DEPLOYMENT GUIDE

Enabling and Configuring DNS Traffic Control in NIOS 8.x

Table of Contents

Introduction........2
Prerequisites........2
Limitations........2
DTC Query Workflow........3
Best Practices........4
NIOS DTC Objects........4
    DTC Servers........4
    DTC Pools........5
    DTC Load Balanced Domain Name (LBDN)........5
    Load Balancing Methods........5
        All Available........6
        Global Availability........7
        Round Robin........7
        Ratio:Fixed........7
        Ratio:Dynamic........8
        Topology........9
    DTC Health Monitors........10
DTC Use Cases........12
    Load Balancing Internet applications........12
    Load Balancing Internal/Intranet Applications........13
    The Disaster Recovery Use case........13
    The Apex Record Use case........13
Deploying DTC........14
    Setup Details........14
    Assign Extensible Attributes to IPAM networks........15
    Configure DTC Servers........21
    Configure Server ruleset for DTC Pools........24
    Configure DTC Pools........33
    Configure Pool Topology Ruleset for LBDN........45
    Configure LBDN........52
    DTC LBDN Visualization........56
    Test DTC LBDN........57
CSV Import/Export Support........60
DTC Backup/Restore Support........61
WAPI support........61
Conclusion........63
Additional Information........63

Introduction

DNS Traffic control (DTC) load balances the 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 8.3 including DTC Health Check Support for Multi-Tier Architecture, CSV Import/Export support, Dynamic Load Balancing Based on SNMP and RTD, and support for SRV records.
- Active Grid with DNS license.
- DNS Traffic Control license.
- At least one NIOS appliance acting as an authoritative DNS Server (Primary).

Limitations

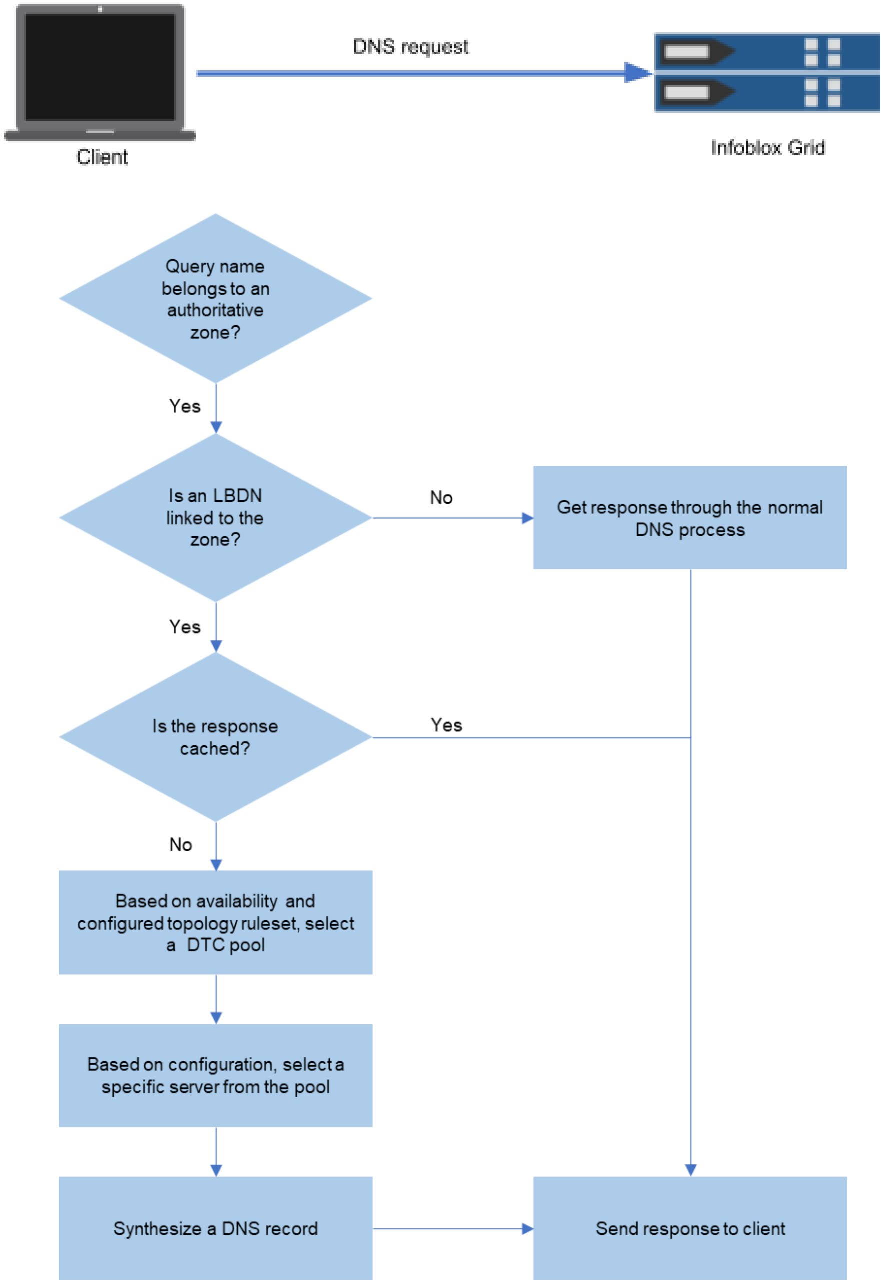
Following general limitations apply:

- 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.
- The DNS Traffic Control querying process is not supported for recursive queries.
- 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.
- DNS Traffic Control license cannot be installed on the Infoblox 4030 appliance as it is intended as a caching only appliance.
- Infoblox does not support running DNS Traffic Control on the TE-810 and TE-820 appliances.

- 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.

- The DNS Traffic Control does not support the Global application of an LBDN pattern against all queries. The appliance returns a result only if the query resolves to an authoritative zone to which an DNS Traffic Control LBDN is explicitly linked.

DTC Query Workflow


DNS request
Client
Infoblox Grid
Query name belongs to an authoritative zone?
Yes
Is an LBDN linked to the zone?
No
Get response through the normal DNS process
Yes
Is the response cached?
Yes
No
Based on availability and configured topology ruleset, select a DTC pool
Based on configuration, select a specific server from the pool
Synthesize a DNS record
Send response to client

1. A client sends a DNS request to a NIOS Grid Member where the DNS server processes it.

2. 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.

3. 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).

4. 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, AAAA, NAPTR, CNAME and/or SRV 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.

DTC Pools

DTC Pools contain one or more Servers. All 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.

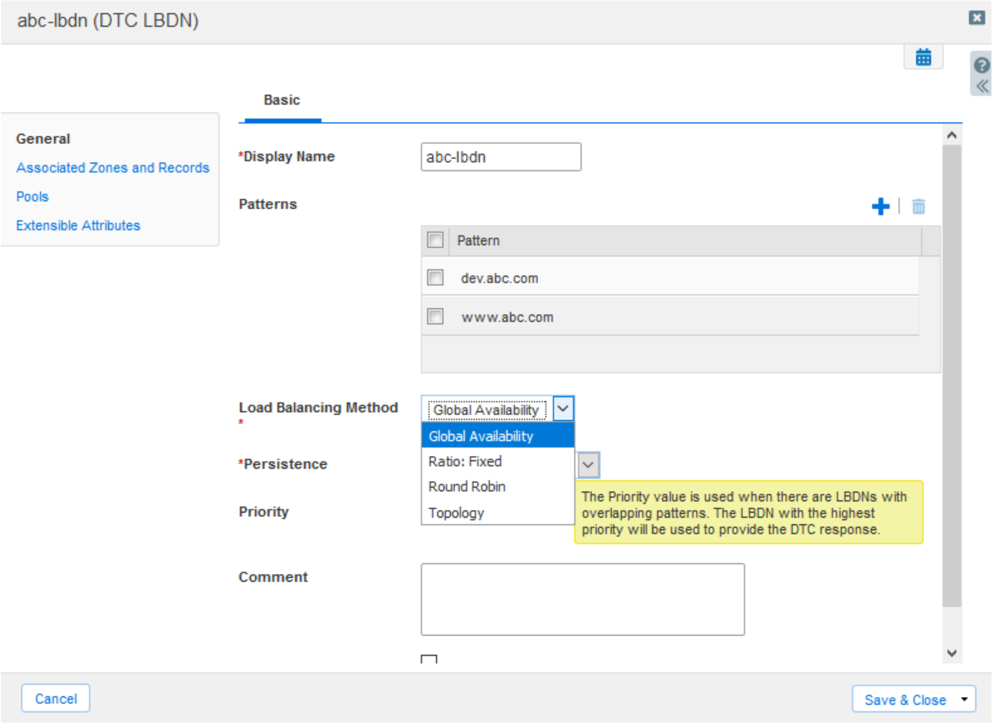
Multiple Pools and a single load balancing method for Pools can be assigned to an LBDN. For example, two LBDNs can co-exist such as www.xyzcorp.com and ftp.xyzcorp.com and can have their own Pools and load balancing methods. So when a DNS query is received by NIOS for www.xyzcorp.com or ftp.xyzcorp.com, the load balancing method for the corresponding LBDN is checked and a response is 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. The image below depicts the hierarchy of the objects.

Load Balancing Methods

Based on the load balancing method defined for an LBDN, the DNS Traffic Control selects an available pool. Based on the method selected for a pool, it selects an available server. You can define the following Load Balancing methods:

Load Balancing Method	LBDN	Pool	Details
All Available	-	+	Responds to the query with all the available servers in the DTC pool for the appropriate record type.
Global Availability	+	+	Clients are directed to the first Pool or Server in the list. Only if the first resource becomes unavailable will DTC direct clients to the next resource in the list.
Round Robin	+	+	Clients are directed to Servers in a Pool or among Pools (in a multiple pool configuration) using round

			robin.
Ratio: Fixed	+	+	Clients are directed to Servers in a Pool or among Pools (in a multiple Pool configuration) using weighted round robin.
Ratio: Dynamic (Round Trip Delay)	-	+	Uses dynamic responses (based on RTD or SNMP responses) received via health check monitors to direct clients to Servers in a Pool, using weighted round robin.
Ratio: Dynamic (SNMP)	-	+	
Topology	+	+	Clients are directed to a Pool or Server based on the Client's IP matching a geo map (External) or a Subnet (Internal or External).


abc-lbdn (DTC LBDN)

Basic

General
Associated Zones and Records
Pools
Extensible Attributes

*Display Name: abc-lbdn

Patterns

☐ Pattern
☐ dev.abc.com
☐ www.abc.com

Load Balancing Method *: Global Availability
- Global Availability
- Ratio: Fixed
- Round Robin
- Topology

*Persistence

Priority

The Priority value is used when there are LBDNs with overlapping patterns. The LBDN with the highest priority will be used to provide the DTC response.

Comment

All Available

The All Available Load Balancing method responds to the query with all the available servers in the DTC pool for the appropriate record type. The responses are returned in the same order in which the servers are listed in the DTC pool, eliminating the unavailable servers. Availability is based on Health Monitor(s) used. The system considers only the order of the servers in the DTC pool and ignores the weight of available servers.

Order	Weight	Server	Availability
1	n/a	1.1.1.1	up
2	n/a	2::2	up
3	n/a	3.3.3.3	down
4	n/a	4::4	down
5	n/a	5.5.5.5	up

With the Pool configuration shown in table above, queries for A records would result in a response of both 1.1.1.1 and 5.5.5.5, and queries for AAAA records would result in 2::2.

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:

Order	Weight	Server	Availability
1	n/a	1.1.1.1	down
2	n/a	2::2	up
3	n/a	3.3.3.3	up
4	n/a	4::4	down

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.

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……..

Ratio:Fixed

For the Ratio:Fixed 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:

Order	Weight	Server	Availability
1	1	1.1.1.1	down
2	2	2::2	up
3	2	3.3.3.3	up

4	2	4::4	up
5	1	5.5.5.5	up

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.

Ratio:Dynamic

- Using the Ratio: Dynamic method, the appliance weights the DTC servers dynamically based on round trip delay or SNMP health monitor data. You can use one of the following options:
- Round trip delay: Based on the round-trip delay from the DTC member that received a client's DNS request, the system sends clients to the server with the minimal latency time, i.e. the closest one. You need a pre-configured health monitor for this load balancing method. An example is shown in the table below:

Server	Latency (ms)
A	25
C	18
D	50

With this configuration, 100% of the traffic is distributed to Server C.

- SNMP: Based on data from the SNMP monitor associated to the server, for example, CPU or memory utilization, the system sends clients to the server with the lowest load. For this load balancing method, you need a pre-configured SNMP health monitor with a required metric to be tracked. The metric is set through an object identifier (OID) in the monitor properties. This method supports only OIDs for which the server can return an integer value.

The value of the monitored metric defines how the traffic is directed. By default, the servers with the highest metric values receive the client requests. There may be cases when your selected metric reflects server availability in the opposite way, that is, the lowest metric values indicate available servers. For such cases, you can invert the value of the OID, that is, of the monitored metric, and have the traffic directed to the lowest-rated servers.

You can select to weigh servers by either priority or ratio. In case of priority, traffic is directed towards the servers that report the best metric values, other servers being bypassed. In case of ratio, traffic is distributed across all servers based on the values of the monitored metric for each of them. If a health check for a server is failed, the server is excluded from the load balancing.

An example is shown in the table below:

Server	CPU utilization (%)
A	90
C	50
D	10

With normal dynamic weights, 60% of the traffic is distributed to Server A, 33% to Server C, and 7% to Server D.
This means that the most loaded server will receive most requests than the less loaded one. For this case, the metric should be inverted to reflect server availability appropriately, resulting in 8% of the traffic being distributed to Server A, 15% to Server C, and 77% to Server D.

Topology

Topology Rules are configured globally and can be reused. Topology rules map a source IP to a destination Pool or Server. With NIOS 8.5, the ability to map topology rules to NOERR/NODATA/NXDOMAIN as responses has been added. This is useful in a scenario where you want to provide one of these responses when queries come from a specific client. Prior to this release, the only way to implement this would have been to have a DTC pool with a single server with a failed health check. This would result in a failure status on the pool and a warning status on the LBDN.

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:

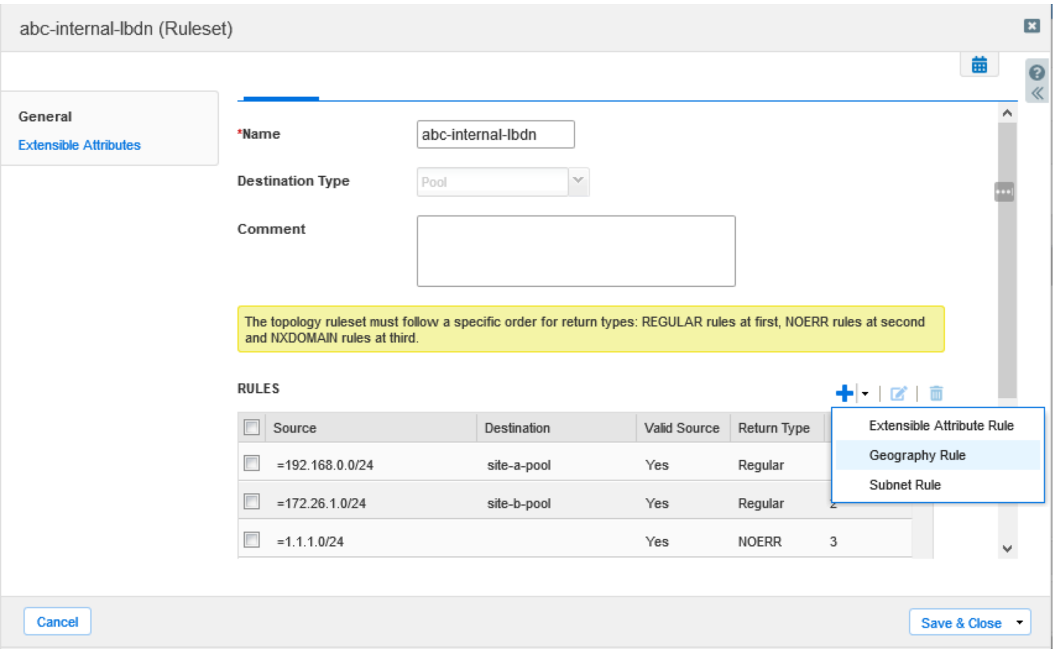
Rule	Source Conditions	Destination
1	CONTINENT IS "North America" COUNTRY IS_NOT "United States"	Pool Non_US_Pool
2	COUNTRY IS "United States"	Pool US_Pool

3	CONTINENT IS "North America"	Pool NA_Pool
4	SUBNET IS_NOT 173.194.33.0/24	Pool DEFAULT_Pool

- 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 matched, then either the alternate LB method is used, if any, or a response is based on content from DNS that is not an LBDN.

The topology ruleset must follow a specific order for return types: REGULAR rules at first, NOERR rules at second and NXDOMAIN rules at third.



abc-internal-lbdn (Ruleset)

General
Extensible Attributes

*Name: abc-internal-lbdn

Destination Type: Pool

Comment:

The topology ruleset must follow a specific order for return types: REGULAR rules at first, NOERR rules at second and NXDOMAIN rules at third.

RULES

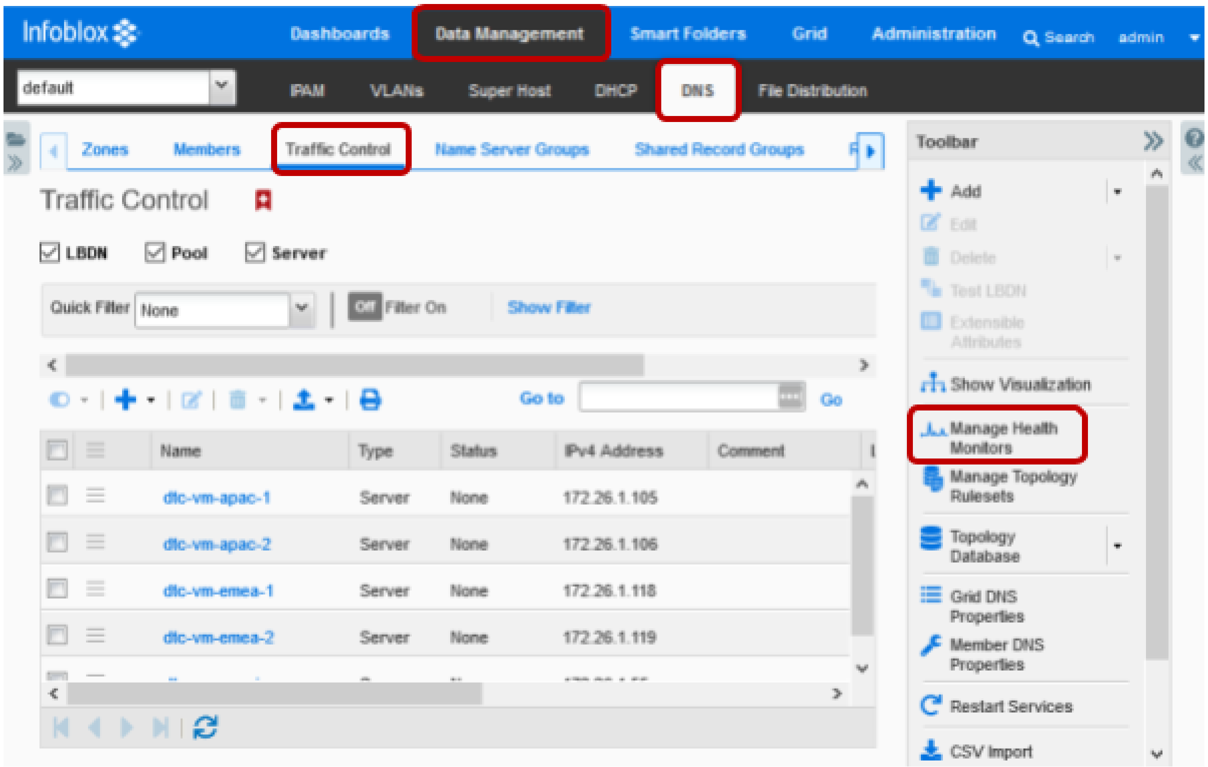
□	Source	Destination	Valid Source	Return Type	
□	=192.168.0.0/24	site-a-pool	Yes	Regular	
□	=172.26.1.0/24	site-b-pool	Yes	Regular	2
□	=1.1.1.0/24		Yes	NOERR	3

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 (HTTP, ICMP, PDP, SIP, SNMP, and TCP) and new custom health monitors can be created.

Health Monitor	Details
HTTP/HTTPS	Sends a GET request and checks the content and return code.
SNMP	Retrieves an OID and compares that value to a constant.
TCP	Validates the health of a Server by attempting a full TCP handshake.
SIP	Sends SIP OPTIONS and check the return code. Supports SIPS, TCP,

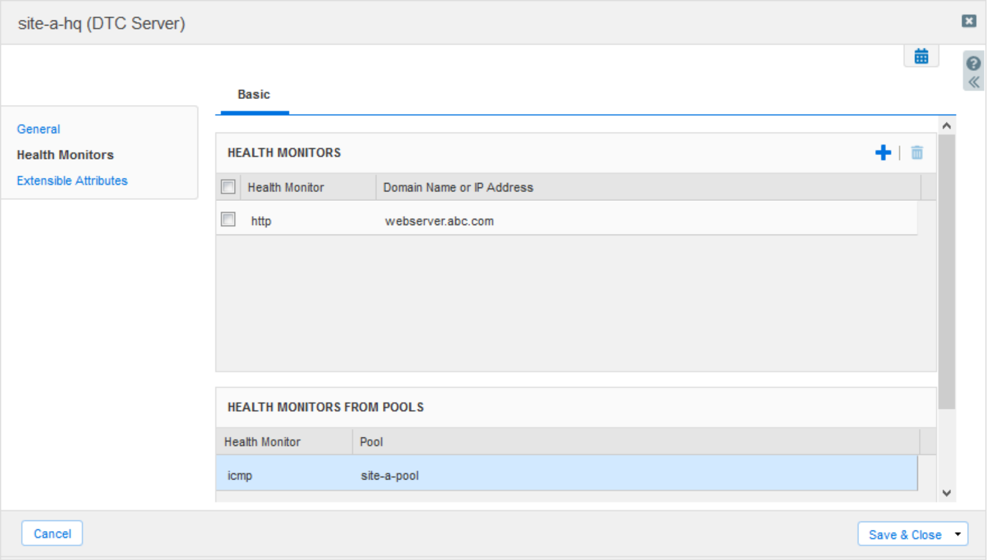
	TLS, and UDP.
PDP	Sends fixed GTP ECHO. Receiving any ECHO response constitutes success.
ICMP	Sends an ICMP/ICMPv6 Echo Request and expects an ICMP/ICMPv6 Echo Response.



Name	Type	Status	IPv4 Address	Comment
dtc-vm-apac-1	Server	None	172.26.1.105	
dtc-vm-apac-2	Server	None	172.26.1.106	
dtc-vm-emea-1	Server	None	172.26.1.118	
dtc-vm-emea-2	Server	None	172.26.1.119	

Custom Monitors can be added by navigating to **Data Management** → **DNS** → **Traffic Control**→**Click Manage Health Monitors** from the Toolbar.

NIOS 8.2 onwards, Multi-tier health check is supported. You can choose if you want to monitor at a pool level or the server level, or both. For example, at the pool level you may choose ICMP as your monitor to ensure that the server is up. Additionally, you can add another monitor at the server level to check the health of the link on the server by polling an external domain. This tests the health of one or more arbitrary servers to determine the availability of the application on the DTC server.



HEALTH MONITORS

	Health Monitor	Domain Name or IP Address
☐	http	webserver.abc.com

HEALTH MONITORS FROM POOLS

Health Monitor	Pool
icmp	site-a-pool

DTC Use Cases

The following four use cases are the most common:

- Load balancing Internet applications
- Load balancing internal/Intranet applications
- Disaster Recovery
- APEX Record to CNAME support

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 the 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". You can even utilize DNS resolution to provide traffic segregation of Microsoft Active Directory (AD) authentication for non-site-aware clients. DTC can be used as a solution by providing site specific Service Record (SRV) responses based on device location, whether on-premises or in the public cloud.

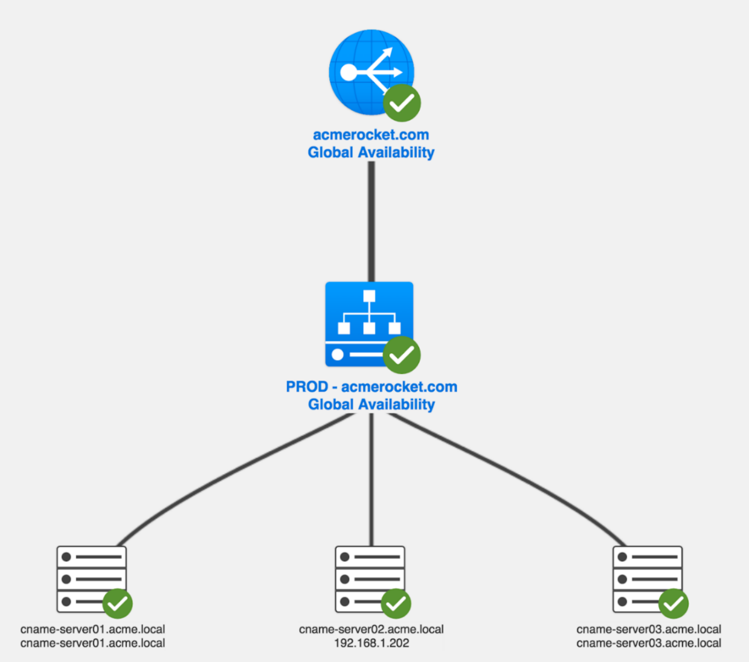
The Disaster Recovery Use case

This use case is based on availability to provide continuity of service for applications. For example, if Servers at a Primary Datacenter are 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.

The Apex Record Use case

The zone apex is where the SOA and NS (and often MX) records for a DNS zone are placed. They are DNS records whose name are the same as the zone itself. The DNS record type CNAME (Canonical Name) is used for rewriting one name in a zone to another different name, which could be in the same zone, or somewhere else. The apex contains record types which are clearly not used in the identification of a canonical host resource (NS, SOA), which cannot be aliased without breaking the standard at a fundamental level.

DTC enables mapping apex record to a CNAME, like below. Here apex "acmerocket.com" is mapped to "acme.local" servers.


acmerocket.com
Global Availability
PROD - acmerocket.com
Global Availability
cname-server01.acme.local
cname-server01.acme.local
cname-server02.acme.local
192.168.1.202
cname-server03.acme.local
cname-server03.acme.local

Deploying DTC

We are going to use “Load balancing DNS resources for the internal enterprise network” as an example.

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

Setup Details

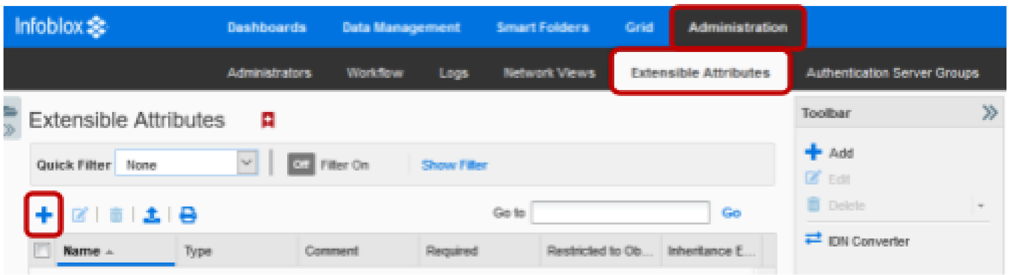
In this use case, there are five Data Center Servers, part of three Pools, that are configured for one LBDN.

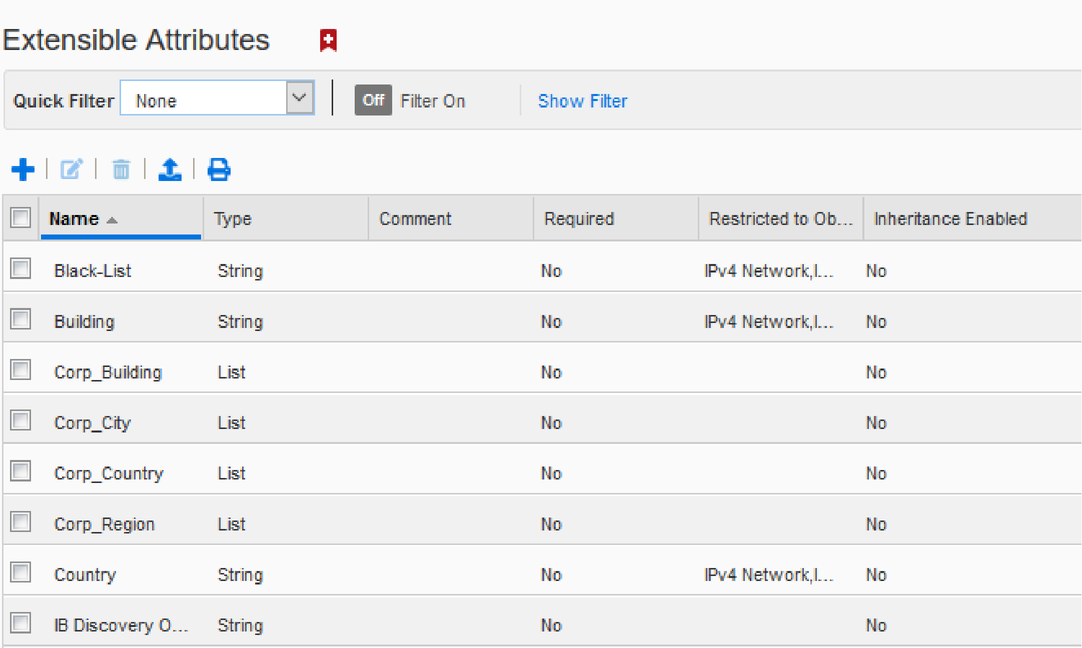
DTC Server	Location	DTC Pool	LBDN	FQDN
dtc-vm-apac-1	Singapore	APAC-Pool	LBDN-demo-dg.com	www.demo-dg.com
dtc-vm-apac-2	Bangalore			
dtc-vm-emea-1	London	EMEA-Pool		
dtc-vm-emea-2	Paris			
dtc-vm-americas	Chicago	Americas-Pool		

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 (EA) used in this use-case are:

Extensible Attribute	Possible values
Corp_Region	APAC/EMEA/NAM
Corp_Country	Singapore/India/UK/France/USA
Corp_City	Singapore/Bangalore/London/Paris/Chicago
Corp_Building	HQ/BO

You can add these EAs by navigating to **Administration** → **Extensible Attributes** → **+.**





□	Name ▲	Type	Comment	Required	Restricted to Ob...	Inheritance Enabled
□	Black-List	String		No	IPv4 Network,I...	No
□	Building	String		No	IPv4 Network,I...	No
□	Corp_Building	List		No		No
□	Corp_City	List		No		No
□	Corp_Country	List		No		No
□	Corp_Region	List		No		No
□	Country	String		No	IPv4 Network,I...	No
□	IB Discovery O...	String		No		No

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.

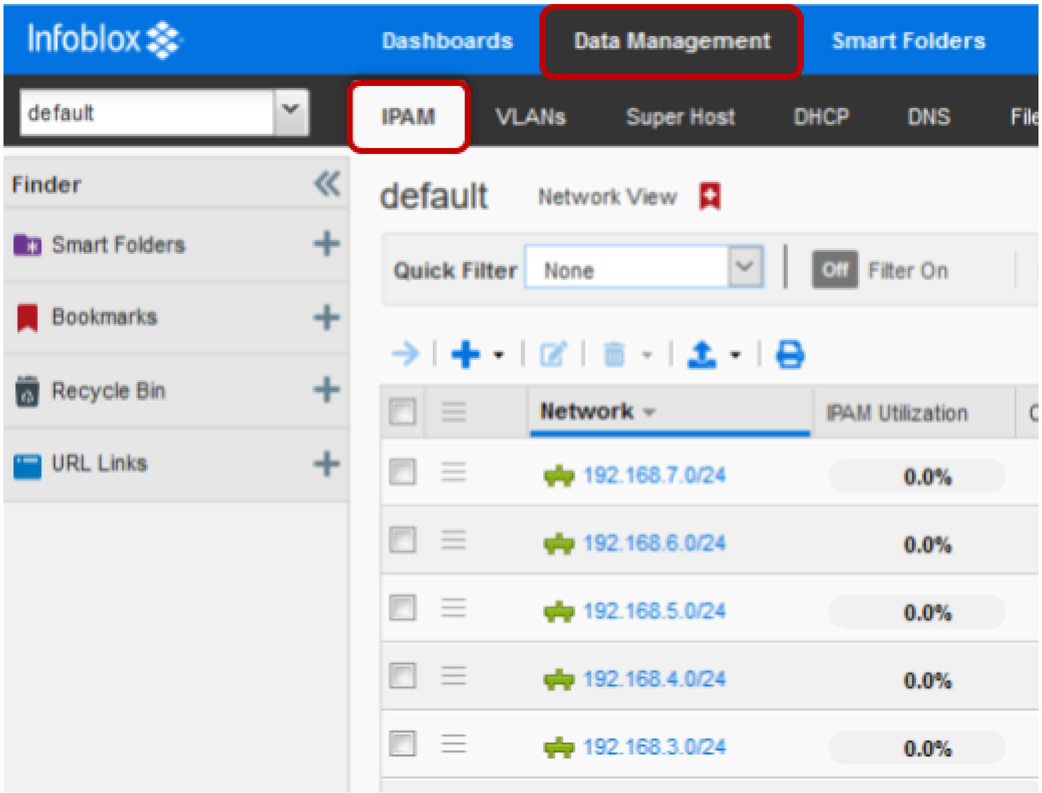
In our example we are using networks,

- 192.168.3.0/24

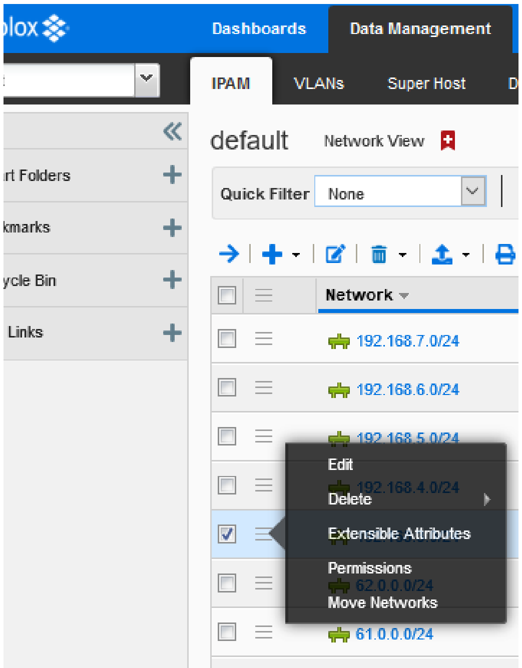
- 192.168.4.0/24
- 192.168.5.0/24
- 192.168.6.0/24
- 192.168.7.0/24

To update the IPAM networks with the EAs:

1. Click **Data Management** → **IPAM** and navigate to networks **192.168.3.0/24**.



2. Click on ☰ the next to 192.168.3.0/24 network.



3. Select **Extensible Attributes** as shown below.

4. Click +.

5. Select `Corp_Region` under Attribute Name column and select APAC from drop-down list in Value column.

6. Click +.

7. Select `Corp_Country` under Attribute Name column and select Singapore from drop-down list in Value Column.

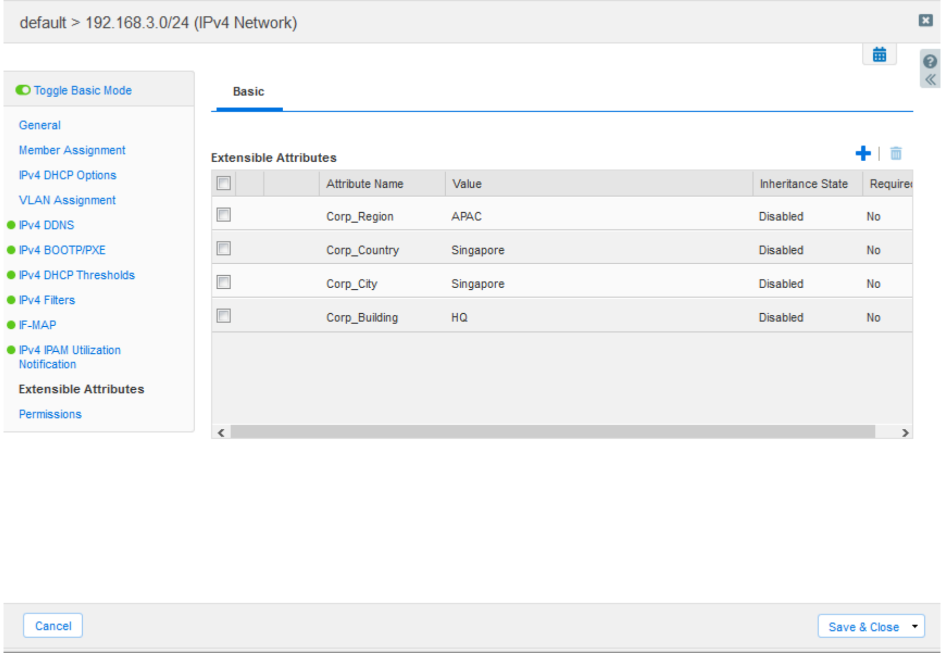
8. Click +.

9. Select `Corp_City` under Attribute Name column and select Singapore 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**.



default > 192.168.3.0/24 (IPv4 Network)

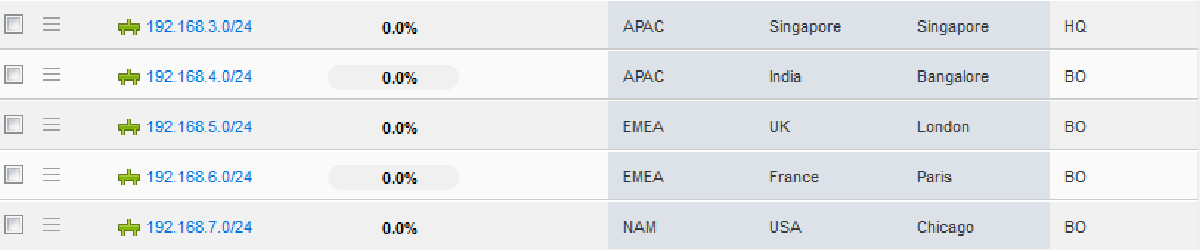
Extensible Attributes

Attribute Name	Value	Inheritance State	Require
Corp_Region	APAC	Disabled	No
Corp_Country	Singapore	Disabled	No
Corp_City	Singapore	Disabled	No
Corp_Building	HQ	Disabled	No

13. Repeat steps 2 to 11 for the following networks:
    - 192.168.4.0/24
        - Corp-Region (APAC)
        - Corp-Country (India)
        - Corp-City (Bangalore)
        - Corp-Building (BO)
    - 192.168.5.0/24
        - Corp-Region (EMEA)
        - Corp-Country (UK)
        - Corp-City (London)
        - Corp-Building (BO)
    - 192.168.6.0/24
        - Corp-Region (EMEA)

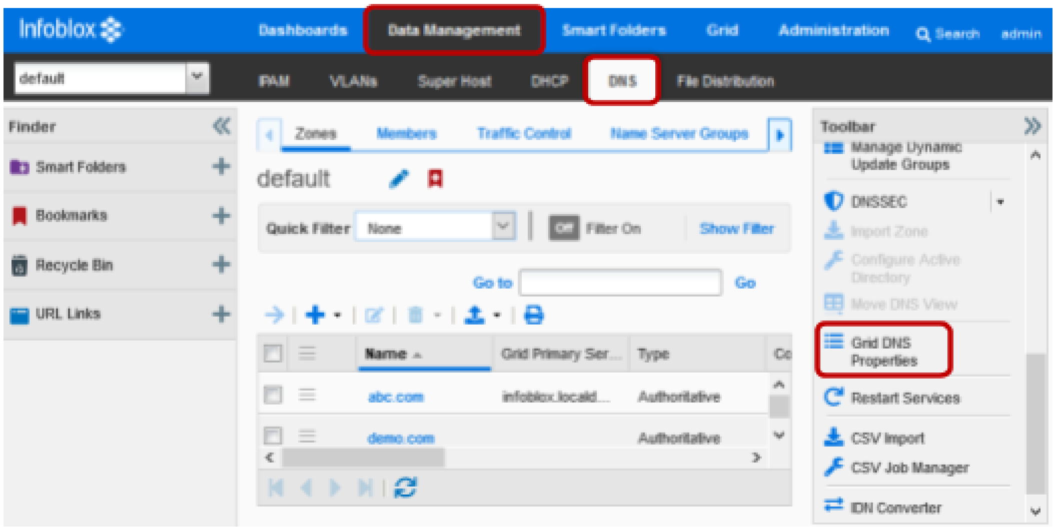
        - Corp-Country (France)
        - Corp-City (Paris)
        - Corp-Building (BO)
    - 192.168.7.0/24
        - Corp-Region (NAM)
        - Corp-Country (USA)
        - Corp-City (Chicago)
        - Corp-Building (BO)

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



□	☰	192.168.3.0/24	0.0%	APAC	Singapore	Singapore	HQ
□	☰	192.168.4.0/24	0.0%	APAC	India	Bangalore	BO
□	☰	192.168.5.0/24	0.0%	EMEA	UK	London	BO
□	☰	192.168.6.0/24	0.0%	EMEA	France	Paris	BO
□	☰	192.168.7.0/24	0.0%	NAM	USA	Chicago	BO

15. Click **Grid DNS Properties** from the Toolbar under **Data Management**→ **DNS**.



16. Click **Traffic Control**.

17. Click **External Attributes** 1 drop down menu and select **Corp-Region**.

18. Click **+** to add External Attribute 2.

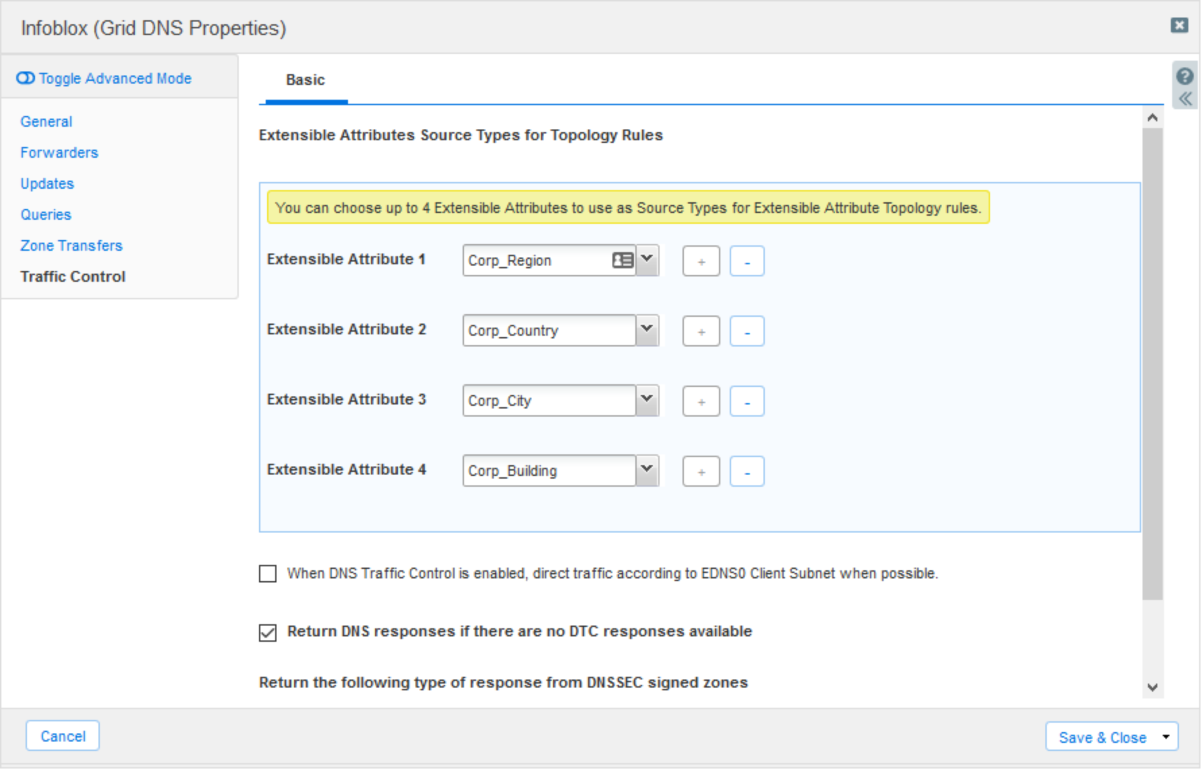
19. Select **Corp-Country**.

20. Click **+** to add External Attribute 3.

21. Select **Corp-City**.

22. Click **+** to add External Attribute 4.

23. Select **Corp-Building**



Infoblox (Grid DNS Properties)

Extensible Attributes Source Types for Topology Rules

You can choose up to 4 Extensible Attributes to use as Source Types for Extensible Attribute Topology rules.

Extensible Attribute 1	Corp_Region	+ -
Extensible Attribute 2	Corp_Country	+ -
Extensible Attribute 3	Corp_City	+ -
Extensible Attribute 4	Corp_Building	+ -

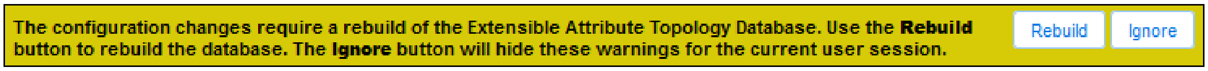
□ When DNS Traffic Control is enabled, direct traffic according to EDNS0 Client Subnet when possible.

☑ **Return DNS responses if there are no DTC responses available**

Return the following type of response from DNSSEC signed zones

24. Click **Save & Close**.

25. Click **Rebuild**.



The configuration changes require a rebuild of the Extensible Attribute Topology Database. Use the Rebuild button to rebuild the database. The Ignore button will hide these warnings for the current user session.

Configure DTC Servers

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

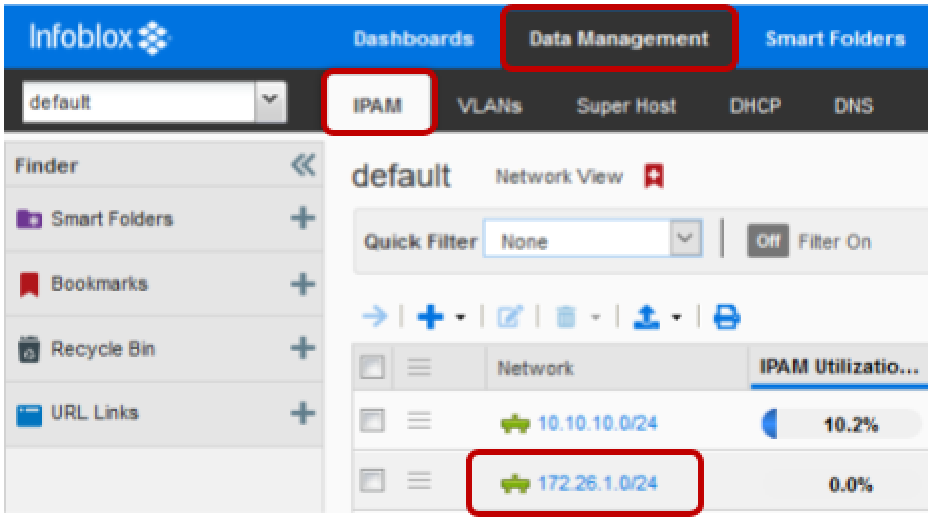
DTC Server	IP address	Datacenter
dtc-vm-apac-1	172.26.1.105	Singapore
dtc-vm-apac-2	172.26.1.106	Bangalore
dtc-vm-emea-1	172.26.1.118	London
dtc-vm-emea-2	172.26.1.119	Paris
dtc-vm-americas	172.26.1.55	Chicago

The steps below are going to add vm-apac-1 DTC server directly through IPAM assuming that there is a DNS record entry for the DTC server in IPAM. If none, then the 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.*

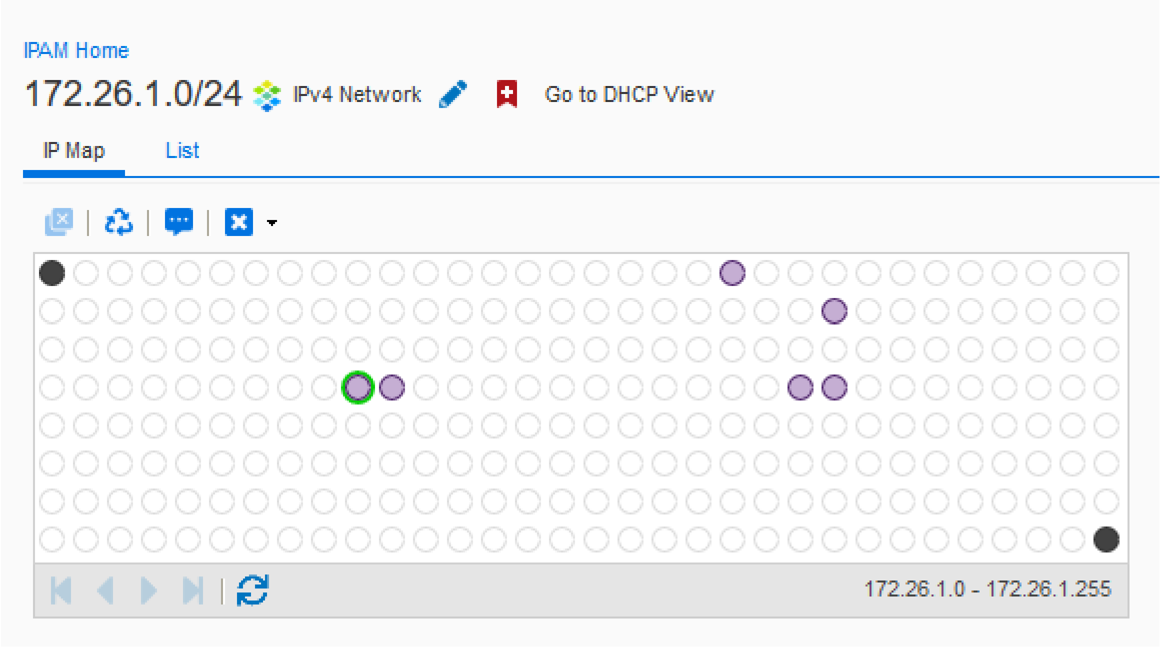
From NIOS 8.0, functionality has been added to directly create DTC servers from discovered data using IPAM. Once the Extensible Attributes (EAs) and the DNS records for the DTC servers have been configured, the user can then add the remaining three servers by repeating these steps:

1. Go to **Data Management** → **IPAM**

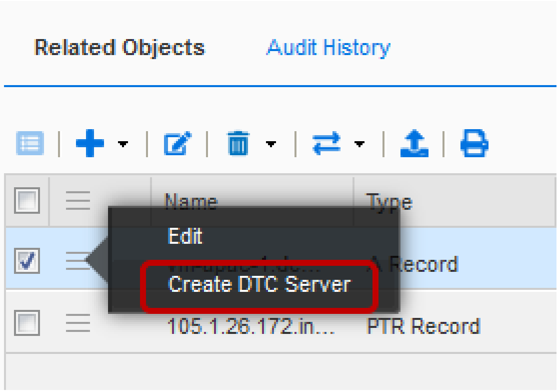
2. Navigate to network IP Map of 172.26.1.0/24 from where dtc-vm-apac-1 server is to be created.



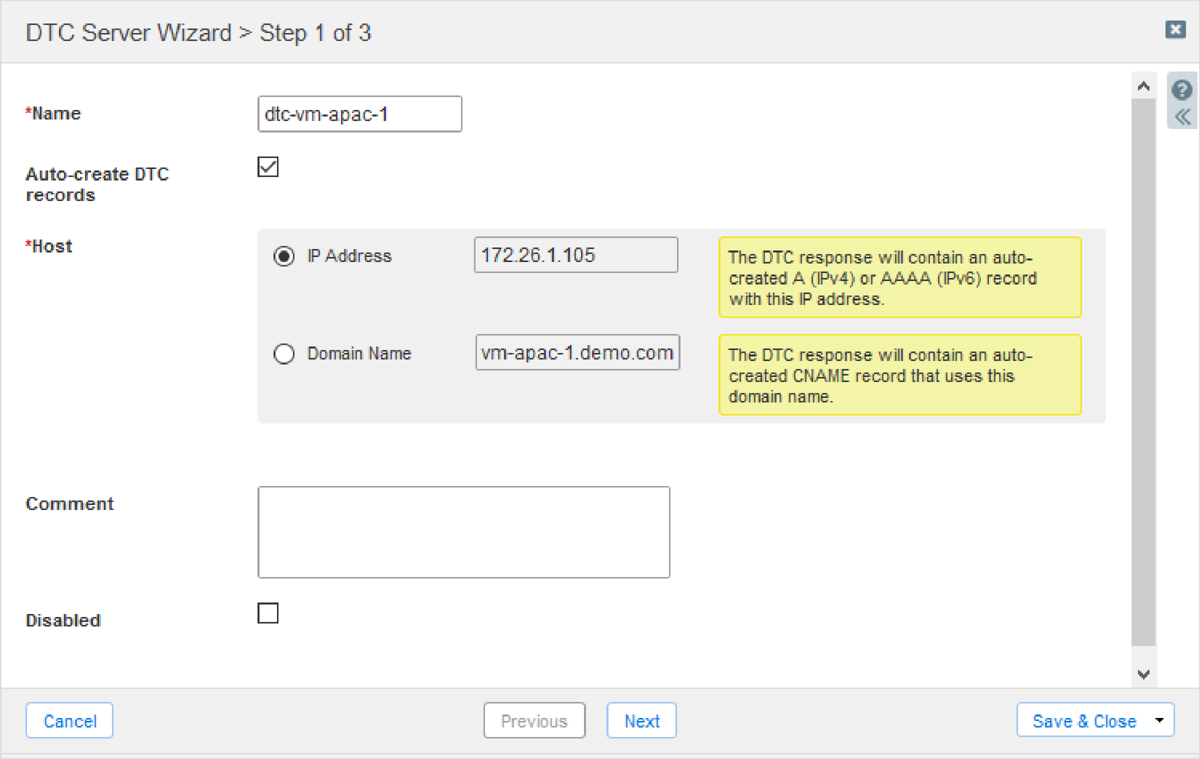
3. Click on **172.26.1.105**.



4. Scroll down all the way to the **Related Objects** section under IP Map, and ☰ Click on **Next** to vm-apac-1.demo.com (A record) and select **Create DTC Server**.



5. Type **dtc-vm-apac-1** in the Name field.



DTC Server Wizard > Step 1 of 3

*Name: dtc-vm-apac-1

Auto-create DTC records: ☑

*Host:

● IP Address: 172.26.1.105 — The DTC response will contain an auto-created A (IPv4) or AAAA (IPv6) record with this IP address.

○ Domain Name: vm-apac-1.demo.com — The DTC response will contain an auto-created CNAME record that uses this domain name.

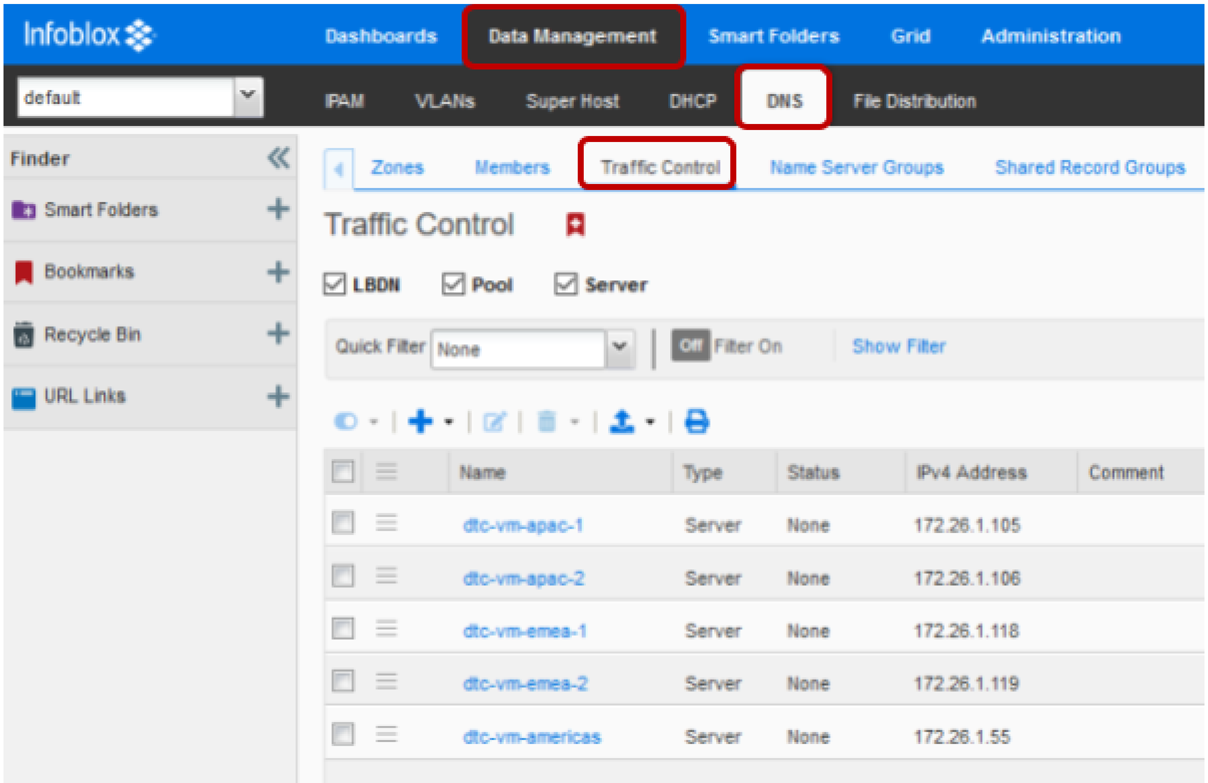
Comment:

Disabled: □

6. Click **Save & Close**.

7. Repeat steps 2 to 4 to add the remaining four DTC servers.

8. Navigate to **Data Management** → **DNS** → **Traffic Control** to view the newly created DTC servers.



Name	Type	Status	IPv4 Address	Comment
dtc-vm-apac-1	Server	None	172.26.1.105	
dtc-vm-apac-2	Server	None	172.26.1.106	
dtc-vm-emea-1	Server	None	172.26.1.118	
dtc-vm-emea-2	Server	None	172.26.1.119	
dtc-vm-americas	Server	None	172.26.1.55	

Configure Server ruleset for DTC Pools

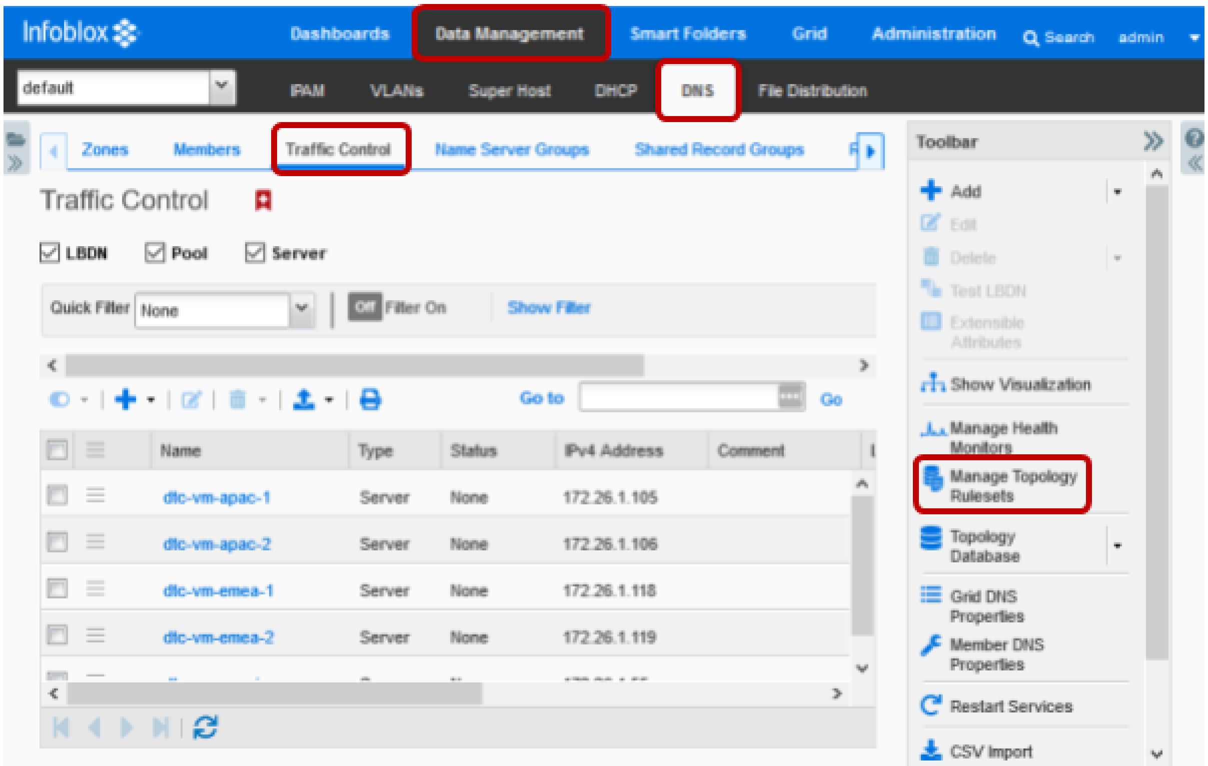
In our example we are going to configure three Server Topology Rulesets, one for Asia Pacific Pool, one for the Europe Pool and one for the North-America Pool. The Topology Rulesets are named APAC-Ruleset, EMEA-Ruleset and NAM-Ruleset, respectively.

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

Ruleset	Rules	Destination Server
APAC-Ruleset	The source DNS query is from Asia and more specifically from Singapore HeadQuarters	dtc-vm-apac-1
	The source DNS query is from Asia and more specifically from Branch Office in Bangalore	dtc-vm-apac-2
EMEA-Ruleset	The source DNS query is from Europe and more specifically from Branch Office in London	dtc-vm-emea-1
	The source DNS query is from Europe and more specifically from Branch Office in Paris HeadQuarters	dtc-vm-emea-2
NAM-Ruleset	The source DNS query is from North America and specifically from Branch Office in Chicago	dtc-vm-americas

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 the Toolbar.



Traffic Control

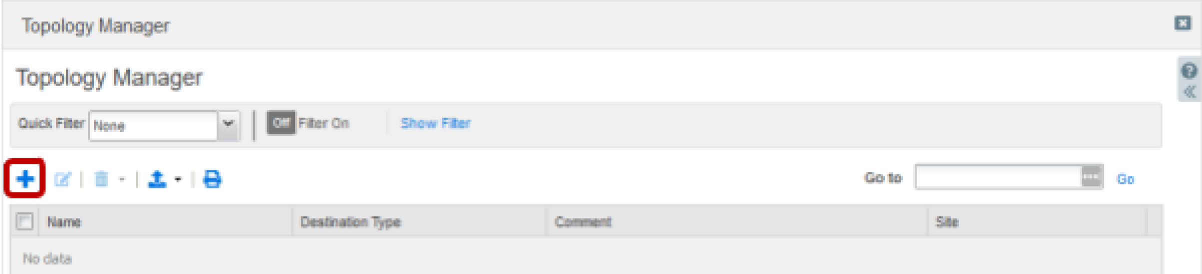
☑ LBDN ☑ Pool ☑ Server

Quick Filter None | Off Filter On | Show Filter

Go to | Go

Name	Type	Status	IPv4 Address	Comment
dtc-vm-apac-1	Server	None	172.26.1.105	
dtc-vm-apac-2	Server	None	172.26.1.106	
dtc-vm-emea-1	Server	None	172.26.1.118	
dtc-vm-emea-2	Server	None	172.26.1.119	

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



Topology Manager

Quick Filter None | Off Filter On | Show Filter

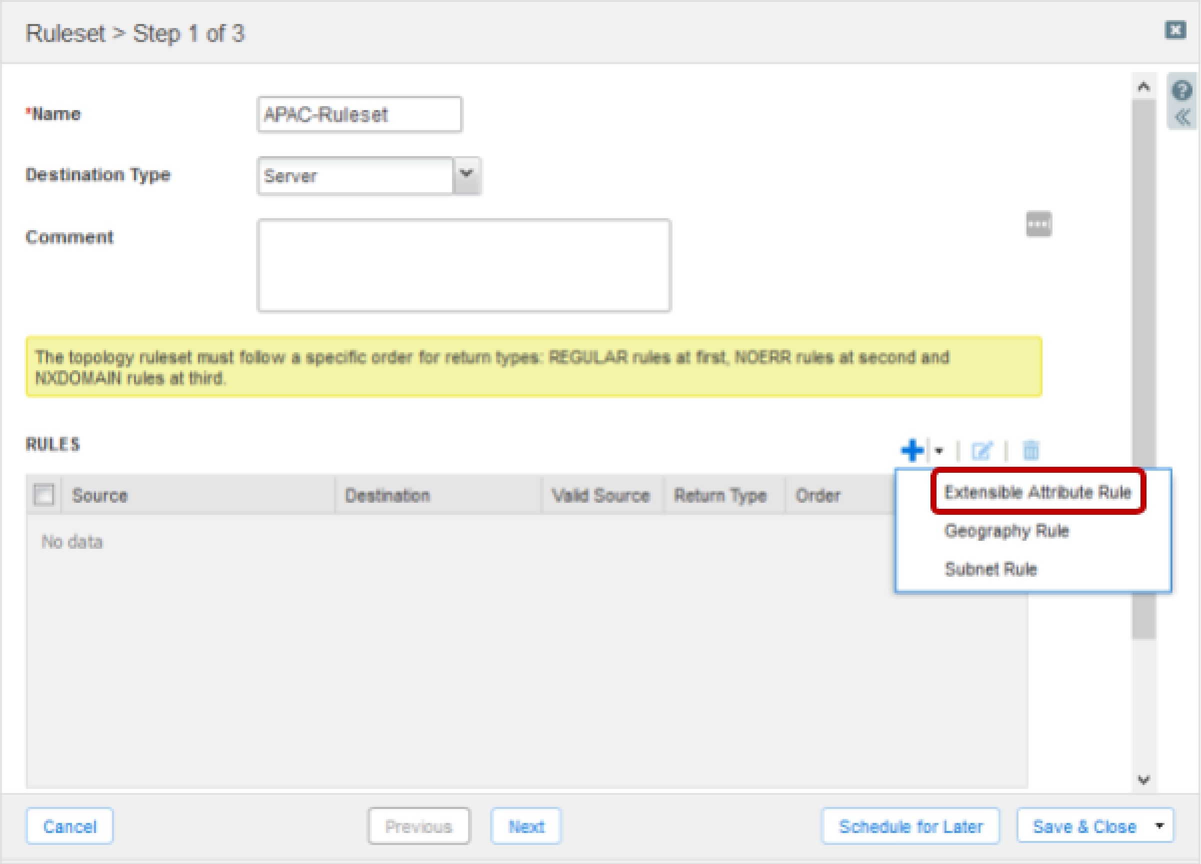
Go to | Go

Name	Destination Type	Comment	Site
No data			

4. Type **APAC-Ruleset** in Name field.

5. Select **Server** as Destination Type.

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



Ruleset > Step 1 of 3

*Name: APAC-Ruleset

Destination Type: Server

Comment:

The topology ruleset must follow a specific order for return types: REGULAR rules at first, NOERR rules at second and NXDOMAIN rules at third.

RULES

□	Source	Destination	Valid Source	Return Type	Order
	No data				

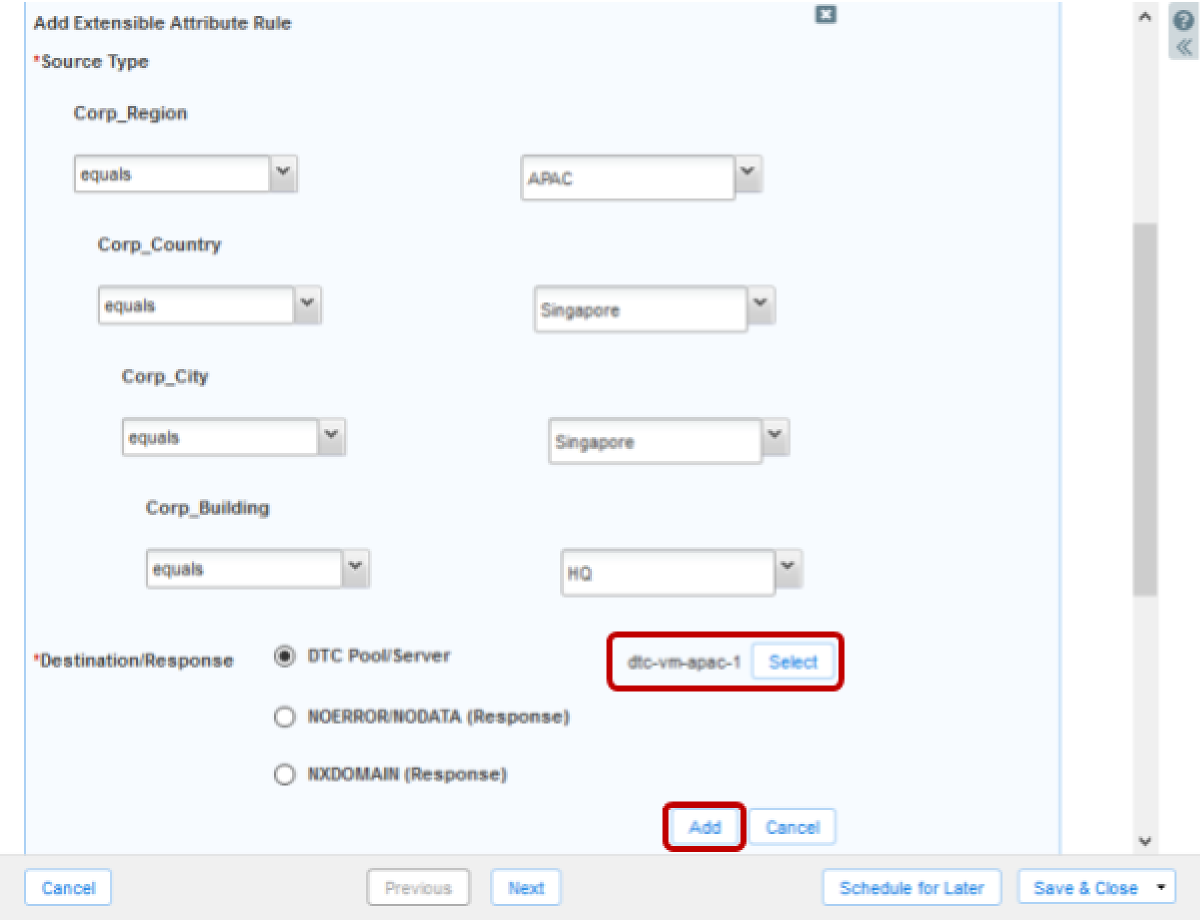
7. Select **APAC** for Corp-Region.

8. Select **Singapore** for Corp-Country.

9. Select **Singapore** for Corp-City.

10. Select **HQ** for Corp-Building.

11. Select **server dtc-vm-apac-1** for Destination.



Add Extensible Attribute Rule

*Source Type

Corp_Region: equals APAC

Corp_Country: equals Singapore

Corp_City: equals Singapore

Corp_Building: equals HQ

*Destination/Response

● DTC Pool/Server dtc-vm-apac-1

○ NOERROR/NODATA (Response)

○ NXDOMAIN (Response)

12. Click **Add**.

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

14. Select **APAC** for Corp-Region.

15. Select **India** for Corp-Country.

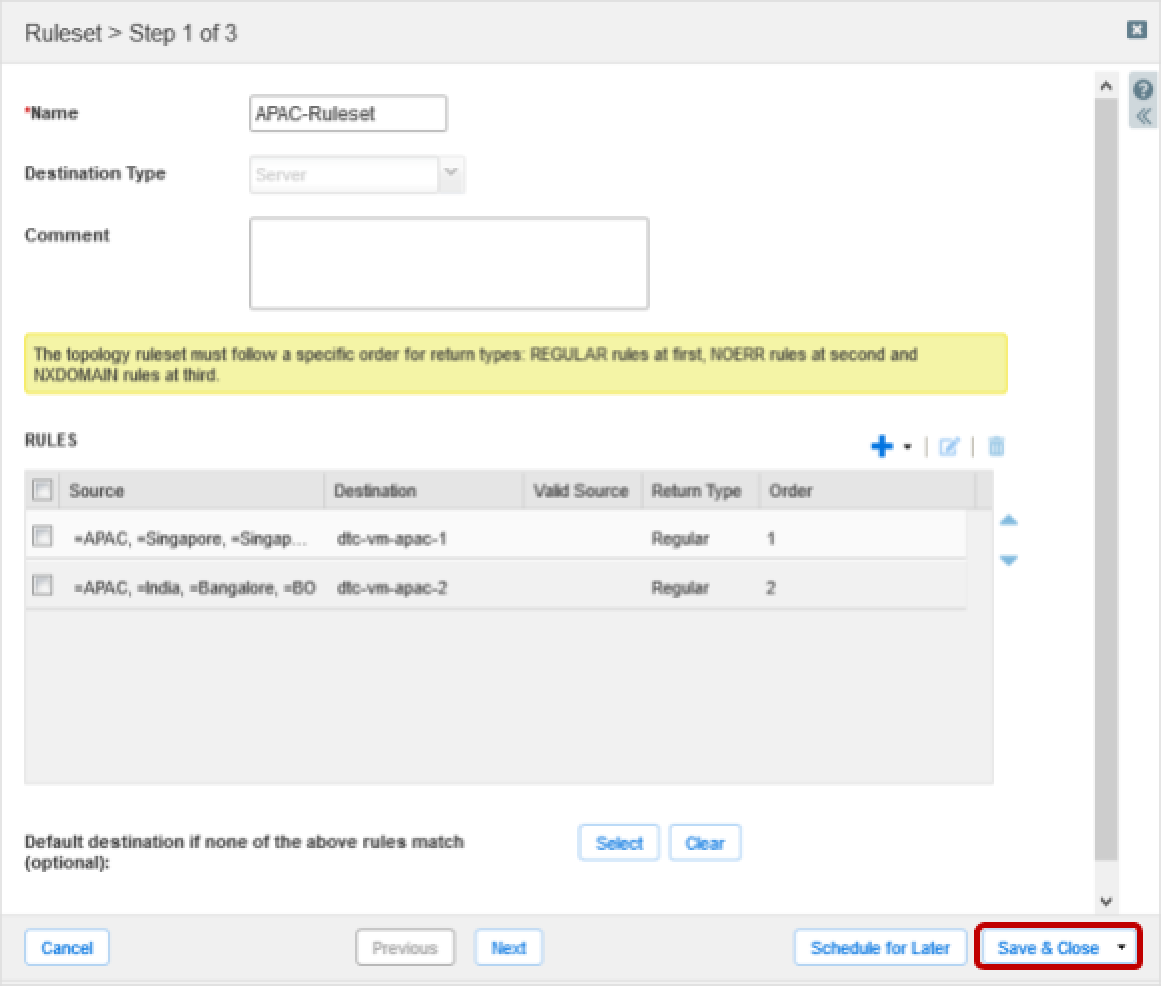
16. Select **Bangalore** for Corp-City.

17. Select **BO** for Corp-Building.

18. Select **server dtc-vm-apac-2** for Destination.

19. Click **Add**.

20. Click **Save & Close**.



*Name: APAC-Ruleset

Destination Type: Server

Comment:

The topology ruleset must follow a specific order for return types: REGULAR rules at first, NOERR rules at second and NXDOMAIN rules at third.

RULES

□	Source	Destination	Valid Source	Return Type	Order
□	=APAC, =Singapore, =Singap...	dtc-vm-apac-1		Regular	1
□	=APAC, =India, =Bangalore, =BO	dtc-vm-apac-2		Regular	2

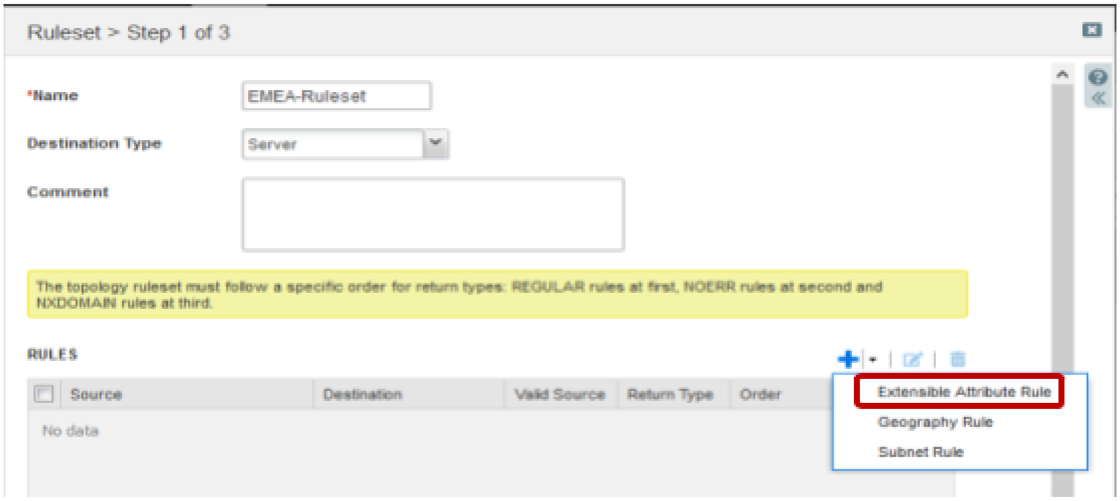
Default destination if none of the above rules match (optional):

21. In Topology Manager Click **+** to open the Ruleset window.

22. Type **EMEA-Ruleset** in Name field.

23. Select **Server** as Destination Type.

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



Ruleset > Step 1 of 3

*Name: EMEA-Ruleset

Destination Type: Server

Comment

The topology ruleset must follow a specific order for return types: REGULAR rules at first, NOERR rules at second and NXDOMAIN rules at third.

RULES

□	Source	Destination	Valid Source	Return Type	Order
	No data				

25. Select **EMEA** for Corp-Region.

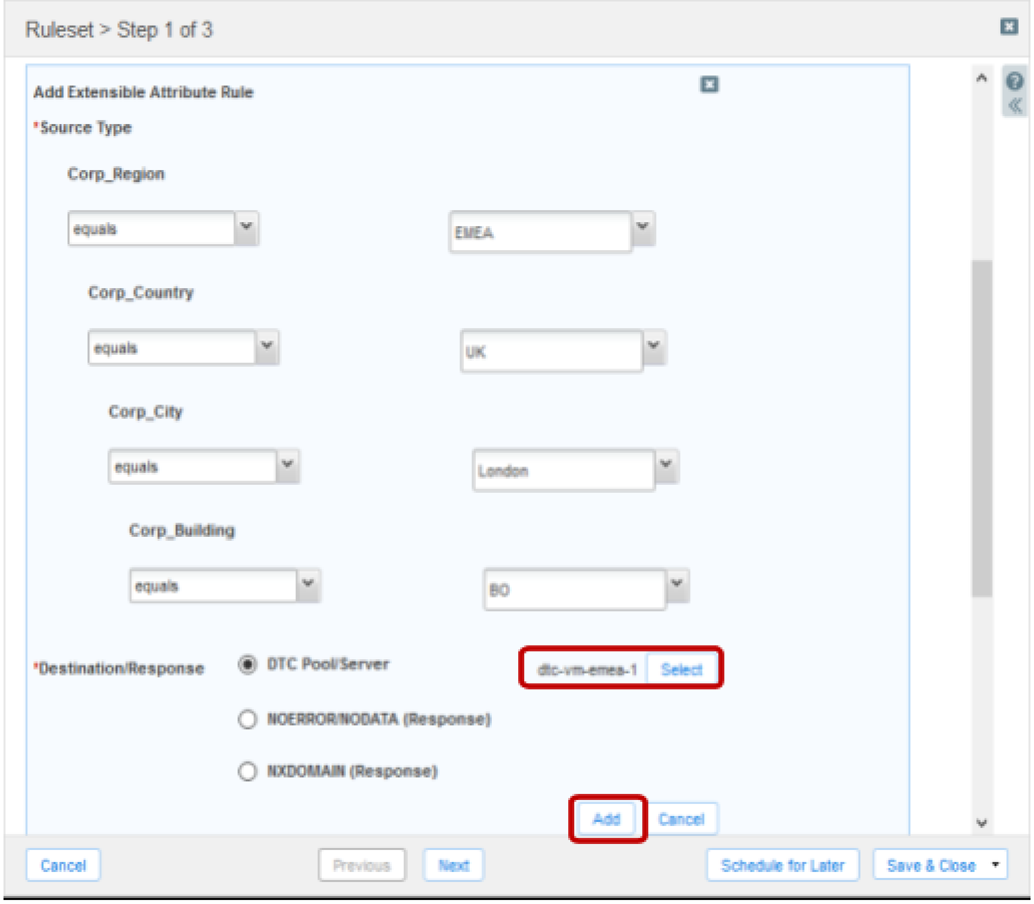
26. Select **UK** for Corp-Country.

27. Select **London** for Corp-City.

28. Select **BranchOffice** for Corp-Building.

29. Select **server dtc-vm-emea-1** for Destination.

30. Click **Add**.



Ruleset > Step 1 of 3

Add Extensible Attribute Rule

*Source Type

Corp_Region: equals — EMEA

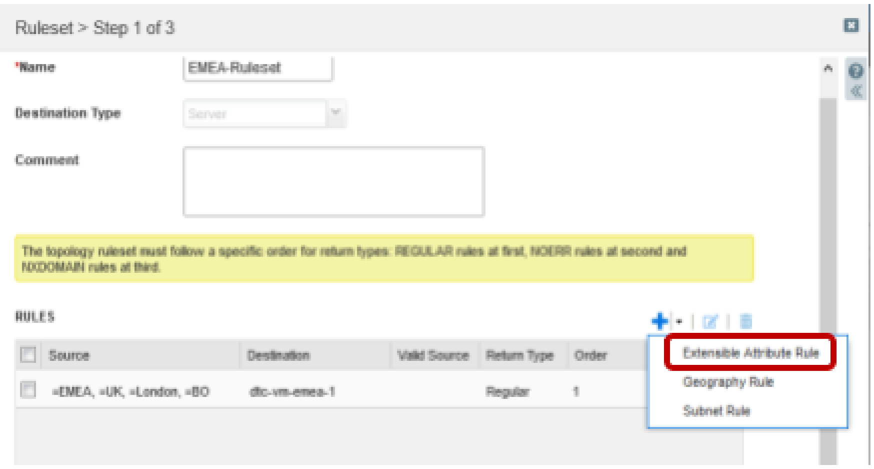
Corp_Country: equals — UK

Corp_City: equals — London

Corp_Building: equals — BO

*Destination/Response: ● DTC Pool/Server — dtc-vm-emea-1 Select

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



Ruleset > Step 1 of 3

*Name: EMEA-Ruleset

Destination Type: Server

Comment:

The topology ruleset must follow a specific order for return types: REGULAR rules at first, NOERR rules at second and NXDOMAIN rules at third.

RULES

□	Source	Destination	Valid Source	Return Type	Order
□	=EMEA, =UK, =London, =BO	dtc-vm-emea-1		Regular	1

32. Select **EMEA** for Corp-Region.

33. Select **France** for Corp-Country.

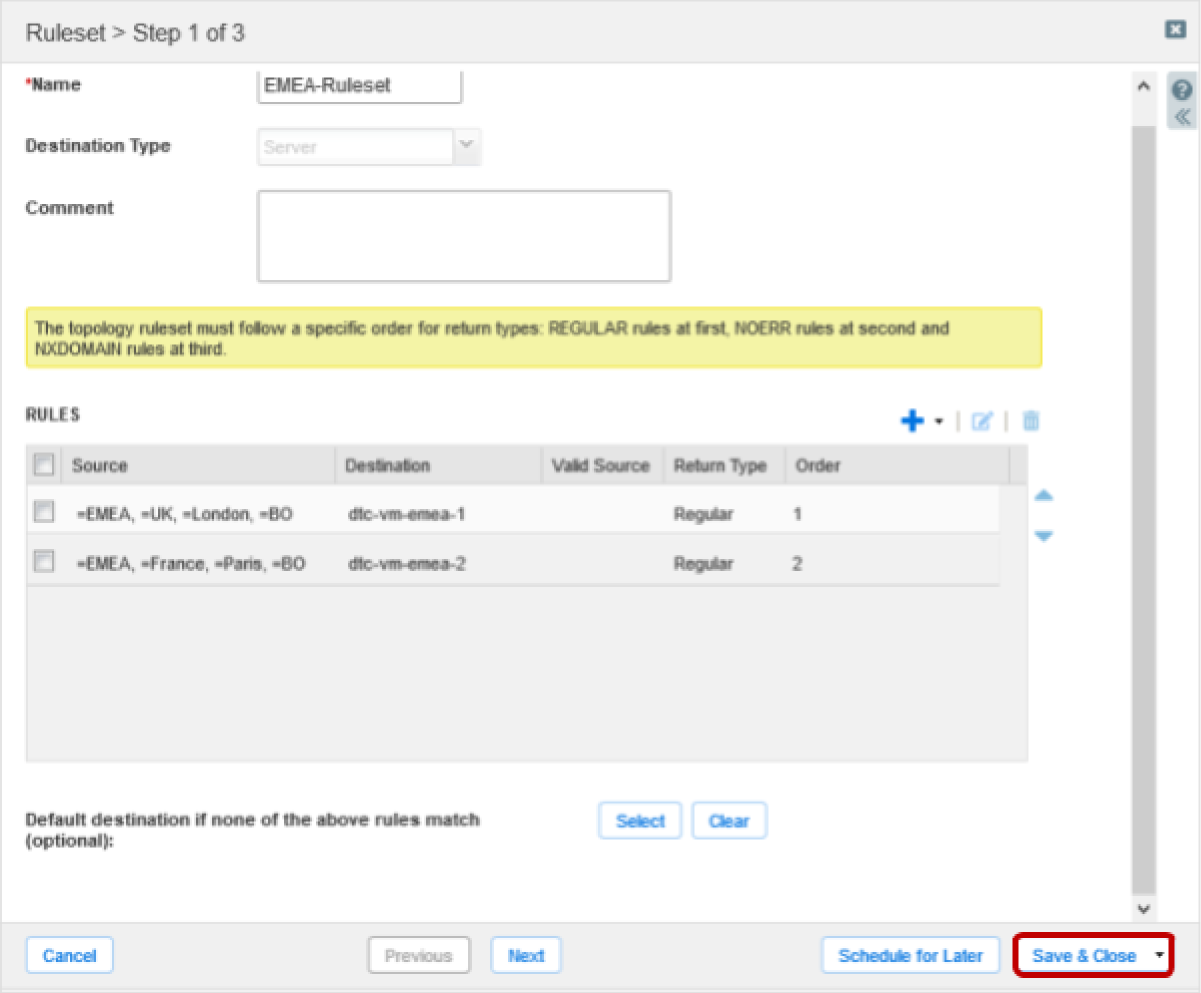
34. Select **Paris** for Corp-City.

35. Select **BranchOffice** for Corp-Building.

36. Select **server dtc-vm-emea-2** for Destination.

37. Click **Add**.

38. Click **Save & Close**.



Ruleset > Step 1 of 3

*Name: EMEA-Ruleset

Destination Type: Server

Comment:

The topology ruleset must follow a specific order for return types: REGULAR rules at first, NOERR rules at second and NXDOMAIN rules at third.

RULES

□	Source	Destination	Valid Source	Return Type	Order
□	=EMEA, =UK, =London, =BO	dtc-vm-emea-1		Regular	1
□	=EMEA, =France, =Paris, =BO	dtc-vm-emea-2		Regular	2

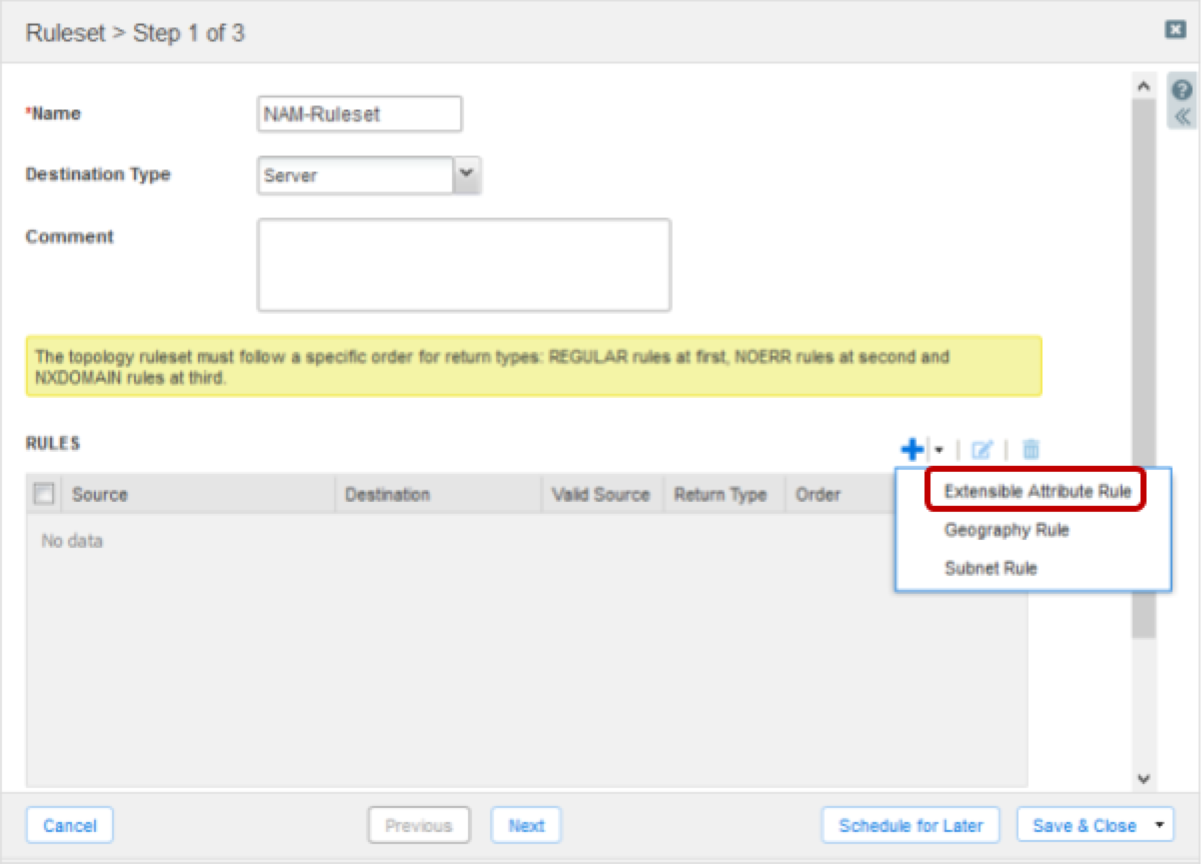
Default destination if none of the above rules match (optional):

39. In Topology Manager Click **+** to open the Ruleset window.

40. Type **NAM-Ruleset** in Name field.

41. Select **Server** as Destination Type.

42. Click **+** in Rules section and select the **Extensible Attribute** Rule.



Ruleset > Step 1 of 3

*Name: NAM-Ruleset

Destination Type: Server

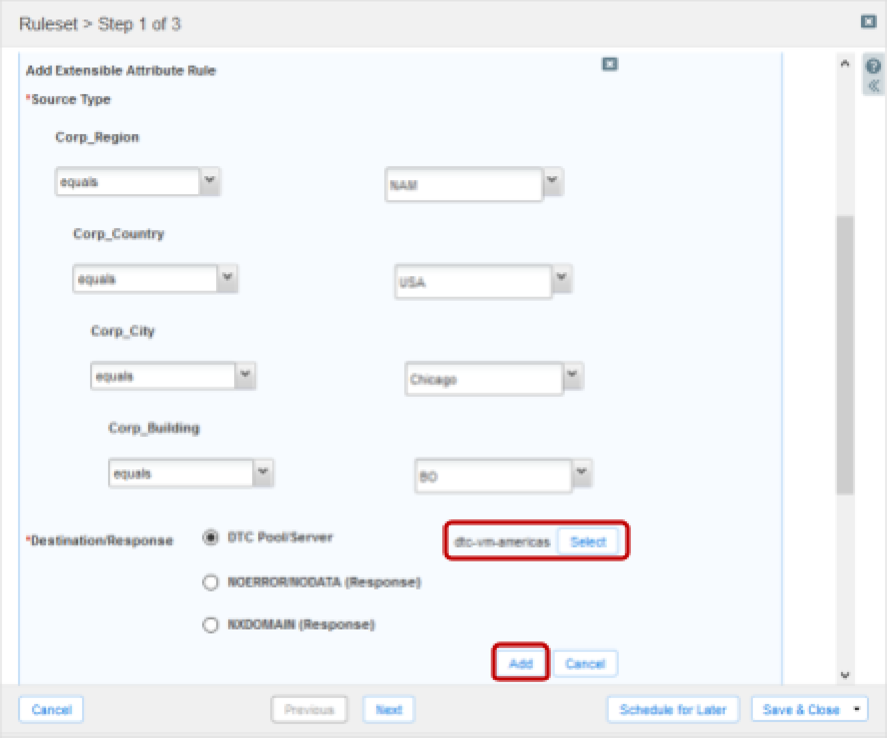
Comment

The topology ruleset must follow a specific order for return types: REGULAR rules at first, NOERR rules at second and NXDOMAIN rules at third.

RULES

□ Source	Destination	Valid Source	Return Type	Order
No data				

43. Select **NAM** for Corp-Region.
44. Select **USA** for Corp-Country.
45. Select **Chicago** for Corp-City.
46. Select **BO** for Corp-Building.
47. Select **server dtc-vm-americas** for Destination.
48. Click **Add**.



Ruleset > Step 1 of 3

Add Extensible Attribute Rule

*Source Type

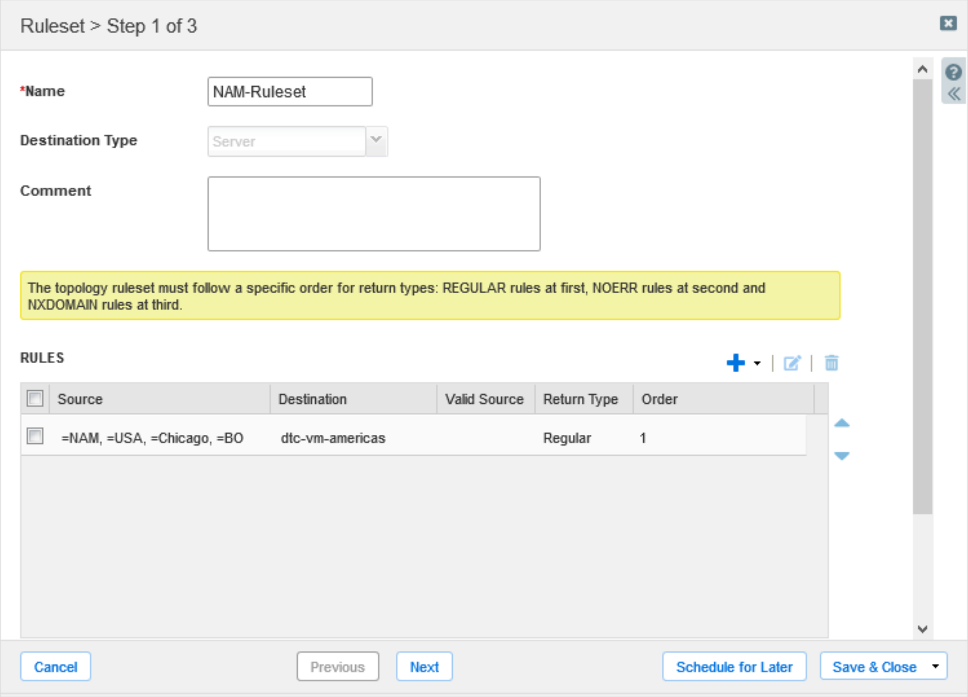
Corp_Region	
equals	NAM
Corp_Country	
equals	USA
Corp_City	
equals	Chicago
Corp_Building	
equals	BO

*Destination/Response ● DTC Pool/Server dtc-vm-americas

○ NOERROR/NODATA (Response)

○ NXDOMAIN (Response)

49. Click **Save & Close**.



Ruleset > Step 1 of 3

*Name: NAM-Ruleset

Destination Type: Server

Comment:

The topology ruleset must follow a specific order for return types: REGULAR rules at first, NOERR rules at second and NXDOMAIN rules at third.

RULES

□	Source	Destination	Valid Source	Return Type	Order
□	=NAM, =USA, =Chicago, =BO	dtc-vm-americas		Regular	1

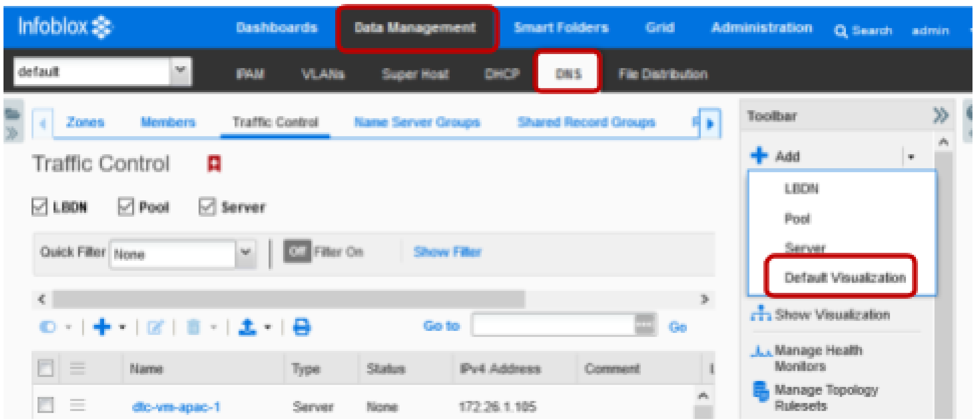
Configure DTC Pools

In our example, we are going to configure three DTC Pools with the following servers and Topology Load Balancing methods.

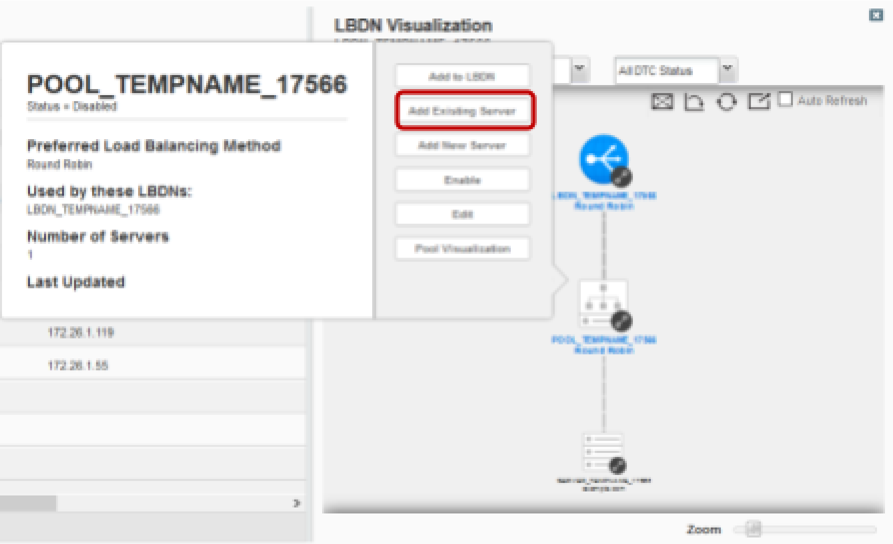
DTC Pool	Ruleset for Topology Load balancing	Member Servers
APAC-Pool	APAC-Ruleset	dtc-vm-apac-1
		dtc-vm-apac-2
EMEA-Pool	EMEA-Ruleset	dtc-vm-emea-1
		dtc-vm-emea-2
Americas-Pool	NAM-Ruleset	dtc-vm-americas

From the NIOS 8.0 release, Default Visualization can be used to configure these DTC objects and in the following section users can learn how to use them. To configure DTC Pools:

1. Go to **Data Management** → **DNS** → **Traffic Control**.
2. From the 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**.



POOL_TEMPNAME_17566
Status • Disabled

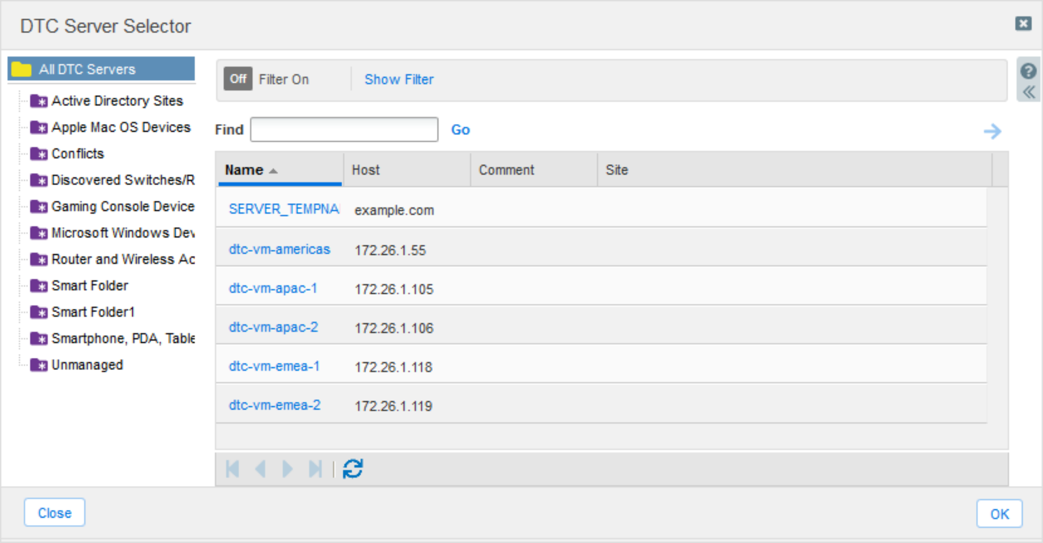
Preferred Load Balancing Method
Round Robin

Used by these LBDNs:
LBDN_TEMPNAME_17566

Number of Servers
1

Last Updated

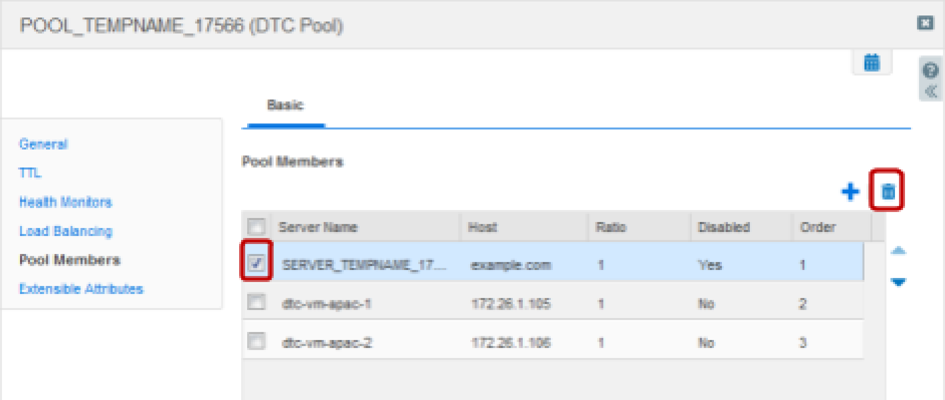
6. Select Servers **dtc-vm-apac-1** and **dtc-vm-apac-2** from DTC Server Selector.



Name	Host	Comment	Site
SERVER_TEMPNA	example.com		
dtc-vm-americas	172.26.1.55		
dtc-vm-apac-1	172.26.1.105		
dtc-vm-apac-2	172.26.1.106		
dtc-vm-emea-1	172.26.1.118		
dtc-vm-emea-2	172.26.1.119		

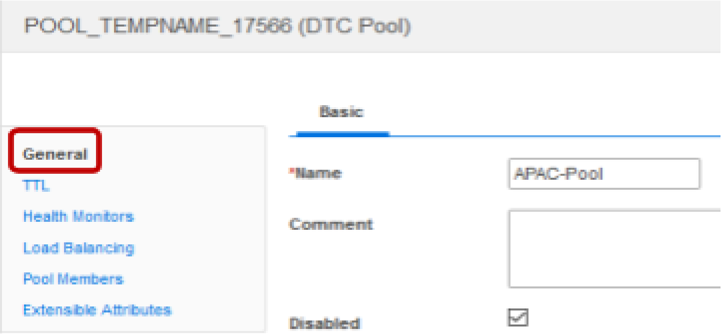
7. Select **SERVER_TEMPNAME_xxxxx** from Pool Members.

8. Click **Delete**.



	Server Name	Host	Ratio	Disabled	Order
☑	SERVER_TEMPNAME_17...	example.com	1	Yes	1
□	dtc-vm-apac-1	172.26.1.105	1	No	2
□	dtc-vm-apac-2	172.26.1.106	1	No	3

9. Click the **General** tab and type **APAC-Pool** in the Name field.

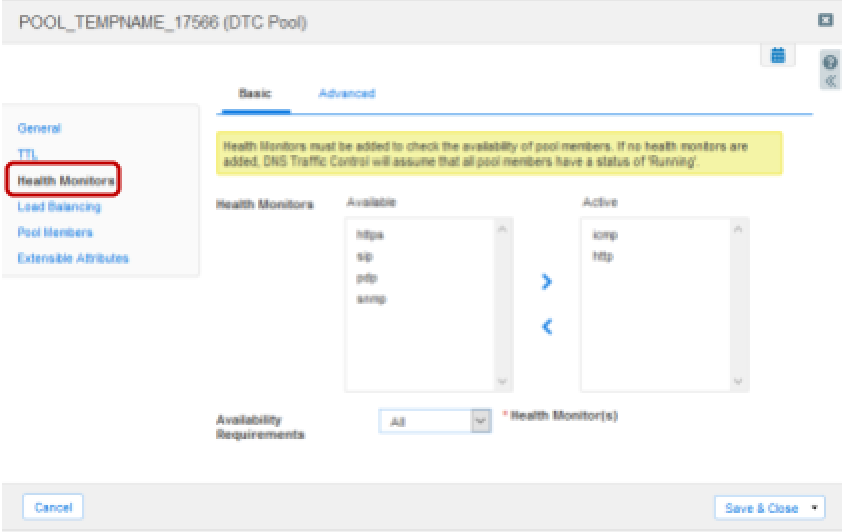

POOL_TEMPNAME_17566 (DTC Pool)

*Name: APAC-Pool

Comment:

Disabled ☑

10. Click the **Health Monitors** tab.
    - ○ Select **ICMP** and **HTTP** health monitors to move them under the Active column.


POOL_TEMPNAME_17566 (DTC Pool)

Health Monitors must be added to check the availability of pool members. If no health monitors are added, DNS Traffic Control will assume that all pool members have a status of 'Running'.

Health Monitors — Available: https, sip, pdp, snmp — Active: icmp, http

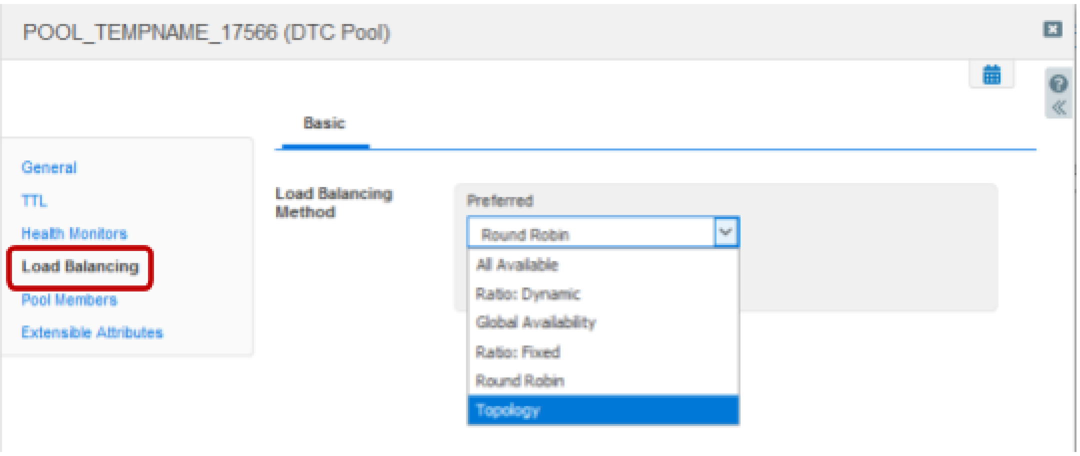
Availability Requirements: All

*Health Monitor(s)

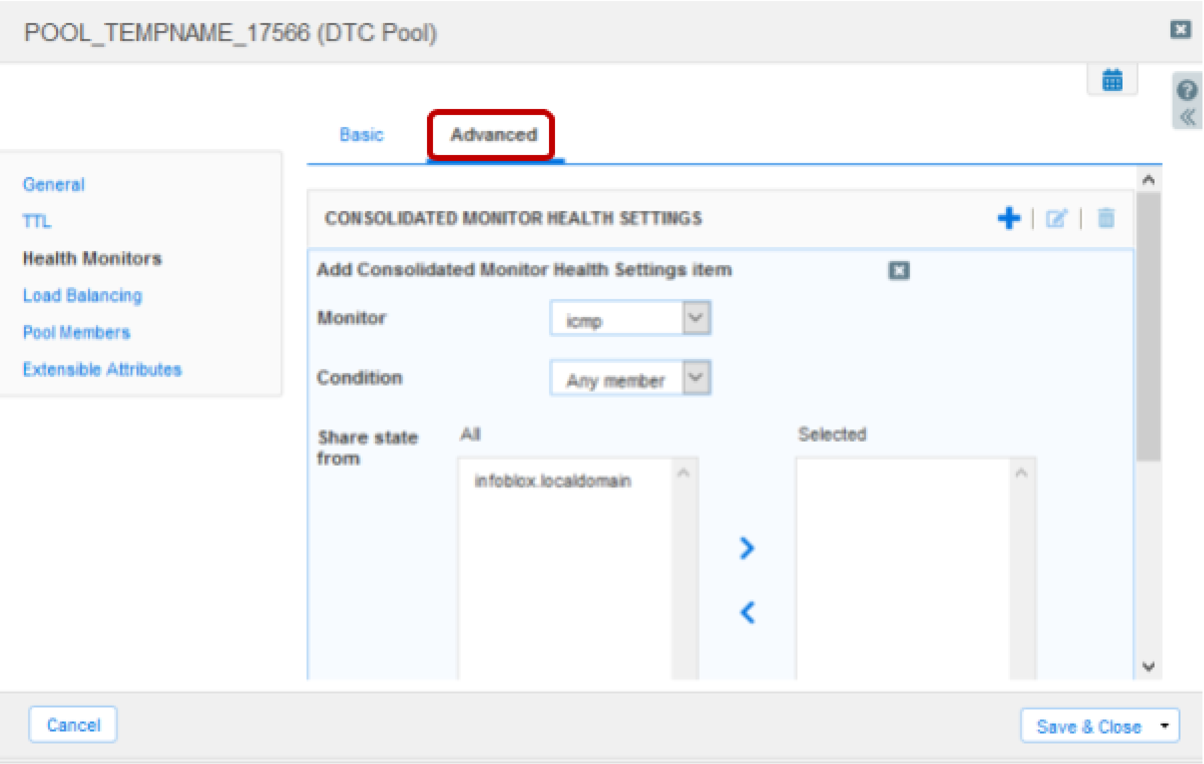
11. Note that with NIOS 8.3, in the Advanced tab, you can select which member will run the monitor.

12. Click the **Load Balancing** tab.

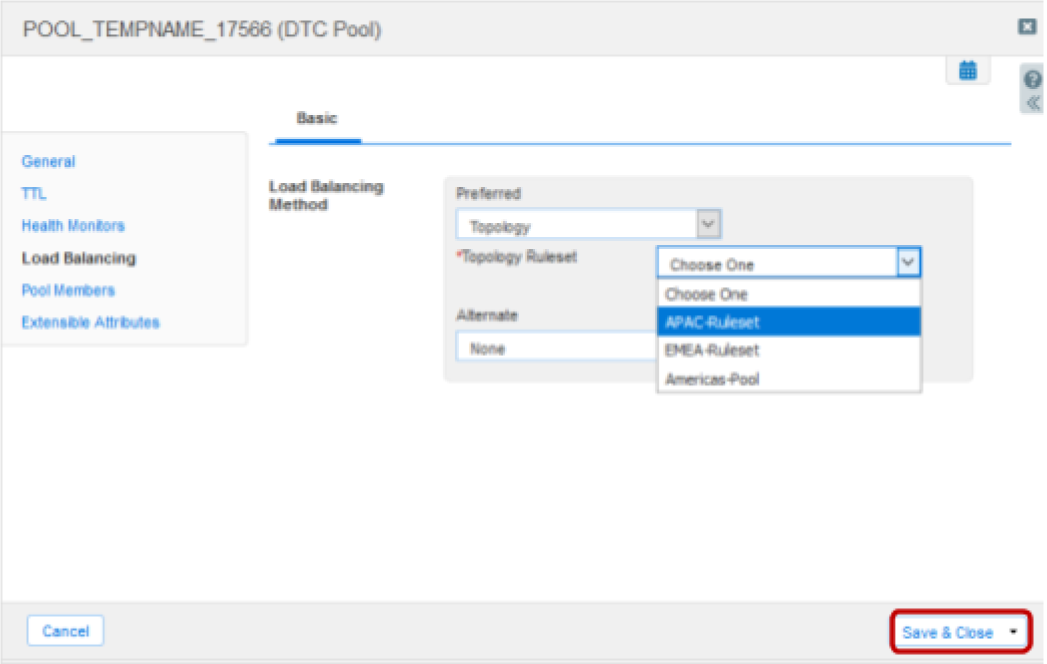
13. Select **Topology** under Preferred.



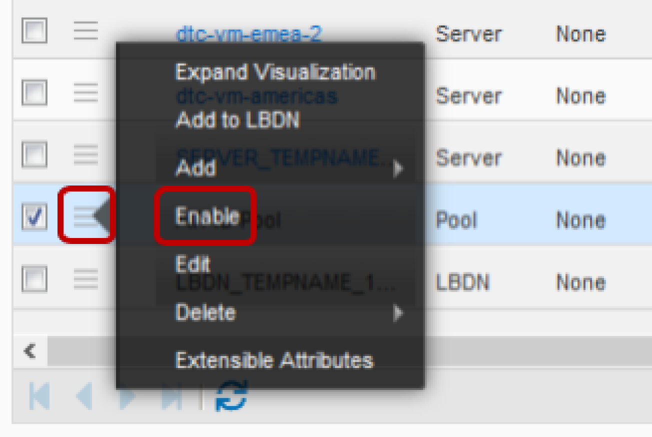
14. Select **APAC-Ruleset** under Topology Ruleset.



15. Click **Save & Close**



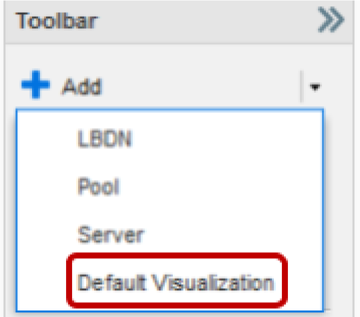
16. Click on hamburger next to APAC-Pool and select **Enable**.



Repeat above steps to add EMEA-Pool as follows:

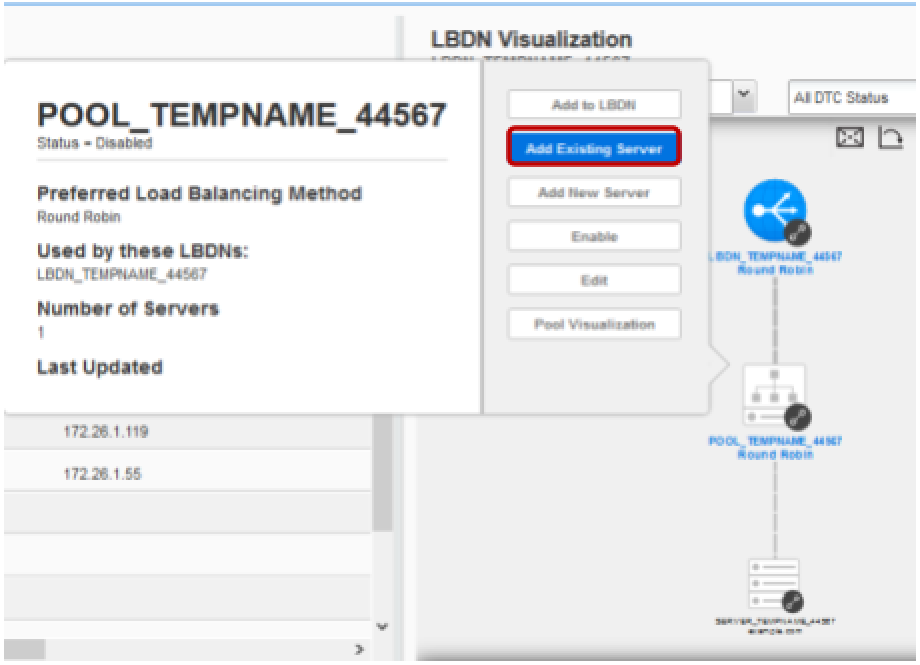
1. From Toolbar, click **+Add**.

2. Select **Default Visualization**.



3. Click on **POOL_TEMPNAME_xxxxx** (where xxxxx is some randomly generated number)

4. Click on **Add Existing Server**.


LBDN Visualization

POOL_TEMPNAME_44567
Status - Disabled

Preferred Load Balancing Method
Round Robin

Used by these LBDNs:
LBDN_TEMPNAME_44567

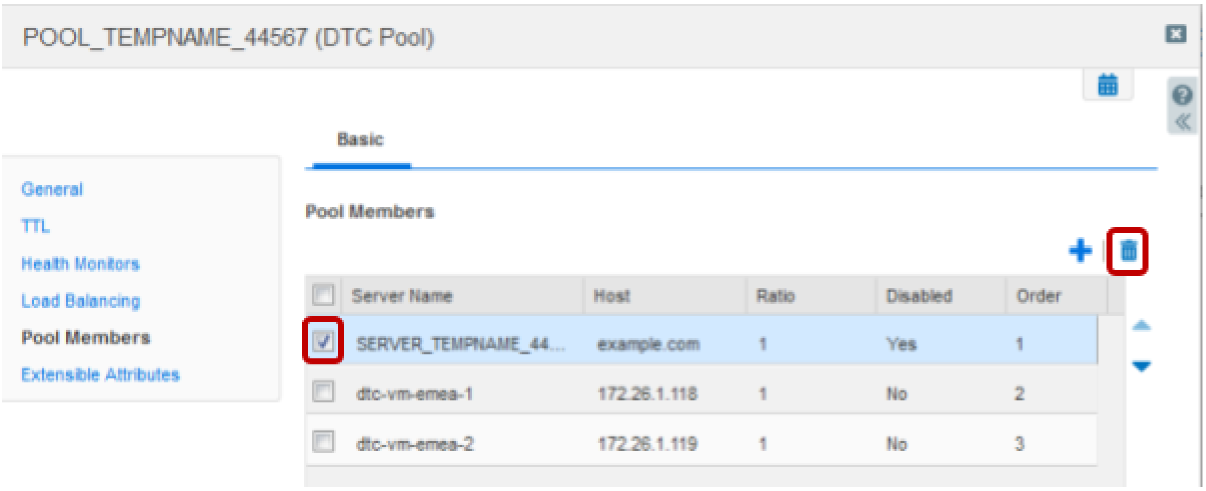
Number of Servers
1

Last Updated

172.26.1.119
172.26.1.55

5. Select Servers **dtc-vm-emea-1** and **dtc-vm-emea-2** from DTC Server Selector.

6. Select **SERVER_TEMPNAME_xxxxx** from Pool Members.



Pool Members

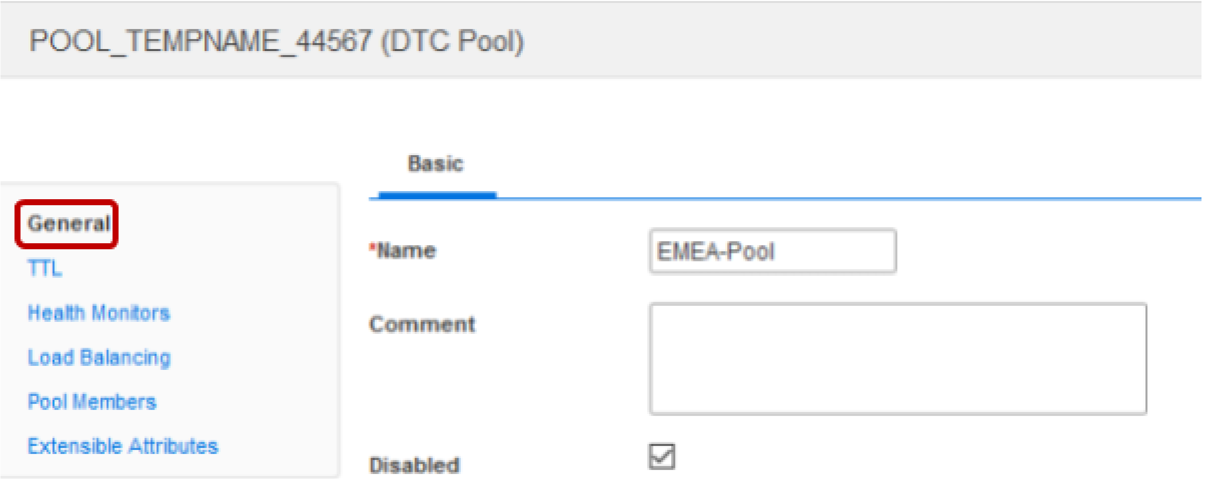
☐	Server Name	Host	Ratio	Disabled	Order
☑	SERVER_TEMPNAME_44...	example.com	1	Yes	1
☐	dtc-vm-emea-1	172.26.1.118	1	No	2
☐	dtc-vm-emea-2	172.26.1.119	1	No	3

7. Click **Delete**.

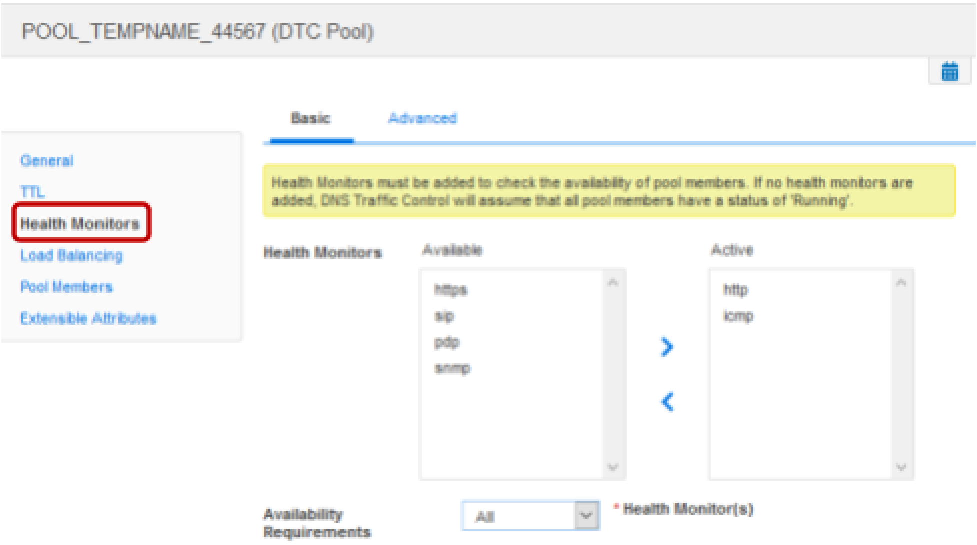
8. Click **General** Tab and type **EMEA-Pool** in the Name field.

9. Click the **Health Monitors** tab.

   a. select **ICMP** and **HTTP** Health Monitors to move them under the Active column.



*Name	EMEA-Pool
Comment	
Disabled	☑



POOL_TEMPNAME_44567 (DTC Pool)

Health Monitors must be added to check the availability of pool members. If no health monitors are added, DNS Traffic Control will assume that all pool members have a status of 'Running'.

Health Monitors: Available: https, sip, pdp, snmp; Active: http, icmp

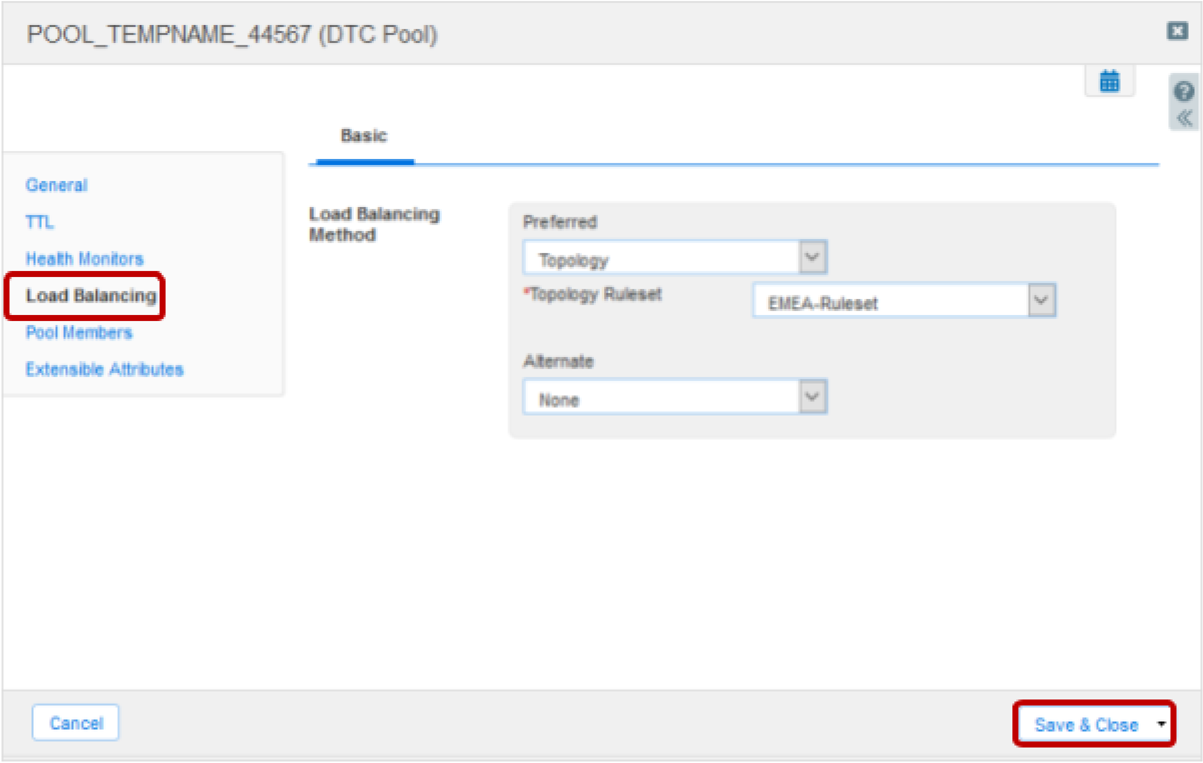
Availability Requirements: All * Health Monitor(s)

10. Click the **Load Balancing** tab.

11. Select **Topology** under Preferred.

12. Select **EMEA-Ruleset** under Topology Ruleset.

13. Click **Save & Close**.



POOL_TEMPNAME_44567 (DTC Pool)

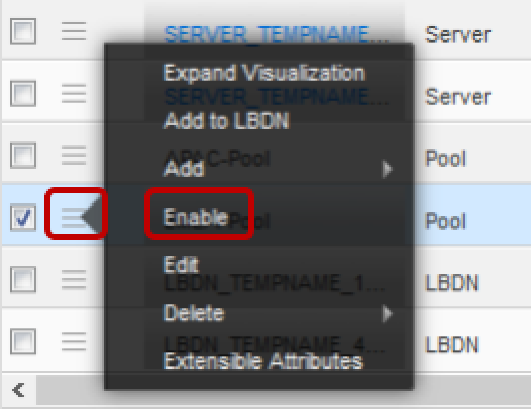
Load Balancing Method

Preferred: Topology

*Topology Ruleset: EMEA-Ruleset

Alternate: None

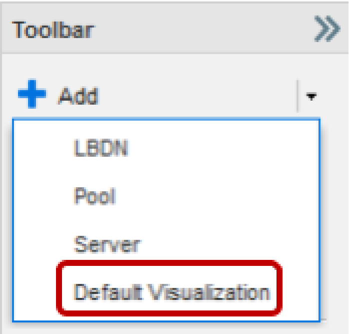
14. Click on hamburger icon next to the EMEA-Pool, and click on **Enable**



Repeat above steps to add Americas-Pool as follows:

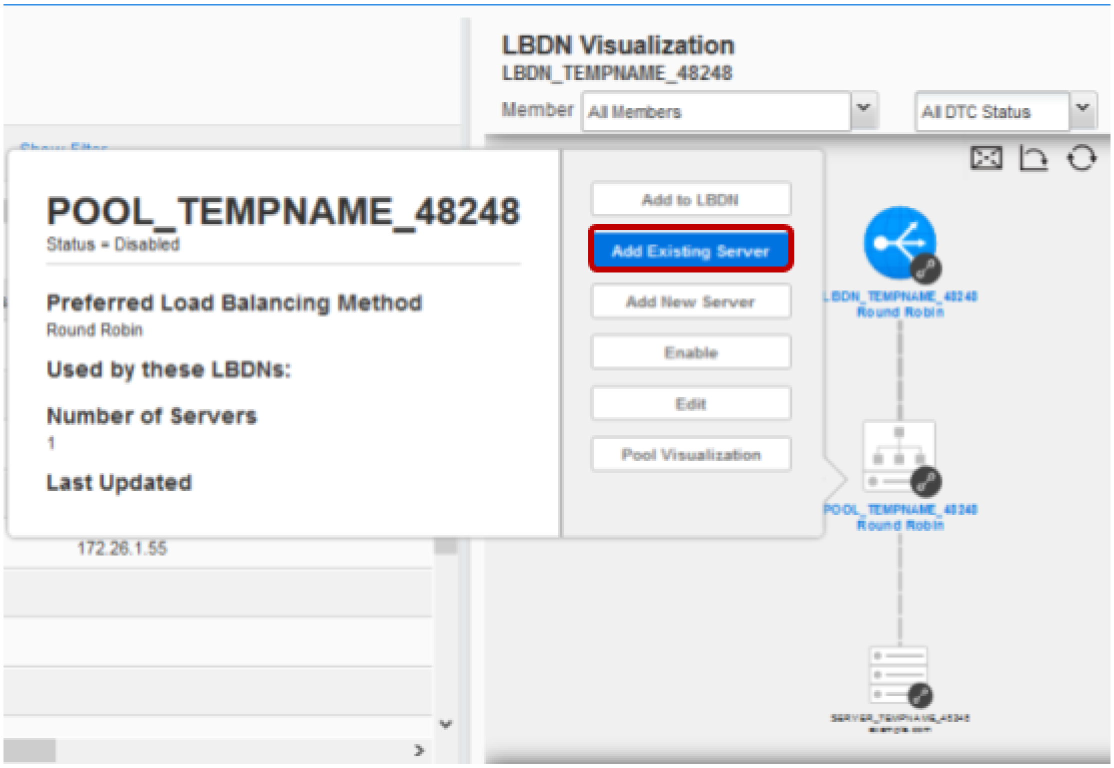
1. From Toolbar, click **+Add**.

2. Select **Default Visualization**.



3. Click on **POOL_TEMPNAME_xxxxx** (where xxxxx is some randomly generated number)

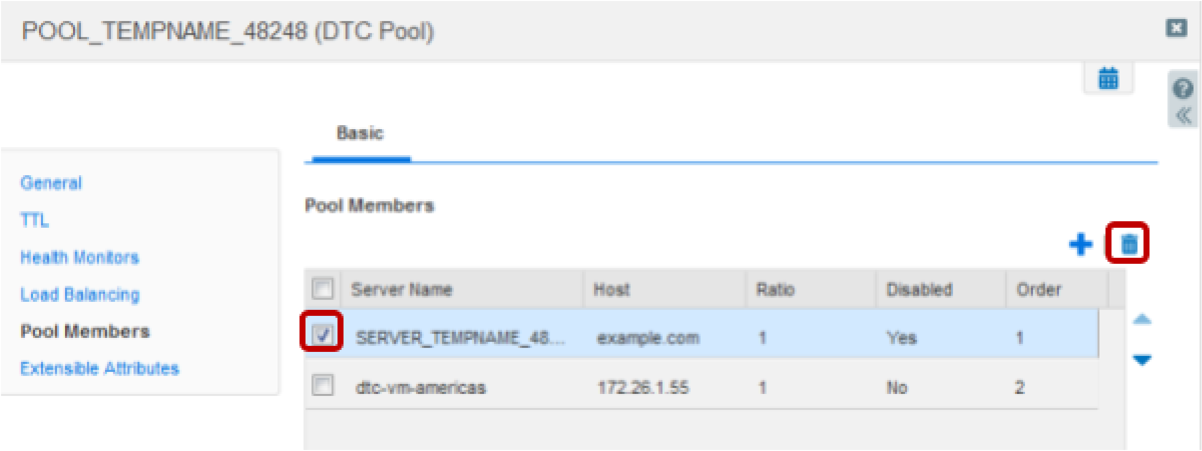
4. Click on **Add Existing Server**.



5. Select Servers **dtc-americas** from DTC Server Selector.

6. Select **SERVER_TEMPNAME_xxxxx** from Pool Members.

7. Click **Delete**.

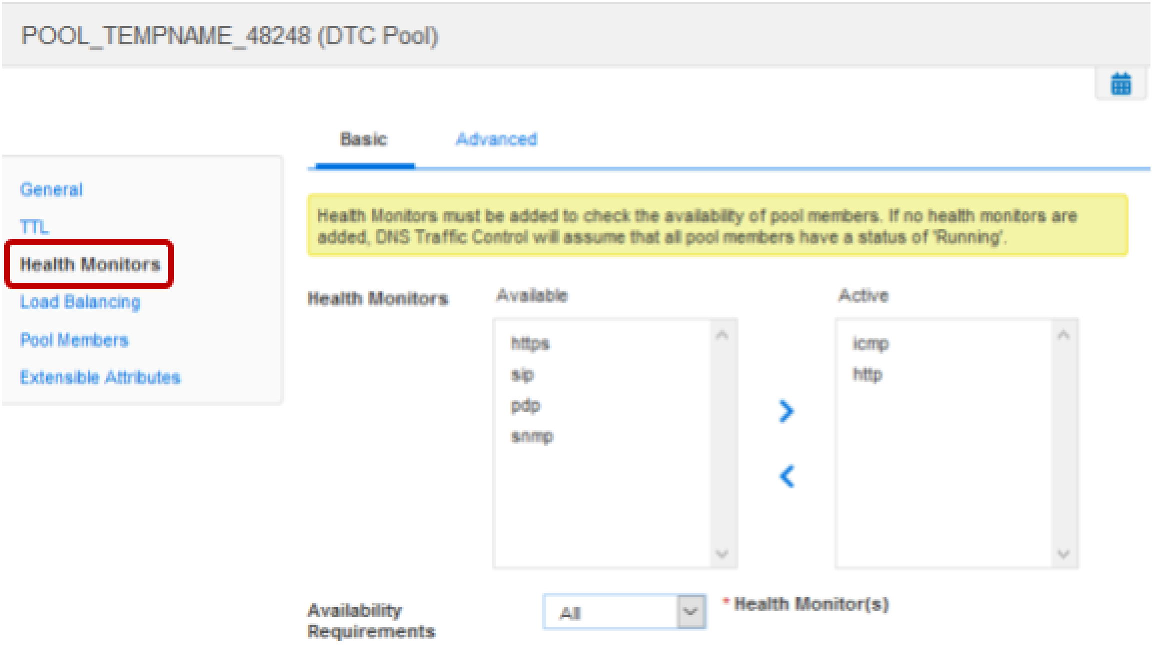


	Server Name	Host	Ratio	Disabled	Order
☑	SERVER_TEMPNAME_48...	example.com	1	Yes	1
□	dtc-vm-americas	172.26.1.55	1	No	2

8. Click the **General** Tab and type **Americas-Pool** in Name field.

9. Click the **Health Monitors** tab.

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



POOL_TEMPNAME_48248 (DTC Pool)

Health Monitors must be added to check the availability of pool members. If no health monitors are added, DNS Traffic Control will assume that all pool members have a status of 'Running'.

Health Monitors: Available: https, sip, pdp, snmp; Active: icmp, http

Availability Requirements: All

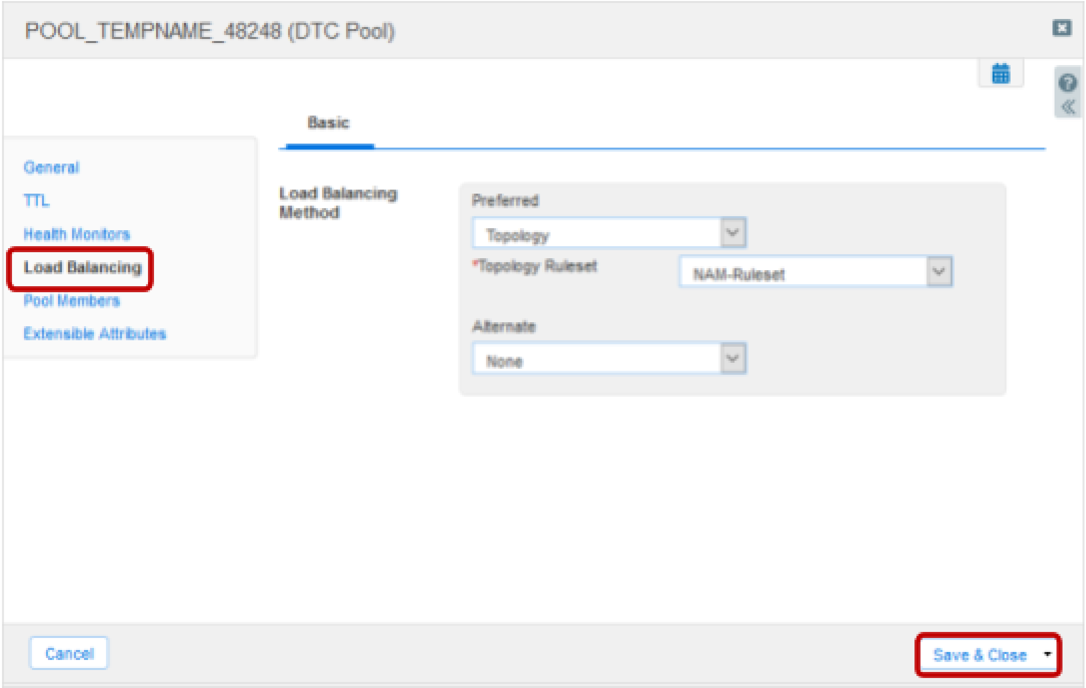
* Health Monitor(s)

10. Click the **Load Balancing** tab.

11. Select **Topology** under Preferred.

12. Select **NAM-Ruleset** under Topology Ruleset.

13. Click **Save & Close**.



POOL_TEMPNAME_48248 (DTC Pool)

Load Balancing Method

Preferred: Topology

*Topology Ruleset: NAM-Ruleset

Alternate: None

14. Click on hamburger icon next to the Americas-Pool and click on **Enable**.

Configure Pool Topology Ruleset for LBDN

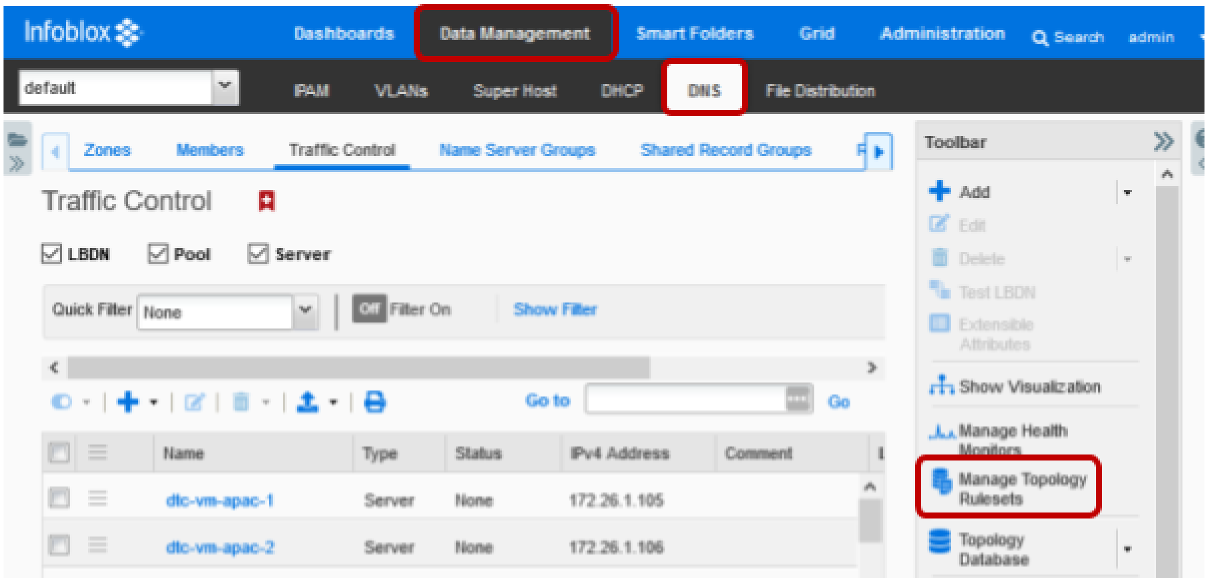
In our example we are going to configure a ruleset for the LBDN named LBDN-demo-dg.com with destination as Pool. The ruleset is going to have five rules as follows:

Ruleset	Rules	Destination Server
LBDN-demo-dg-Ruleset	The source DNS query is from Asia Pacific region	APAC-Pool
	The source DNS query is from Europe region	EMEA-Pool
	The source DNS query is from North America region	Americas-Pool
	The source DNS query is from the subnet 192.168.1.0/24 (Please note that this feature is only available from NIOS 8.5)	NOERROR/NODATA
	The source DNS query is from the subnet 192.168.2.0/24 (Please note that this feature is only available from NIOS 8.5)	NXDOMAIN

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

1. Go to **Data Management** → **DNS** → **Traffic Control**.

2. From the Toolbar, Click **Manage Topology Rulesets**.



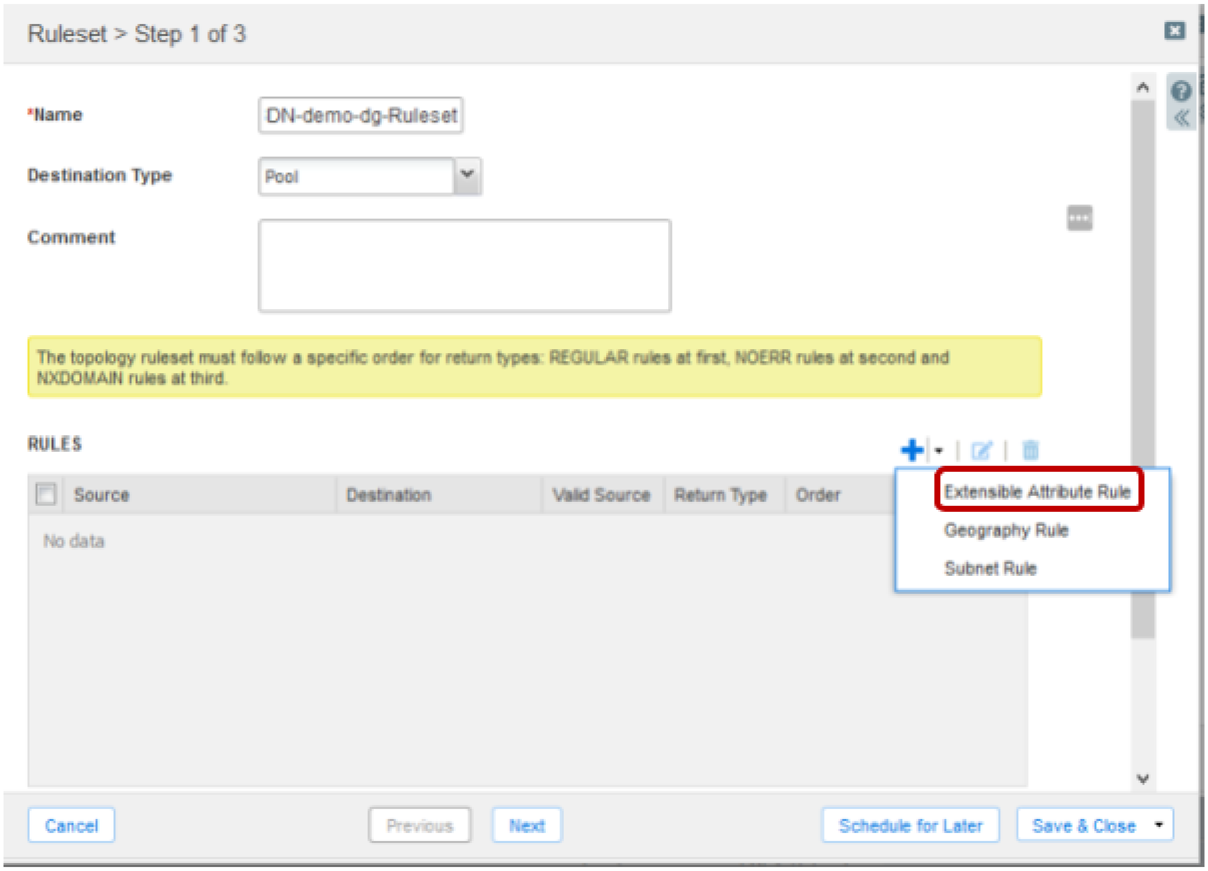
		Name	Type	Status	IPv4 Address	Comment
□	☰	dtc-vm-apac-1	Server	None	172.26.1.105	
□	☰	dtc-vm-apac-2	Server	None	172.26.1.106	

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

4. Type **LBDN-demo-dg-ruleset** in Name field.

5. Select **Pool** as Destination Type.

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



Ruleset > Step 1 of 3

*Name: DN-demo-dg-Ruleset

Destination Type: Pool

Comment:

The topology ruleset must follow a specific order for return types: REGULAR rules at first, NOERR rules at second and NXDOMAIN rules at third.

RULES

□	Source	Destination	Valid Source	Return Type	Order
	No data				

7. Select **APAC** for Corp-Region.

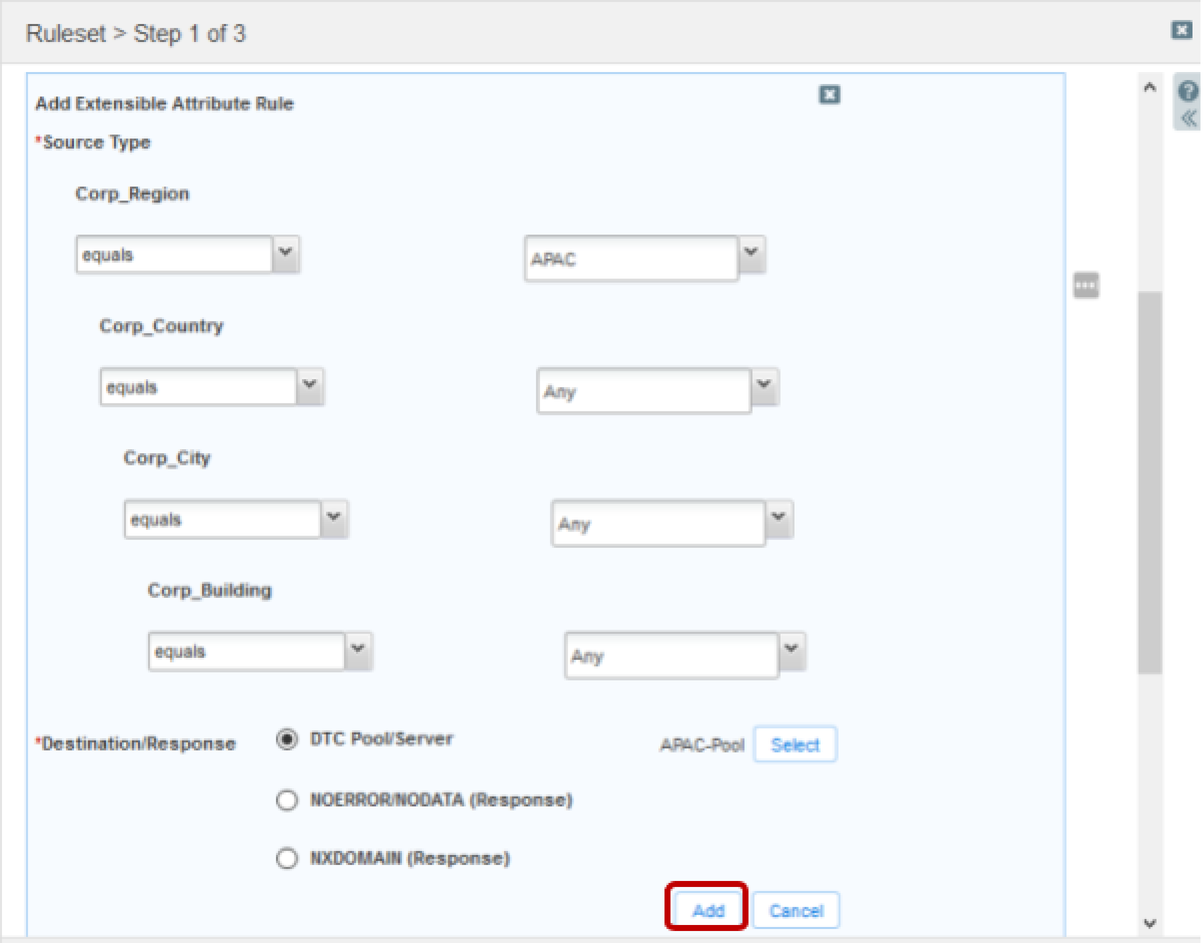
8. Select **Any** for Corp-Country.

9. Select **Any** for Corp-City.

10. Select **Any** for Corp-Building.

11. Select pool **APAC-Pool** for Destination.

12. Click **Add**



Ruleset > Step 1 of 3

Add Extensible Attribute Rule

*Source Type

Corp_Region

equals | APAC

Corp_Country

equals | Any

Corp_City

equals | Any

Corp_Building

equals | Any

*Destination/Response
● DTC Pool/Server APAC-Pool Select
○ NOERROR/NODATA (Response)
○ NXDOMAIN (Response)

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

14. Select **EMEA** for Corp-Region.

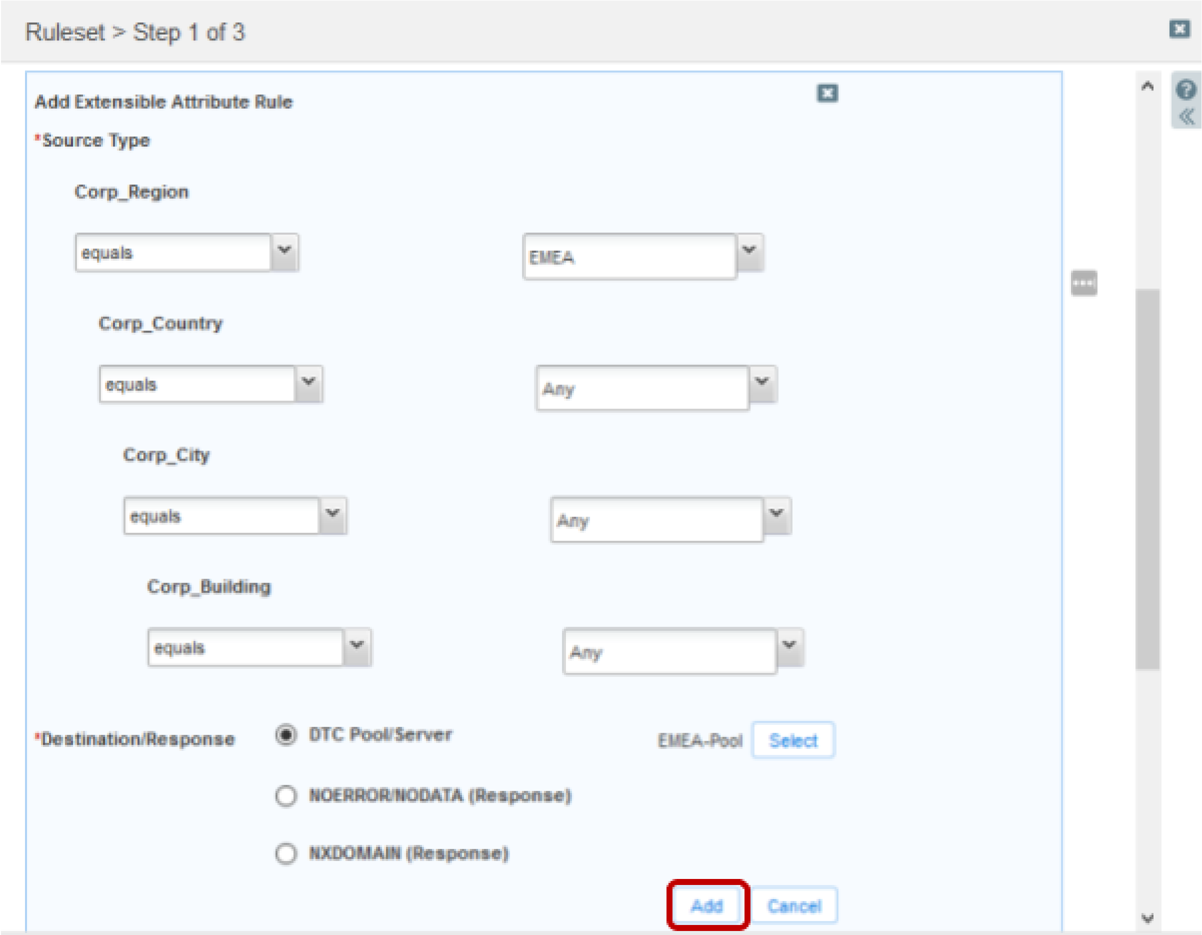
15. Select **Any** for Corp-Country.

16. Select **Any** for Corp-City.

17. Select **Any** for Corp-Building.

18. Select pool **EMEA-Pool** for Destination.

19. Click **Add**.



Ruleset > Step 1 of 3

Add Extensible Attribute Rule

*Source Type

Corp_Region

equals EMEA

Corp_Country

equals Any

Corp_City

equals Any

Corp_Building

equals Any

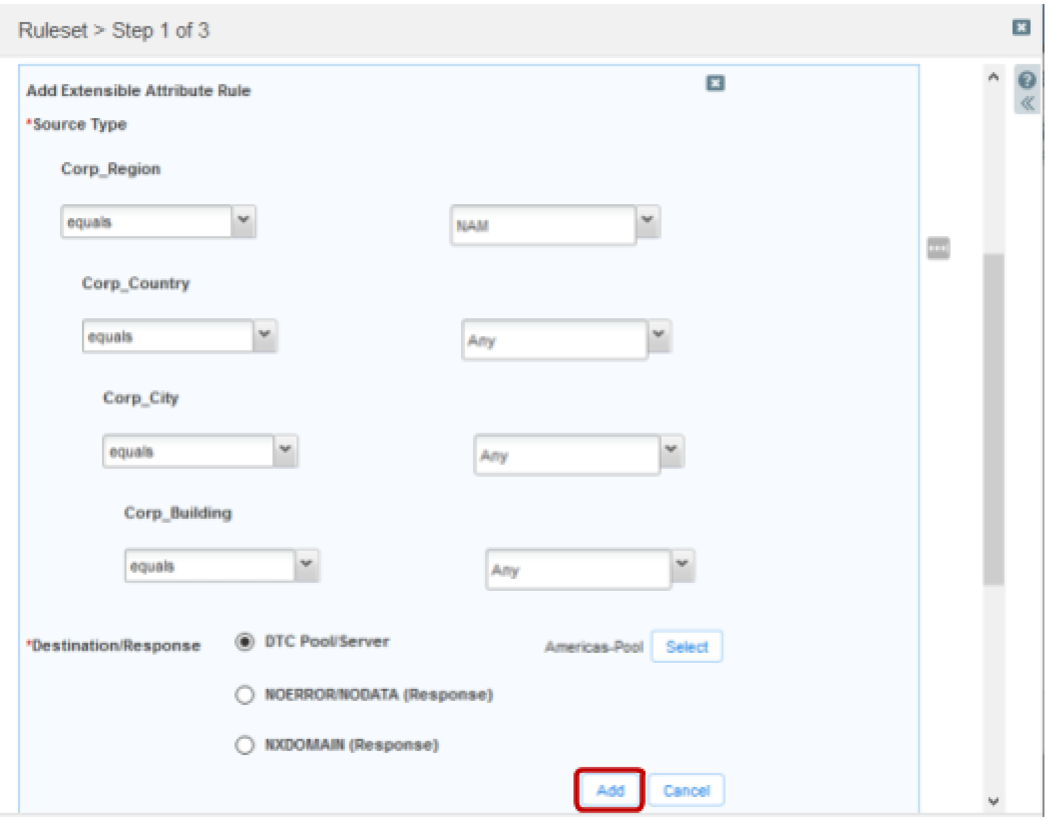
*Destination/Response ● DTC Pool/Server EMEA-Pool Select

○ NOERROR/NODATA (Response)

○ NXDOMAIN (Response)

20. Click **+** in Rules section and select Extensible Attribute Rule.
21. Select **NAM** for Corp-Region.
22. Select **Any** for Corp-Country.
23. Select **Any** for Corp-City.
24. Select **Any** for Corp-Building.
25. Select pool **Americas-Pool** for Destination.

26. Click **Add**.



Ruleset > Step 1 of 3

Add Extensible Attribute Rule

*Source Type

Corp_Region: equals NAM

Corp_Country: equals Any

Corp_City: equals Any

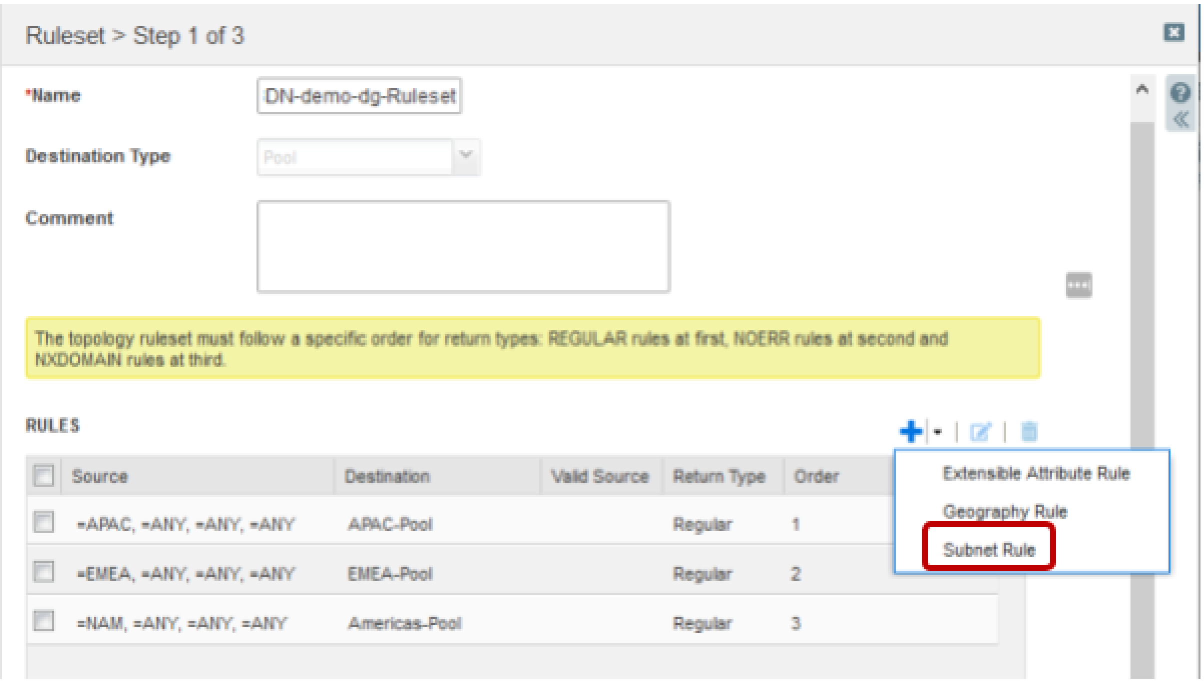
Corp_Building: equals Any

*Destination/Response: ● DTC Pool/Server Americas-Pool

○ NOERROR/NODATA (Response)

○ NXDOMAIN (Response)

27. Click **+** in Rules section and select the **Subnet Rule**.



Ruleset > Step 1 of 3

*Name: DN-demo-dg-Ruleset

Destination Type: Pool

Comment:

The topology ruleset must follow a specific order for return types: REGULAR rules at first, NOERR rules at second and NXDOMAIN rules at third.

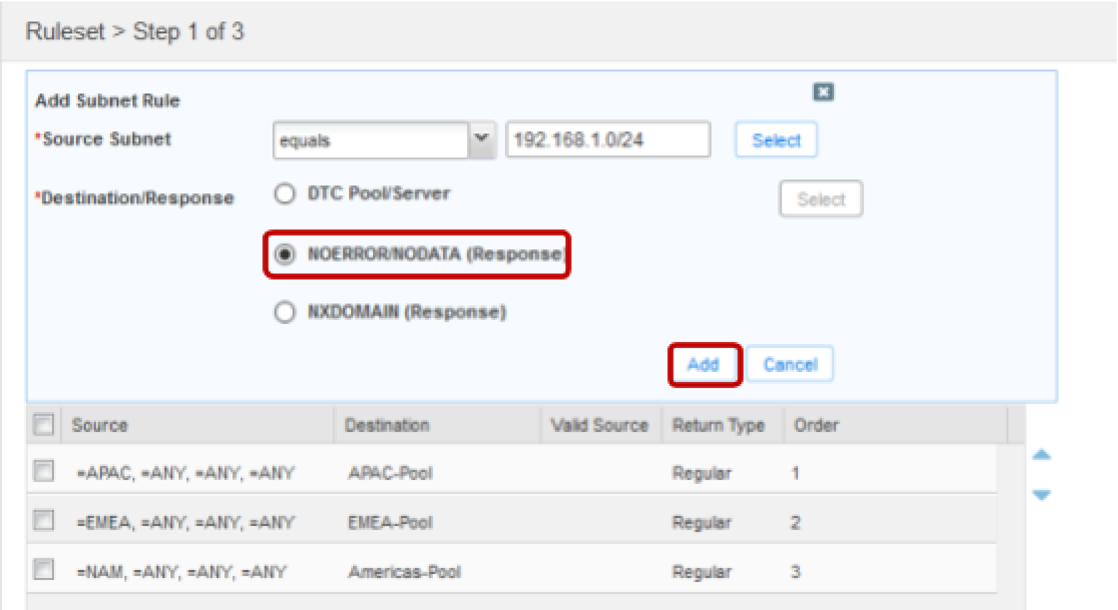
RULES

□	Source	Destination	Valid Source	Return Type	Order
□	=APAC, =ANY, =ANY, =ANY	APAC-Pool		Regular	1
□	=EMEA, =ANY, =ANY, =ANY	EMEA-Pool		Regular	2
□	=NAM, =ANY, =ANY, =ANY	Americas-Pool		Regular	3

28. Set the Source Subnet equals value to 192.168.1.0/24

29. Select **NOERROR/NODATA** for the Response

30. Click **Add**.



Ruleset > Step 1 of 3

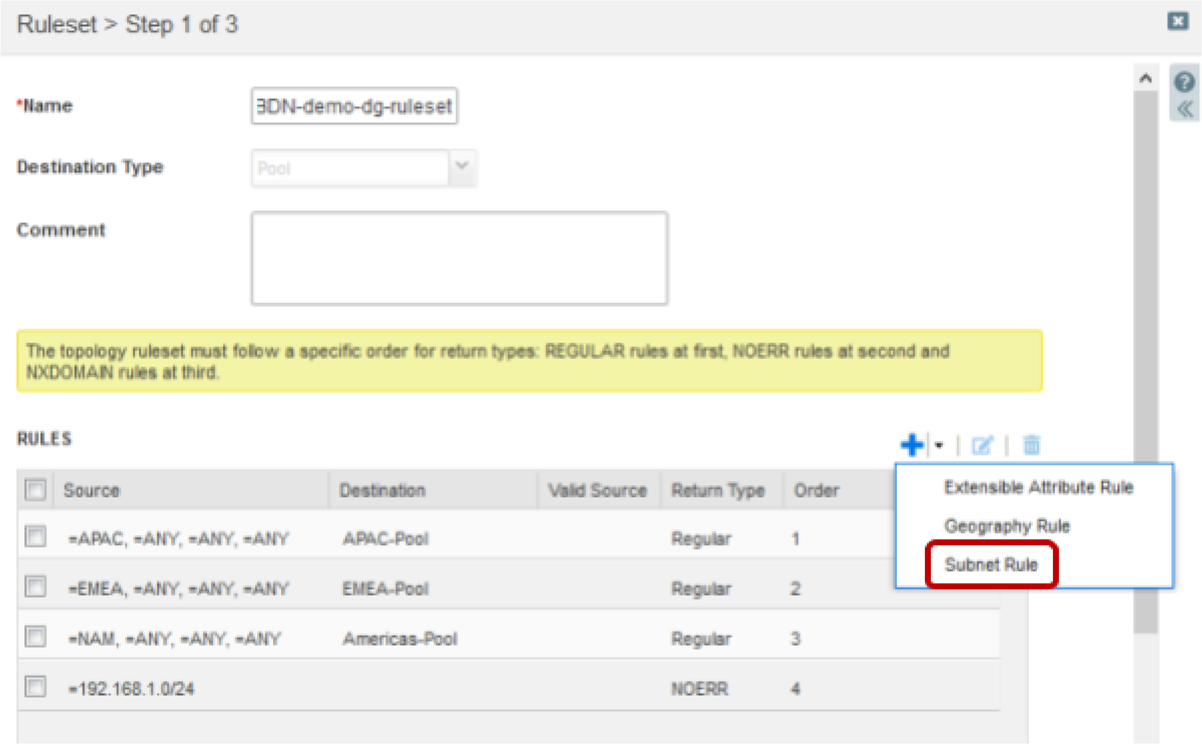
Add Subnet Rule

*Source Subnet: equals | 192.168.1.0/24

*Destination/Response:
○ DTC Pool/Server
● NOERROR/NODATA (Response)
○ NXDOMAIN (Response)

□	Source	Destination	Valid Source	Return Type	Order
□	=APAC, =ANY, =ANY, =ANY	APAC-Pool		Regular	1
□	=EMEA, =ANY, =ANY, =ANY	EMEA-Pool		Regular	2
□	=NAM, =ANY, =ANY, =ANY	Americas-Pool		Regular	3

31. Click **+** in the Rules section and select **Subnet Rule**.



Ruleset > Step 1 of 3

*Name: 3DN-demo-dg-ruleset

Destination Type: Pool

Comment:

The topology ruleset must follow a specific order for return types: REGULAR rules at first, NOERR rules at second and NXDOMAIN rules at third.

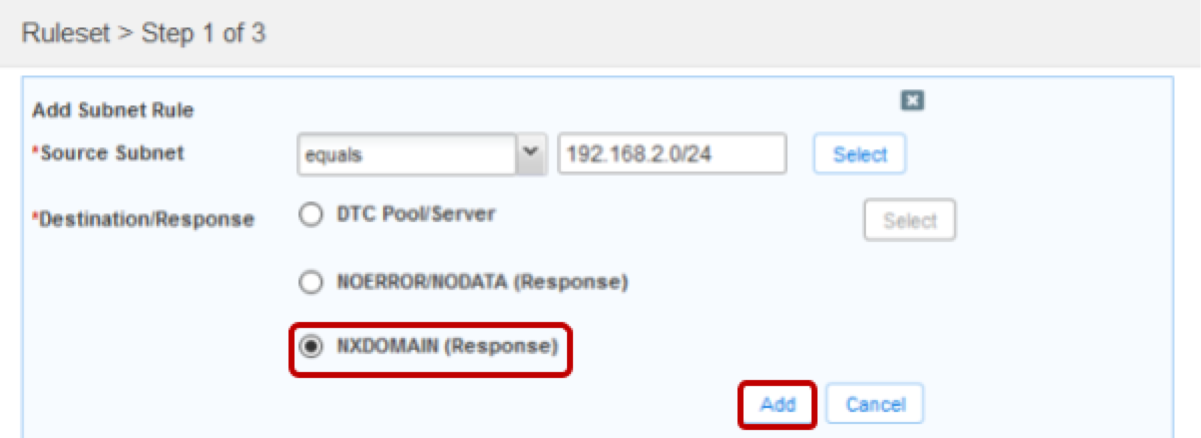
RULES

□	Source	Destination	Valid Source	Return Type	Order
□	=APAC, =ANY, =ANY, =ANY	APAC-Pool		Regular	1
□	=EMEA, =ANY, =ANY, =ANY	EMEA-Pool		Regular	2
□	=NAM, =ANY, =ANY, =ANY	Americas-Pool		Regular	3
□	=192.168.1.0/24			NOERR	4

32. Set the Source Subnet equals value to 192.168.2.0/24

33. Select **NXDOMAIN** for the Response

34. Click **Add**.



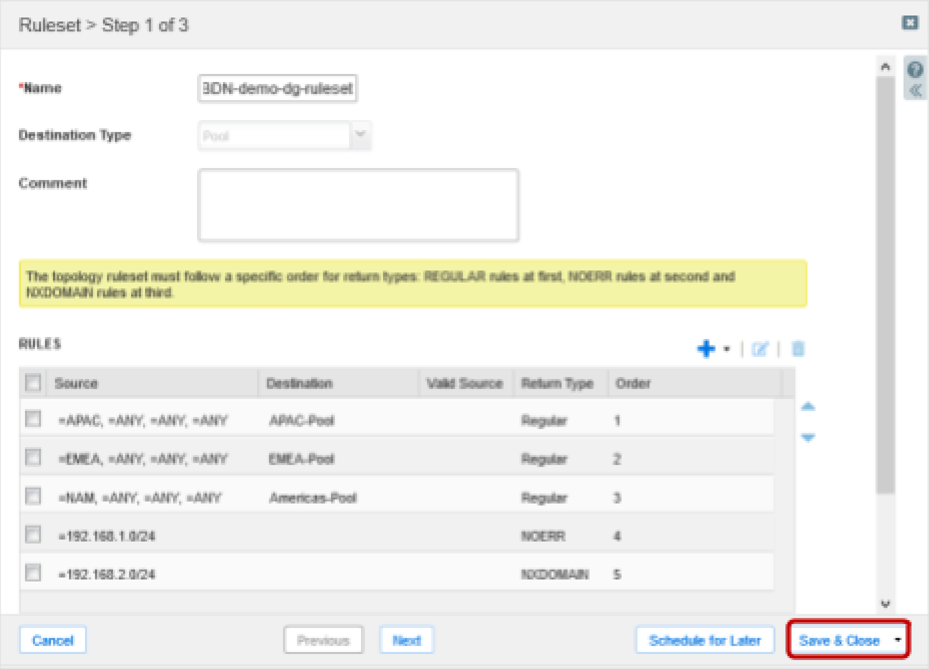
Ruleset > Step 1 of 3

Add Subnet Rule

*Source Subnet: equals | 192.168.2.0/24

*Destination/Response:
○ DTC Pool/Server
○ NOERROR/NODATA (Response)
● NXDOMAIN (Response)

35. Click **Save & Close**.



Ruleset > Step 1 of 3

*Name: 3DN-demo-dg-ruleset

Destination Type: Pool

Comment:

The topology ruleset must follow a specific order for return types: REGULAR rules at first, NOERR rules at second and NXDOMAIN rules at third.

RULES

□	Source	Destination	Valid Source	Return Type	Order
□	=APAC, =ANY, =ANY, =ANY	APAC-Pool		Regular	1
□	=EMEA, =ANY, =ANY, =ANY	EMEA-Pool		Regular	2
□	=NAM, =ANY, =ANY, =ANY	Americas-Pool		Regular	3
□	=192.168.1.0/24			NOERR	4
□	=192.168.2.0/24			NXDOMAIN	5

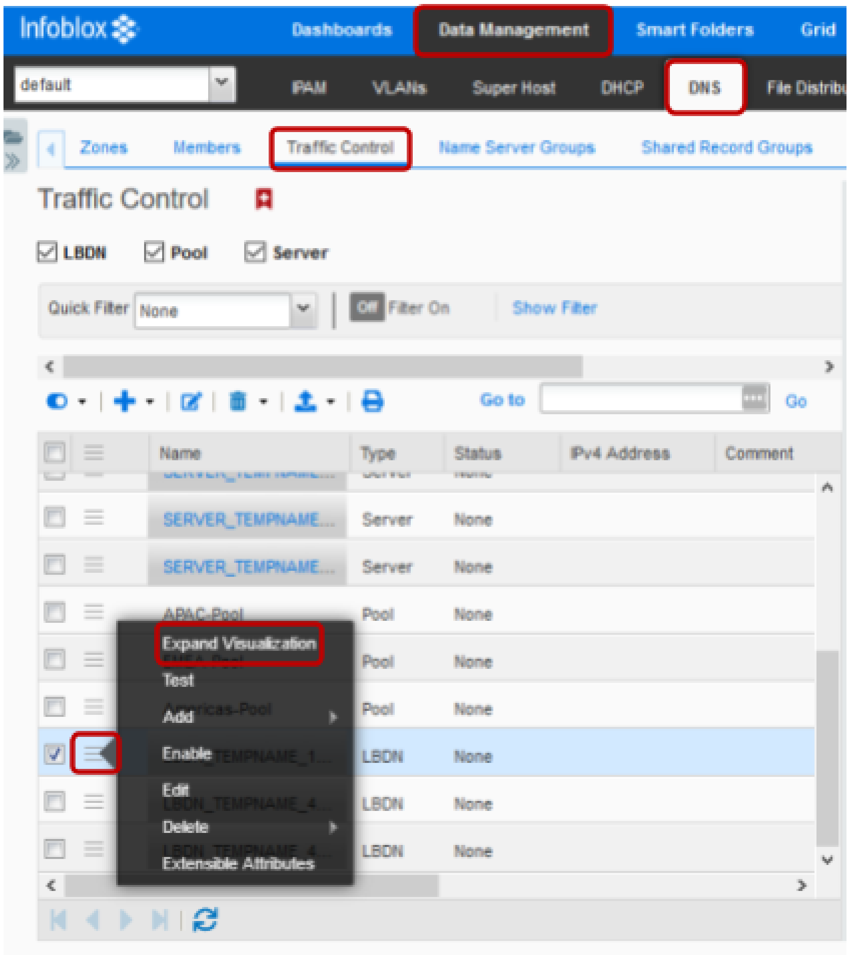
Configure LBDN

In our example we are going to create a Load balanced domain name LBDN-demo-dg.com using Default Visualization.

DTC LBDN	Pattern	Authoritative zone	Ruleset for Topology Load balancing	Member Pools
LBDN-demo-dg.com	*.demo-dg.com	demo-dg.com	LBDN-demo-dg-ruleset	APAC-Pool EMEA-Pool Americas-Pool

To configure LBDN:

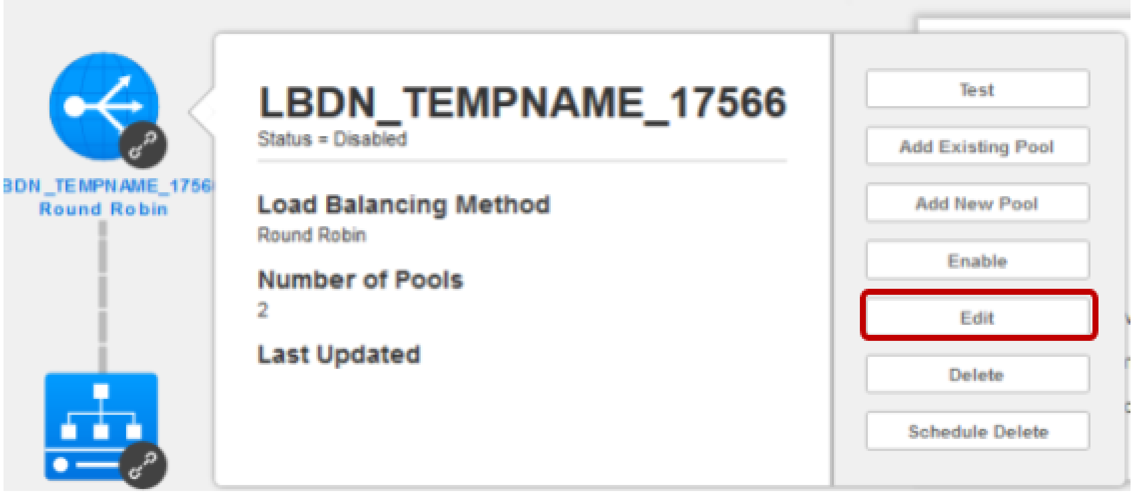
1. Go to **Data Management → DNS → Traffic Control**.
2. Click on hamburger next to a **LBDN_TEMPNAME_xxxxx** (where xxxxx is a random number).
   a. Select **Expand Visualization**.



Name	Type	Status	IPv4 Address	Comment
SERVER_TEMPNAME...	Server	None		
SERVER_TEMPNAME...	Server	None		
SERVER_TEMPNAME...	Server	None		
APAC-Pool	Pool	None		
EMEA-Pool	Pool	None		
Americas-Pool	Pool	None		
LBDN_TEMPNAME_1...	LBDN	None		
LBDN_TEMPNAME_4...	LBDN	None		
LBDN_TEMPNAME_4...	LBDN	None		

3. Move cursor over LBDN_TEMPNAME_xxxxx.

   a. Select **Edit**.



LBDN_TEMPNAME_17566

Status = Disabled

Load Balancing Method

Round Robin

Number of Pools

2

Last Updated

4. In the General Tab, Type **LBDN-demo-dg.com** in the **Display Name** field.

5. Click **+**.

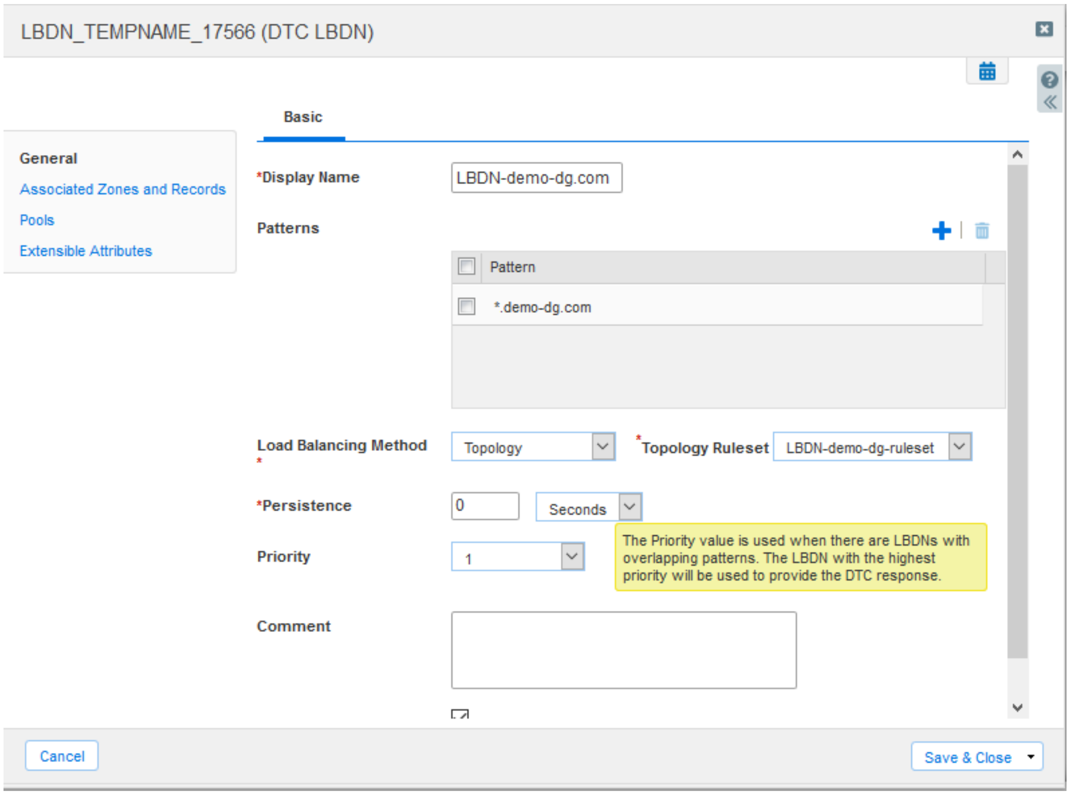
6. Type ***.demo-dg.com** in row under **Patterns** table.

7. Select **Topology** as Load Balancing Method.

8. Select **LBDN-demo-dg-ruleset** as Topology Ruleset.

Note: With NIOS 8.3, state persistence was introduced. When you enable persistence for an LBDN, the appliance stores the results for specific LBDN responses in the DNS Traffic Control cache. When a request originates from the respective FQDN or an IP address within the specified period, the DNS server directs the request to the same server.

With NIOS 8.5, maximum DTC record persistency has been increased from 30 minutes to 2 hours.
This makes the responses faster since they are cached for longer.



LBDN_TEMPNAME_17566 (DTC LBDN)

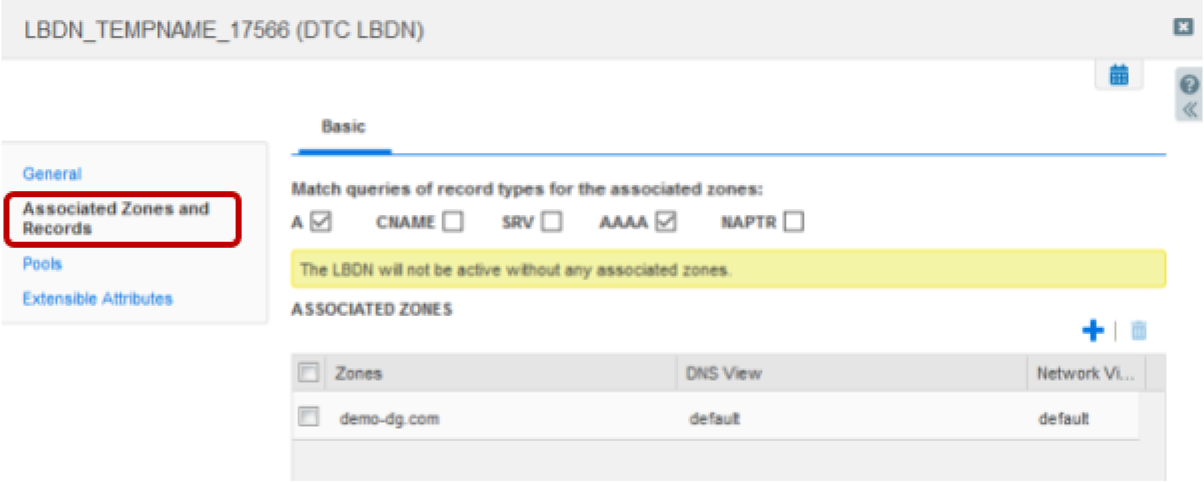
*Display Name	LBDN-demo-dg.com
Patterns	Pattern *.demo-dg.com
Load Balancing Method *	Topology
*Topology Ruleset	LBDN-demo-dg-ruleset
*Persistence	0 Seconds
Priority	1
Comment	

The Priority value is used when there are LBDNs with overlapping patterns. The LBDN with the highest priority will be used to provide the DTC response.

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

10. Select **demo-dg.com zone** from the list.

11. In the Pools Tab, click **+**.



LBDN_TEMPNAME_17566 (DTC LBDN)

Match queries of record types for the associated zones:

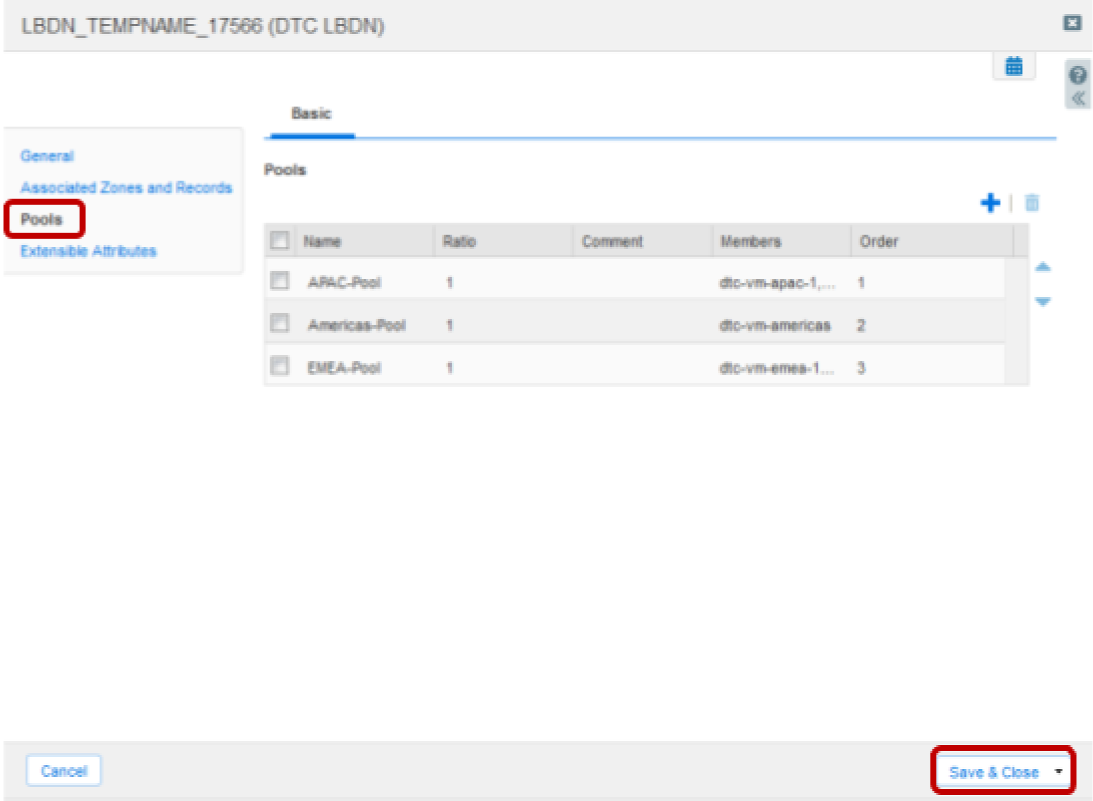
A ☑ CNAME □ SRV □ AAAA ☑ NAPTR □

The LBDN will not be active without any associated zones.

ASSOCIATED ZONES

Zones	DNS View	Network Vi...
demo-dg.com	default	default

12. Select **APAC-Pool** and repeat step 11 for EMEA-Pool and Americas-Pool.


LBDN_TEMPNAME_17566 (DTC LBDN)

Pools

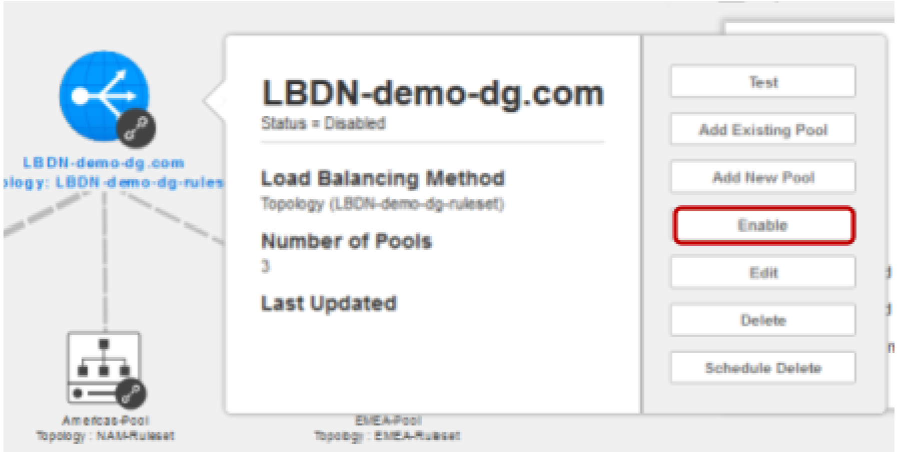
Name	Ratio	Comment	Members	Order
APAC-Pool	1		dtc-vm-apac-1,...	1
Americas-Pool	1		dtc-vm-americas	2
EMEA-Pool	1		dtc-vm-emea-1...	3

13. Click **Save & Close**.

14. Move cursor over **LBDN-demo-dg.com** in Visualization.

15. Click **Enable**.

16. Click **Yes**.


LBDN-demo-dg.com

Status = Disabled

Load Balancing Method

Topology (LBDN-demo-dg-ruleset)

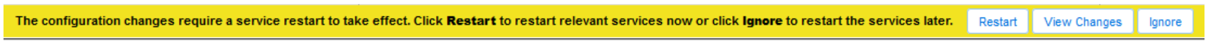
Number of Pools

3

Last Updated

17. Close Visualization display.

18. Click **Restart**.

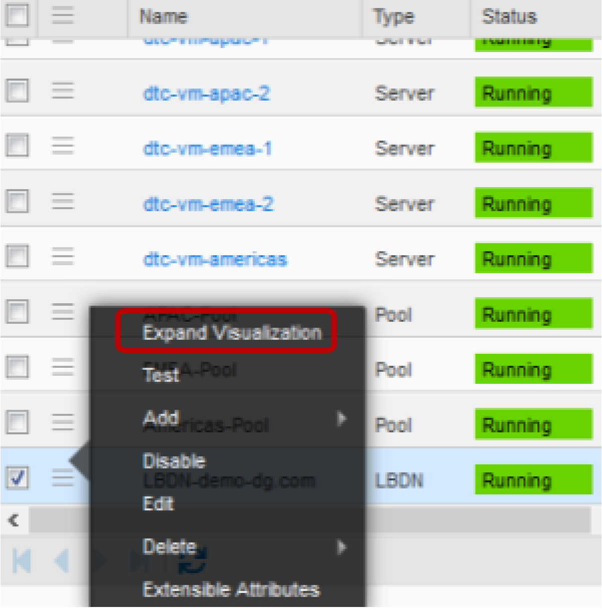


The configuration changes require a service restart to take effect. Click **Restart** to restart relevant services now or click **Ignore** to restart the services later.

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-demo-dg.com by clicking on the icon next to the DTC LBDN and selecting Expand Visualization.



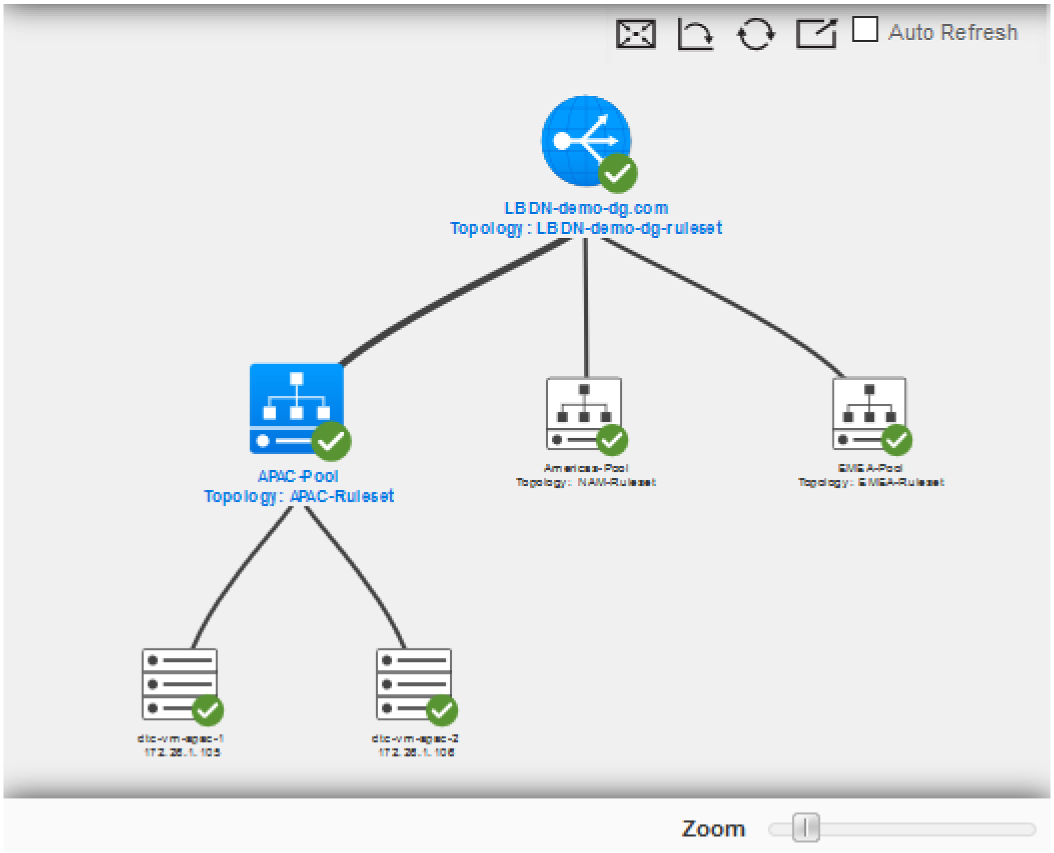
Name	Type	Status
dtc-vm-apac-1	Server	Running
dtc-vm-apac-2	Server	Running
dtc-vm-emea-1	Server	Running
dtc-vm-emea-2	Server	Running
dtc-vm-americas	Server	Running
APAC-Pool	Pool	Running
EMEA-Pool	Pool	Running
Americas-Pool	Pool	Running
LBDN-demo-dg.com	LBDN	Running

This takes us to a page with graphical representation of the selected DTC LBDN. The working configuration is displayed with all check marks 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 three DTC Pools named APAC-Pool, EMEA-Pool and Americas-Pool, 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.

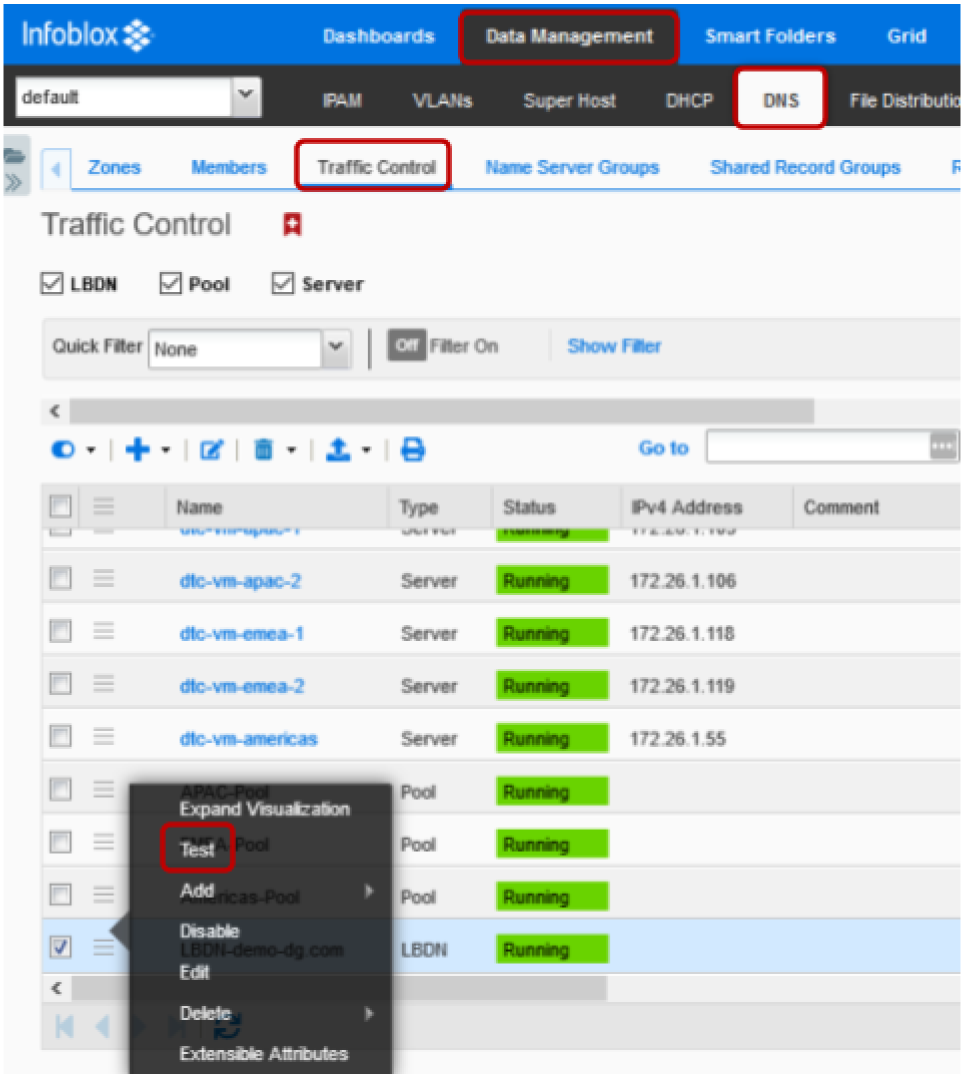


Test DTC LBDN

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 the hamburger icon next to LBDN-demo-dg.com.
3. Click **Test**.



		Name	Type	Status	IPv4 Address	Comment
□		dtc-vm-apac-1	Server	Running	172.26.1.105	
□		dtc-vm-apac-2	Server	Running	172.26.1.106	
□		dtc-vm-emea-1	Server	Running	172.26.1.118	
□		dtc-vm-emea-2	Server	Running	172.26.1.119	
□		dtc-vm-americas	Server	Running	172.26.1.55	
□		APAC-Pool	Pool	Running		
□		EMEA-Pool	Pool	Running		
□		Americas-Pool	Pool	Running		
☑		LBDN-demo-dg.com	LBDN	Running		

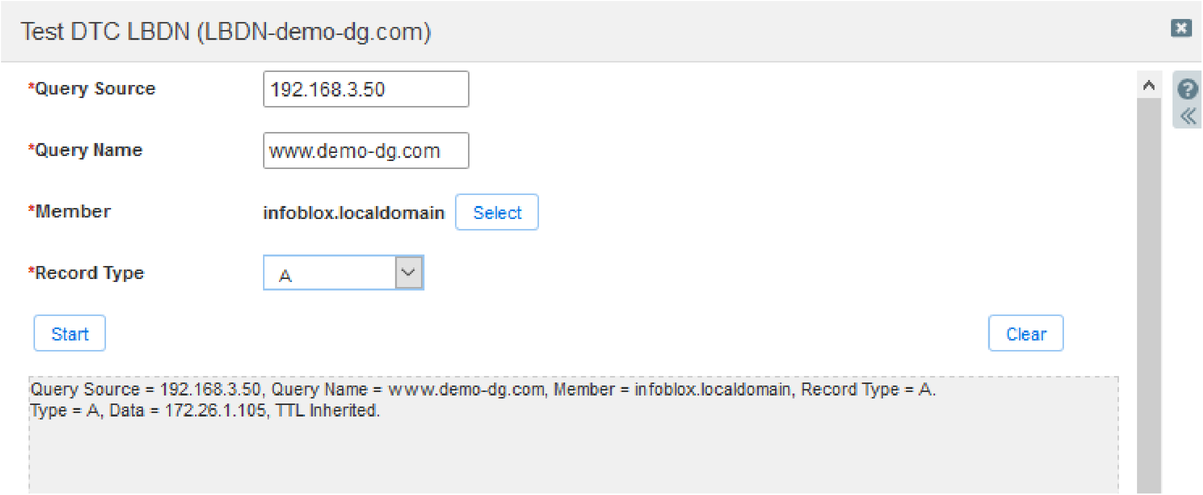
4. Type 192.168.3.50 in **Query Source** field.

5. Type www.demo-dg.com in **Query Name** field.

6. Select nios.dtc-demo.com in Member field by clicking **Select** button.

7. Select A for Record Type.

8. Click **Start**.



*Query Source: 192.168.3.50

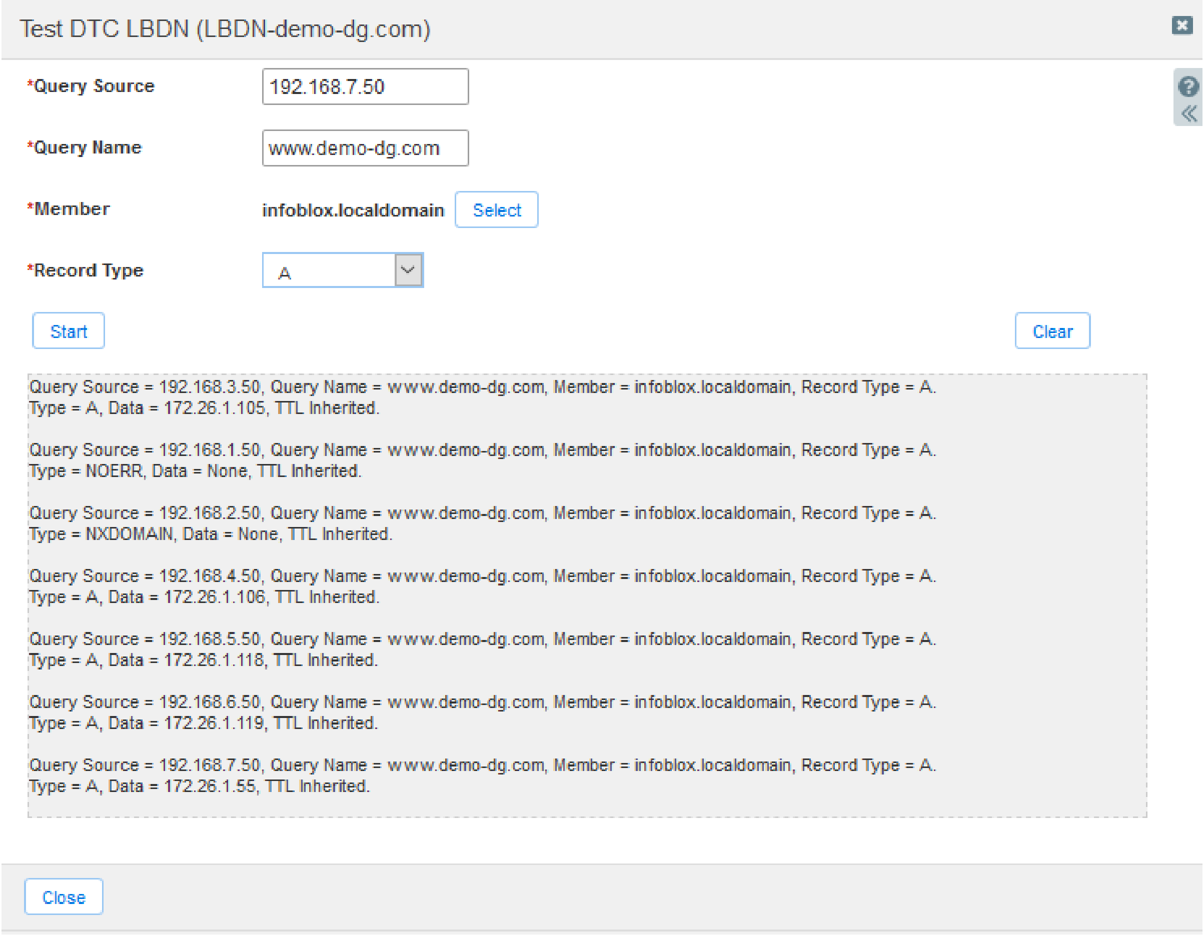
*Query Name: www.demo-dg.com

*Member: infoblox.localdomain

*Record Type: A

```
Query Source = 192.168.3.50, Query Name = www.demo-dg.com, Member = infoblox.localdomain, Record Type = A.
Type = A, Data = 172.26.1.105, TTL Inherited.
```

Verify the Query Response as "172.26.1.105". It is Server dtc-vm-apac-1 served when query originated from HQ/Singapore/Singapore/APAC. Similarly, you can test it out for other source IPs as well, as shown below



*Query Source: 192.168.7.50

*Query Name: www.demo-dg.com

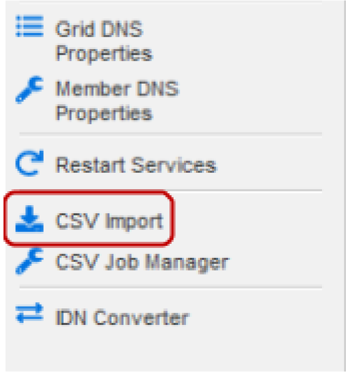
*Member: infoblox.localdomain

*Record Type: A

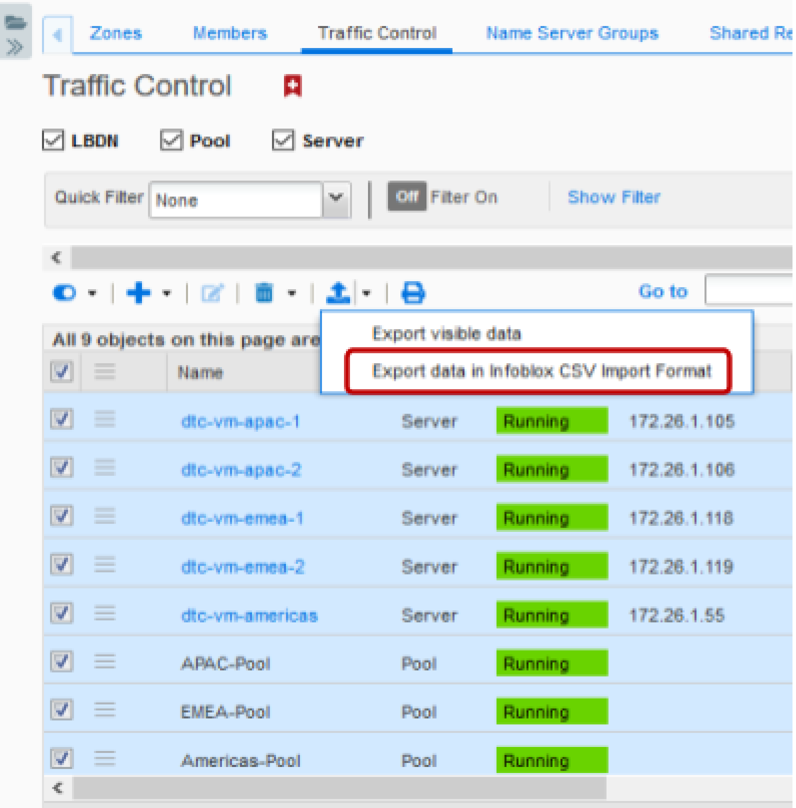
```
Query Source = 192.168.3.50, Query Name = www.demo-dg.com, Member = infoblox.localdomain, Record Type = A.
Type = A, Data = 172.26.1.105, TTL Inherited.

Query Source = 192.168.1.50, Query Name = www.demo-dg.com, Member = infoblox.localdomain, Record Type = A.
Type = NOERR, Data = None, TTL Inherited.

Query Source = 192.168.2.50, Query Name = www.demo-dg.com, Member = infoblox.localdomain, Record Type = A.
Type = NXDOMAIN, Data = None, TTL Inherited.

Query Source = 192.168.4.50, Query Name = www.demo-dg.com, Member = infoblox.localdomain, Record Type = A.
Type = A, Data = 172.26.1.106, TTL Inherited.

Query Source = 192.168.5.50, Query Name = www.demo-dg.com, Member = infoblox.localdomain, Record Type = A.
Type = A, Data = 172.26.1.118, TTL Inherited.

Query Source = 192.168.6.50, Query Name = www.demo-dg.com, Member = infoblox.localdomain, Record Type = A.
Type = A, Data = 172.26.1.119, TTL Inherited.

Query Source = 192.168.7.50, Query Name = www.demo-dg.com, Member = infoblox.localdomain, Record Type = A.
Type = A, Data = 172.26.1.55, TTL Inherited.
```

CSV Import/Export Support

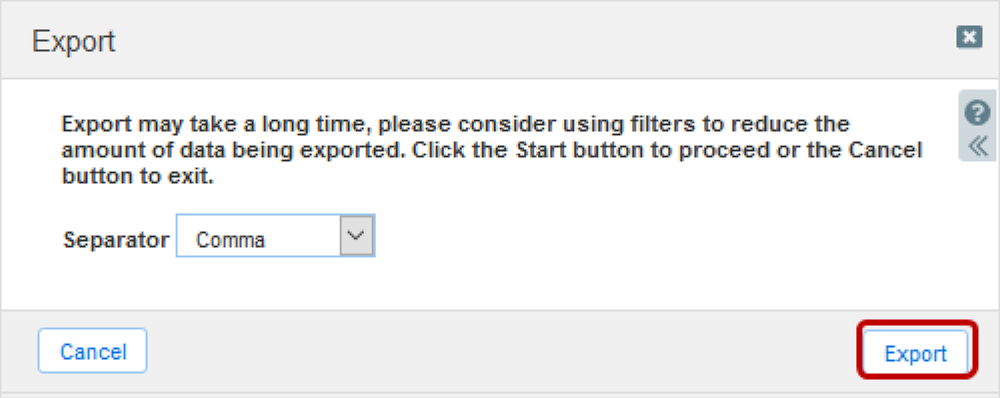
From NIOS 8.3 onwards, you can use the CSV Import feature to migrate data from other load balancing solutions or modify multiple objects at a time. You can do so, by clicking on the **CSV Import** option on the Toolbar. You can refer to the CSV import reference available on the Infoblox Documents portal.



You can also export DTC data as a CSV for external parsing or historical backups of the configuration. You can do so by selecting all the DTC objects, and clicking on the export option and selecting Export data in Infoblox CSV Import Format. Click on **Export**.



☑	Name			
☑	dtc-vm-apac-1	Server	Running	172.26.1.105
☑	dtc-vm-apac-2	Server	Running	172.26.1.106
☑	dtc-vm-emea-1	Server	Running	172.26.1.118
☑	dtc-vm-emea-2	Server	Running	172.26.1.119
☑	dtc-vm-americas	Server	Running	172.26.1.55
☑	APAC-Pool	Pool	Running	
☑	EMEA-Pool	Pool	Running	
☑	Americas-Pool	Pool	Running	

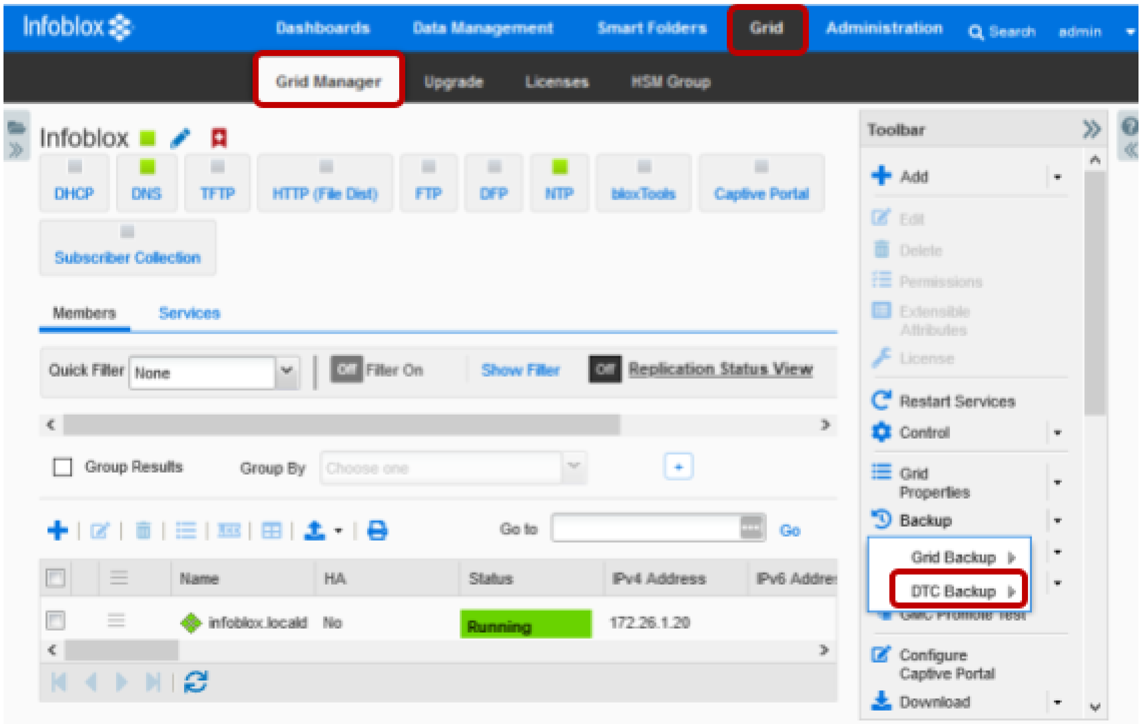

Export

Export may take a long time, please consider using filters to reduce the amount of data being exported. Click the Start button to proceed or the Cancel button to exit.

Separator: Comma

DTC Backup/Restore Support

From NIOS 8.3 onwards, you can backup DTC specific information, by navigating to **Grid** → **Grid Manager**, and selecting **DTC Backup** from the **Backup** option in the Toolbar.



Name	HA	Status	IPv4 Address	IPv6 Addre
infoblox.localdc	No	Running	172.26.1.20	

Similarly, you can restore a DTC backup, by selecting the DTC Restore from the Restore option in the Toolbar.

WAPI support

You can use the Infoblox RESTful APIs to create DTC configuration. The endpoints supported are as shown below:

```
dtc : DTC object
```

```
dtc:allrecords : DTC AllRecords object

dtc:certificate : DTC Certificate object

dtc:lbdn : DTC LBDN object

dtc:monitor : DTC monitor object

dtc:monitor:http : DTC HTTP monitor object

dtc:monitor:icmp : DTC ICMP monitor object

dtc:monitor:pdp : DTC PDP monitor object

dtc:monitor:sip : DTC SIP monitor object

dtc:monitor:snmp : DTC SNMP monitor object

dtc:monitor:tcp : DTC TCP monitor object

dtc:object : DTC object

dtc:pool : DTC Pool object

dtc:record:a : DTC A Record object

dtc:record:aaaa : DTC AAAA Record object

dtc:record:cname : DTC CNAME Record object

dtc:record:naptr : DTC NAPTR Record object

dtc:record:srv : DTC SRV Record object

dtc:server : DTC Server object

dtc:topology : DTC Topology object

dtc:topology:label : DTC Topology Label object

dtc:topology:rule : DTC Topology Rule object
```

For more information on each of the objects, you can refer to the RESTful API documentation available on the Infoblox Documentation Portal.

For sample API calls, you refer to the DNS Traffic Control section in the Infoblox REST API Reference Guide.

Conclusion

Infoblox DNS Traffic Control combines DNS management with intelligent GSLB functionality, so you can have automated and scalable high performance, all in one solution.

Additional Information

Community article: Create full DTC configuration in WAPI (v2.1 and above) from scratch in a single Request

Community blog: Using DNS Traffic Control for Microsoft Active Directory Domain Controller Selection

Tech Video: DTC Features Webinar

Tech Video: DTC: Saving Time using the DTC API vs. Web UI when Configuring New Applications

Community blog: What is New with DNS Traffic Control with NOS 8.5?

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com