM.

Once the Extensible Attributes (EAs) and the DNS records for the DTC servers have been configured, the user can then add the remaining three servers by repeating these steps:

1. Go to Data Management > IPAM
   
   Navigate to network IP Map of 10.61.2.0/24 from where dtc-2-53 server is to be created.
2. Click on 10.61.2.53.

3. Scroll down all the way to Related Objects section under IP Map, and Click on Gear next to external-2.nios (A record) and select Create DTC Server.

Type dtc-2-53 in the Name field.

4. Click Save & Close.

Repeat steps 2 to 4 to add remaining three DTC servers.

Configure Server ruleset for DTC Pools

In our example we are going to configure two Server Topology Rulesets, one for North-America Pool and Europe Pool for the other. The Topology Rulesets are named NAM-Ruleset and EMEA-Ruleset.

The topology rulesets are Extensible Attribute rulesets introduced in NIOS release 8.0.

The NAM-Ruleset is going to have two rules as follows:

- Rule 1: If the source DNS query is from North America and specifically from Branch Office in Chicago, then the destination is dtc-2-53 Datacenter.
- Rule 2: If the source DNS query is from North America and specifically from Branch Office in Vancouver, then the destination is dtc-2-141 Datacenter.

The **EMEA-Ruleset** is going to have two rules as follows:

- Rule 1: If the source DNS query is from Europe and more specifically from Branch Office in London, then the destination is dtc-2-199 Datacenter.

- Rule 2: If the source DNS query is from Europe and more specifically from Paris HeadQuarters, then the destination is dtc-2-129 Datacenter.

To configure the Topology Rulesets for DTC Pools, follow the steps below:

1. Go to Data Management > DNS > Traffic Control.

2. Click Manage Topology Rulesets from Toolbar.

3. In Topology Manager, click + to open Ruleset window.

4. Type EMEA-Ruleset in Name field.

5. Select Server as Destination Type.

6. Click + in Rules section and select Extensible Attribute Rule.

7. Select EMEA for Corp-Region.

8. Select France for Corp-Country.

9. Select Paris for Corp-City.

10. Select HQ for Corp-Building.

12. Click Add.

13. Click + in Rules section and select Extensible Attribute Rule.

14. Select EMEA for Corp-Region.

15. Select UK for Corp-Country.

16. Select London for Corp-City.

17. Select BranchOffice for Corp-Building.


19. Click Add.

20. Click Save & Close.
21. In Topology Manager Click + to open Ruleset window.

22. Type NAM-Ruleset in Name field.

23. Select Server as Destination Type.

24. Click + in Rules section and select Extensible Attribute Rule.

25. Select NAM for Corp-Region.


27. Select Vancouver for Corp-City.

28. Select BranchOffice for Corp-Building.

29. Select server dtc-2-141 for Destination.

30. Click Add.

31. Click + in Rules section and select Extensible Attribute Rule.

32. Select NAM for Corp-Region.

33. Select USA for Corp-Country.

34. Select Chicago for Corp-City.

35. Select BO for Corp-Building.


37. Click Add.
Configure DTC Pools

In our example, we are going to configure two DTC Pools named **POOL_NAM** and **POOL_EMEA**

**POOL_NAM** is going to use **Topology** Load balancing method and **NAM_Ruleset** for rules. It is going to have DTC Servers dtc-2-53 and dtc-2-141 as its Pool members.

**POOL_EMEA** is also going to use **Topology** load balancing method and **EMEA-Ruleset** for rules. It is going to have DTC Servers dtc-2-129 and dtc-2-199 as its Pool members.

In NIOS 8.0 release, Default Visualization can be used to configure these DTC objects and in the following section user can learn how to use them.

To configure DTC Pools:

1. Go to **Data Management > DNS > Traffic Control**.
2. From Toolbar, Click **Add**.
3. Select **Default Visualization**.
4. Click on POOL_TEMPNAME_xxxxx (where xxxxx is some randomly generated number).

5. Click on Add Existing Server.


7. Select SERVER_TEMPNAME_xxxxx from Pool Members.

8. Click Delete.

9. Click General Tab and type POOL_EMEA in Name field.

10. Click Health Monitors tab.
   a. select ICMP and HTTP health monitors to move them under Active column
11. Click Load Balancing Tab.

12. Select Topology under Preferred.


14. Click Save & Close

Repeat above steps to add POOL_NAM as follows:

1. From Toolbar, Click +Add

2. Select Default Visualization

3. Click on POOL_TEMPNAME_xxxxx (where xxxxx is some randomly generated number)
4. Click on Add Existing Server.


6. Select SERVER_TEMPNAME_xxxxx from Pool Members.

7. Click Delete.

8. Click General Tab and type POOL_NAM in Name field.

9. Click Health Monitors tab.

   a. select ICMP and HTTP health monitors to move them under Active column.

10. Click Load Balancing Tab.

11. Select Topology under Preferred.

Configure Pool Topology Ruleset for LBDN

In our example we are going to configure a ruleset for the LBDN named LBDN-xyzcorp-ruleset with destination as Pool.

The ruleset is going to have two rules as follows:

- Rule 1: If the source DNS query is from North America Region, then the destination is POOL_NAM.
- Rule 2: If the source DNS query is from Europe Region, then the destination is POOL_EMEA.

To configure the Topology ruleset for LBDN follow the steps below:

15. Go to Data Management > DNA > Traffic Control.
16. From Toolbar, Click Manage Topology Rulesets.
3. In Topology Manager Click + to open Ruleset window.
4. Type LBDN-xyzcorp-ruleset in Name field.

13. Click Save & Close.
5. Select Pool as Destination Type.

6. Click + in Rules section and select Extensible Attribute Rule.

7. Select EMEA for Corp-Region.

8. Select Any for Corp-Country.

9. Select Any for Corp-City.

10. Select Any for Corp-Building.

11. Select pool POOL_EMEA for Destination.

12. Click Add.

13. Click + in Rules section and select Extensible Attribute Rule.

14. Select NAM for Corp-Region.

15. Select Any for Corp-Country.

16. Select Any for Corp-City.

17. Select Any for Corp-Building.
18. Select pool POOL_NAM for Destination.

19. Click Add.

![Image of pool selection]

20. Click Save & Close.

**Configure LBDN**

In our example we are going to create a Load balanced domain name LBDN_xyzcorp.com using Default Visualization. This LBDN is going to load balance DNS queries that match pattern *.xyzcorp.com for authoritative zone xyzcorp.com. The Topology Ruleset used is Extensible Attribute ruleset named LBDN-xyzcorp-ruleset and the associated Pools are POOL_NAM and POOL_EMEA.

To configure LBDN:

1. Go to Data Management > DNS > Traffic Control.

2. Click gear icon next to a LBDN_TEMPNAME_xxxxx (where xxxxx is a random number).

   a. Select Expand Visualization.

   ![Image of expand visualization]

3. Move cursor over LBDN_TEMPNAME_xxxxx.

   a. Select Edit.
4. In General Tab, Type LBDN_xyzcorp.com in Display Name field.

5. Click +.

6. Type *.xyzcorp.com in row under Patterns table.

7. Select Topology as Load Balancing Method.

8. Select LBDN-xyzcorp-ruleset as Topology Ruleset.

9. In Associated Zones and Records Tab, click +.

10. Select xyzcorp.com zone from the list.

11. In Pools Tab, click +.

12. Select POOL_NAM and repeat step 11 for POOL_EMEA.

13. Click Save & Close.

15. Click Enable.

16. Click Yes.

17. Close Visualization display.

18. Click Restart.

**DTC LBDN Visualization**

As complicated DTC configurations can be created, the GUI provides a graphical view where an administrator can visualize the hierarchy of DTC objects along with the configuration status.

In our example, we are going to see the Traffic Management structure of our configured DTC LBDN named LBDN_xyzcorp.com by clicking on the gear icon next to the DTC LBDN and selecting Expand Visualization.

This takes us to a page with graphical representation of the selected DTC LBDN. The working configuration is displayed with all checkmarks in Green.
The Legend shows colors that provide the status of the DTC LBDN, for example Green means everything is running. The traffic management structure is an inverted tree representation with its root at DTC LBDN. In our example, the root is branching out to two DTC Pools named POOL_NAM and POOL_EMEA, which are further, branched out to their respective DTC Server members. We can click on any of the DTC objects to view the next DTC objects under it. The NIOS DTC visualization tool is not just a read-only tool a user can add, delete and modify DTC config with a click of a button. Note: You may need to wait about 3 minutes after a service restart for the all items on the visualization to be displayed as a green status.

**Test DTC LBDN**

Infoblox NIOS provides a testing function to test the DTC response for a specific LBDN. Using this the configuration of the DTC LBDN can be validated. Only Infoblox LBDNs can be tested using this feature.

To test an LBDN:

1. Go to Data Management > DNS > Traffic Control.
2. Click on Gear icon next to LBDN_xyzcorp.com.
3. Click Test.
4. Type 10.61.3.150 in Query Source field.
5. Type www.xyzcorp.com in Query Name field.
6. Select gm.nios in Member field by clicking Select button.
7. Select A for Record Type.
8. Click Start.
Verify the Query Response as “10.61.2.129”. It is Server dtc-2-129 served when query originated from HQ/Paris/France/EMEA.