Infoblox®
CONTROL YOUR NETWORK

# Infoblox BFD Configuration Guide

## Copyright Statements

## Trademark Statements

## Company Information

http://www.infoblox.com/contact/

## Product Information

Hardware Models

Infoblox Advanced Appliances: PT-1400, PT-1405, PT-2200, PT-2205, PT-2205-10GE, PT-4000, and PT-4000-10GE

Network Insight Appliances: ND-800, ND-805, ND-1400, ND-1405, ND-2200, ND-2205, and ND-4000

Trinzic Appliances: TE-100, TE-810, TE-815, TE-820, TE-825, TE-1410, TE-1415, TE-1420, TE-1425, TE-2210, TE-2215, TE-2220, TE-2225, IB-4010, and IB-4020

Cloud Network Automation: CP-V800, CP-V1400, and CP-V2200

Trinzic Reporting: TR-800, TR-805, TR-1400, TR-1405, TR-2200, TR-2205, and TR-4000

DNS Cache Acceleration Appliances: IB-4030 and IB-4030-10GE

NetMRI: NetMRI-1102-A, NT-1400, NT-2200, and NT-4000

Document Number: Rev. C

Document Updated: October 20, 2016

## Warranty Information

Your purchase includes a 90-day software warranty and a one year limited warranty on the Infoblox appliance, plus an Infoblox Warranty Support Plan and Technical Support. For more information about Infoblox Warranty information, refer to the Infoblox Web site, or contact Infoblox Technical Support.

# Preface

This preface describes the content and organization of this guide, how to find additional product information, and how to contact technical support. It comprises the following sections:

## Document Overview

This guide explains how to configure Bidirectional Forwarding Detection (BFD) for OSPF Area and BGP Neighbors. For the latest Infoblox documentation, visit the Infoblox Support web site at https://support.infoblox.com/.

### Conventions

This guide follows the Infoblox documentation style conventions, as listed in the following table.

| Style | Usage |
|---|---|
| `screen` | Indicates session text or system information displayed on the screen. |
| **`boldface screen`** | Signifies command line entries that you type. |
| *`italic screen`* | Signifies variables that you enter for your configuration, such as file names and group names. |

## Related Documentation

Other Infoblox documentation:

- *Infoblox CLI Guide*
- *Infoblox API Documentation*
- *Infoblox WAPI Documentation*
- *Infoblox CSV Import Reference*
- *Infoblox Installation Guide for the Trinzic 100 Appliance*
- *Infoblox Installation Guide for the 800 Series Platforms*
- *Infoblox Installation Guide for the 805 Series Platforms*
- *Infoblox Installation Guide for the 1400 Series Platforms*
- *Infoblox Installation Guide for the 1405 Series Platforms*
- *Infoblox Installation Guide for the 2200 Series Platforms*
- *Infoblox Installation Guide for the 2205Series Platforms*

- *Infoblox Installation Guide for the 4000 Series Platforms*
- *Infoblox Installation Guide for the Infoblox-4010 Appliance*
- *Infoblox Installation Guide for the IB-4030 and IB-4030-10GE Appliances*
- *Infoblox DNS Cache Acceleration Administrator Guide*
- *Infoblox Installation Guide for vNIOS for Microsoft Azure*
- *Infoblox Installation Guide for vNIOS for AWS*
- *Infoblox Installation Guide for vNIOS for VMware*
- *Infoblox Installation Guide for vNIOS on Microsoft 2008 R2 for Hyper-V*
- *Infoblox Installation Guide for vNIOS for KVM Hypervisor and KVM-based OpenStack*
- *Infoblox Safety Guide*

To provide feedback on any of the Infoblox technical documents, please e-mail *techpubs@infoblox.com*.

# Customer Care

This section addresses user accounts, software upgrades, and technical support.

## User Accounts

The Infoblox appliance ships with a default user name and password. Change the default `admin` account password immediately after the system is installed to safeguard its use. Make sure that the appliance has at least one administrator account with superuser privileges at all times, and keep a record of your account information in a safe place. If you lose the `admin` account password, and did not already create another superuser account, the system will need to be reset to factory defaults. This may cause you to lose all existing data on the appliance. You can create new administrator accounts, with or without superuser privileges. For more information, refer to the *Infoblox NIOS Administrator Guide*.

## Software Upgrades

Software upgrades are available according to the Terms of Sale for your system. Infoblox notifies you when an upgrade is available. Register immediately with Infoblox Technical Support at http://www.infoblox.com/support/customer/evaluation-and-registration to maximize your Technical Support.

## Technical Support

Infoblox Technical Support provides assistance via the Web, e-mail, and telephone. The Infoblox Support web site at https://support.infoblox.com/ provides access to product documentation and release notes, but requires the user ID and password you receive when you register your product online at: http://www.infoblox.com/support/customer/evaluation-and-registration.

# About BFD (Bidirectional Forwarding Detection)

NIOS supports Anycast addressing for DNS using BGP and OSPF routing protocols. Since BGP and OSPF have timer granularity in seconds, the network re-convergence is slow in case of faults in forwarding path. BFD protocol is designed to provide faster failure detection using millisecond timer intervals. It can be enabled with routing protocols to achieve fast network re-convergence.

BFD can be enabled for OSPF or BGP and you can create BFD templates and assign it to OSPF Area or BGP neighbors. You can enable BFD simultaneously for OSPF and BGP, but only one BFD session will be created for a given neighbor. Infoblox recommends you to use the same BFD template for both OSPF and BGP neighbor whenever such a configuration is required.

The BFD protocol feature is supported in NIOS 8.0.0 and later releases. For more information about loopback interface (anycast), DNS, BGP, and OSPF configuration, refer to the *Infoblox NIOS Administrator Guide*.

This document provides a brief overview about enabling BFD for OSPF Area and BGP Neighbors, creating BFD templates, SNMP, and CLI commands.

*WARNING: The default advertised setting for BFD holddown is 300 ms (100 ms transit/receive intervals and detection multiplier 3). This setting is optimized for typical routers and directly connected endpoint configurations. If your network requires an implementation of L2 multi-path or port redundancy, you must adjust the holddown interval value higher than the spanning-tree rebalance latency to avoid unnecessary changes to the L3 network topology or the forwarding path for DNS traffic.*

# Enabling BFD for OSPF

You can enable BFD for IPv4 or IPv6 OSPF Area. To support DNS anycast and other routing-dependent applications on NIOS appliances, you must first configure the LAN1, LAN1 (VLAN), or HA (for HA pairs only) interface as an OSPF advertising interface, and then assign an area ID on the interface to associate it with a specific OSPF area. For more information, refer to the *NIOS Administration Guide*.

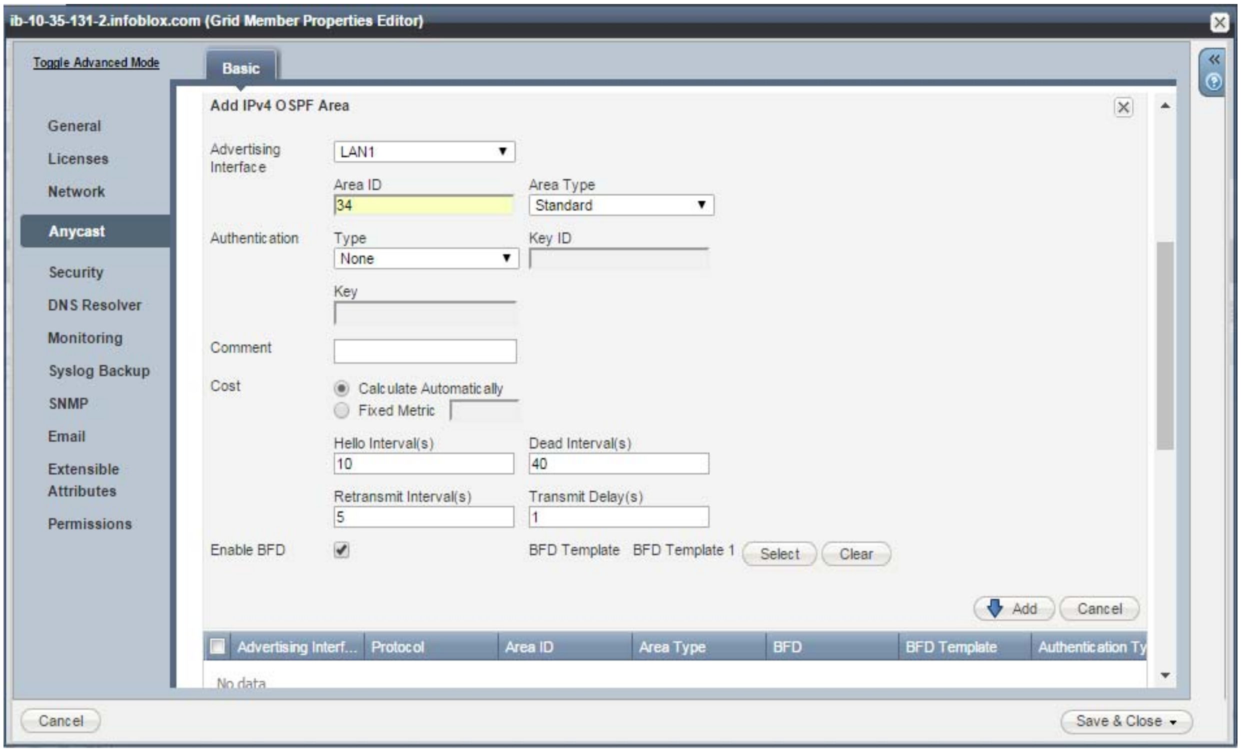
To enable BFD for IPv4 or IPv6 OSPF Area:

1. From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> *Grid_member* check box, and then click the Edit icon.
2. In the *Grid Member Properties* editor, select the **Anycast** tab.
3. In the OSPF Area Configuration table, select the OSPF advertising interface, click the Edit icon, and then complete the following:
   - **Enable BFD**: Select this check box to enable BFD for the OSPF advertising interface.
   - **BFD template:** Click **Select BFD Template** and select a BFD template from the *Select BFD Template* dialog box. You can click **Clear** to remove the selected BFD template and select a new one.
4. Save the configuration.

When OSPF session with a neighbor router in the OSPF Area reaches FULL state, BFD session is automatically created.

By default, BFD runs with no authentication and timer intervals of 100ms transmit, 100ms receive and multiplier 3 (hold down time = 300ms). The actual runtime intervals are negotiated with the peer as per BFD standard RFC 5880. If these intervals are not suitable or authentication needs to be enabled for BFD, you must create a BFD Template as described in *Creating a BFD Template* section.

*Figure 1.1 Enabling BFD for OSPF*



Add IPv4 OSPF Area

Advertising Interface: LAN1

Area ID: 34

Area Type: Standard

Authentication Type: None

Key ID:

Key:

Comment:

Cost: ● Calculate Automatically ○ Fixed Metric

Hello Interval(s): 10

Dead Interval(s): 40

Retransmit Interval(s): 5

Transmit Delay(s): 1

Enable BFD ☑

BFD Template: BFD Template 1

| ☐ | Advertising Interf... | Protocol | Area ID | Area Type | BFD | BFD Template | Authentication Ty |
|---|---|---|---|---|---|---|---|
| No data | | | | | | | |

## Viewing Runtime BFD Information for OSPF

You can use the show `ipv6_ospf neighbor` CLI command to view runtime BFD information for OSPF.

```
Infoblox > show ipv6_ospf neighbor
 Neighbor 10.40.16.16%bond0
    Area 0.0.0.2 via interface bond0 (ifindex 40)
    His IfIndex: 5 Link-local address: fe80::5a8d:9ff:fec2:46b2
    State Full for a duration of 00:12:33
    His choice of DR/BDR 10.40.16.16/10.34.54.68, Priority 1
    Using BFD to detect fast fallover
      BFD last signalized state : Up
    DbDesc status: Slave SeqNum: 0x8a63b025
    Summary-List: 0 LSAs
    Request-List: 0 LSAs
    Retrans-List: 0 LSAs
    0 Pending LSAs for DbDesc in Time 00:00:00 [thread off]
    0 Pending LSAs for LSReq in Time 00:00:00 [thread off]
    0 Pending LSAs for LSUpdate in Time 00:00:00 [thread off]
    0 Pending LSAs for LSAck in Time 00:00:00 [thread off]
```

# Enabling BFD for BGP Neighbor

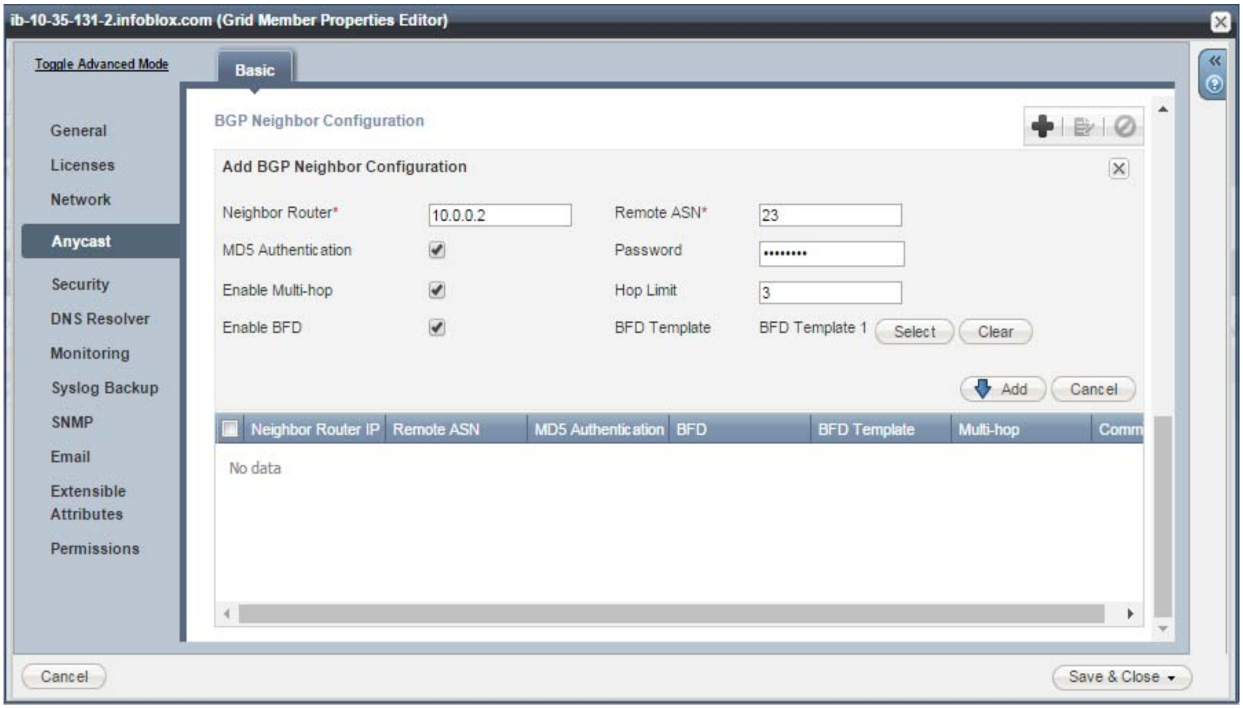
BFD can be enabled for each configured BGP neighbor individually. You can also use the Enable Multi-hop option, which allows BGP to connect to BGP neighbors which are more than one IP hops away.

To enable BFD for the BGP neighboring router:

1. From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> *Grid_member* check box, and then click the Edit icon.
2. In the *Grid Member Properties* editor, select the **Anycast** tab.
3. In the BGP Neighbor Configuration table, select the BGP neighboring router, click the Edit icon, and then complete the following:
   - **Enable Multi-hop (optional)**: Select this check box to allow BGP to connect with the neighbors which are more than one IP hops away.
   - **Hop Limit**: Enter the maximum hop limit. The default value is 255.
   - **Enable BFD**: Select this check box to enable BFD for the BGP neighboring router.
   - **BFD template**: You can assign a BFD template to the BGP neighboring router to run BFD with non-default settings. Click **Select BFD Template** and select a BFD template from the *Select BFD Template* dialog box. You can click **Clear** to remove the selected BFD template and select a new one. For information about creating a BFD template, see *Creating a BFD Template* on page 8.
4. Save the configuration.

BFD session for a given BGP neighbor is created when BGP state reaches ‘Established’.

*Figure 1.2 Enabling BFD for BGP Neighbor*



ib-10-35-131-2.infoblox.com (Grid Member Properties Editor)

BGP Neighbor Configuration

Add BGP Neighbor Configuration

| | | | |
|---|---|---|---|
| Neighbor Router* | 10.0.0.2 | Remote ASN* | 23 |
| MD5 Authentication | ☑ | Password | •••••••• |
| Enable Multi-hop | ☑ | Hop Limit | 3 |
| Enable BFD | ☑ | BFD Template | BFD Template 1 |

| ☐ | Neighbor Router IP | Remote ASN | MD5 Authentication | BFD | BFD Template | Multi-hop | Comm |
|---|---|---|---|---|---|---|---|

No data

## Viewing Runtime BFD Information for BGP

You can use the `show bgp neighbor` CLI command to view runtime BFD information for BGP.

```
Infoblox > show bgp neighbor
BGP neighbor is 10.34.54.16, remote AS 100, local AS 10, external link
  BGP version 4, remote router ID 10.40.16.16
  BGP state = Established, up for 00:00:42
  Using BFD to detect fast fallover in standard mode
  BFD last signalized state : Added
  Last read 00:00:00, hold time is 16, keepalive interval is 4 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
```

# Creating a BFD Template

BFD advertises the default hold-down interval of 300ms and authentication is disabled, by default. In order to configure faster or slower hold-down intervals, you can create BFD templates and assign it to the OSPF Area or BGP neighbors. You can configure a BFD template at the Grid level and assign it to multiple Grid members. The BFD template can be assigned to the BGP neighbor or OSPF Area of any Grid member in the Grid and it can be assigned to multiple BGP neighbors or OSPF Areas.

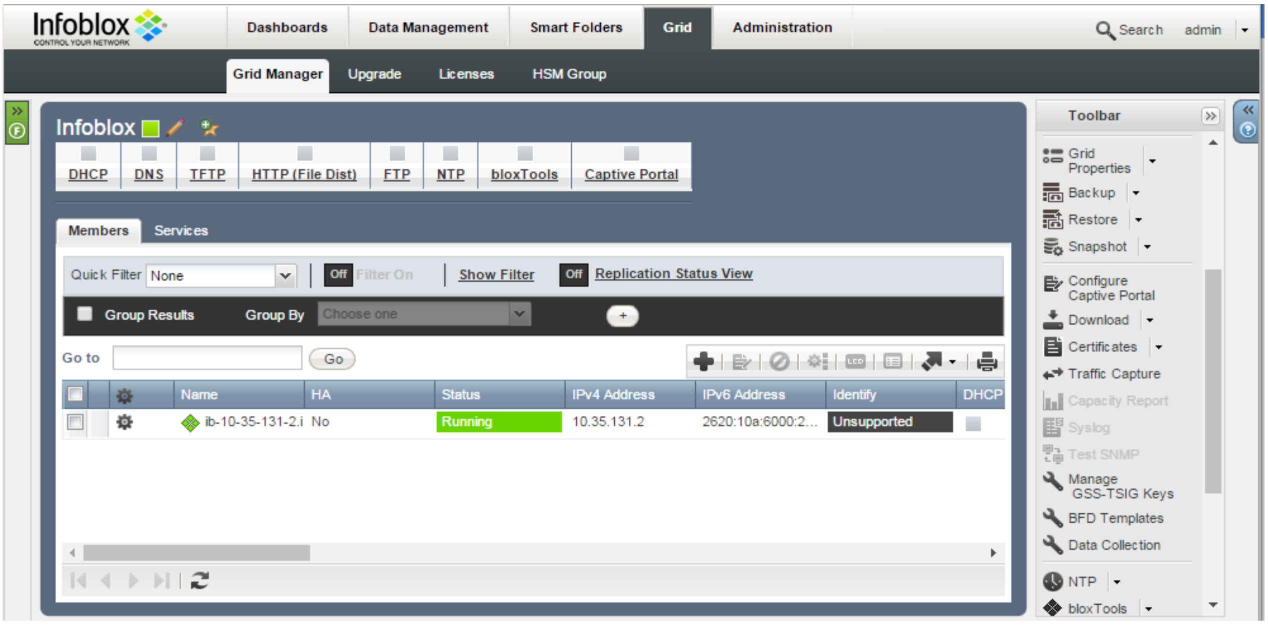
To create BFD templates:

1. From the **Grid** tab -> **Grid Manager** tab, expand the Toolbar and click **Manage BFD Templates**.
2. In the *Manage BFD Templates* wizard, click the Add icon, and then complete the following:
   - **Name**: Enter the name of the BFD template.
   - **Authentication Type**: Select the authentication type from the drop-down list. You can select one of the following authentication types: **MD5**, **SHA-1**, **Meticulous MD5**, or **Meticulous SHA-1**. The BFD authentication type fully conforms to RFC 5883.
   - **Authentication Key ID**: Enter the key identifier to use to specify the correct hash algorithm after you select the authentication type. **If you do not enter a value here, the appliance by default sets 'one' as the authentication key ID.** The authentication key ID configured on the Grid member must match the authentication key ID of the upstream router configuration.
   - **Authentication Secret/Password**: Enter the authentication password to use to verify after you select the authentication type. You can enter password with 4-16 printable ASCII characters. The authentication password configured on the Grid member must match the authentication key of the upstream router configuration.
   - **Intervals**: Specify the following BFD timer intervals for each router interface.
     - **Min Rx Interval (ms)**: Enter the minimum receive interval. The default is 100ms.
     - **Min Tx Interval (ms)**: Enter the minimum transmit interval. The default is 100ms.
     - **Multiplier:** Enter the detection multiplier. You can enter a value between 3 and 50. The default is 3.
3. Click **Add**.

After you have added BFD templates, you can do the following:

- Select a BFD template and click the Edit icon to edit the configuration.
- Select a BFD template and click the Delete icon to delete it.

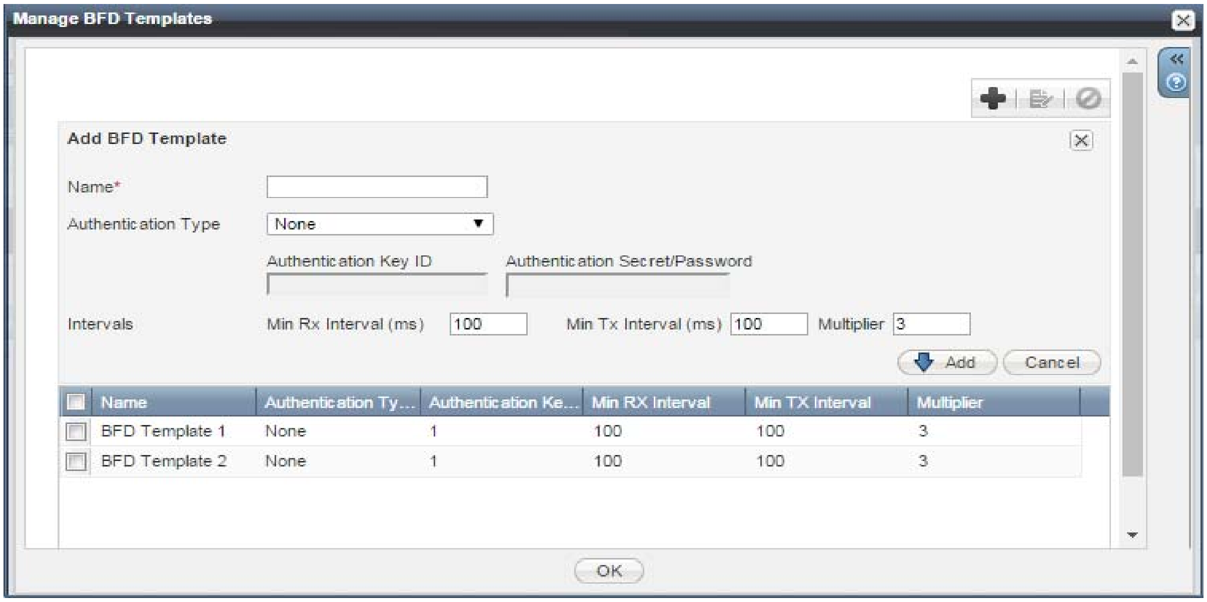
*Figure 1.3  Manage BFD Templates*



Quick Filter: None

| Name | HA | Status | IPv4 Address | IPv6 Address | Identify | DHCP |
|---|---|---|---|---|---|---|
| ib-10-35-131-2.i | No | Running | 10.35.131.2 | 2620:10a:6000:2... | Unsupported | |

*Figure 1.4  Manage BFD Templates Wizard*



Name*:

Authentication Type: None

Authentication Key ID:

Authentication Secret/Password:

Intervals: Min Rx Interval (ms) 100  Min Tx Interval (ms) 100  Multiplier 3

| Name | Authentication Ty... | Authentication Ke... | Min RX Interval | Min TX Interval | Multiplier |
|---|---|---|---|---|---|
| BFD Template 1 | None | 1 | 100 | 100 | 3 |
| BFD Template 2 | None | 1 | 100 | 100 | 3 |

## Enabling and Disabling DNS Health Check Monitor

In order to minimize downtime for DNS and ensure high availability, NIOS implements DNS process monitoring and self-recovery on each Grid member, in order to minimize downtime for DNS and ensure high availability. You can enable the DNS health check monitor to monitor whether the DNS server is responding to client requests. When you enable this feature, the appliance sends a query to the DNS server and waits for the response until the specified timeout duration. If the appliance is unable to receive a response from the DNS server after the specified number of retries, the appliance sends SNMP traps and email notifications about the failure. The appliance performs the DNS health check periodically based on the specified time interval.

If BFD is used for anycast fault detection, the BFD session state advertised from the member can be in the Down state whenever there is a DNS health check failure. This allows quick anycast route tear-down and the network might converge with another DNS server that can serve same anycast IP.

Additionally, you can also configure domain names in the DNS health check monitor, which are probed simultaneously and if any one of the domains fail to resolve for consecutive attempts, the DNS health is considered as Down. If recursion is enabled on the Grid member, the queries to these domains help to assert the ability of the DNS server to reach the external authoritative servers and optionally trigger network re-convergence in case of a failure. When no domains are configured, local PTR queries are used to probe the DNS process.

*WARNING: The DNS Health Check monitor might not work properly if DNS blackhole feature is enabled or if any named ACL is blocking the query sent to the loopback interface.*

To enable or disable the DNS health check monitor:

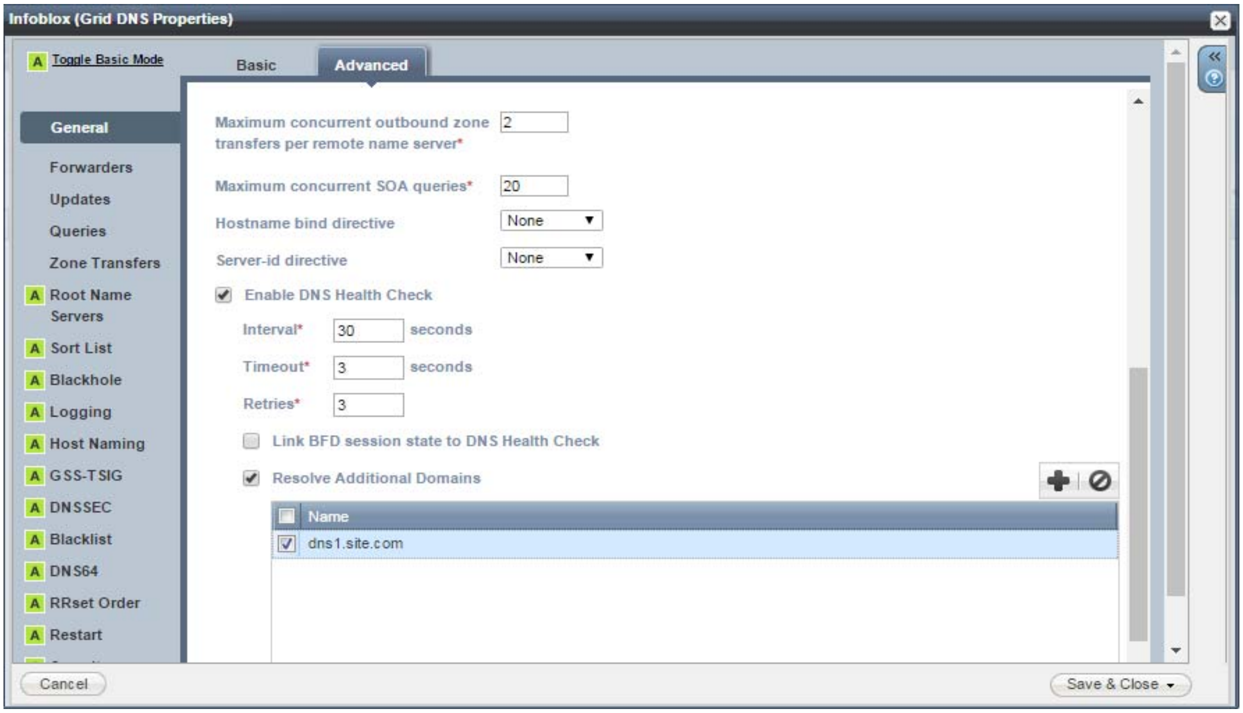
1. **Grid**: From the **Data Management** tab, select the **DNS** tab, and then select **Grid DNS Properties** from the Toolbar.

   **Member:** From the **Data Management** tab, select the **DNS** tab and click the **Members** tab -> *member* check box -> Edit icon.

   In the *Grid DNS Properties* or the *Member DNS Properties* editor, click **Toggle Advanced Mode** if the editor is in the basic mode.
2. Click the **Advanced** subtab of the **General** tab and then complete the following:
   - **Enable DNS Health Check:** This check box is deselected by default, meaning the DNS health check monitor is disabled. Select this check box to enable the DNS health check monitor and specify the following:
   - **Interval:** Enter the time interval in seconds. The interval value is measured from the end of the previous monitoring cycle. The default is 30 seconds. You can enter a value between 10 and 21600 seconds.
   - **Timeout:** Enter the timeout value in seconds. This is the time the appliance waits for a response to the query. The default is 3 seconds. You can enter a value between 1 and 10 seconds.
   - **Retries:** Enter the number of times the appliance tries to send the query after a failed attempt. The default is 3. You can enter a value between 1 and 10.
   - **Link BFD session state to DNS Health Check:** Select this check box to link the BFD session state with the DNS health check monitor.
   - **Resolve Additional Domains:** Click the Add icon and enter the domain name. The DNS health check monitor sends recursive queries to the local DNS server (BIND/Unbound) for the domain names listed in this table. You can add up to 16 domain names.
3. Save the configuration.

**Note:** You must carefully select the domain names for DNS health check monitor with BFD session in order to avoid unnecessary changes in downstream DNS traffic due to transient health check query failures. Setting a higher timeout or retry count might help in avoiding false alarms.

*Figure 1.5  Enabling DNS Health Check Monitor*



Maximum concurrent outbound zone transfers per remote name server* 2

Maximum concurrent SOA queries* 20

Hostname bind directive None

Server-id directive None

☑ Enable DNS Health Check

Interval* 30 seconds

Timeout* 3 seconds

Retries* 3

☐ Link BFD session state to DNS Health Check

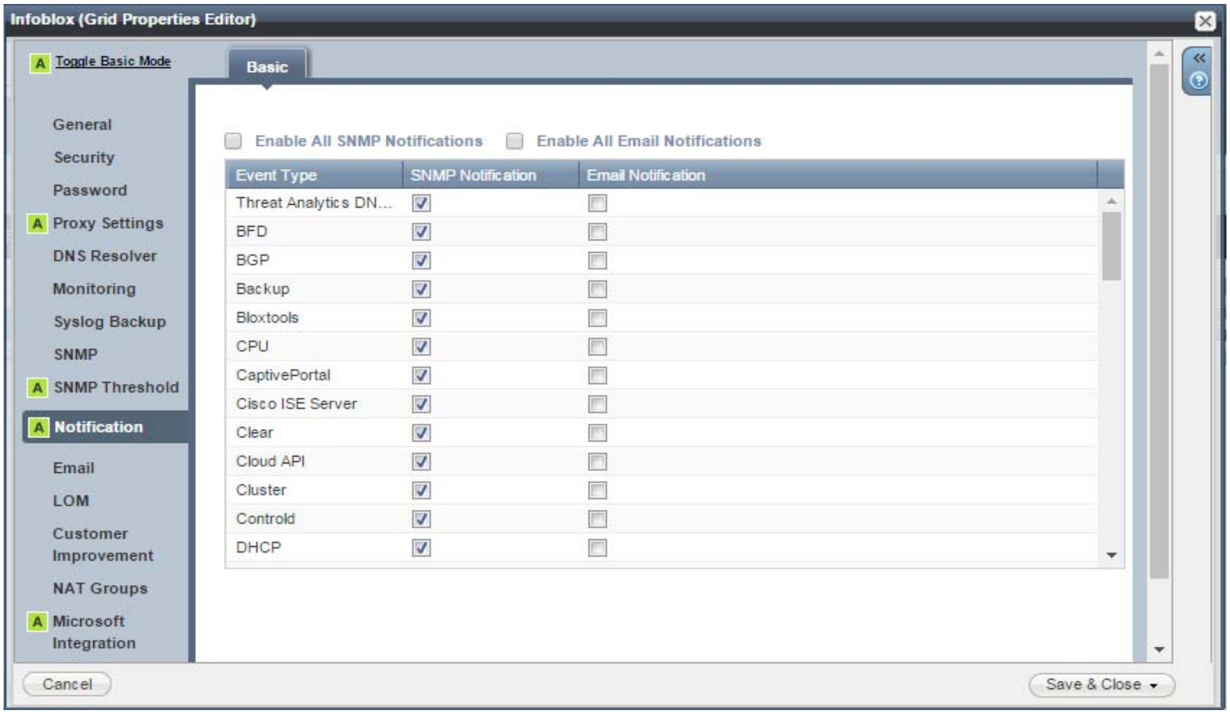
☑ Resolve Additional Domains

| ☐ | Name |
|---|---|
| ☑ | dns1.site.com |

## Monitoring with SNMP

Infoblox MIBs (IB-TRAP-MIB, IB-PLATFORMONE-MIB) are updated to include a notification for BFD process failure (ibBFDSoftwareFailure). By default, SNMP notifications are enabled for the BFD process failure event. You can enable or disable SNMP and email notifications for specific event types, by selecting the corresponding check boxes in the **Notification** tab of the *Grid Properties* or *Member Properties* editor.

*Figure 1.6 Grid Properties Editor*



□ Enable All SNMP Notifications □ Enable All Email Notifications

| Event Type | SNMP Notification | Email Notification |
|---|---|---|
| Threat Analytics DN... | ☑ | □ |
| BFD | ☑ | □ |
| BGP | ☑ | □ |
| Backup | ☑ | □ |
| Bloxtools | ☑ | □ |
| CPU | ☑ | □ |
| CaptivePortal | ☑ | □ |
| Cisco ISE Server | ☑ | □ |
| Clear | ☑ | □ |
| Cloud API | ☑ | □ |
| Cluster | ☑ | □ |
| Controld | ☑ | □ |
| DHCP | ☑ | □ |

In addition, BFD process can generate SNMP traps for session state changes according to the standard BFD MIBs described in *RFC 7330* and *RFC 7331*:

- .1.3.6.1.2.1.222.0.1 (bfdSessUp): This notification (aka trap) is sent when one of the neighbors changes the BFD-session state as ‘Up.’
- .1.3.6.1.2.1.222.0.2 (bfdSessDown): This notification (aka trap) is sent when one of the neighbors changes the BFD-session state as ‘Down’ or ‘AdminDown.’
- .1.3.6.1.2.1.222.1.2.1.13 (bfdSessDiag): The diagnostic code which can be one of the following:
  - noDiagnostic (0)
  - controlDetectionTimeExpired (1)
  - echoFunctionFailed (2)
  - neighborSignaledSessionDown (3)
  - forwardingPlaneReset (4)
  - pathDown (5)
  - concatenatedPathDown (6)
  - administrativelyDown (7)
  - reverseConcatenatedPathDown (8)
  - misConnectivityDefect (9)

Note that you must download the following MIBs to enable the trap-receiver to parse the notifications:

- BFD-STD-MIB
- BFD-TC-STD-MIB

- DIFFSERV-MIB
- DIFFSERV-DSCP-TC
- INTEGRATED-SERVICES-MIB
- IANA-BFD-TC-STD-MIB

## CLI Commands

### set bfd

You can use the `set bfd` command to set the BFD logging level. The default logging level is ‘informational’. Changing the BFD logging level might cause disruption in advertising due to `bfdd.conf` change.

Syntax

```
set bfd log [ debugging | informational | notifications | warnings | errors | critical
| alerts | emergencies ]
```

Example

```
Infoblox > set bfd log debugging
```

### show bfd details

The `show bfd details` command displays the detailed BFD session details.

Syntax

```
show bfd details
```

Example

```
Infoblox > show bfd details
OutAddr          NeighAddr         LD/RD Holdown(mult) State     Int
10.34.54.68      10.34.54.16        2/4    300(3)        Up    bond0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 100000, MinRxInt: 100000, Multiplier: 3
Received MinRxInt: 100000, Received Multiplier: 3
Holdown (hits): 300(0), Hello (hits): 100(1638)
Authentication:  None
             Last Sequence Number: Rx: 0, Tx: 1566182577
Rx Count: 1638
Tx Count: 1686
Last packet: Version: 1               - Diagnostic: 0
             State bit: Up            - Demand bit: 0
             Poll bit: 0              - Final bit: 0
             Multiplier: 3            - Length: 24
             My Discr: 2              - Your Discr: 4
             Min tx interval: 100000  - Min rx interval: 100000
             Min Echo interval: 100000
```