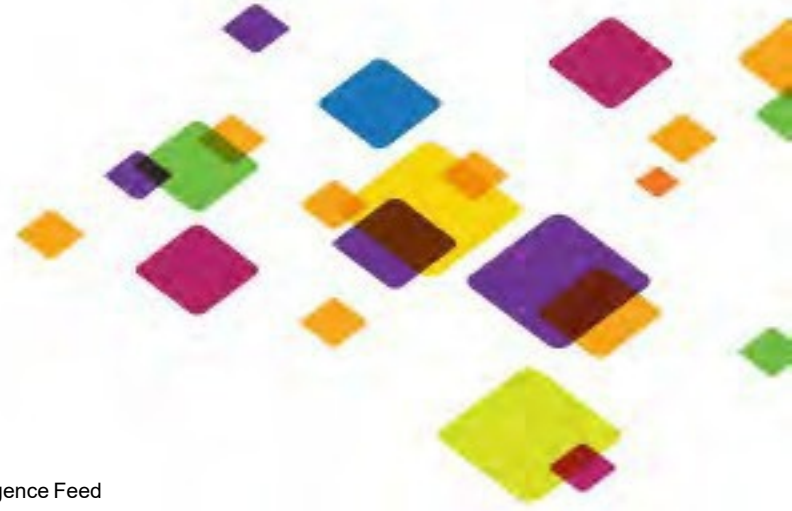
Deployment Guide

Infoblox Threat Intelligence Feed



© 2020 Infoblox Inc.

Table of Contents

Introduction

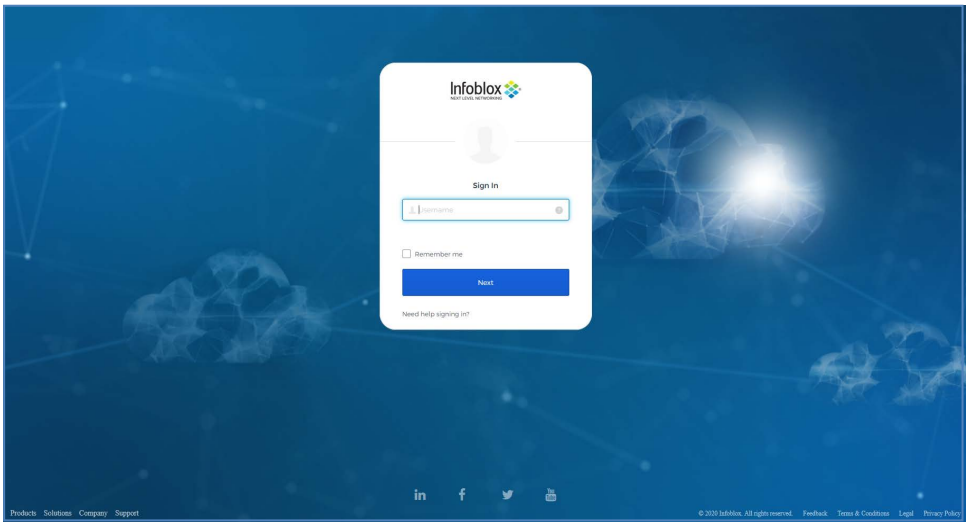
This document provides you with a quick-start guide on how to get to and deploy the Infoblox Threat Intelligence feed.

Portal

Account Registration

Upon completion of the sales cycle, you will receive a notification that your account has been provisioned. To access the portal, log in to the Infoblox Cloud Services Portal.

csp.infoblox.com



Portal Navigation

The portal has a top navigation which contain the following sections:

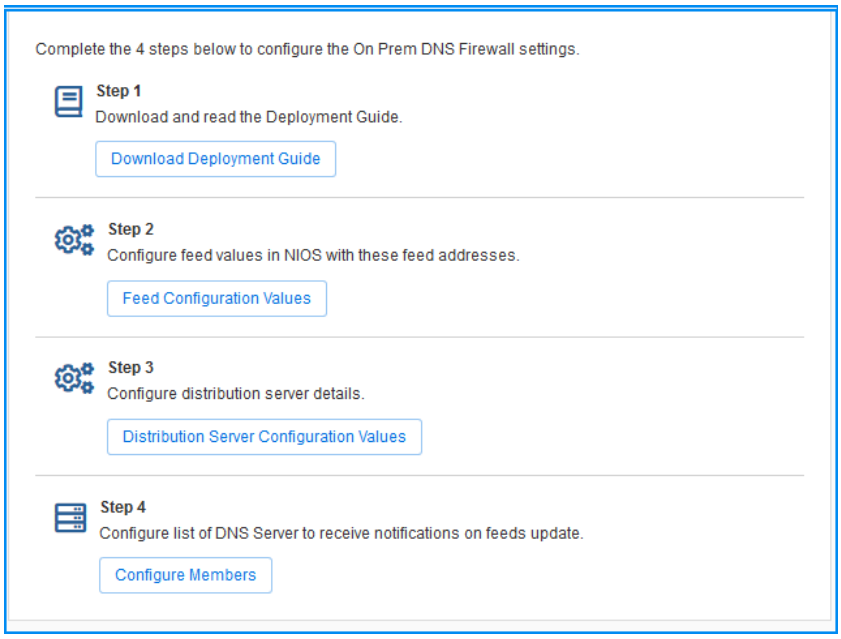
Analyze	Includes Threat Lookup where you can research suspicious indicators for more information and context.
Administration	Includes Threat Feeds, where descriptions of the feeds are found that are included in your subscription.
	Includes Portal Users, to configure additional users for your organization.
Policies	Includes On-Prem DNS Firewall Configuration where you can perform the configuration of your feed and retrieve NIOS settings.

On-Prem DNS Firewall Configuration

Navigate to **Policies** > **On-Prem DNS Firewall** to configure the On-Prem DNS Firewall service. Complete the four-step process to configure your On-Prem DNS Firewall settings. Please note, downloading the *Infoblox Threat Intelligence Feed Deployment Guide* is **Step 1** of the process. Once you have reviewed the guide, please proceed to **Step 2** to begin the configuration process.

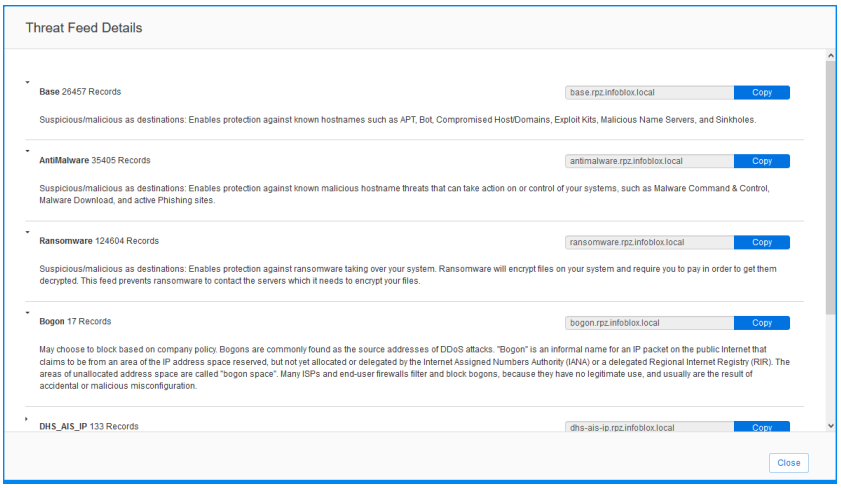
Step 1: Download Deployment Guide

Click **Download Deployment Guide**. Read through the guide thoroughly before proceeding to the next step where you will configure your NIOS feeds.



Step 2: Feed Configuration

Click **Feed Configuration Values** to configure the NIOS feed values with the provided feed addresses based on your subscription. Copy these values to a text editor as you require them later for NIOS configuration. Please note, the record count associated with a feed is published along with the feed's description. Once completed, click **Close** and proceed to **Step 3**.



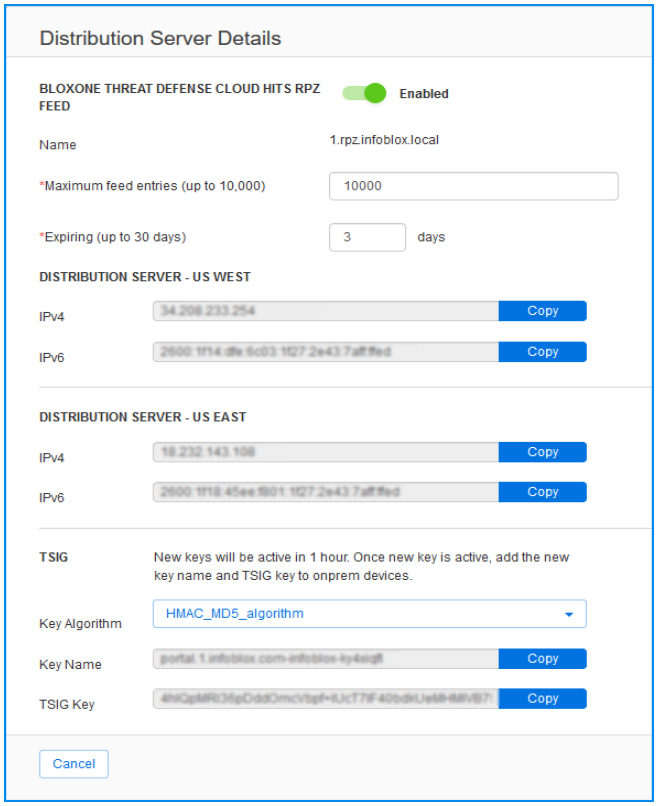
Note: The feed(s) you transfer to your grid have an impact on performance of your DNS server. On the right-hand side of the page, you can see some performance guidance of what size of feed will work on your appliances. If you are unsure, work with your account team or support to ensure you apply what is best for your environment.

Step 3: Distribution Server Configuration Values

Click **Distribution Server Configuration Values** to configure your distribution servers. Both IPv4 and IPv6 IP addresses may be used to serve your feeds, depending on your specific requirements. TSIG Key encryption algorithms supported include HMAC MD5 512-bit and HMAC 256 256-bit. Please be aware, it may take up to one hour before your newly created TSIG keys become active.

To set up where your feeds server, complete the following steps:

1. On the **Distribution Server Details** screen, for **BLOXONE THREAT DEFENSE CLOUD HITS RPZ FEED**, toggle the switch to **Enable** to add the option of a custom RPZ feed to the feed distribution. When enabling the custom RPZ feed, specify the maximum number of feed indicators the custom RPZ feed will return with a name along with an expiration date for the indicators. The name of the RPZ feed is the name of your custom RPZ zone file.
2. **Maximum feed entries**: If BloxOne Threat Defense is enabled, the RPZ can have a maximum of 10,000 records. This value can be set to any number of entries less than 10,000.
3. **Expiring days:** In this field you can set a TTL from 1 to 30 days. This setting determines how long indicators are retained in the RPZ. Indicators will be removed when this limit is exceeded.
4. For distribution servers. select either the IPv4 or IPv6 IP options for both the US West Distribution and the East Distribution Servers.
5. Copy and save your selected IP addresses before proceeding. You will need them later when configuring NIOS.
6. **TSIG**: Select a TSIG Key algorithm from among the drop-down menu choices. Algorithm choices include HMAC MD5 512-bit and HMAC 256 256-bit. Once you have made your selection, click **Generate** to generate a new TSIG key. The Cloud Services Portal generates a TSIG key based on your account information. The key name and TSIG key will be added to your on-prem devices. This provides required authorization to transfer zone files.
7. Copy and save the Key Name and TSIG Key.
8. Once completed, click **Close** and proceed to **Step 4.**



Step 4: Configuring Threat Feed Retrieval Members

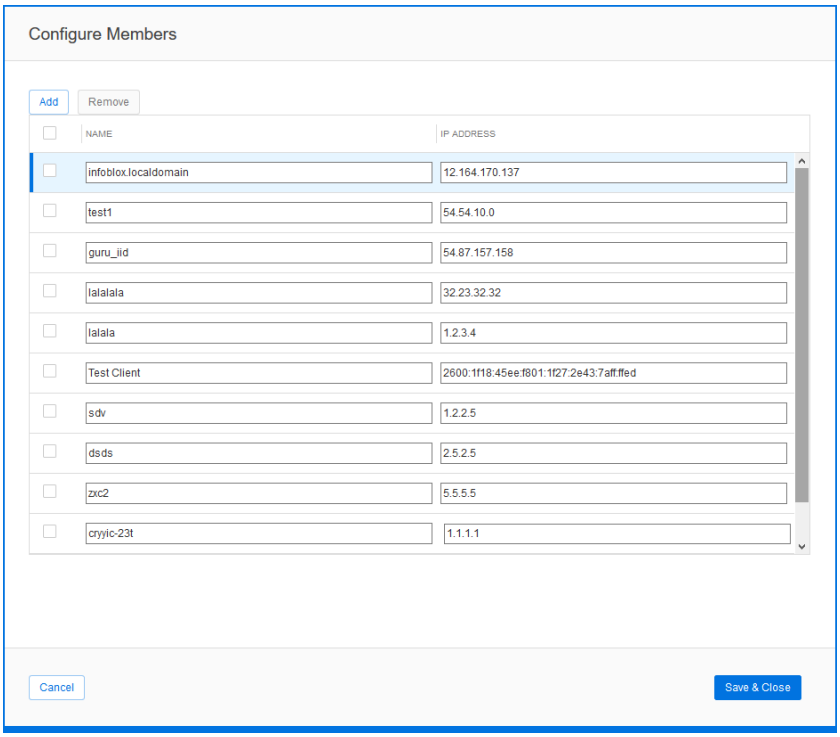
Click **Configure Members** to configure your list of threat retrieval members. You can add and remove members as needed

To add a threat retrieval member, complete the following steps:

1. Click **Add.** A new row will populate at the bottom of the list.
2. Select the new row by selecting the box next to it.
3. In the **NAME** field, add a name for the member you are adding.
4. In the **IP ADDRESS** field, add the IP address you want to use for the new member.
5. Once you have finished adding members, you can remove any members you will not be using.

To remove a threat retrieval member, complete the following steps:

1. Select the configured member you want to remove by selecting the box next to it.
2. Click **Remove.**
3. Once you have configured your threat retrieval members, click **Save & Close**.



This completes the Cloud Services Portal On-Prem DNS Firewall portion for the set up and configuration of Infoblox Threat Intelligence feeds. Please proceed to the next page to configure NIOS.

NIOS Configuration

License and Configuration Requirements

In order to deploy remote RPZ feeds, you will need a Grid member with at least a DNS and a RPZ license.

In order to obtain the feeds, your member will need access to our Threat Intelligence Feed servers on port 53 (UDP and TCP) as the feed data is transferred through a DNS zone transfer. Your server will also need to be able to perform recursion in order to obtain response from the internet.

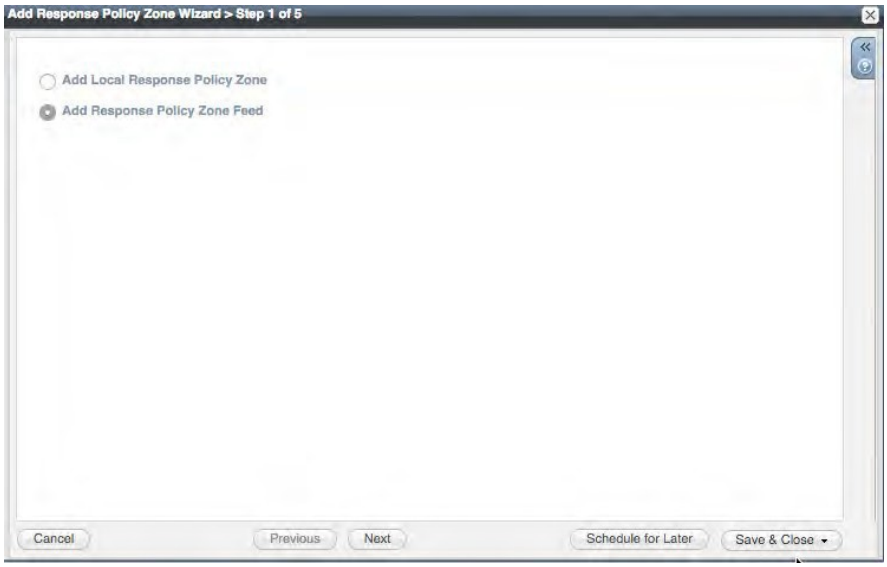
In order to review the log hits, you need to enable the member or grid level of the RPZ logging category (grid settings, toggle advanced, logging, check RPZ).

Configuration Steps

In NIOS go to **Data Management** -> **DNS** -> **Response Policy Zones.**

Click the **+** button or use **Add** in the sidebar.

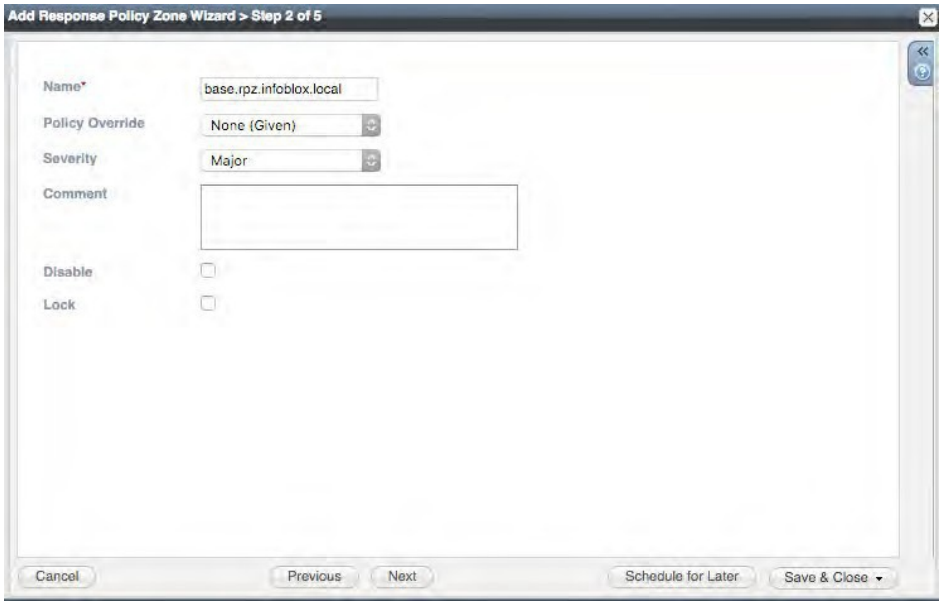
1. Select **Add a Response Policy Zone Feed**



Click **Next**.

2. Add the feed you want to use.

Note that each feed is a subset of the data and deploying multiple feeds is required to cover all bases. You will have to repeat these steps for each RPZ.



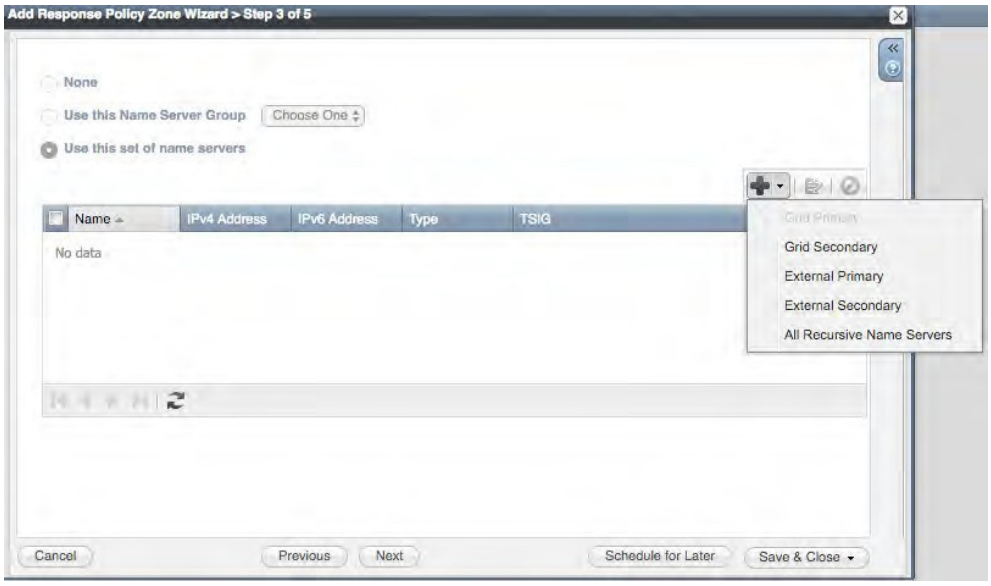
Leave Policy override on “None (Given)” for now. For the other policy override settings, please refer to the Admin Guide.

Modify logging Severity if needed.

Click **Next**.

3. Add the External Primary[3] -

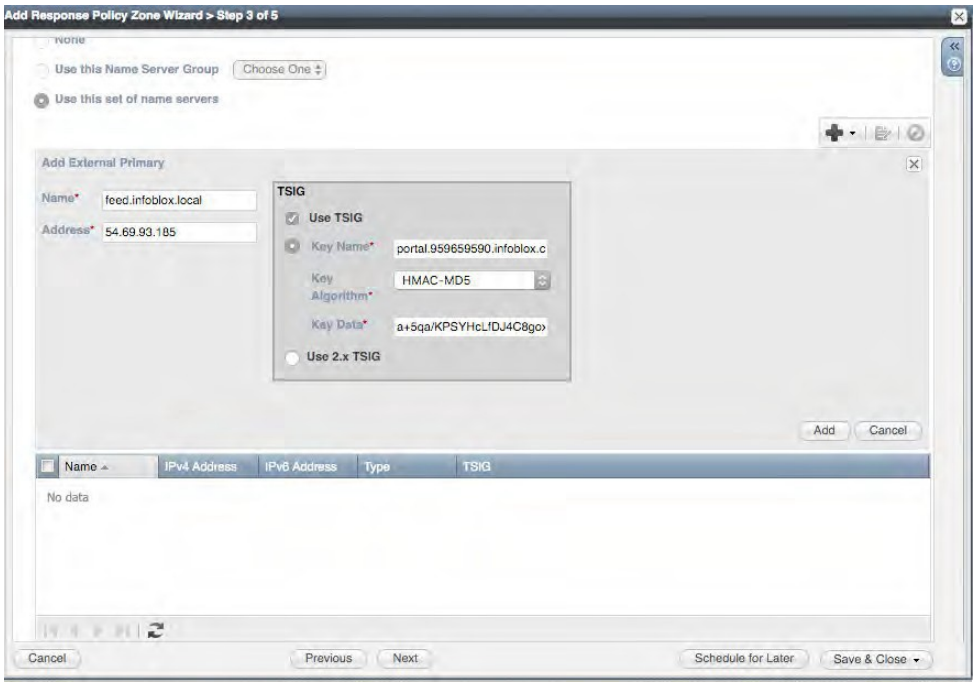
Use the drop-down next to the **+** sign to select External Primary



[1] If you want to save time, create a nameserver group with the external primaries and any grid secondaries that you want to use with this RPZ. You can then later use nameserver groups for each RPZ instead of adding the nodes one by one.

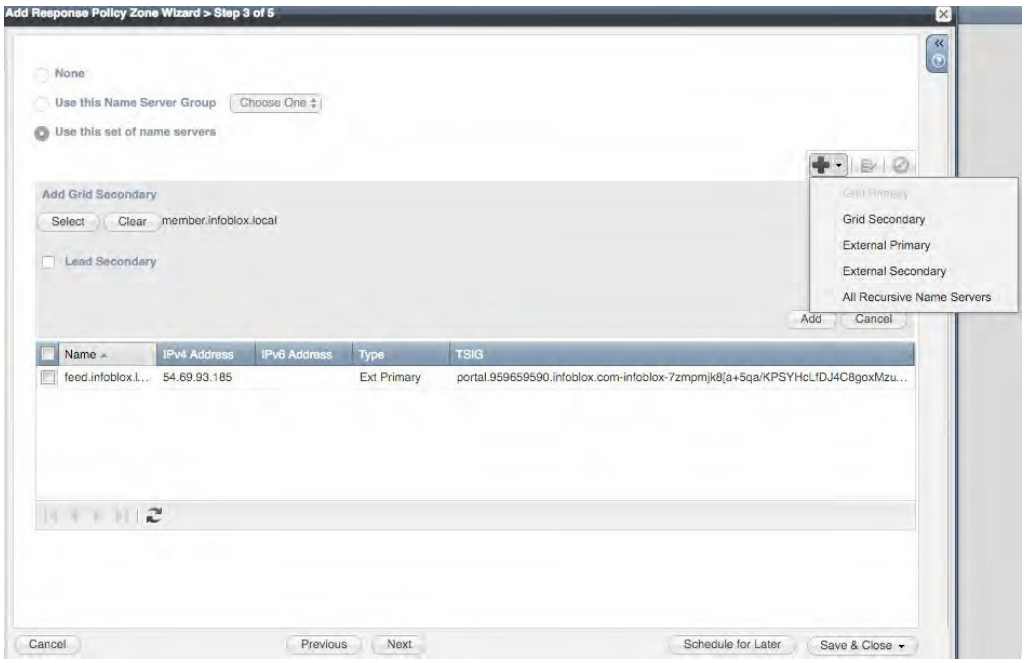
4. Define the External Primary's settings

Refer to the portal for the values from your account. Select the nearest name server and use the values you copied from the Cloud Services Portal during feed configuration. Note that the name field is only for reference purposes and you can use any name you choose.



Press Add

5. Add a Grid Secondary



Use "Select" to select which member(s) you want to add or use "**All recursive servers**" if you want to add all recursive nodes with an RPZ license.

Note that you can configure a single secondary to be “Lead secondary”. If you set this up that member will be the only one to reach out to the external primary. You will then redistribute the feed internally between your members through zone transfers.

Click **Add.**

Click Save and Close, then restart services as required (use the banner at the top)

Give services 5 minutes to fetch the zone. If you refresh the GUI you will see the last updated value for when the last transfer was successful.

Troubleshooting

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

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”

Generating & Reviewing Hits

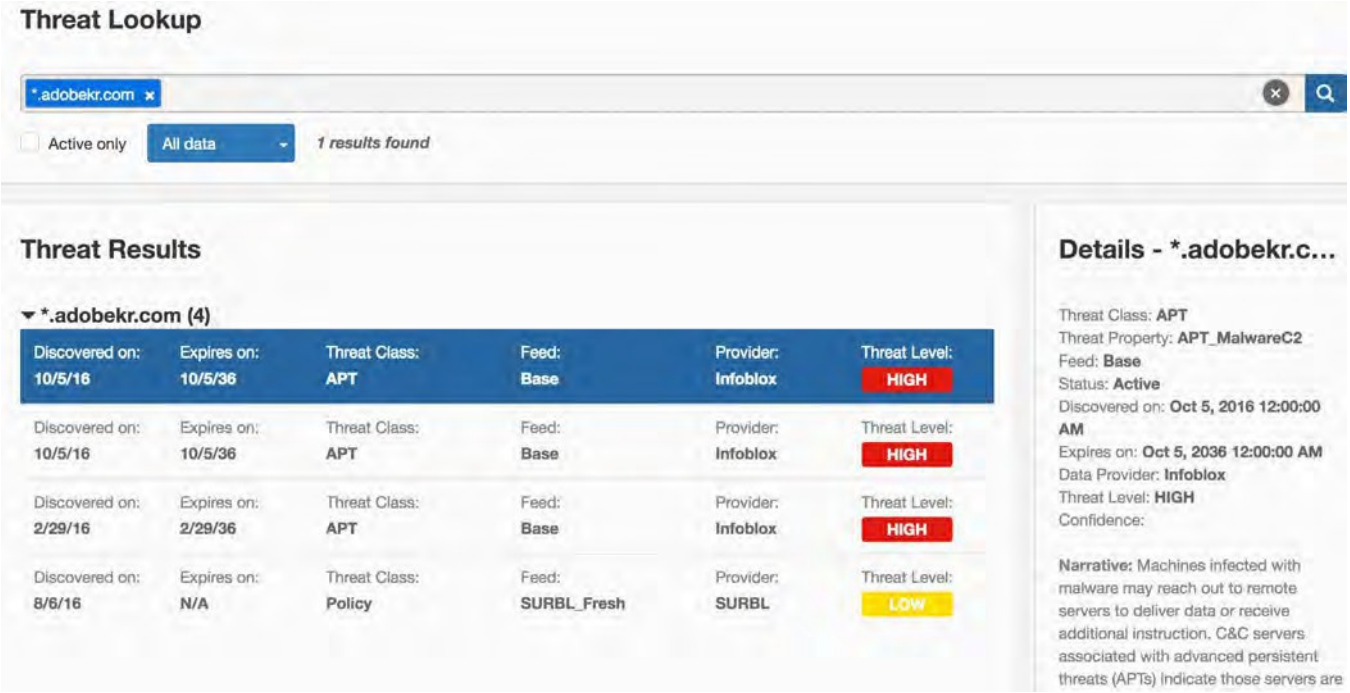
In order to generate a hit against the feed, query a member that has the zone running for “adobekr.com”

If you want more inspiration for testing, once the base.rpz.infoblox.local zone you configured is showing as “Last updated,” you can click the name and download it as a csv file.

Check the syslog for security hits you should see a CEF entry with the domain(s) you are testing, you can also refer to the security dashboard for graphed out results based on the last 30 minutes of traffic.

Portal Investigation

To research suspicious indicators for more information and for context, take the domain from the log entry and use the “Threat Lookup” feature under “Analyze” in tthe op navigation panel.



You can also use IP’s from your logs, be aware that you need to inverse them and take the first octet as the hostmask.

For example: 32.1.0.0.10 becomes 10.0.0.1/32

More investigation can be done in Dossier. Dossier is accessible under **Research** in the Cloud Services Portal.