Infoblox
NEXT LEVEL NETWORKING

Deployment Guide

DNS Firewall Deployment Guide

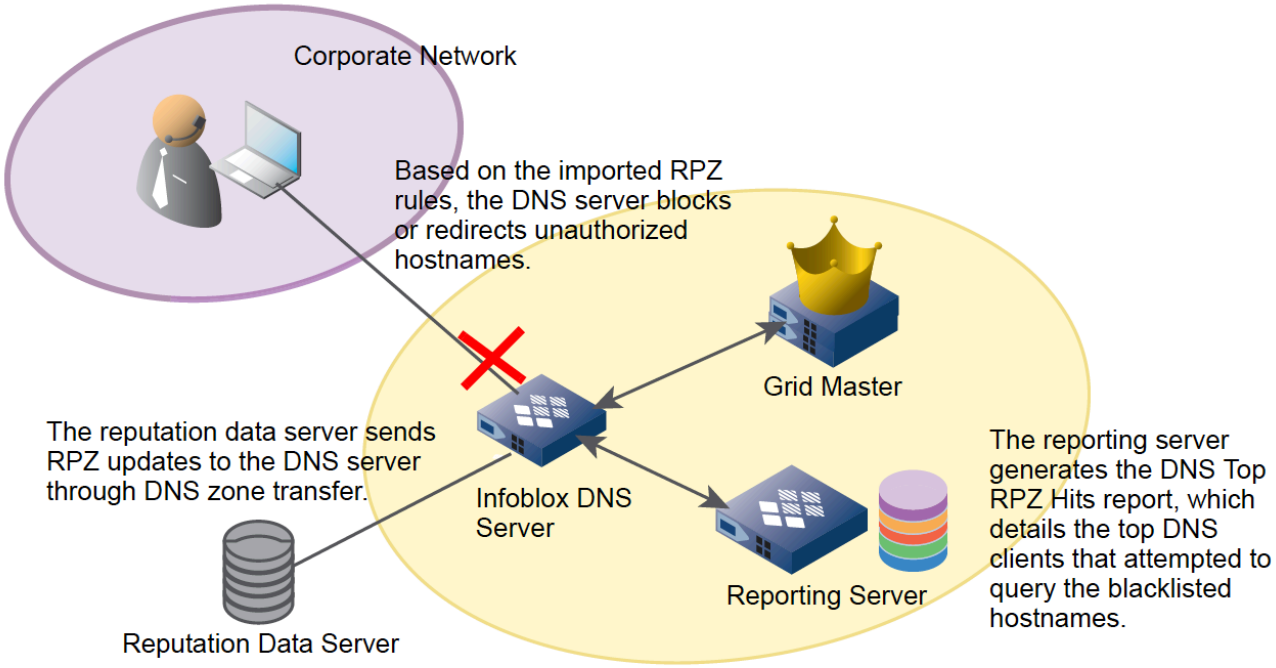
Table of Contents

Introduction

Infoblox DNS Firewall employs DNS RPZs (Response Policy Zones), a technology developed by ISC (Internet System Consortium) for allowing reputable sources to dynamically communicate domain name reputation so you can implement policy controls for DNS lookups.

This deployment guide shows how to deploy DNS Firewall.

Data Flow for DNS Firewall



There are five steps to a malware attack*:

1. Entry – downloading of the malware code from either an infected website or email with an attachment or link that hijacks the user's browser.
2. Distribution – Initial malware redirects the user's browser to a select malicious site.
3. Exploit – an exploit kit now probes the computer for vulnerabilities.
4. Infection – Malicious payload is downloaded and infects the user's system with malware.
5. Execution – The malware calls home with sensitive data or attempts to extort the user for money (ransomeware).

*source: Sophos.com

Step 5 is where DNS firewall gets involved. The malware performs a command and control step to steal sensitive data. In order to talk to the command and control server, the malware makes a call to the DNS to resolve the name of the command and control server. With DNS firewall and its local reputation entries and/or reputation entries from a reputation feed, the DNS resolution can be blocked or redirected to a walled garden website. With Infoblox, indications of a reputation hit can be seen in the syslog (i.e. CEF messages) or DNS RPZ report from the reporting server. At this point, the workstation can be tracked down via IP address, username, and switchport to clean off the malware.

Requirements

The following items are required for DNS Firewall:

- RPZ license per recursive DNS member that will have DNS Firewall enabled.
- Access to the Infoblox Cloud Service Platform RPZ management portal (https://csp.infoblox.com) or other reputation feeds like Spamhaus.
- Infoblox NIOS 8.0 or later is recommended.

Types of RPZs

- Local RPZ–A local RPZ is a zone that allows administrators to define multiple response policies locally. Query responses sent are based on the defined rules.
- RPZ Feed–An RPZ feed receives response policies from external sources. DNS clients receive responses based on the imported rules from a reputable source.
- FireEye integrated RPZ–By integrating the NIOS appliance with the FireEye appliance, you can detect malware and APTs and take necessary actions to mitigate those threats by importing updates from FireEye appliance into a FireEye RPZ.

Best Practices

- When you enable Infoblox DNS Firewall, DNS performance for all queries, recursive or authoritative, will be affected.
- If you have multiple DNS servers in a Grid, ensure that you configure RPZs on the recursive server that is closest to your DNS clients. If you configure RPZs on second level DNS caching servers, you will not be able to identify the DNS clients because only the IP addresses of the forwarding name servers can be identified.
- Infoblox recommends that you preview your RPZ rules to ensure ruleset integrity and to avoid unexpected results. You can preview your rules by selecting Log Only (Disabled) when you configure Policy Override for an RPZ, RPZ feed, or FireEye integrated RPZ.
- The appliance logs all matching and disabled rules for all queries in the syslog. You can view the syslog to ensure that the rules are set up correctly before they take effect. Ensure that you enable rpz in the Logging Category of Grid DNS Properties editor to log these events.
- You can use the standard TSIG mechanism to ensure that feed zones come from the correct servers. Grid members can function either as a primary or secondary server for the RPZ. As with hosting any zone as a secondary, please ensure that the appliance is sized properly to hold the zone contents in memory.
- You can only export or import the RPZ local zones using the CSV export or import feature, but you cannot import or export FireEye zones using this feature.
- Note that the NIOS blacklist and NXDOMAIN features take precedence over RPZs.
- In order to leverage DNS notify messages to trigger zone transfer of the feed zone, port 53 incoming on the lead secondary must be open to receive such messages (TCP and UDP). If not, the zone will refresh based on the refresh setting in the SOA.
- The name of the zone, which is assigned to an RPZ member, must not exceed 256 characters. The name can be a combination of alphanumeric characters. When the name exceeds this limit, respective zone fails to load.

Best Practices for FireEye Integrated RPZs

Before you configure a FireEye integrated RPZ, consider the following:

- FireEye integrated RPZs inherit default values from local RPZs. You can create, edit and delete rules using the Infoblox GUI, API, and RESTful API.
- To avoid false positives, Infoblox recommends that you create a whitelist of allowed zones using a local RPZ that is sorted above the FireEye RPZ and add your own domain to the whitelist RPZ. For example, you can add your company domain name, such as corp100.com. This list must contain popular domains, such as Alexa 250, and other desired domains.

- Note that there will be an impact on the storage capacity when you create a new FireEye alert and map it with an RPZ rule. The processing of alerts will consume a few CPU cycles, which will have some impact on the system.
- You must properly configure the settings on a FireEye appliance. NIOS supports only Per Event delivery mechanism and JSON Normal message format. To ensure that the NIOS appliance process alerts properly, configure the FireEye appliance accordingly.
- You cannot add a FireEye integrated RPZ during a scheduled full upgrade. However, updates to the CNAME record are processed during a full upgrade. NIOS updates CNAME records in the database to store information that is specific to FireEye alerts.
- The rules created due to insertion of alerts will be visible through the FireEye RPZ viewer. Infoblox recommends that you do not modify any internal objects. For more information, see Viewing RPZs on page 1690.
- Note that SSL certificate validation is not supported.
- You must verify the following after you configure the FireEye and NIOS appliances:
    - The URL configured on the FireEye appliance matches the URL in the FireEye integrated RPZ on NIOS.
    - Verify the username and password for FireEye admin on the FireEye appliance.
    - Ensure that the settings are properly configured on the FireEye appliance.
    - Verify the state of the FireEye appliance.
    - Do note that all settings are case sensitive.
- Note that the frequency of alerts received from FireEye can be minimal. A very small number of alerts are generated on a weekly basis. For example, the FireEye appliance may generate only tens of alerts per day.

Deployment Summary

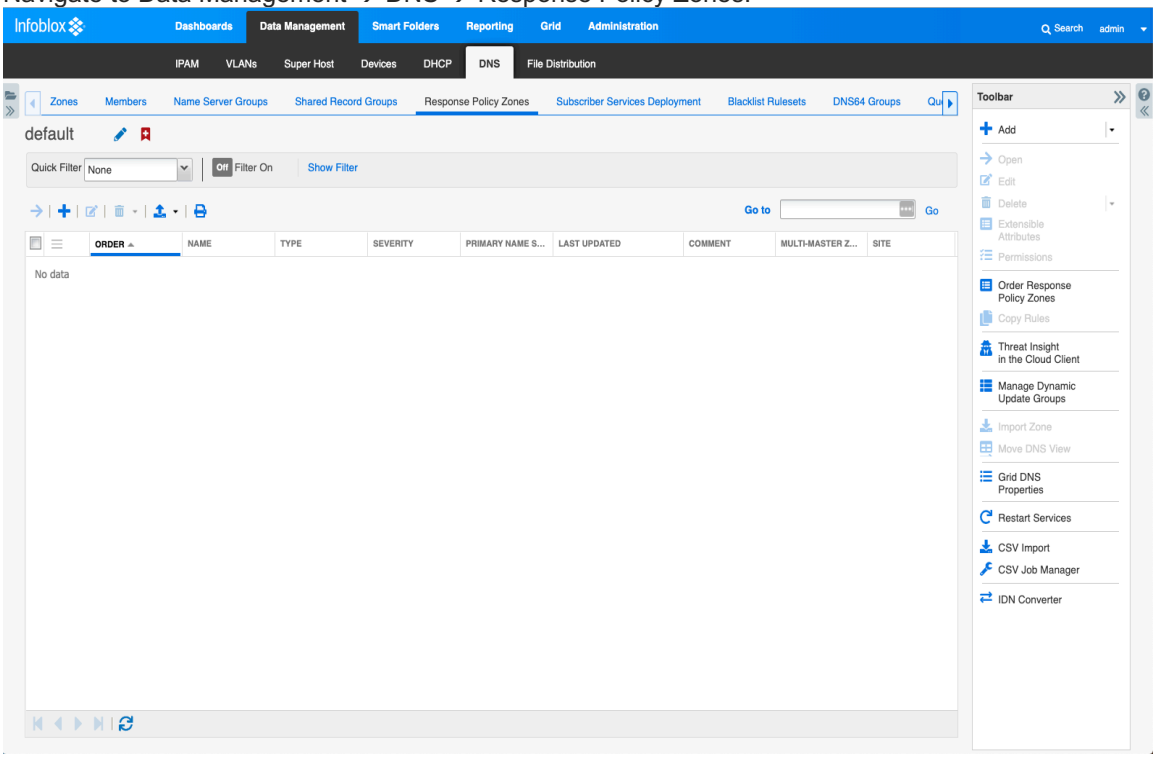
- Install a valid RPZ license. Refer to the Infoblox NIOS administrators guide for more information.
- Enable recursion for your DNS view in which you want to deploy RPZs.
- Configure RPZ logging to ensure all matching and disabled rules for all queries are logged in the syslog. Refer to the Infoblox NIOS administrator guide for more information.
- Configure RPZs.

Deployment Instructions

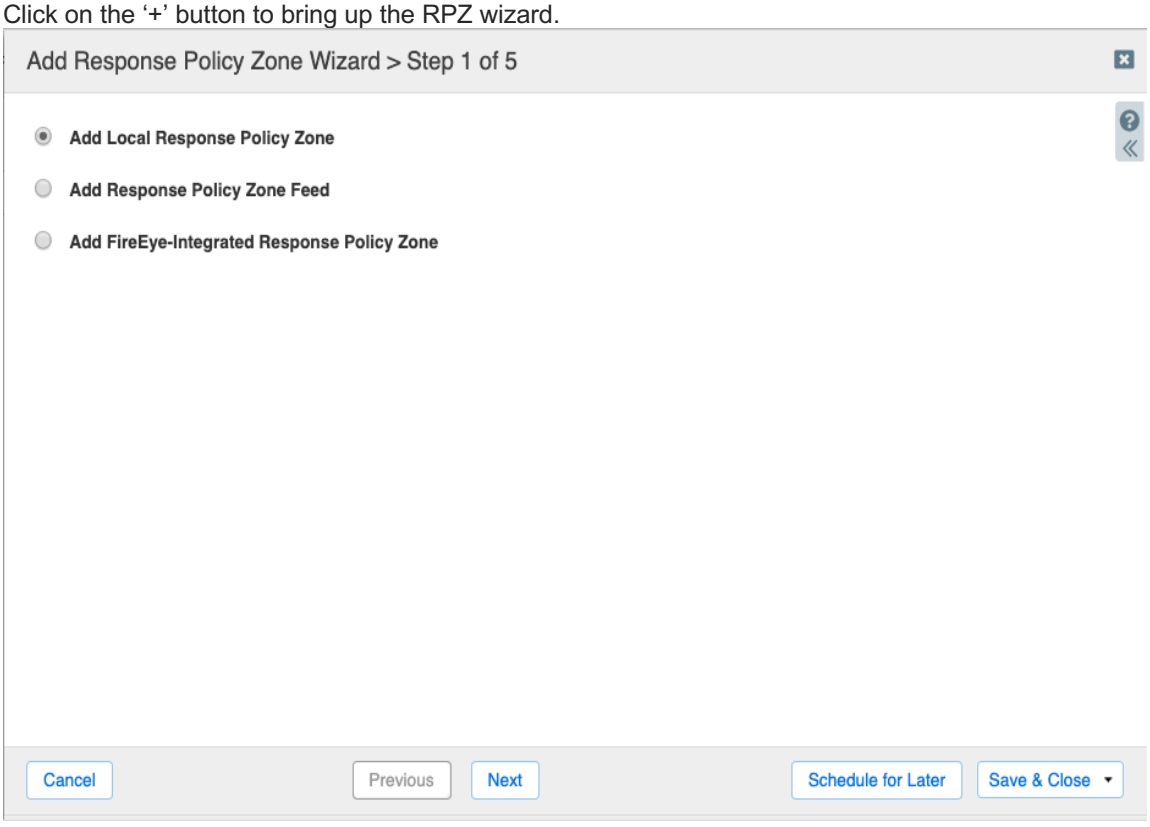
Configure Local RPZ.

1. Log into the Infoblox GUI.

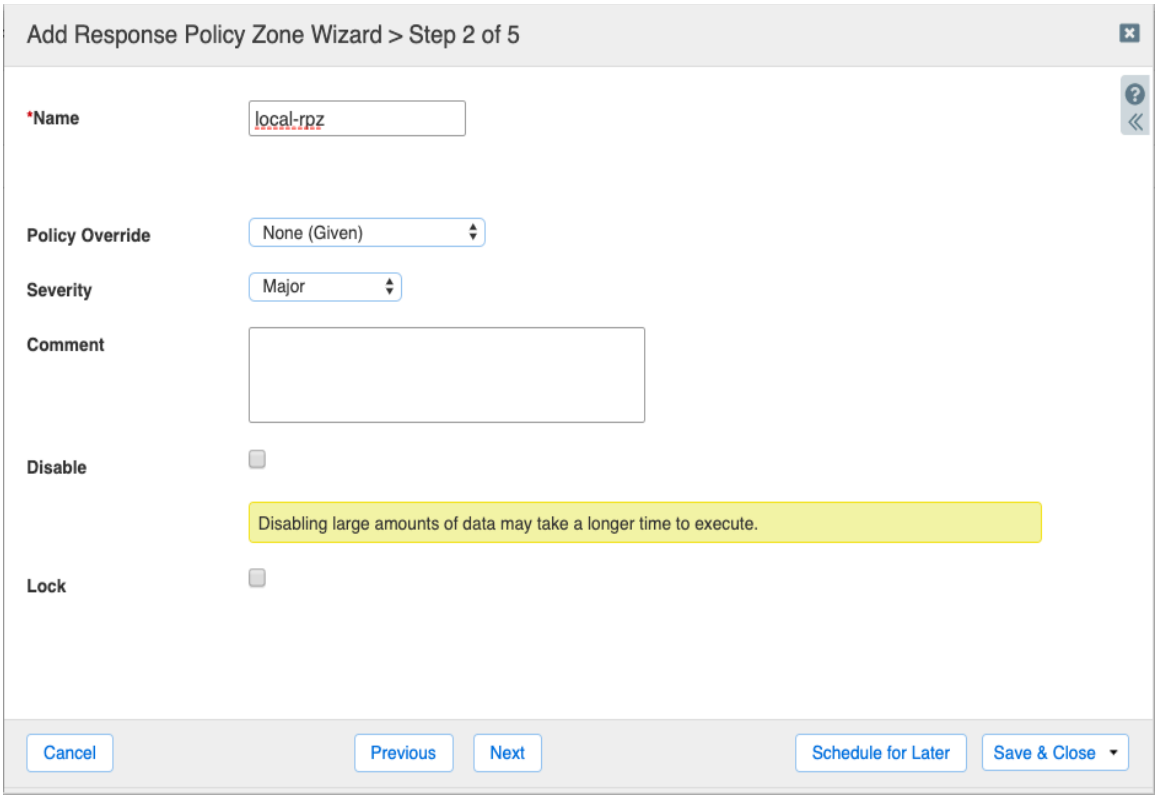
2. Navigate to Data Management → DNS → Response Policy Zones.



3. Click on the '+' button to bring up the RPZ wizard.

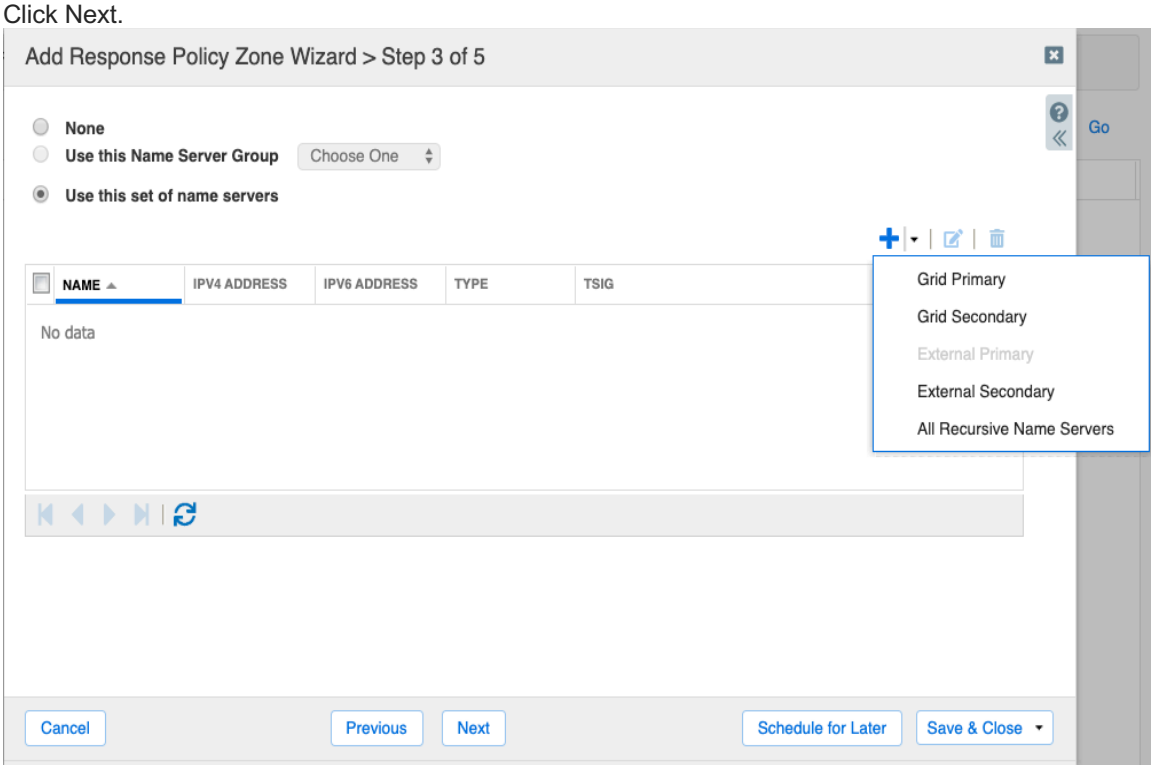


4. Click on the Next button.



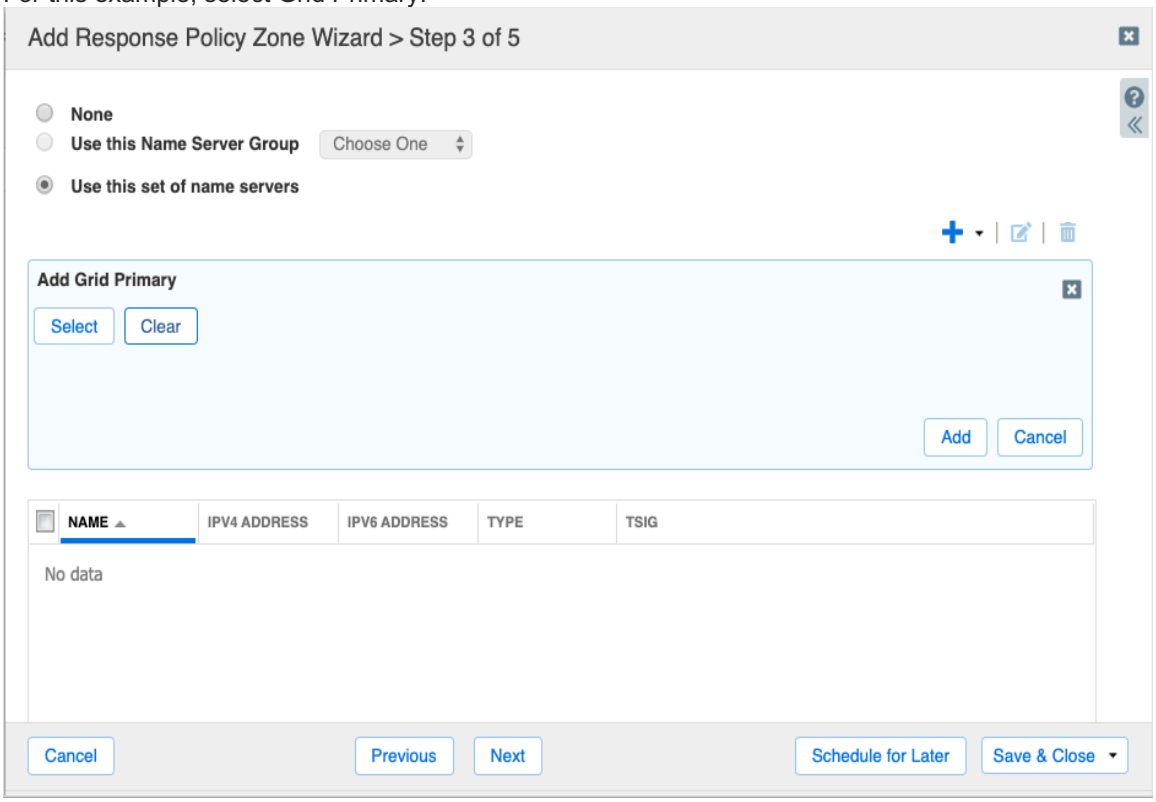
5. Type in a name for the local RPZ.
6. The Policy Override drop down menu allows you to override all of the policy rules for each RPZ entry. The choices are:
    I. None – means allow the policy to be enforced at the rule level.
    II. Log only – if a rule is hit, then no action will be taken and a syslog message will be logged. This setting is good for testing purposes.
    III. Block (No data) – on a rule hit, the response will contain no data.
    IV. Block (No such domain) – on a rule hit, the response will be no such domain. This is the same as NXDomain in the output of a dig command.
    V. Passthru-sends a response without modification
    VI. Substitute – a preconfigured domain is passed back as a response such as a walled garden website.
7. Severity drop down menu specifies the severity number to be assigned in the syslog entry. The choices are:
    I. Major (default)
    II. Critical
    III. Warning
    IV. Informational
8. Enter details of this RPZ into the comment box.
9. The Disable button allows for disabling this RPZ.
10. The Lock button allows for locking the configuration to prevent other users from making changes.

11. Click Next.

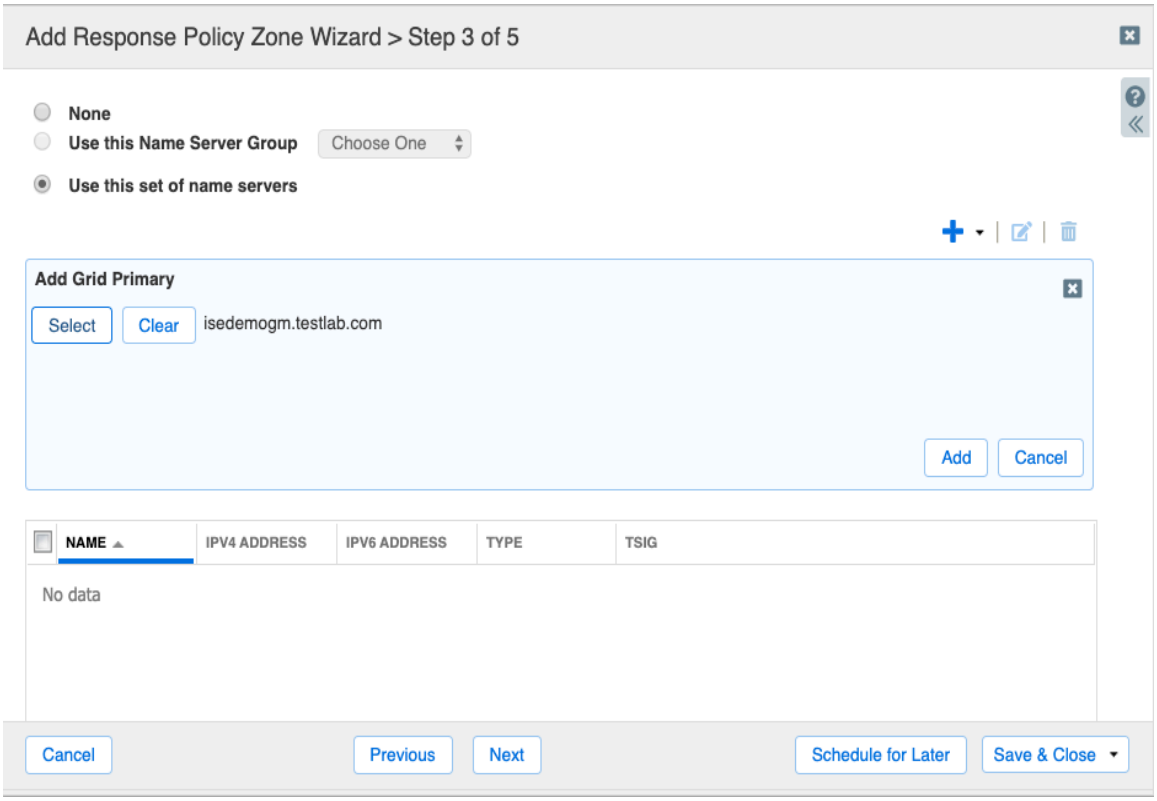


12. Click on 'Use this set of name servers' to assign the DNS member that will service this local RPZ.
13. Click on the '+' button to select the server. The choices are:
    I. Grid Primary – this will be the primary server for the zone.
    II. Grid Secondary – this will be the secondary server for the zone.
    III. External Secondary – specify an external server that is outside of the Grid.
    IV. All Recursive Name Servers – this zone is assigned to all recursive servers as secondary servers.

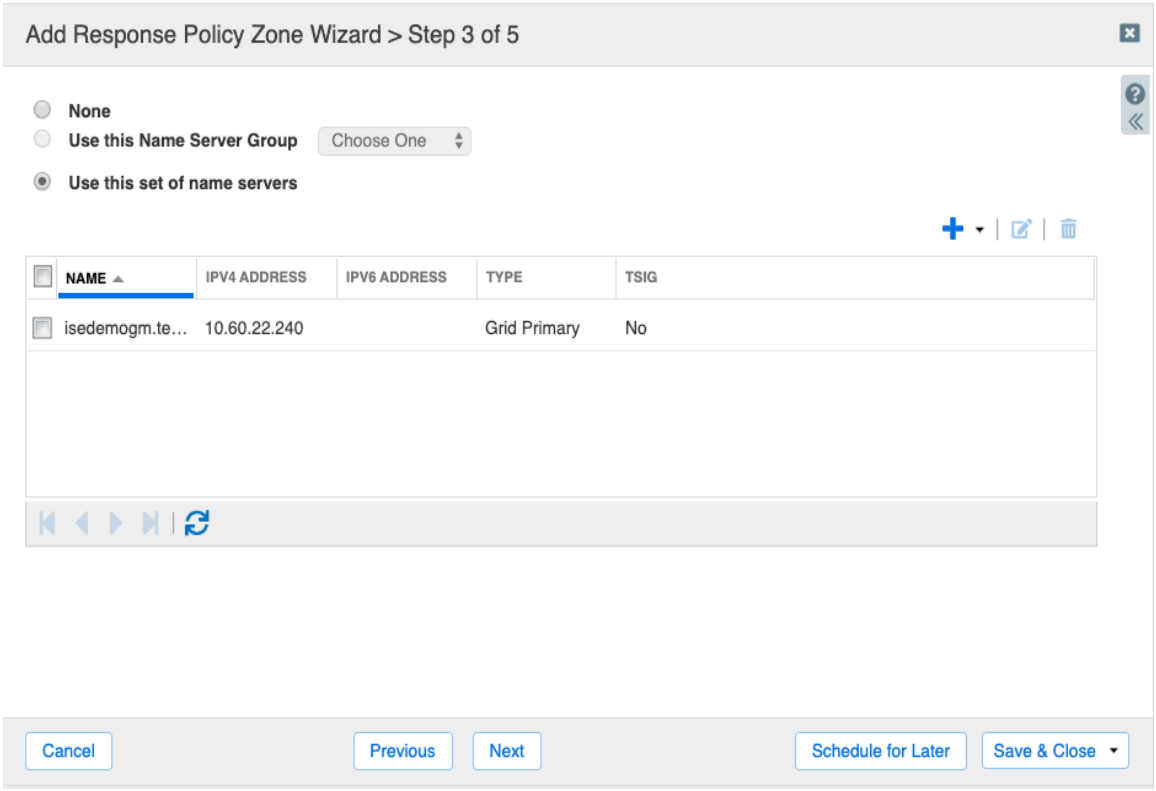
14. For this example, select Grid Primary.



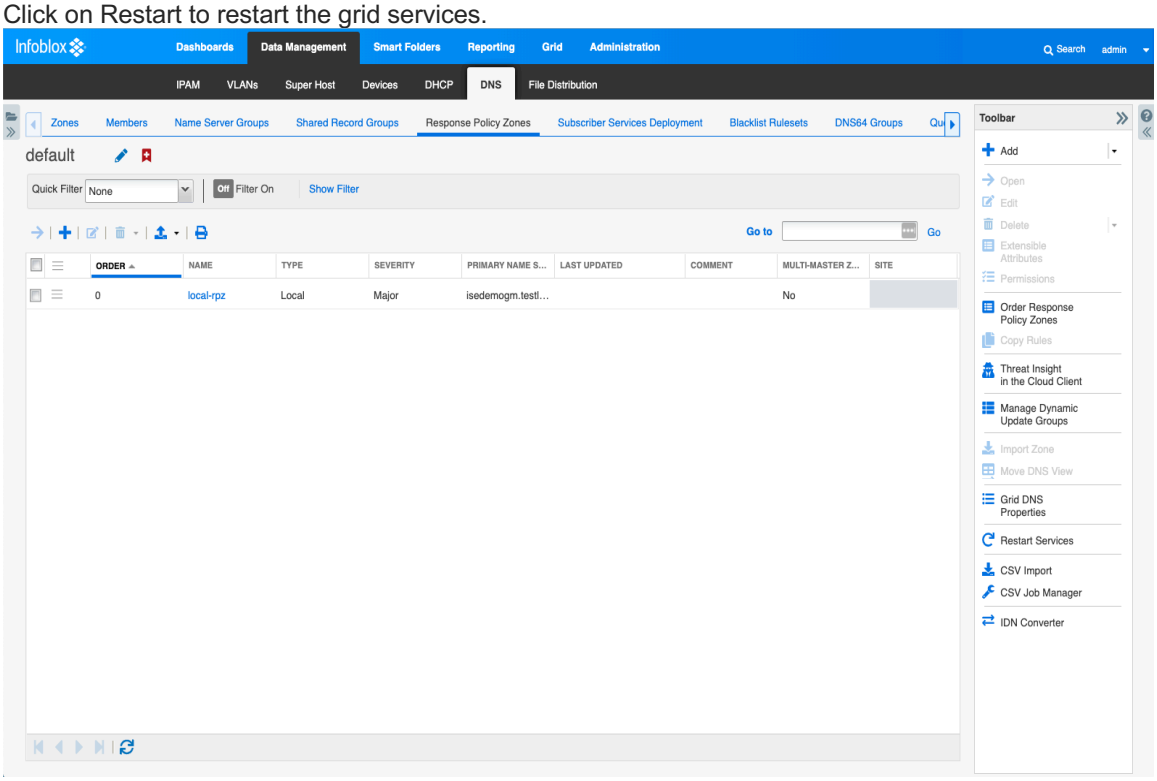
15. Click on the Select button.



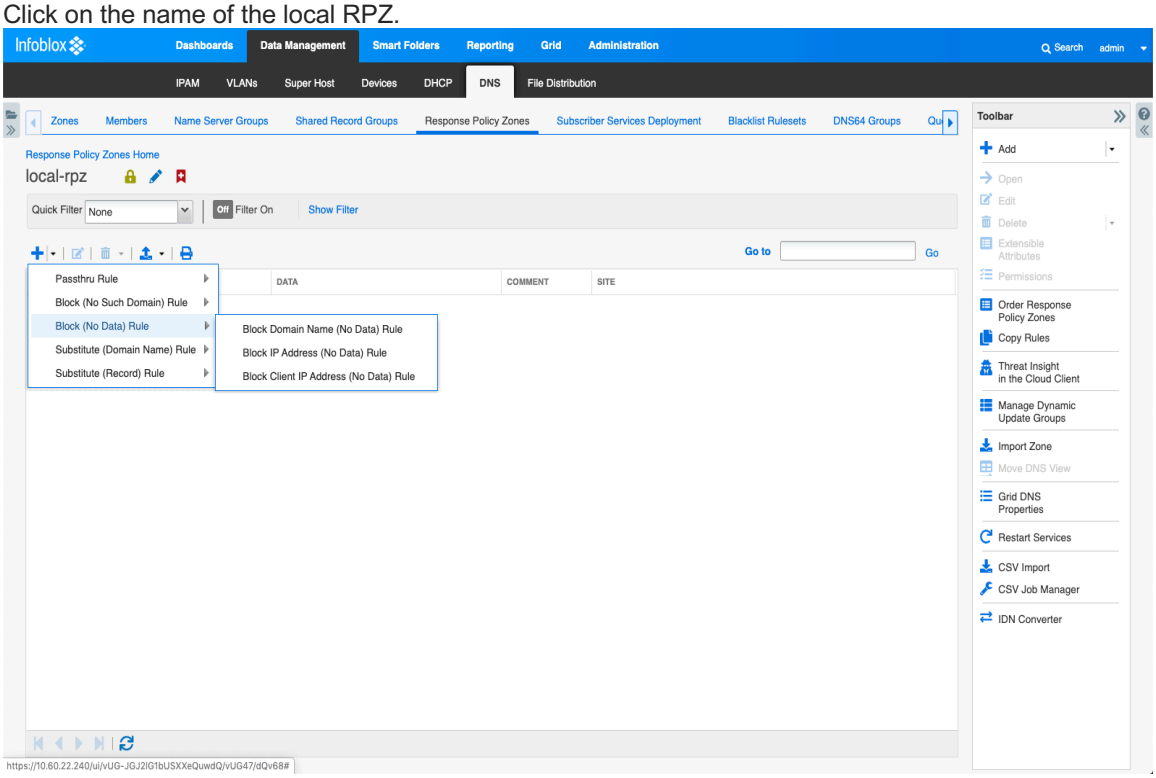
16. Click on the Add button.



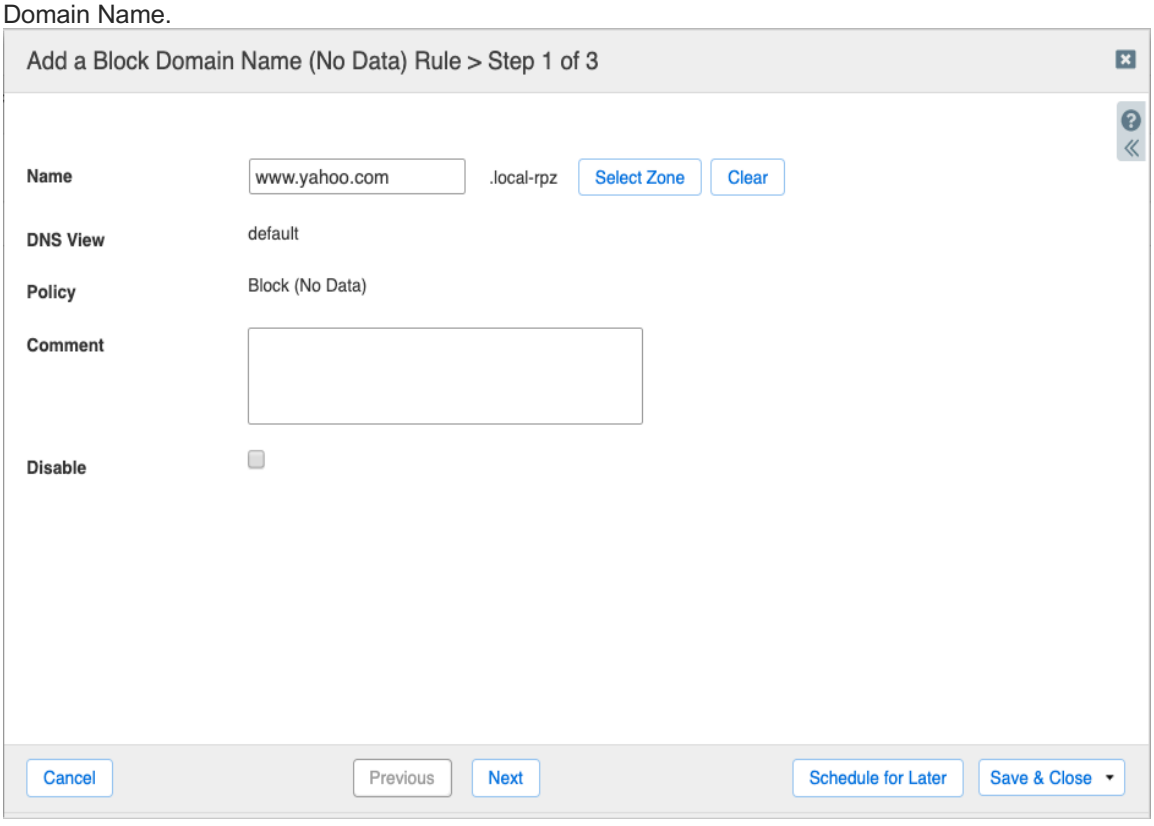
17. Click on Save and Close.
18. Click on Restart to restart the grid services.



19. Click on the name of the local RPZ.

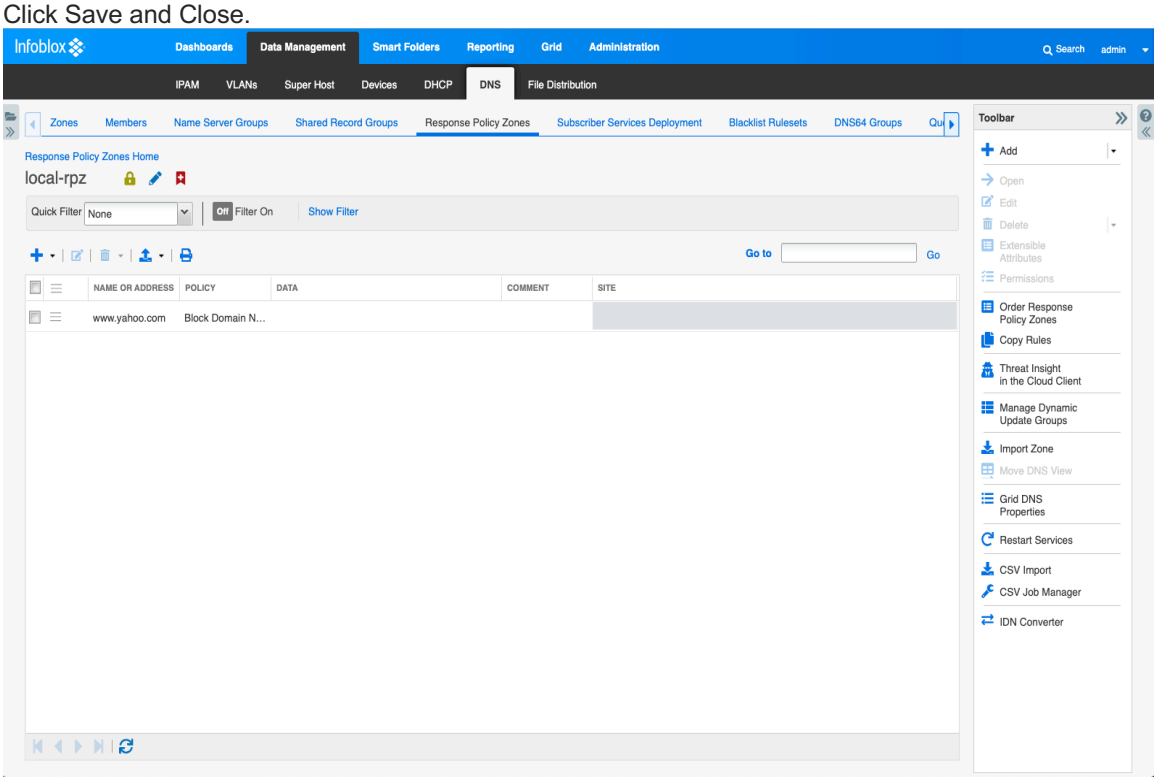


20. Click on the '+' button to select a rule type. For example, select Block (No Such Domain) → Block Domain Name.

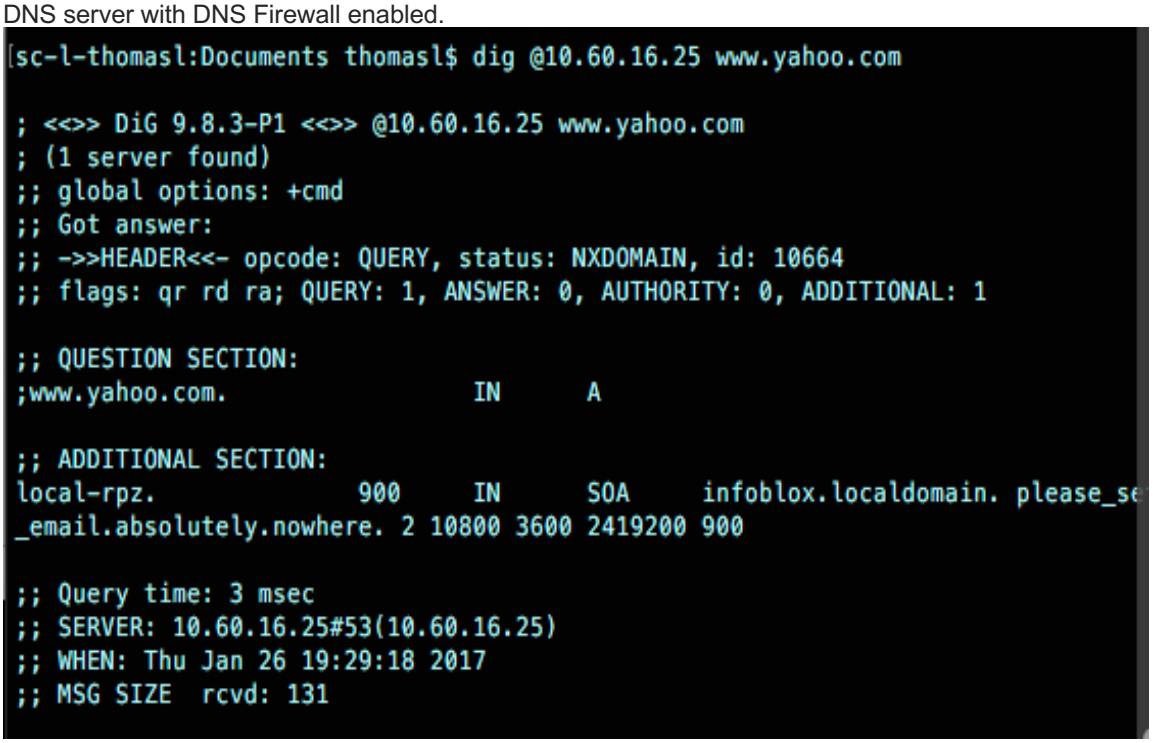


21. Enter a URL or domain like the above.

22. Click Save and Close.



23. To test, run a dig (linux) or nslookup (windows). You should see a similar output. 10.60.16.25 is the DNS server with DNS Firewall enabled.

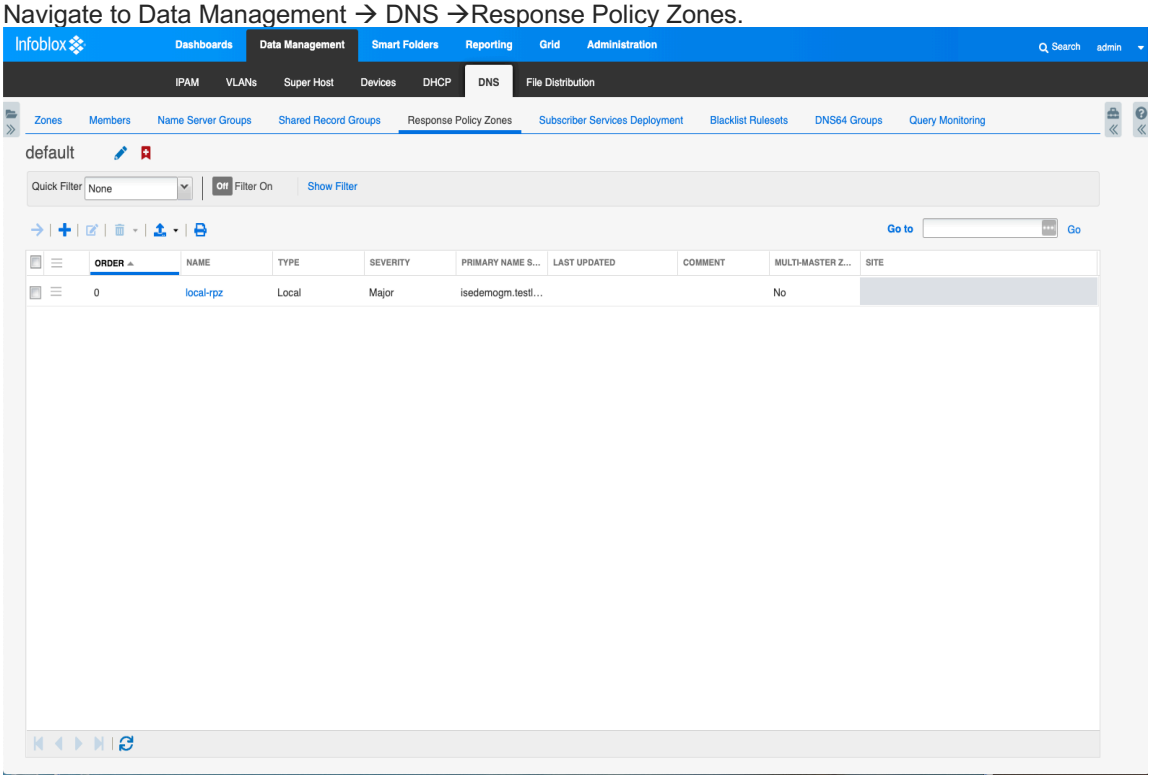


24. Notice the NXDOMAIN status.

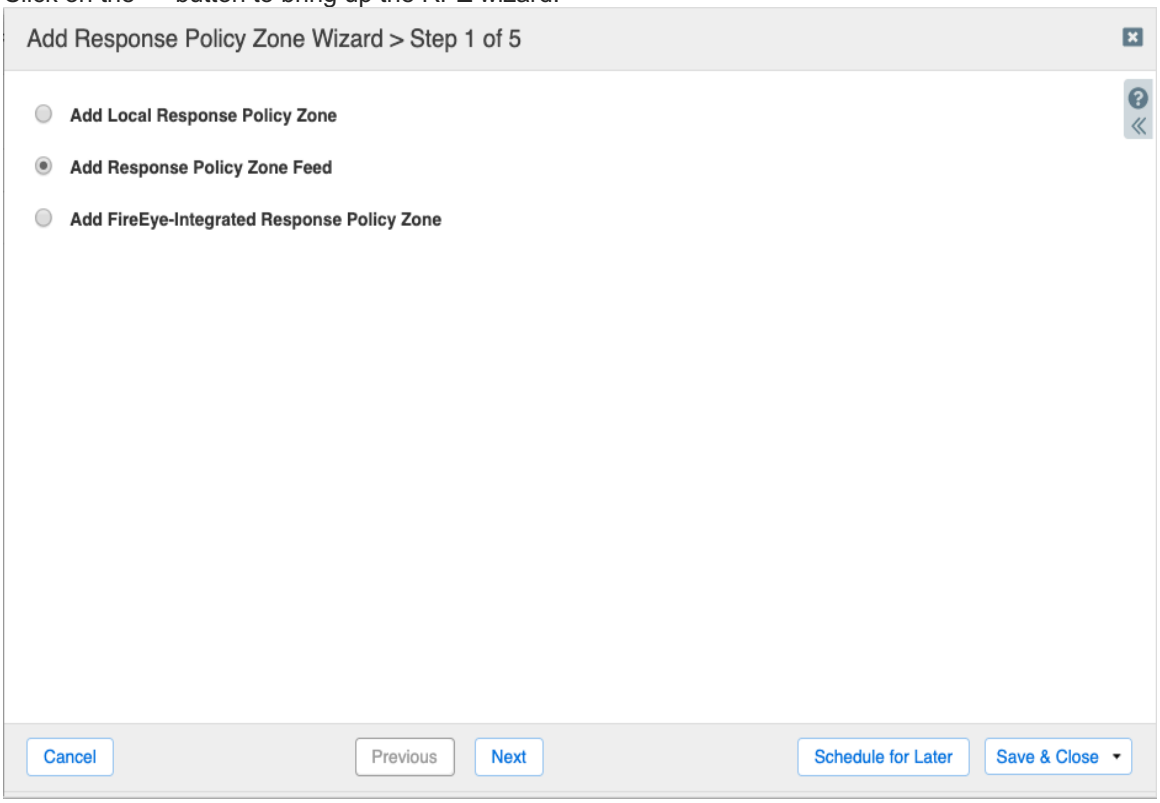
25. In addition, navigate to Administration → Logs → Syslog. Search for CEF (common event format) messages. This shows an RPZ hit did occur.

Configure RPZ Feed with Cloud Services Portal.

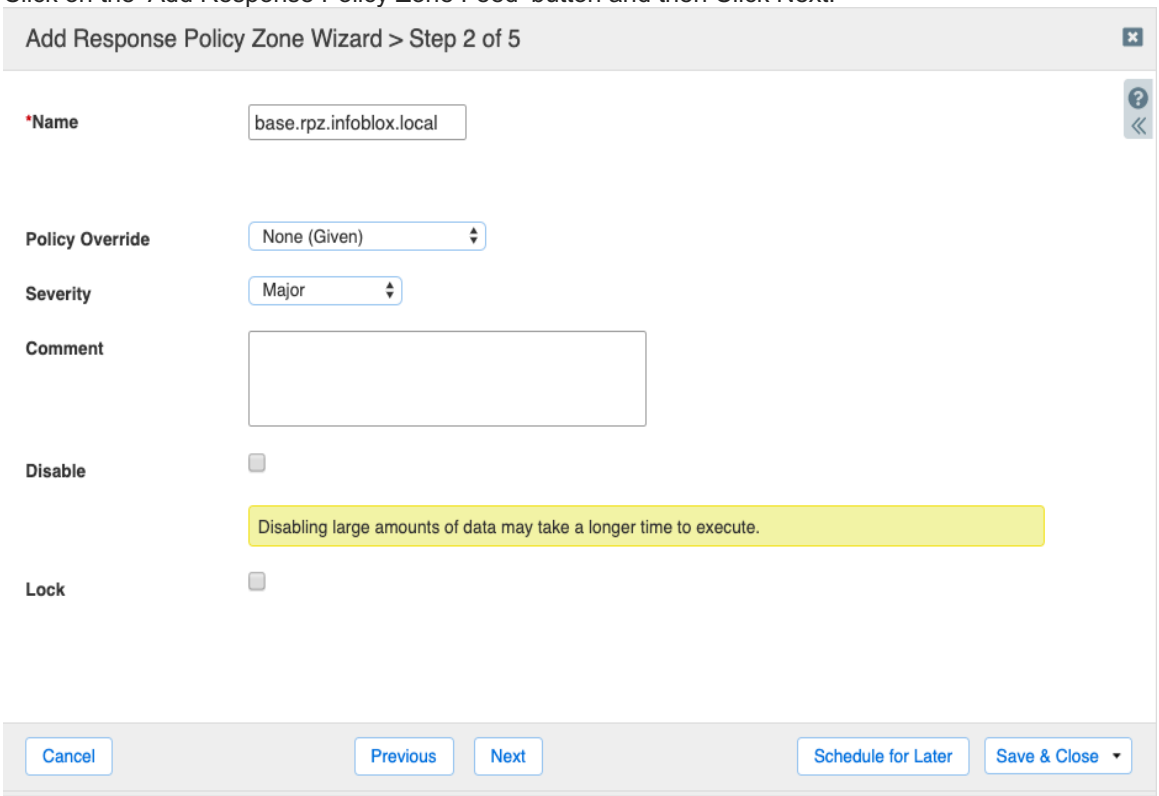
1. Log into the Infoblox GUI.
2. Navigate to Data Management → DNS →Response Policy Zones.



3. Click on the '+' button to bring up the RPZ wizard.



4. Click on the 'Add Response Policy Zone Feed' button and then Click Next.



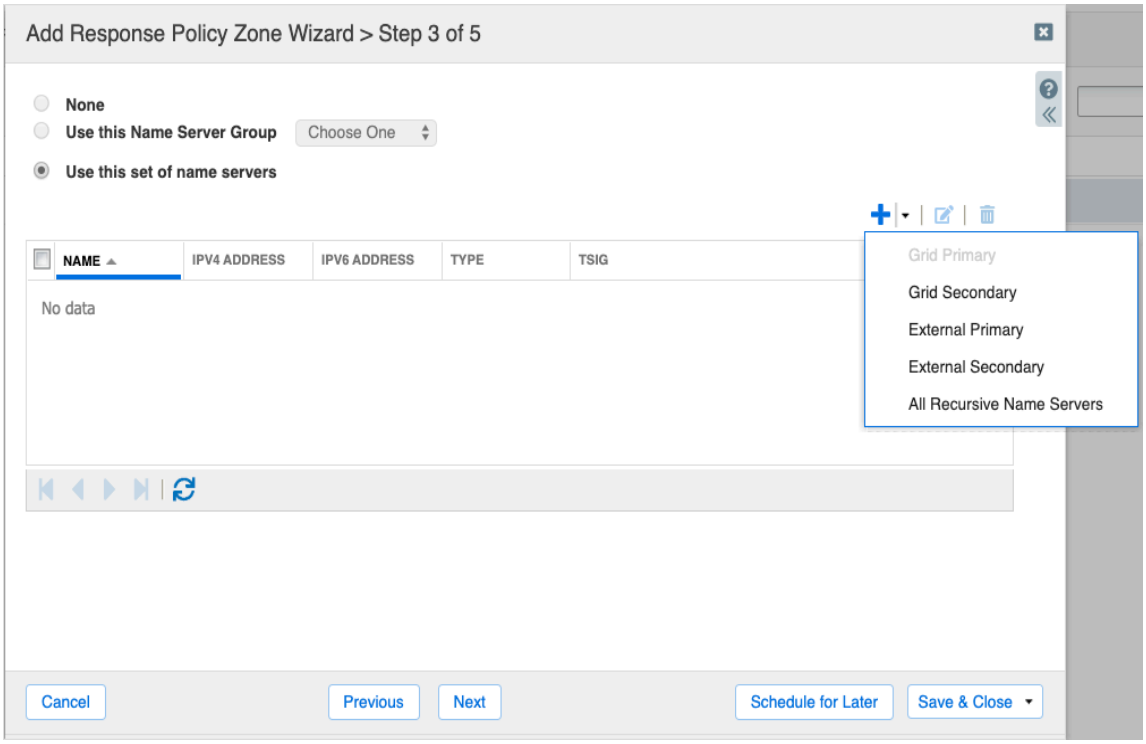
5. Enter the name of the feed.
    a. The choices for standard feeds are:

1. Base.rpz.infoblox.local
2. antimalware.rpz.infoblox.local
3. ransomware.rpz.infoblox.local
4. bogon.rpz.infoblox.local

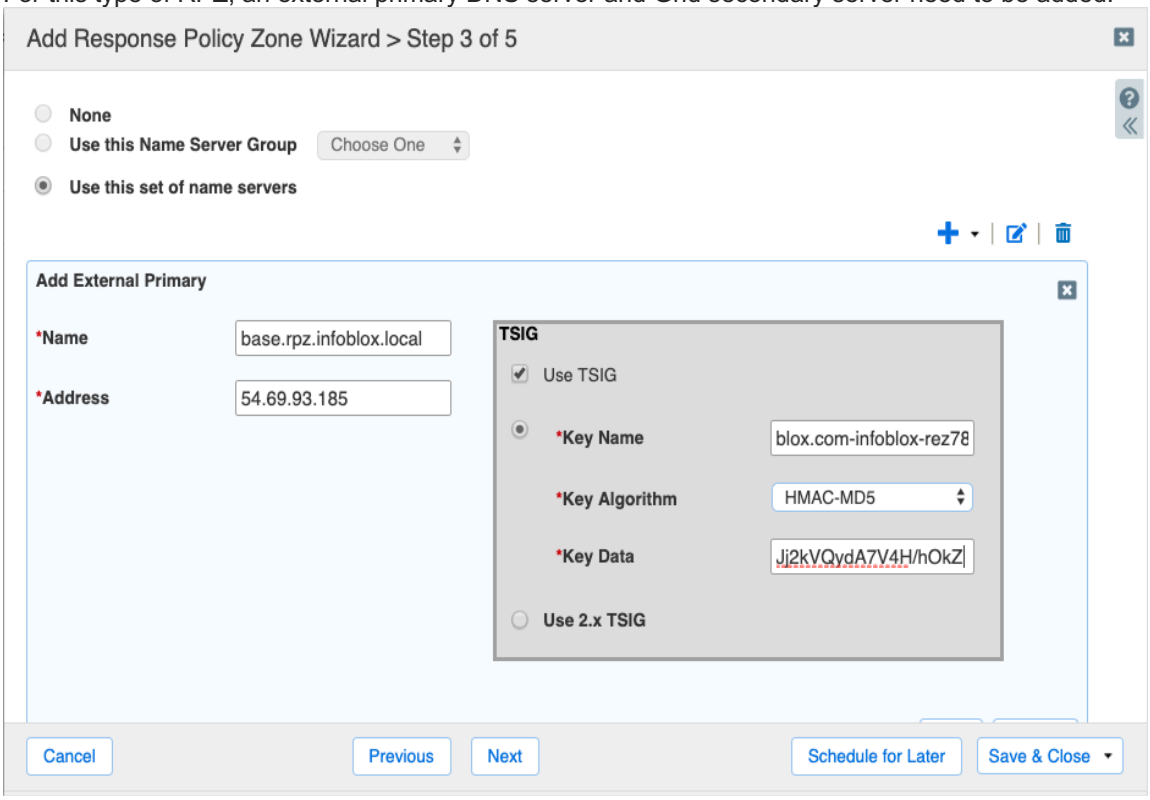
b. The choices for Plus or Advanced feeds are:
1. Antimalware-ip.rpz.infoblox.local
2. Bot-ip.rpz.infoblox.local
3. Exploit-ip.rpz.infoblox.local
4. Malware-dga.rpz.infoblox.local
5. Tor-exit-node-ip.rpz.infoblox.local
6. Multi-domain.surbl.rpz.infoblox.local
7. Fresh-domain.surbl.rpz.infoblox.local

6. The Policy Override drop down menu allows you to override all of the policy rules for each RPZ entry. The choices are:
   a. None – means allow the policy to be enforced at the rule level.
   b. Log only – if a rule is hit, then no action will be taken and a syslog message will be logged. This setting is good for testing purposes.
   c. Block (No data) – on a rule hit, the response will contain no data.
   d. Block (No such domain) – on a rule hit, the response will be no such domain. This is the same as NXDomain in the output of a dig command.
   e. Passthru-sends a response without modification
   f. Substitute – a preconfigured domain is passed back as a response such as a walled garden website.
7. Severity drop down menu specifies the severity number to be assigned in the syslog entry. The choices are:
   a. Major (default).
   b. Critical.
   c. Warning.
   d. Informational.
8. Enter details of this RPZ into the comment box.
9. The Disable button allows for disabling this RPZ.
10. The Lock button allows for locking the configuration to prevent other users from making changes.

11. Click Next.



12. For this type of RPZ, an external primary DNS server and Grid secondary server need to be added.

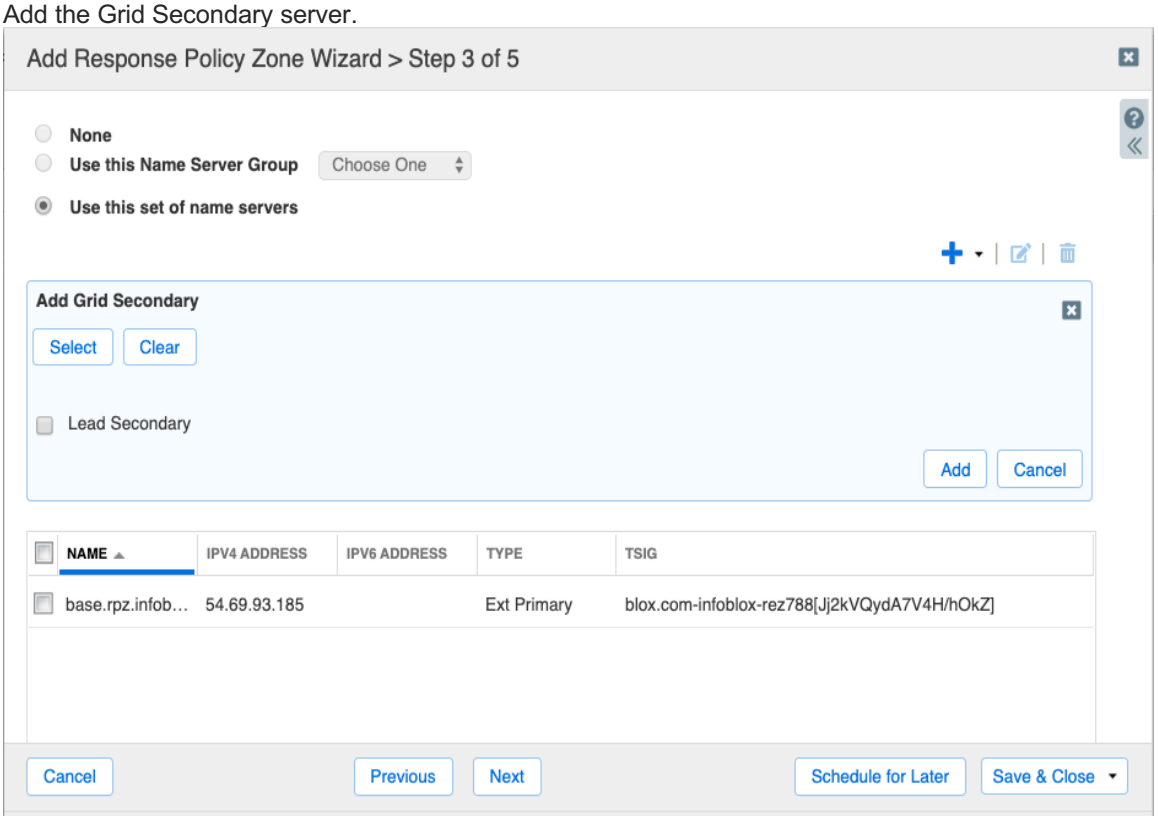


13. Add:
    a. The name of the feed.
    b. The IP address of the feed server.
    c. Key name.

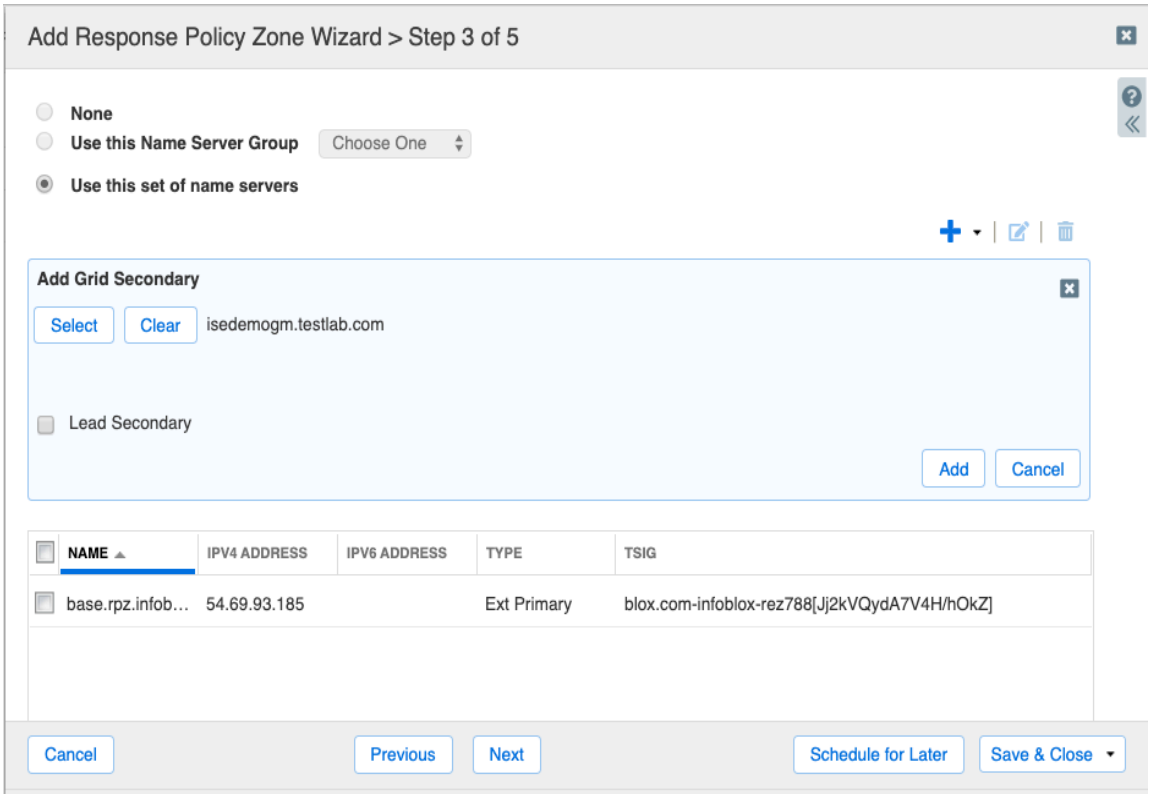
d. Key data which is the TSIG key.

Note: The feed name, external primary IP address, key name and TSIG key details will be provided from https://csp.infoblox.com.

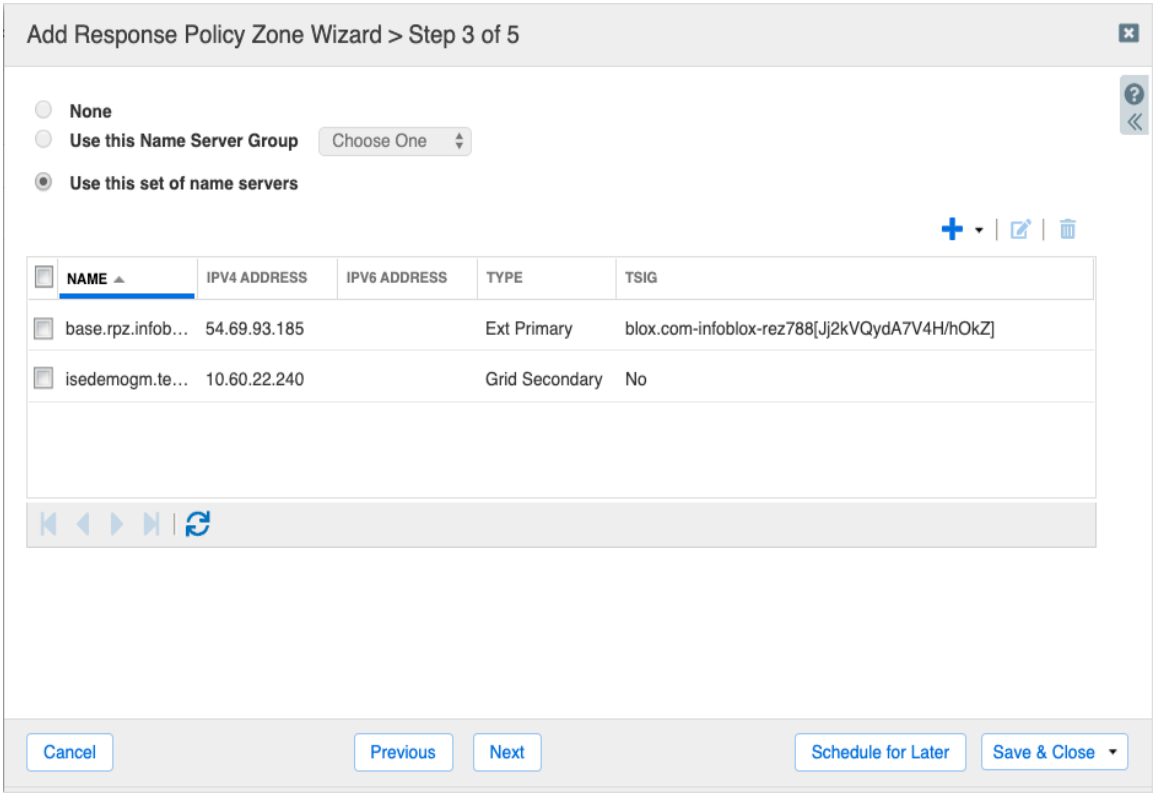
14. Click on the ‘Add’ button.
15. Add the Grid Secondary server.



16. Click on the one of the names. This server will store the feed when it is transferred.

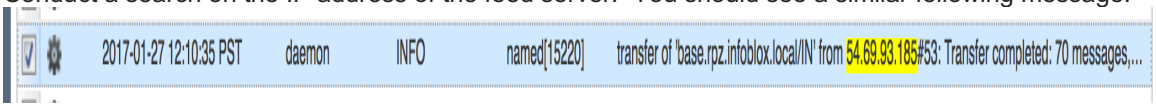


17. Click on the ‘Add’ button.

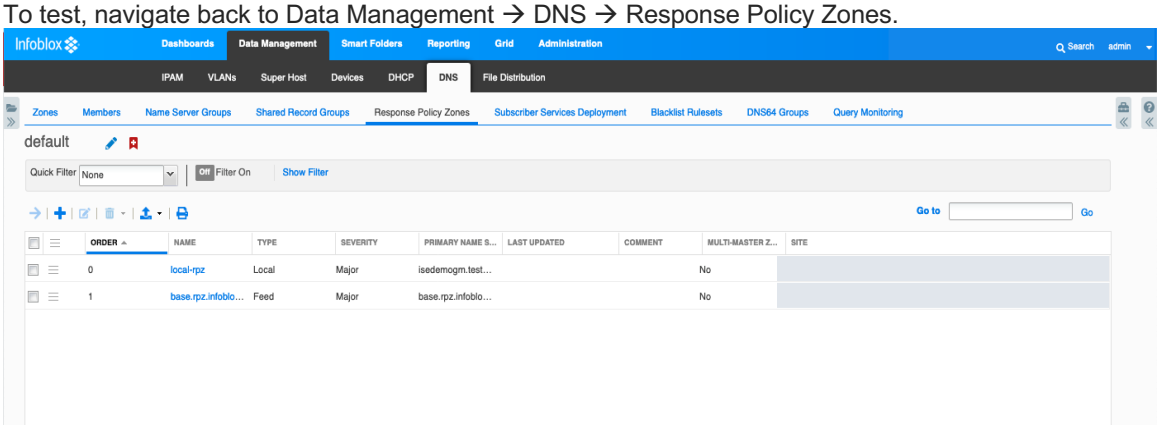


18. Click on ‘Save & Close’ button and then click on the ‘Restart’ button.

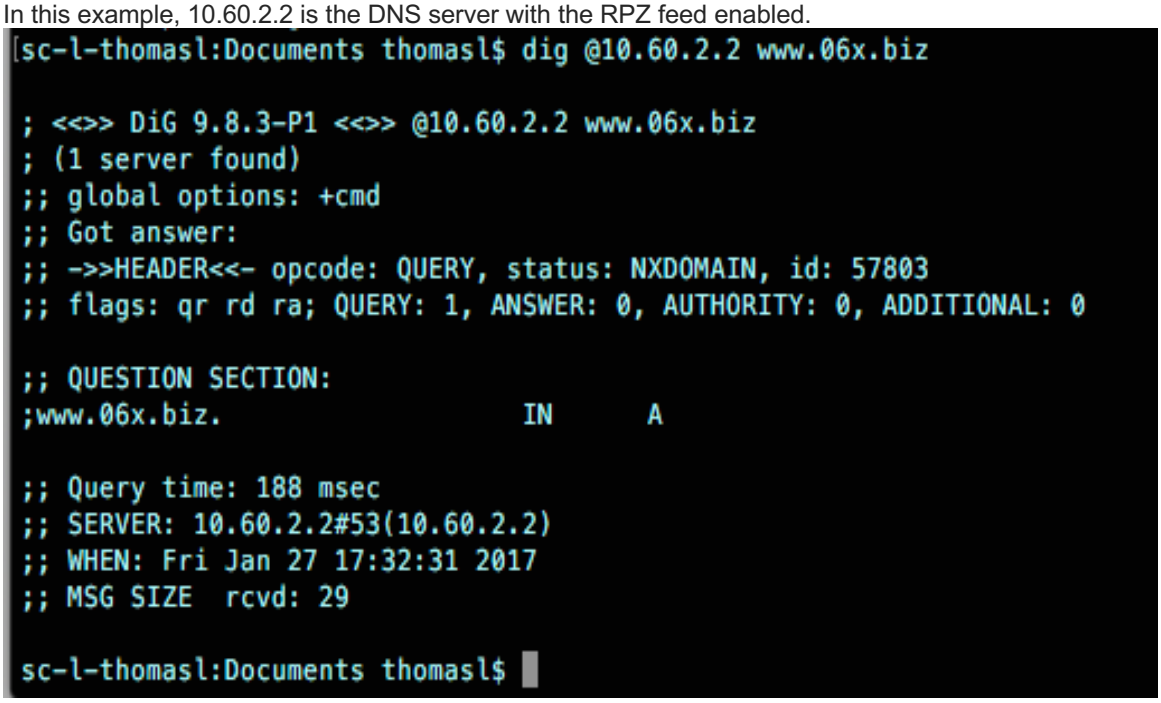
19. To verify that the zone transfer of the feed was correct, navigate to the Administration → Logs → Syslog and then select the member.
20. Conduct a search on the IP address of the feed server. You should see a similar following message:



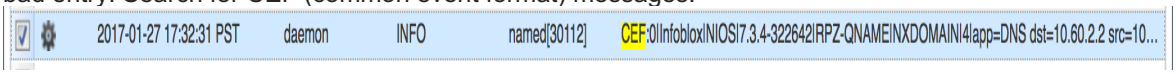
21. To test, navigate back to Data Management → DNS → Response Policy Zones.



22. Click on the feed entry to download the contents to a .CSV file.
23. Pick an item in the file to run a DNS resolution.
24. Depending upon the OS of your workstation run a 'dig' or 'nslookup' against the name server and URL. In this example, 10.60.2.2 is the DNS server with the RPZ feed enabled.



25. Notice the status of NXDOMAIN.
26. In addition, navigate to Administration → Logs → Syslog and select the member that was resolving the bad entry. Search for CEF (common event format) messages.

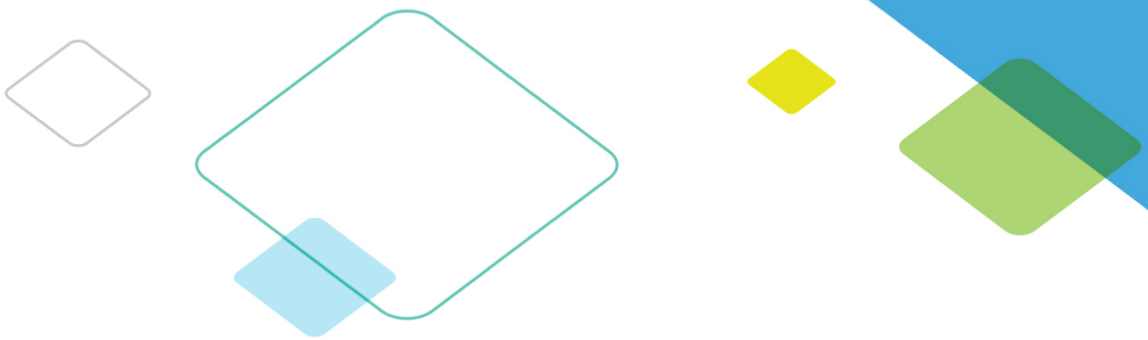


Troubleshooting

In case you are not getting a feed from our servers verify if:

- You used the right feed name.
- Your time is set correctly (NTP should be used).
- You use the right key name, TSIG key, and algorithm.

For further troubleshooting check the syslog of your (lead) secondary for message that include “transfer”.



Infoblox enables next level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com