

SlashNext Agentless Phishing Protection Guide Infoblox DNS RPZ Feed

TABLE OF CONTENTS

1 INTRODUCTION	3
2 INFOBLOX CONFIGURATIONS	3
Step 1	3
Step 2	3
Step 3	4
Step 4	5
Step 5	6
Step 6	7
Step 7	7
Step 8	8
Step 8.1	8
Step 8.2	9
Step 8.3	9
Step 8.4	9
Step 8.5	10
Step 9	10
Step 10	11
Step 10.1	11
Step 10.2	12
Step 11	12

TABLE OF CONTENTS

Step 12 13

Step 13 13

Step 14 14

Step 15 14

Step 16 15

Step 17 15

Step 18 15

Step 19 16

Step 20 17

Step 21 18

Step 22 18

Step 23 18

Step 24 19

3 | VERIFICATION OF RPZ WORKING 19

 Step 1 19

 Step 2 19

 Step 3 20

1 | INTRODUCTION

A response policy zone (RPZ) is a mechanism to introduce a customized policy in Domain Name System servers, so that recursive resolvers return possibly modified results. By modifying a result, access to the corresponding host can be blocked. Usage of an RPZ is based on DNS data feeds, known as zone transfer, from an RPZ provider to the deploying server.

Customer shall receive a XXXX-XXXX-XX.tsig.key file from SlashNext which is to be used in Infoblox Configurations section to enable the reception of RPZ feed from SlashNext cloud

Note

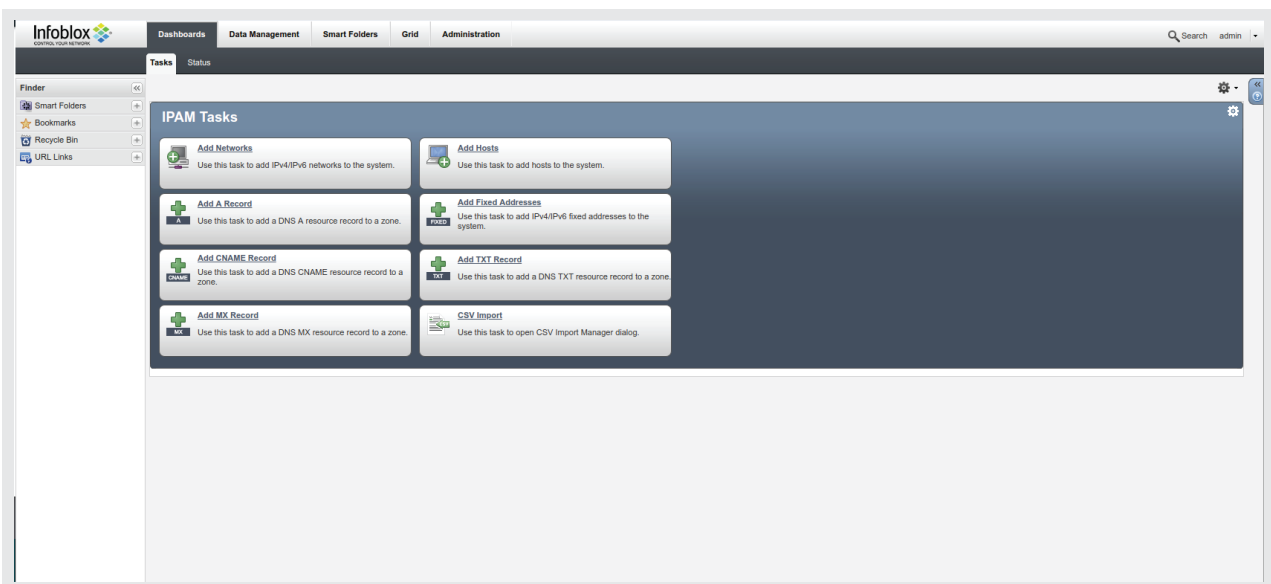
This guide is made using Infoblox Version: 8.2.4-366880, some menu structures and contents with Infoblox might be updated if you have a different version.

2 | INFOBLOX CONFIGURATIONS

Please follow the instructions below to enable the reception of the SlashNext RPZ feed on a Infoblox DNS server.

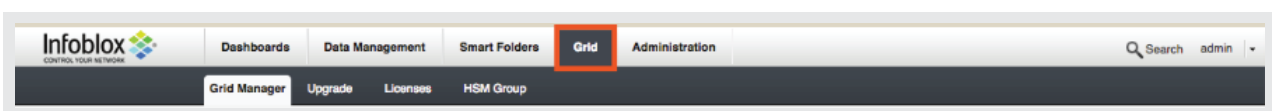
2.1 | STEP 1

Login to Infoblox



2.2 | STEP 2

Verify if the “DNSone with Grid (DNS, DHCP, Grid)” license is installed on Infoblox . If “DNSone with Grid” license is already installed then Grid tab will be shown adjacent to Administration tab.



If “DNSone with Grid” license is not installed then please access the CLI of Infoblox and execute the following command:

Command

```
Infoblox > set temp_license
```

Please select the option "DNSone with Grid (DNS,DHCP,Grid) ", when prompted press "y" and enter the key to confirm

```

Infoblox > set temp_license

 1. DNSone (DNS, DHCP)
 2. DNSone with Grid (DNS, DHCP, Grid)
 3. Network Services for Voice (DHCP, Grid)
 4. Add DNS Server license
 5. Add DHCP Server license
 6. Add Grid license
 7. Add Microsoft management license
 8. Add vNIOS license
 9. Add Multi-Grid Management license
10. Add Query Redirection license
11. Add Load Balancer license
12. Add Response Policy Zones license
13. Add FireEye license
14. Add DNS Traffic Control license
15. Add Cloud Network Automation license
16. Add Security Ecosystem license
17. Add Threat Analytics license

Select license (1-17) or q to quit: 2

This action will generate a temporary 60-day DNSone with Grid license.
Are you sure you want to do this? (y or n): y
DNS temporary license installed.
DHCP temporary license installed.
Grid temporary license installed.

Temporary license is installed.

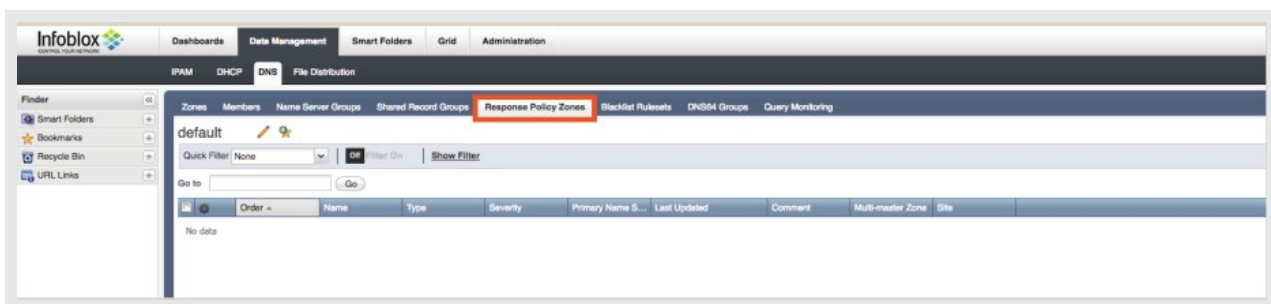
The UI needs to be restarted in order to reflect license changes.
Restart UI now, this will log out all UI users? (y or n):y

Are you sure you want to do this? (y or n): y
UI restarted.
Infoblox >

```

2.3 | STEP 3

Verify that the "Response Policy Zone" license is installed on Infoblox . Navigate to the Data Management DNS tab. If the "Response Policy Zone license" is already installed then it will appear under the DNS tab.



If "Response Policy Zone license" is not installed then access the CLI of Infoblox and execute the following command:

Command

```
Infoblox > set temp_license
```

Select the option "Add Response Policy Zones license", when prompted press "y" and enter key to confirm

```

Infoblox > set temp_license

 1. DNSone (DNS, DHCP)
 2. DNSone with Grid (DNS, DHCP, Grid)
 3. Network Services for Voice (DHCP, Grid)
 4. Add DNS Server license
 5. Add DHCP Server license
 6. Add Grid license
 7. Add Microsoft management license
 8. Add vNIOS license
 9. Add Multi-Grid Management license
10. Add Query Redirection license
11. Add Load Balancer license
12. Add Response Policy Zones license
13. Add FireEye license
14. Add DNS Traffic Control license
15. Add Cloud Network Automation license
16. Add Security Ecosystem license
17. Add Threat Analytics license

Select license (1-17) or q to quit: 12

This action will generate a temporary 60-day Response Policy Zones license.
Are you sure you want to do this? (y or n): y
Response Policy Zones temporary license installed.

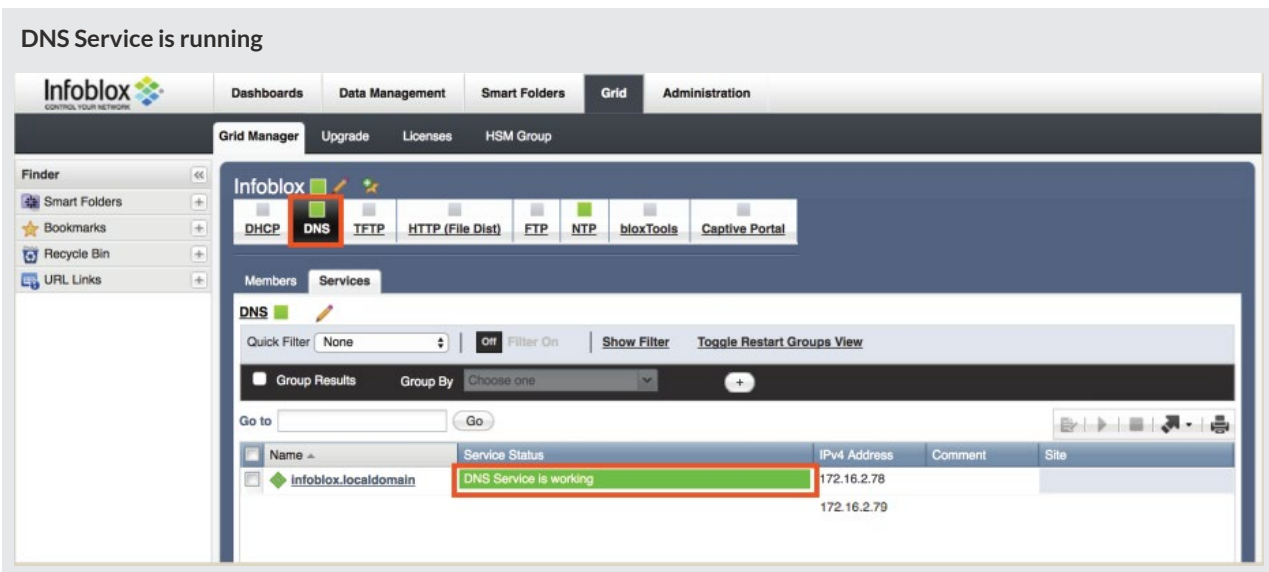
Temporary license is installed.

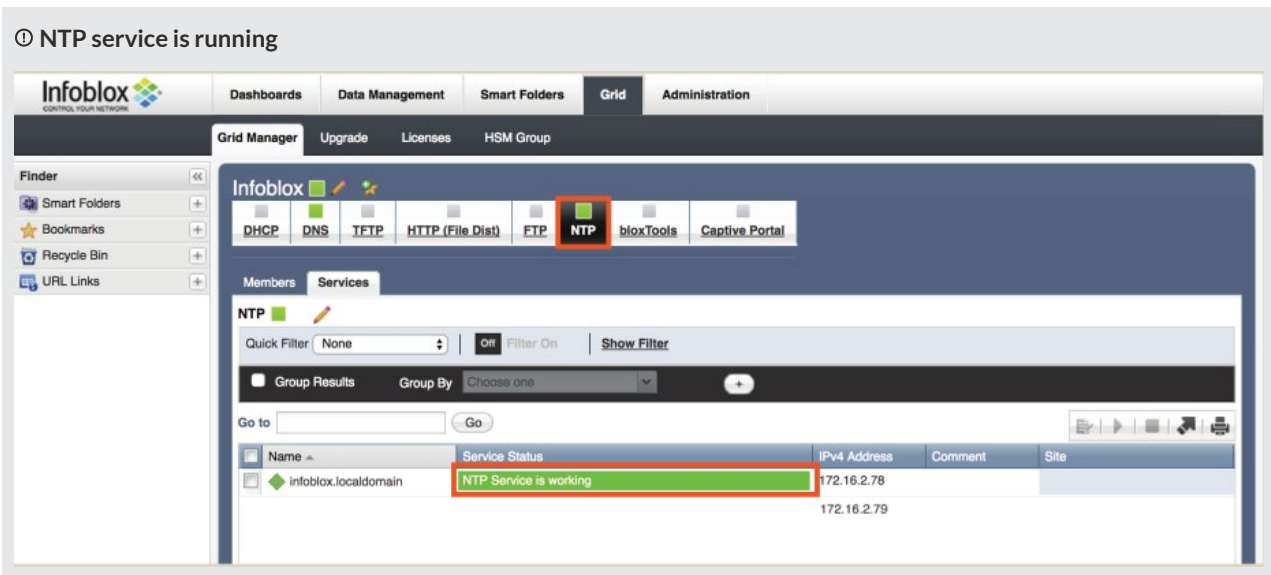
The UI needs to be restarted in order to reflect license changes.
Restart UI now, this will log out all UI users? (y or n):y

Are you sure you want to do this? (y or n): y
UI restarted.
Infoblox >
    
```

2.4 | STEP 4

Navigate to Grid → Grid Manager tab, verify that the DNS and NTP services are both running.

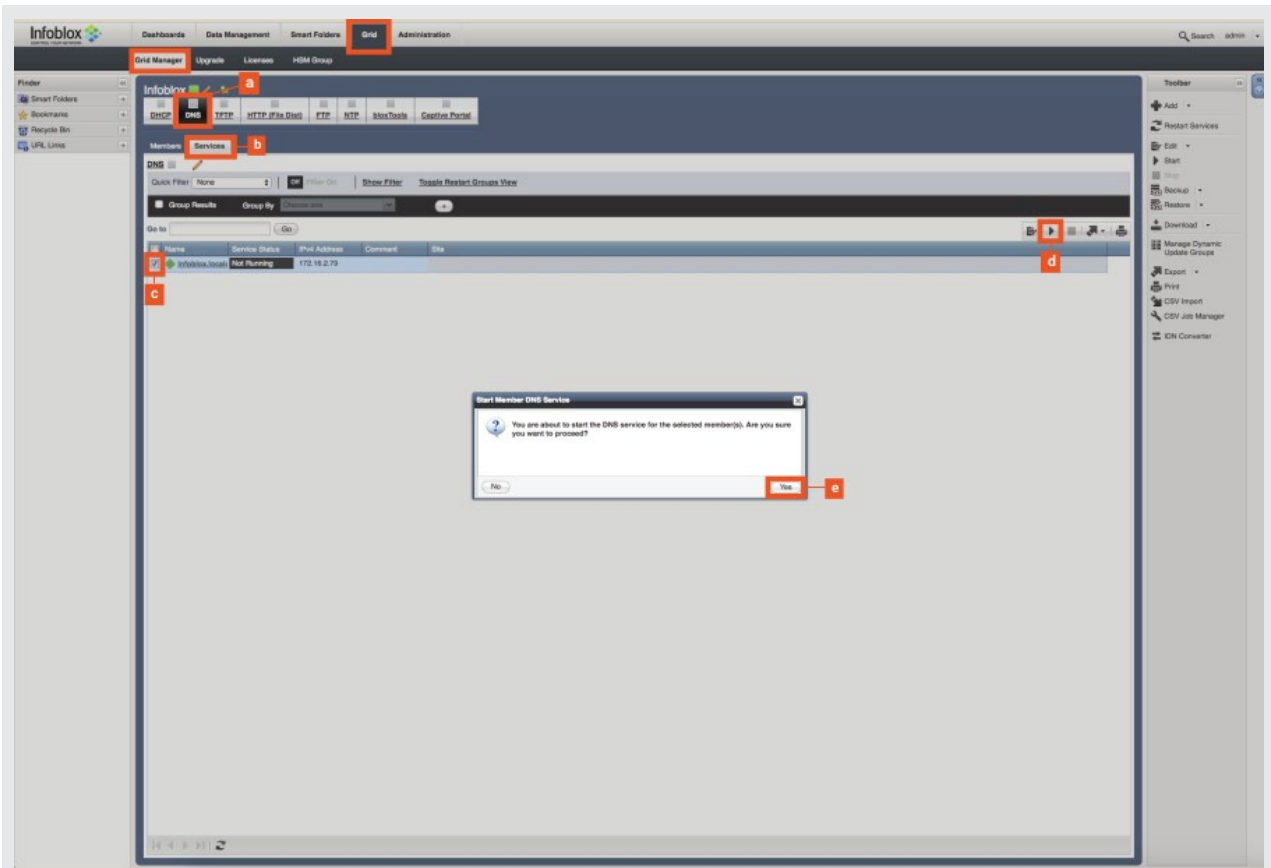




2.5 | STEP 5

If the DNS Service is not running, go to Grid → Grid Manager tab

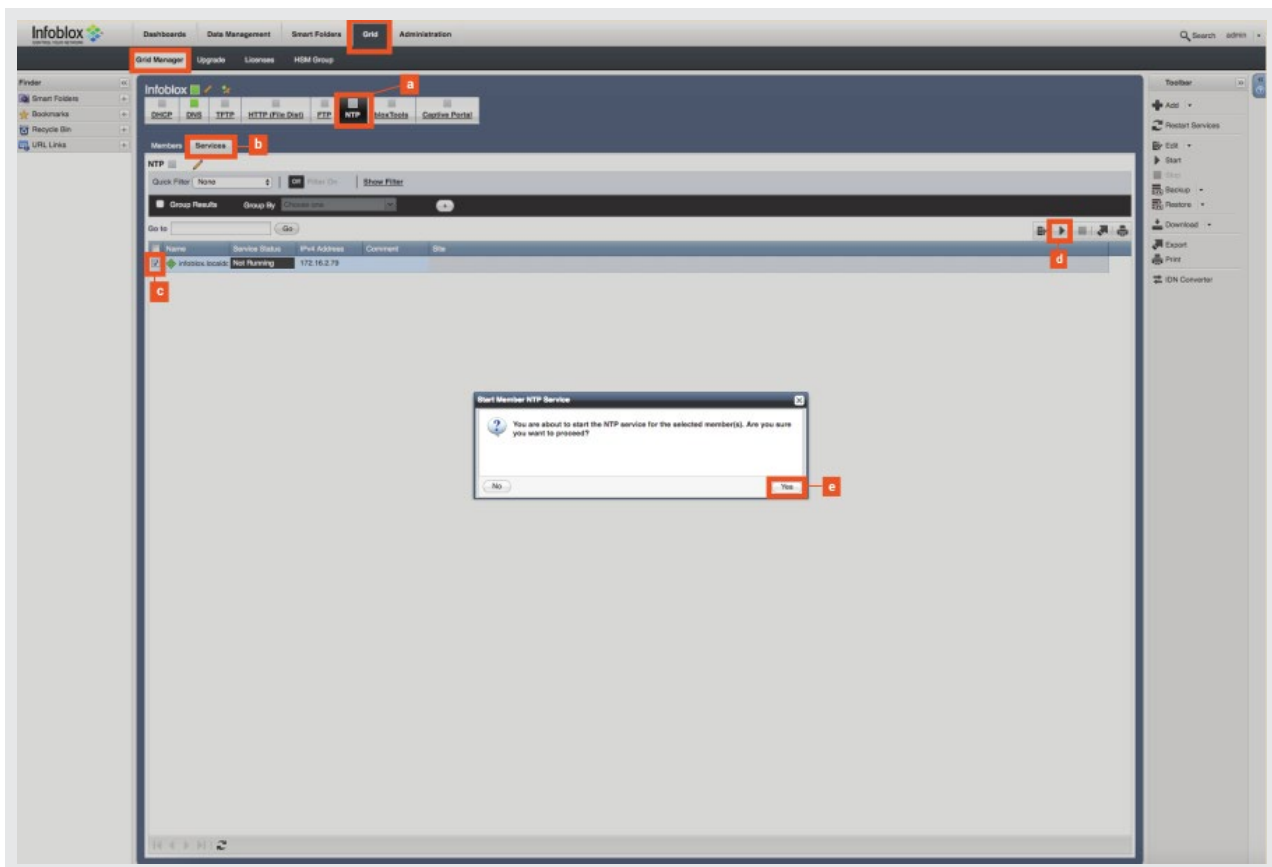
- a. Select DNS
- b. Go to Services tab
- c. Mark checkbox for DNS Service
- d. Click on Start button
- e. Click “yes” to confirmation message
- f. Please refresh the page in order to get the latest status



2.6 | STEP 6

If the NTP Service is not running, go to **Grid** → **Grid Manager** tab

- Select NTP
- Go to Services tab
- Mark checkbox for NTP Service
- Click on Start button
- Click “yes” to confirmation message
- Please refresh the page in order to get the latest status.

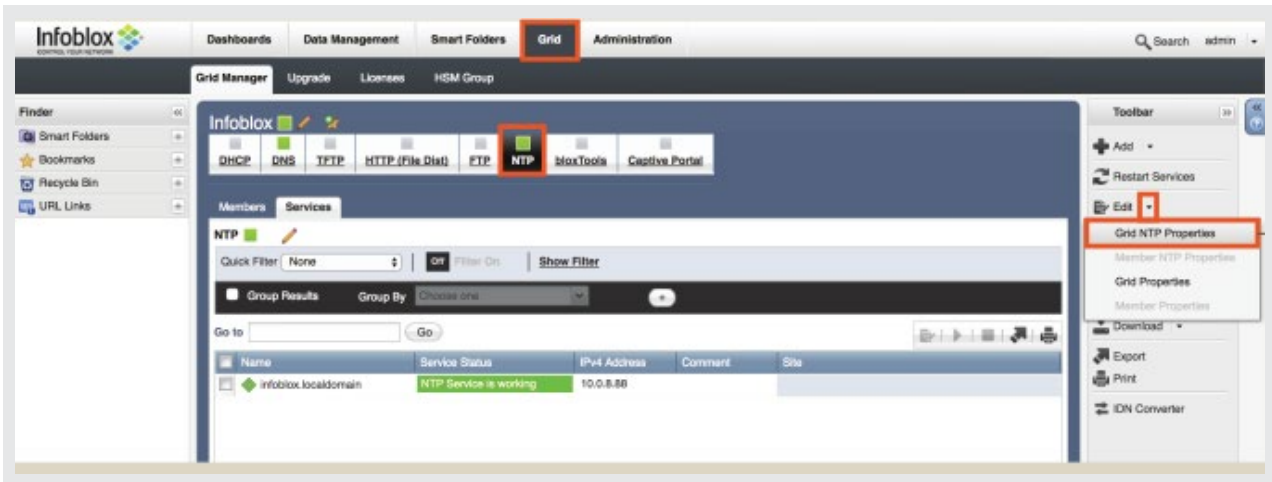


2.7 | STEP 7

If you want to sync with the NTP Server, please then follow Step 8 otherwise proceed to Step 10.

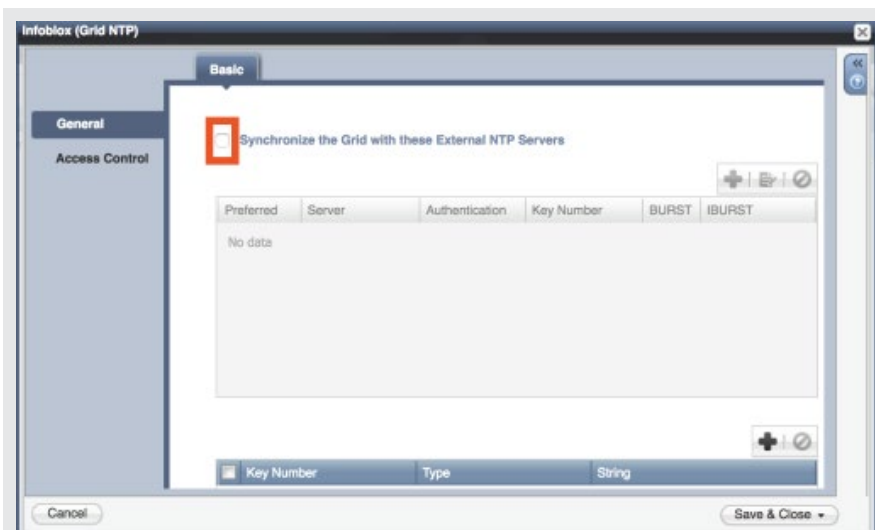
2.8 | STEP 8

In Infoblox navigate to “Grid” tab, select “NTP”, then from right side tool bar click on the “Edit” drop-down and select “Grid NTP Properties”



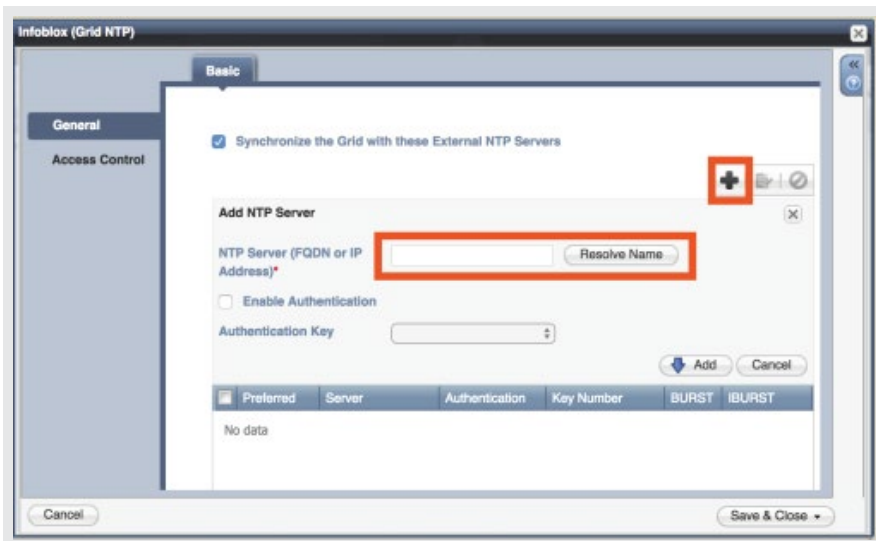
2.8.1 | STEP 8.1

From the “General” tab, please mark the check box “Synchronize the Grid with these External NTP Servers”



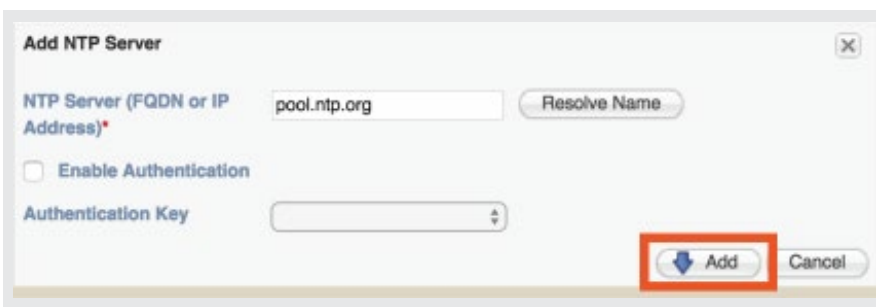
2.8.2 | STEP 8.2

Click on the Add icon (+) and please Enter the NTP Server information (FQDN or IP Address)



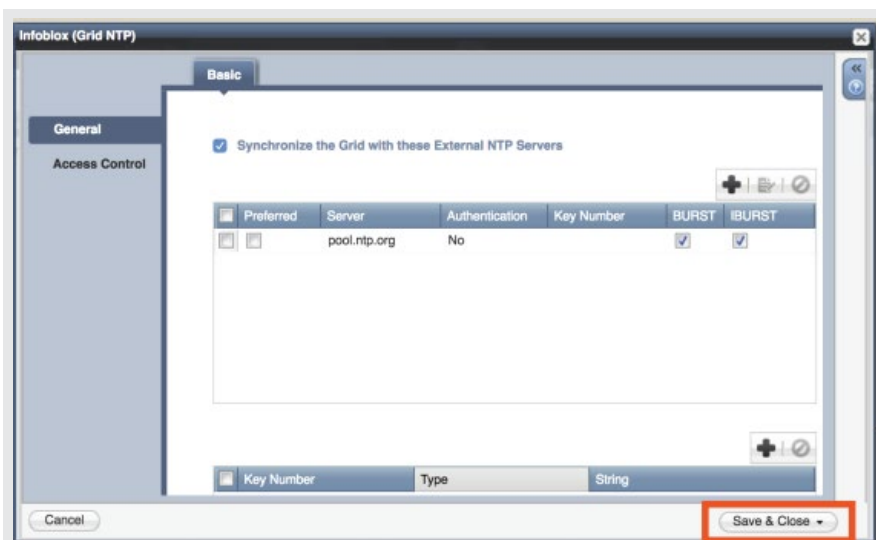
2.8.3 | STEP 8.3

Click on the Add button



2.8.4 | STEP 8.4

“Save & Close” configuration



2.8.5 | STEP 8.5

Access the CLI of Infoblox & type command “reboot”. Press “y” when prompted

```
[Infoblox > reboot
[      REBOOT THE SYSTEM? (y or n): y

SYSTEM REBOOTING!

SYSTEM REBOOTING!
```

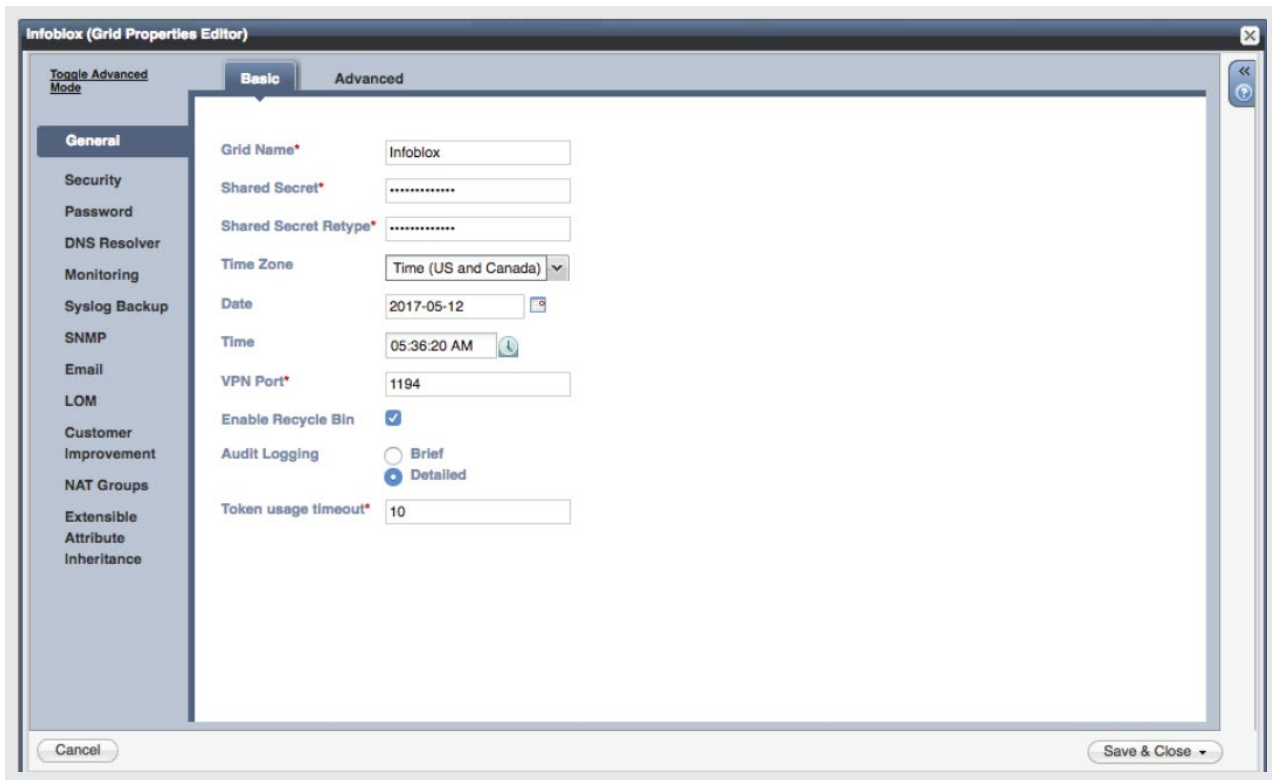
2.9 | STEP 9

The time zones for both the RPZ Feed Server and Infoblox should be synced in order to transfer the zones.

- From Grid tab, select Grid Manager tab and then click Edit from Grid Properties drop-down button in the Grid Manager Toolbar.



b. From Grid Properties Editor, check the timezone and time of Infoblox



The screenshot shows the 'Infoblox (Grid Properties Editor)' window with the 'Basic' tab selected. The left sidebar contains a navigation menu with options: General, Security, Password, DNS Resolver, Monitoring, Syslog Backup, SNMP, Email, LOM, Customer Improvement, NAT Groups, Extensible Attribute, and Inheritance. The main area displays the following configuration fields:

Grid Name*	Infoblox
Shared Secret*
Shared Secret Retype*
Time Zone	Time (US and Canada) ▼
Date	2017-05-12
Time	05:36:20 AM
VPN Port*	1194
Enable Recycle Bin	<input checked="" type="checkbox"/>
Audit Logging	<input type="radio"/> Brief <input checked="" type="radio"/> Detailed
Token usage timeout*	10

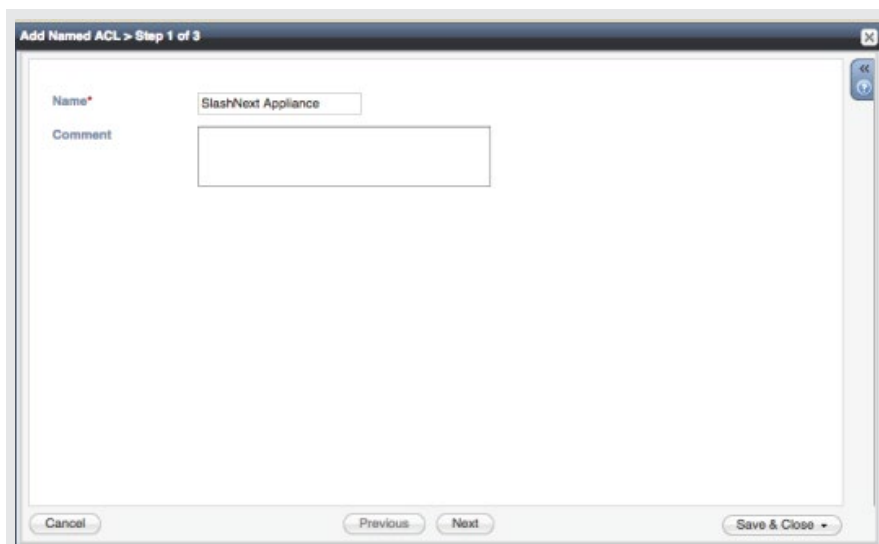
Buttons at the bottom include 'Cancel', 'Save & Close', and a help icon.

2.10 | STEP 10

From the Infoblox Grid Manager, go to the Administration tab and select Named ACL. Click on the Add icon (+) to configure RPZ Feed Server IP as follows:

2.10.1 | STEP 10.1

Add ACL Name and click "Next"



The screenshot shows the 'Add Named ACL > Step 1 of 3' dialog box. It contains the following fields:

Name*	SlashNext Appliance
Comment	

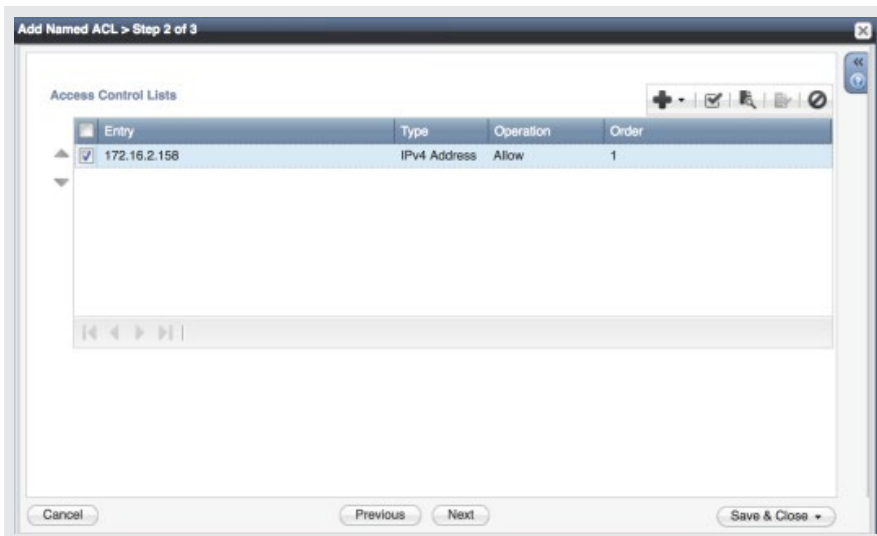
Buttons at the bottom include 'Cancel', 'Previous', 'Next', and 'Save & Close'.

Note

You can change the **Name** field as per your liking.

2.10.2 | STEP 10.2

Click on “Add icon (+)”. Click in the entry field and enter “RPZ Feed Server IP”.



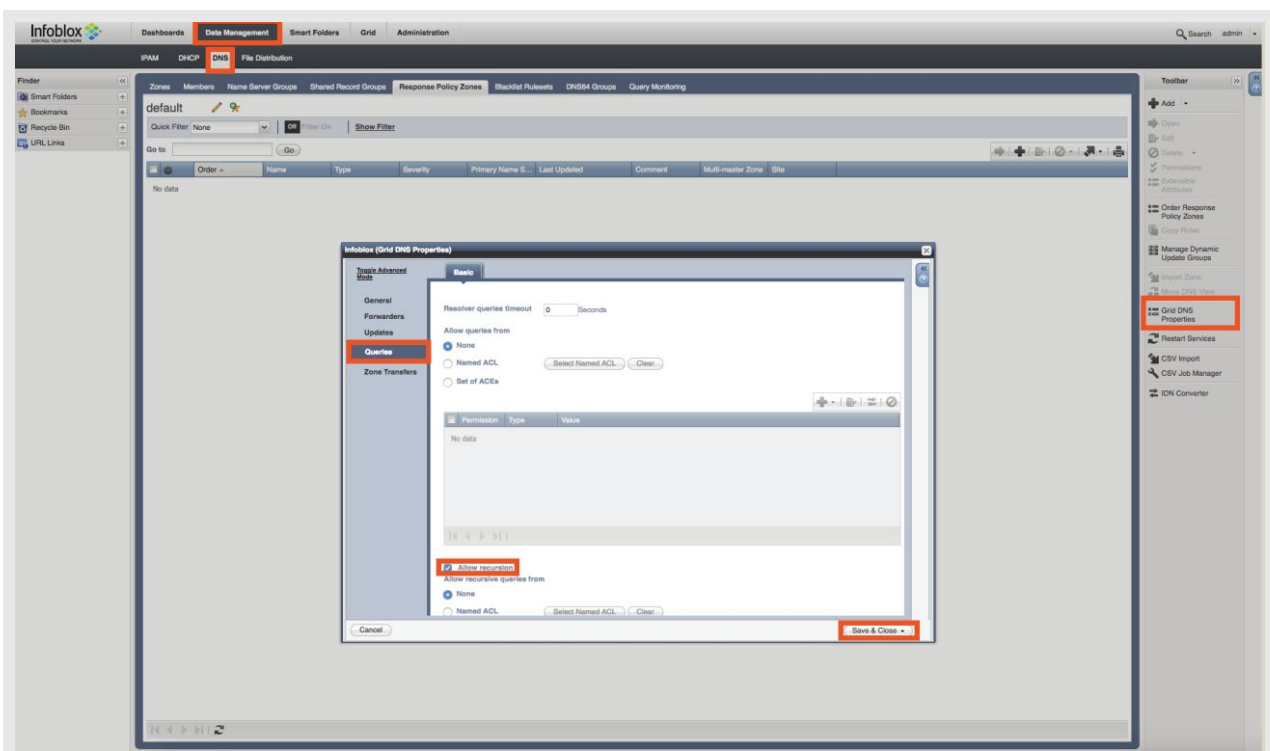
Note

Replace 172.16.2.158 with RPZ FEED SERVER IP which shall be provided by SlashNext.

After configuration Save and Close “Add Named ACL” window.

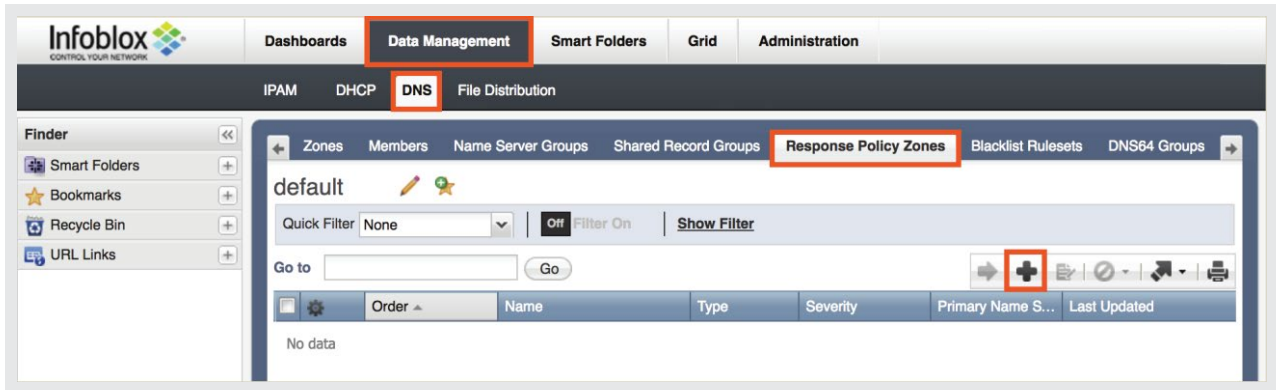
2.11 | STEP 11

From the Data Management tab, navigate to DNS → Response Policy Zone tab. From the right toolbar, click on “Grid DNS Properties”, click on “Queries” from left side menu list and mark check-box “Allow recursion”



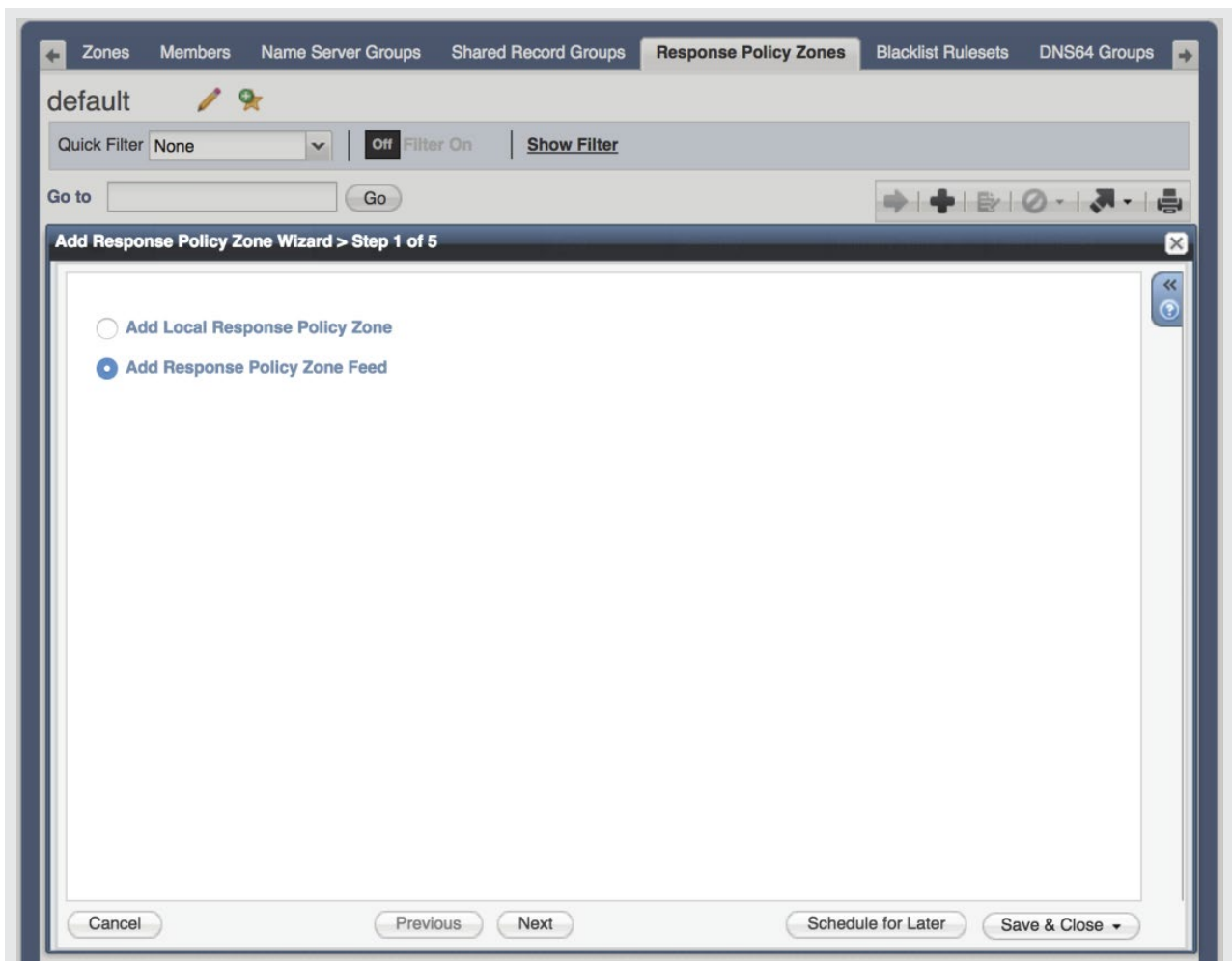
2.12 | STEP 12

From the Data Management tab, please navigate to DNS Response Policy Zone tab. Click the Add icon (+) and the Add Response Policy Zone Wizard will be displayed.



2.13 | STEP 13

Select the radio button “Add Response Policy Zone Feed” and click Next



2.14 | STEP 14

In the Add Response Policy Zone Wizard, specify the following

Attributes

- Name:** Enter the name "XXXX-XXXX-XX.snxblocking.rpz". Here XXXX-XXXX-XX prefix is the TSIG key name and shall be provided by SlashNext.
- Policy Override:** Select a value from the drop-down list.
- Severity:** Select the threat severity level for the RPZ zone. The threat severity level selected here determines the severity for the RPZ rule. Select Critical, Major, Warning, or Informational. The default threat severity level is Major.

Add Response Policy Zone Wizard > Step 2 of 5

Name*

Policy Override

Severity

Comment

Disable

Lock

Cancel Previous Next Schedule for Later Save & Close

2.15 | STEP 15

Click Next

Add Response Policy Zone Wizard > Step 3 of 5

None

Use this Name Server Group

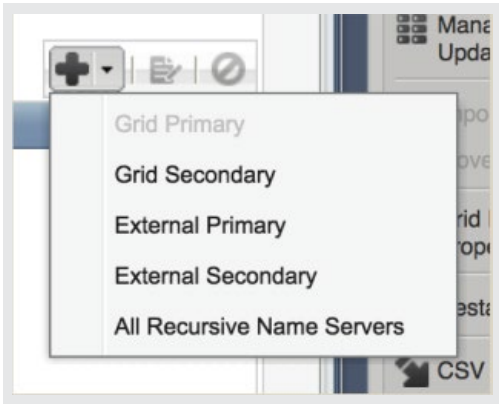
Use this set of name servers

Name	IPv4 Address	IPv6 Address	Type	TSIG
No data				

Cancel Previous Next Schedule for Later Save & Close

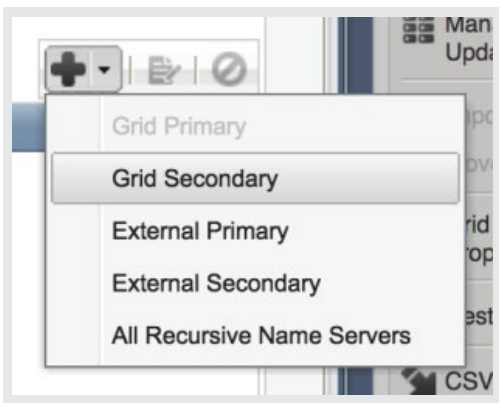
2.16 | STEP 16

Click on the drop down adjacent to add icon (+)



2.17 | STEP 17

Click on "Grid Secondary"



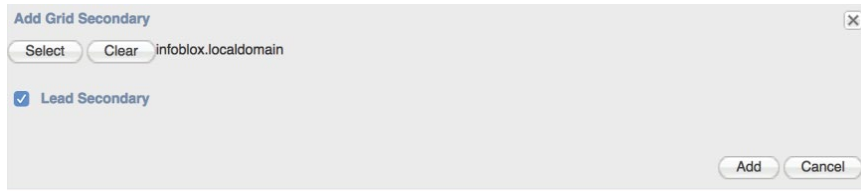
2.18 | STEP 18

Click on the "Select" button



Note

You can associate a lead secondary with an RPZ feed if you have more than one secondary servers by selecting check-box “Lead Secondary”



Add Grid Secondary

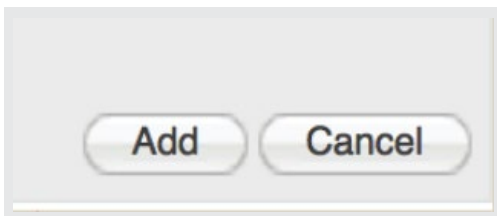
Select Clear infoblox.localdomain

Lead Secondary

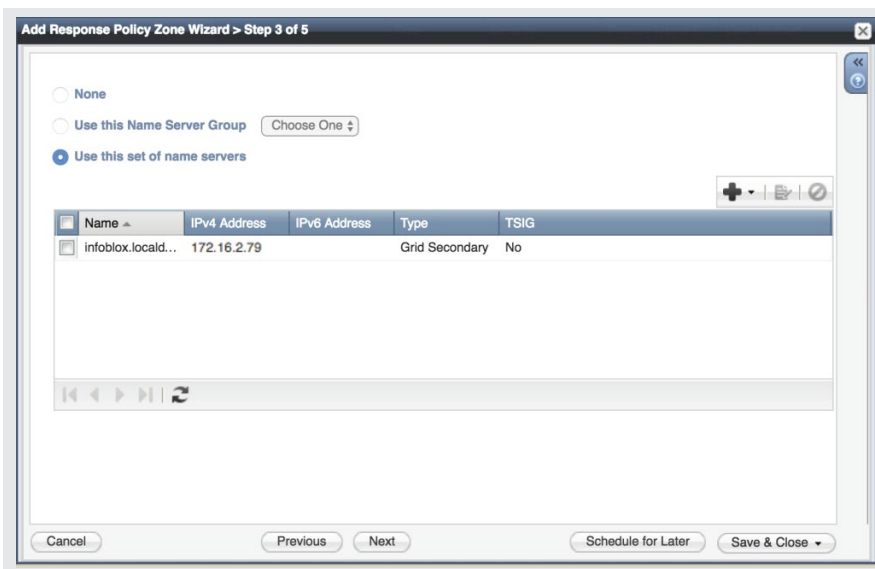
Add Cancel

2.19 | STEP 19

Click on the “Add” button.



Now Grid Secondary has been added.



Add Response Policy Zone Wizard > Step 3 of 5

None

Use this Name Server Group Choose One

Use this set of name servers

Name	IPv4 Address	IPv6 Address	Type	Tsig
infoblox.locald...	172.16.2.79		Grid Secondary	No

Cancel Previous Next Schedule for Later Save & Close

2.20 | STEP 20

Click on the drop down adjacent to add icon (+) and select “External Primary” option. For external primary servers, specify the following:

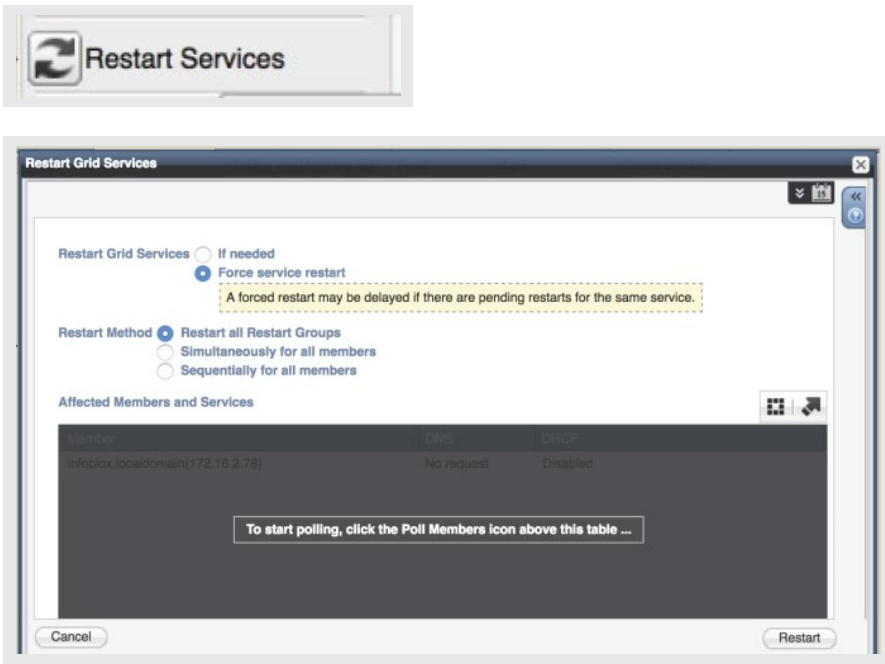
Note

- Name:** Enter external primary server name "SlashNext RPZ Feed Server".
- Address:** Enter the SlashNext RPZ Feed Server IP.
- Use TSIG:** Select the check box to specify TSIG settings.
- Key Name:** Enter the TSIG Key Name provided by SlashNext with format XXXX-XXXX-XX
- Key Algorithm:** Select hmac-md5
- Key Data:** Enter the TSIG string provided by SlashNext and click on Add button.

Click **Add** and then **Save & Close**.

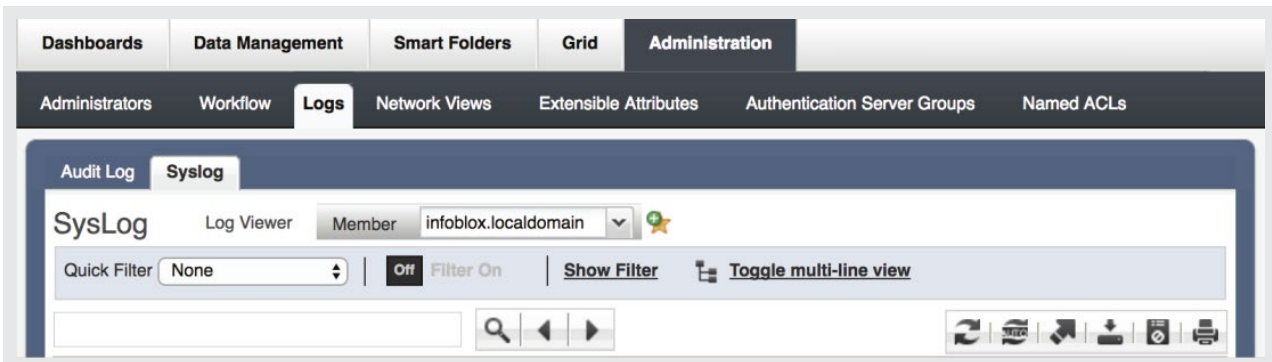
2.21 | STEP 21

Click **Restart** if it appears at top of the screen otherwise restart it from Toolbar at right side



2.22 | STEP 22

To verify that the zone transfer is working the way it should, navigate to the Administration **Logs** → **Syslog** and then select the member.



2.23 | STEP 23

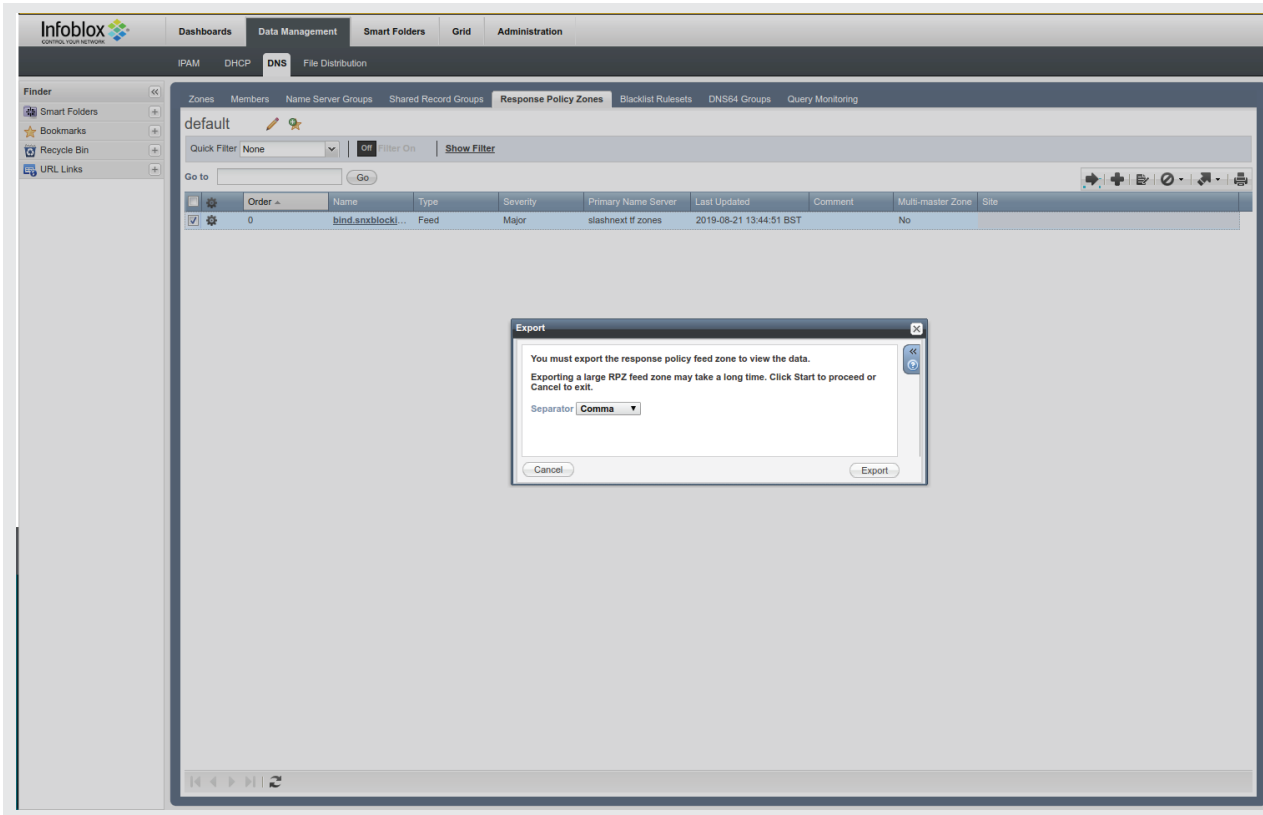
Conduct a search on the IP address of the feed server. You should see a similar message:

log message

transfer of 'XXXX-XXXX-XX.snxblocking.rpz/IN' from x.x.x.x#53: Transfer completed: 1 messages, 21 record, 745 bytes, 0.001 secs (745000 bytes/sec)

2.24 | STEP 24

To test, navigate back to Data Management → DNS → Response Policy Zones.



Click on the feed entry "Name" to download the contents to a .CSV file`

3 | VERIFICATION OF RPZ WORKING

For this you will need a machine which is using above configured Infoblox as DNS server. If you don't know if an machine is using above Infoblox as DNS, please consult your network administrator. If you have a ubuntu machine with access to above Infoblox, you can configure it using following steps.

3.1 | STEP 1

Open the file `/etc/resolv.conf` and append the following line if its not already there.

```
nameserver INFOBLOX_DNS_IP
```

3.2 | STEP 2

Select a domain from the .CSV file downloaded in Step 24 of Infoblox Configuration section and copy it so that it can be used in the next step.

3.3 | STEP 3

Use following command on your ubuntu machine to confirm if RPZ is properly redirecting to SlashNext Sinkhole aka Walled Garden.

```
nslookup SELECTED_DOMAIN
```

Example

```
nslookup 1929641ee50c450adb5c9e06066bbd02.336727.xyz
```

```
Server: INFOBLOX_DNS_IP  
Address: INFOBLOX_DNS_IP#53
```

```
Non-authoritative answer:  
Name: 1929641ee50c450adb5c9e06066bbd02.336727.xyz  
Address: SLASHNEXT_SINKHOLE_IP
```

Where **SLASHNEXT_SINKHOLE_IP**=69.25.58.50 or will be specified by SlashNext.