Infoblox®
CONTROL YOUR NETWORK

Quick Start Guide for Infoblox Threat Intelligence Feed

Copyright Statements

For Open Source Copyright information, see *Appendix C, Open Source Copyright and License Statements* in the *Infoblox NIOS Administrator Guide*.

Trademark Statements

Company Information

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

Product Information

Hardware Models

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

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

Trinzic Appliances: TE-100, TE-810, TE-820, TE-1410, TE-1420, TE-2210, TE-2220, and Infoblox-4010

All Trinzic Rev-1 and Rev-2 appliances

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

Trinzic Reporting: TR-800, TR-1400, TR-2200, and TR-4000

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

Document Version: Rev. A

Document Updated: May 18, 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.

Contents

Preface

This guide describes how to configure RPZ policies and manage at a more granular level how your DNS firewall handles queries to suspicious hostnames. This enables you to effectively detect and block the communications channels for malware, botnets and other cyber security threats.

The preface describes the content and organization of this guide, how to find additional product information, and how to contact Infoblox Technical Support. It comprises the following sections:

Document Overview

This guide describes how to configure a custom policy on your DNS firewalls to handle queries to suspicious hostnames.

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
bold	Indicates anything that you input by clicking, choosing, selecting, typing or by pressing on the keyboard.
`input`	Signifies command line entries that you type.
variable	Signifies variables typed into the GUI that you need to modify specifically for your configuration, such as command line variables, file names, and keyboard characters.

Navigation

Infoblox technical documentation uses an arrow "->" to represent navigation through the GUI. For example, to access member information, the description is as follows:

From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab.

Related Documentation

Other NIOS appliance documentation:

- *Infoblox NIOS Administrator Guide*
- *Infoblox CLI Guide*
- *Infoblox API Documentation*
- *Infoblox CSV Import Reference*
- *Infoblox Safety Guide*

Go to the Infoblox Technical Support web site to access technical documentation. 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, licenses and warranties, 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 NIOS 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, causing you to lose all existing data on the NIOS appliance. You can create new administrator accounts, with or without superuser privileges.

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

Setting Up Infoblox Threat Intelligence Feed

This document provides information about how to set up Infoblox Threat Intelligence Feed. It includes the following sections:

About Infoblox Threat Intelligence Feed

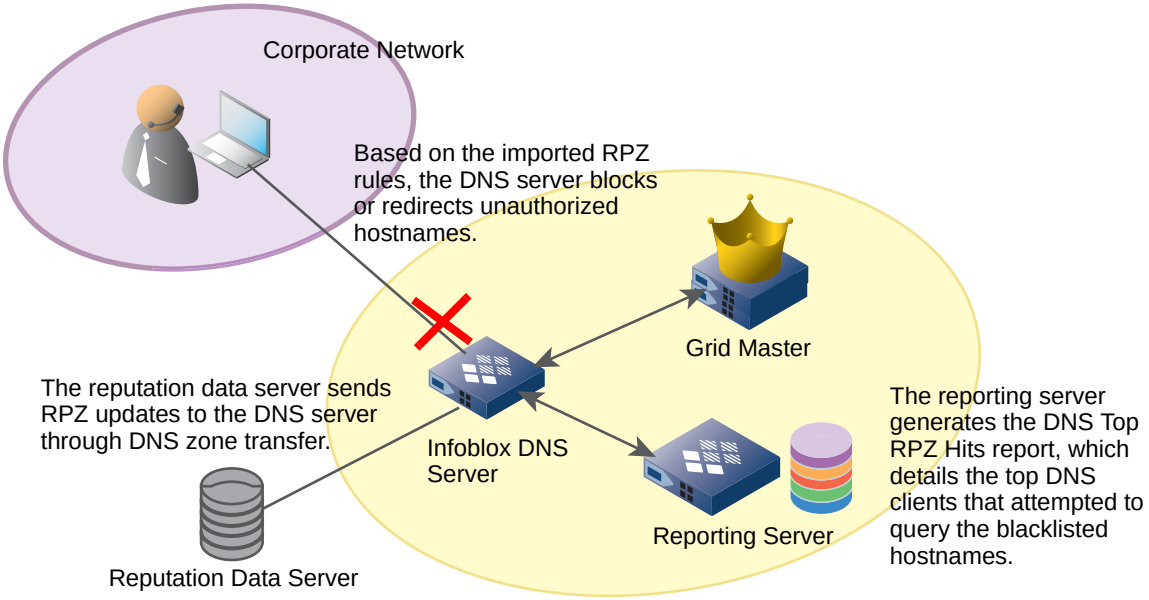
Infoblox Threat Intelligence Feed employs DNS RPZs (Response Policy Zones), a technology developed by ISC (Internet System Consortium) for allowing reputable sources to dynamically communicate domain name reputation so you can implement policy controls for DNS lookups.

On an Infoblox appliance, you can configure RPZs and define RPZ rules to block DNS resolution for malicious or unauthorized hostnames, or redirect clients to a walled garden by substituting responses. You can assign actions to RPZ rules. For example, abc.com can have an action of pass thru or substitute (domain) with the domain xyz.com. You can also configure a Grid member to act as a lead secondary that receives RPZ updates from external reputation sources and redistributes the updates to other Grid members. Infoblox Threat Intelligence Feed supports both IPv4 and IPv6 networks. It also facilitates the detection of malware and APTs (Advanced Persistent Threats) by integrating the NIOS appliance with a FireEye appliance. You can now employ APT mitigation strategy using FireEye as an external threat detection source. For more information about FireEye RPZ, refer to the *Infoblox NIOS Administrator Guide.*

An Infoblox Grid performs RPZ actions for queries that originate from external sources. The name server recursive cache on an RPZ enabled Grid member uses the address of the client from which the query originates to identify if the query is generated from an external source or an internal Grid. If the query originates from a Grid Master or a Grid member that has RPZ license installed, RPZ actions are automatically bypassed for those queries. For RPZ, Infoblox uses the ACL *infoblox-deny-rpz*, which contains a list of addresses for bypassing RPZ actions. The *infoblox-deny-rpz* list excludes Grid members that do not have an RPZ license. Note that RPZ action is performed only once for a single recursion.

As illustrated in *Figure 3.1*, the Infoblox DNS server receives RPZ updates, which include blacklisted hostnames and responses, from a reputation data server through a DNS zone transfer. The appliance then blocks or redirects queries and responses based on the imported RPZ rules. The reporting server can then generate the *Security* reports that details the top DNS clients that have received redirected responses through RPZs, the total number of RPZ hits from a client during an interval, and the FireEye alerts received by the NIOS appliance.

Figure 3.1 Infoblox Threat Intelligence Feed



There are three types of RPZs:

- Local RPZ–A local RPZ is a zone that allows administrators to define multiple response policies locally. Responses sent are based on the defined rules. For information about how to configure local RPZs, refer to the *Infoblox NIOS Administrator Guide*.

- RPZ Feed–An RPZ feed receives response policies from Threat Intelligence feeds and external sources. DNS clients receive responses based on the imported rules from a reputable source, such as a commercial RPZ provider. For information about RPZ feeds, see *Configuring Infoblox Threat Intelligence Feeds* on page 11.
- 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. For information about FireEye integrated RPZ, refer to the *Infoblox NIOS Administrator Guide*.

Note: You can also define custom RPZ policies using the Infoblox Threat Intelligence Feed Custom Feed Zones tool available on the Infoblox Support web site. For more information about this feature, refer to *Infoblox DNS Firewall Custom Feed Zones Tool* section of the *Infoblox NIOS Administrator Guide*.

Account Registration

To use Infoblox DNS Threat Analytics, you must first subscribe to the service. Contact Infoblox sales representatives to sign up. You will receive an email, which allows you to register your account.

To register your account:

1. Click **Get Started** in the welcome email.
2. Complete the following:
   - **Full Name**: Enter your full name.
   - **Phone Number**: Enter the contact phone number.
   - **Password**: Enter the password.
   - **Password Confirmation**: Enter the same password again.
   - Review the end-user license agreement and select the **I accept Infoblox's End User License Agreement** check box.
3. Click **Register**.

Configuring DNS Firewall Clients

Once you register your account successfully, you must configure a Grid member to act as a lead secondary that receives RPZ updates from the Threat Intelligence data server and redistributes the updates to other Grid members.

To register your Grid member as a client:

1. Login to the *https://csp.infoblox.com/home* using the registered email ID and password.
2. In the Infoblox Security Portal, click the **Services** tab. You need to use information in the following fields when configuring the Infoblox Threat Intelligence feeds: **Feeds**, **Distribution Service - US West**, **Distribution Service - US East**, **Key Name**, **TSIG Key**, and **Key Algorithm**. You can copy this information and save it in a text editor of your choice, or you can refer to this information while configuring the Threat Intelligence feeds. For more information, see *Configuring Infoblox Threat Intelligence Feeds* on page 11.
3. Click **Next Step**.
4. Click **Add Client**.
5. In the **Add DNS Firewall Client** dialog box, complete the following:
   - **Name**: Enter the name of the Grid member.
   - **IP Address**: Enter the IP address of the Grid member.
6. Click **Add**.
7. Click **Finish**.

   The Grid member details are added to the client list.

You can do the following:

- Click the Edit icon to edit the Grid member name and the IP address.
- Click the Delete icon to delete the entry.

License Requirements and Admin Permissions

You must install an RPZ license before you can use the RPZ feature. You can install either a temporary or a permanent license on the NIOS appliance. The temporary license provides a 60-day free trial, which can be upgraded to a permanent license. Infoblox provides RPZ licenses that are compatible with each product model. After the license expires, the Threat Intelligence service stops, RPZ feed entries expire, and your network will not receive protection against malicious hostnames.

Note: Apply RPZ licenses only on Infoblox members that have DNS recursion enabled.

Before you install an RPZ license, ensure that the following are completed:

- The entire Grid is running NIOS 6.6 or later.
- Grid members are properly configured and DNS is enabled on the members.

Note: Install RPZ licenses only on Infoblox members that have DNS recursion enabled. For RPZ rules to function properly, you must enable DNS recursion. You can enable DNS recursion at the Grid, member, or DNS view level. For information about how to enable recursion, refer to the *Infoblox NIOS Administrator Guide*.

Setting Up Infoblox Threat Intelligence Feed

For a successful Infoblox Threat Intelligence Feed deployment to protect your endpoint devices and servers from stealthy malware and malicious hostnames, consider the guidelines described in *Best Practices for Configuring RPZs* on page 11. To configure Infoblox Threat Intelligence Feed, complete the following tasks:

1. Install a valid RPZ license on the appliance. For more information about RPZ licenses, see *License Requirements and Admin Permissions* on page 10.

   Note: Ensure that you have installed a valid DNS license on the same appliance.

2. Enable recursive queries for a DNS view, member, or Grid. For information about enabling recursion for RPZs, refer to the *Infoblox NIOS Administrator Guide.*

   Note: Ensure that you enable recursive queries for RPZ rules to take effect.

3. Configure RPZ logging to ensure that all matching and disabled rules for all queries are logged 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. For information about how to set logging categories, refer to the *Infoblox NIOS Administrator Guide*.
4. Complete the following to receive RPZ updates from Threat Intelligence feeds:
   - Configure an RPZ feed, as described in *Configuring Infoblox Threat Intelligence Feeds* on page 11.
   - Download rules from the RPZ feed, as described in *Downloading RPZ Feed Rules* on page 14.

Note: To apply the configured RPZ policies regardless of whether a DNS query requests DNSSEC data, configure the appliance accordingly. For more information about how to configure this, refer to the “Applying Policies and Rules to DNS Queries that Request DNSSEC Data section in the *Infoblox NIOS Administrator Guide*.

5. Test your RPZ configuration and verify that RPZ is functioning properly by viewing the syslog and the **Last Updated** column in the **Response Policy Zones** tab. For more information, see *Testing RPZ Feed Rules* on page 14.

Best Practices for Configuring RPZs

Before configuring RPZs, consider the following best practices to ensure a successful configuration:

- When you enable Infoblox Threat Intelligence Feed, DNS performance for all queries, recursive or authoritative, will be affected.
- For performance reasons, Infoblox recommends that you maintain a reasonable number of zones.
- Do not enable RPZ on multiple layers, such as on DNS client facing servers and forwarders.
- 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 or RPZ feed. 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. For information about how to preview your rules and set logging categories, refer to the *Infoblox NIOS Administrator Guide*.
- 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 servers 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.
- Note that the NIOS blacklist and NXDOMAIN features take precedence over RPZs.
- The name of the zone, which is assigned to an RPZ member, must not exceed 241 characters. When the name exceeds this limit, respective zone fails to load.

Configuring Infoblox Threat Intelligence Feeds

You can configure Threat Intelligence feeds and receive reputation RPZ updates on a regular basis. Infoblox offers subscription services for RPZ updates. Contact your sales representative for pricing and availability information.

The RPZ data is transferred to Grid name servers through zone transfers with or without a TSIG key. To ensure proper authentication and integrity of the feed zone transfers, using a TSIG key is recommended. To propagate RPZs as quickly as possible, the secondary DNS server needs an address to which the RPZ source feed can send NOTIFY messages. For example, if the secondary DNS server is configured behind a NAT, you may want to establish a one-to-one NAT for the lead secondary DNS server so it can receive NOTIFY messages from the RPZ source feed. Otherwise, the lead secondary DNS server will need to periodically poll the RPZ source feed, which could take longer than expected.

Note: To enter IDNs (Internationalized Domain Name) in an RPZ feed, you can use the punycode representation of the IDN.

You can use third party RPZ sources or create your own RPZ sources. You can also configure an RPZ feed with multiple RPZ sources.

To configure RPZ feeds:

1. From the **Data Management** tab, select the **DNS** tab -> **Response Policy Zones** tab, and then click the *Add* icon.
2. When you click the *Add* icon, either the *Add Response Policy Zone Wizard* or the *Add DNS View* wizard is displayed based on the following:
   - When you click the *Add* icon, the *Add Response Policy Zone Wizard* is displayed, if you have not created additional *DNS views* and only have the *default view.*

- If you have configured multiple DNS views, you must drill-down to the corresponding *DNS_View* to assign an RPZ feed. Click the *Add* icon and the *Add Response Policy Zone Wizard* is displayed. To create a new DNS view for your RPZ feed, click the *Add* icon and complete the details in the *Add DNS View* wizard. For information about how to add a DNS view and modify an existing view, refer to the *Infoblox NIOS Administrator Guide*.

3. In the *Add Response Policy Zone Wizard*, select **Add Response Policy Zone Feed**, click **Next** and specify the following:
   - **Name:** Enter the name of the RPZ feed. It can be a combination of alphanumeric characters. You can enter up to 256 characters.
   - **DNS View:** The name of the view that you have selected is displayed by default. You can select a view from the drop-down list to associate it with the RPZ feed.
   - **Policy Override:** Select a value from the drop-down list. You can override the policy actions that are specified in the rule level.
     - **Log Only (Disabled)**–Select this if you want to disable an RPZ rewrite using rules in the RPZ zone. If the response to the recursive query matches any RPZ rule, the rule is logged, but the response will not be altered. You cannot overwrite the response to the user. Note that this option will not override RPZ rules in other RPZ zones, if they take precedence.
     - **None (Given)**–Select this if you want to use the policy from the rule level.
     - **Block (No Data)**–Select this if you want the user to receive a response, which indicates that there is no data.
     - **Block (No Such Domain)**–Select this if you want the user to receive a NXDOMAIN in the response. All the policy actions in an RPZ are replaced with a NXDOMAIN block.
     - **Passthru**–Select this if you want the user to see the actual response without modification. All the policy actions in an RPZ are replaced with the passthru action.
     - **Substitute (Domain Name)**–Select this if you want to replace all the policy actions in an RPZ with the substitution action that is specified.
       - **Domain Name**: This appears only when you select **Substitute (Domain Name)** from the **Policy Override** list. Enter the domain name that you want the client to receive instead of the actual domain name, which is malicious or unauthorized.
   - **Severity**: Select the threat severity level for the RPZ zone. The threat severity you select here determines the severity for the RPZ rule. Select Critical, Major, Warning, or Informational. The default threat severity level is Major. Note that each of these levels is represented by a number in the syslog (8 being Critical and 4 being Informational). When you upgrade to NIOS 7.0.0, the appliance automatically updates the threat severity level to Informational (displayed as 4 in the syslog) for existing RPZ zones. For information about RPZ syslog messages and severity levels, refer to the *Infoblox NIOS Administrator Guide*.
   - **Comment**: Optionally, enter additional information about the RPZ feed.
   - **Disable:** Select the check box to disable an RPZ feed without deleting its configuration. Clear the check box to enable the RPZ feed.
   - **Lock:** Select the check box to lock the RPZ feed so that you can make changes to it and prevent others from making conflicting changes.

     For information about to enable the RPZ feed and how to lock the RPZ feed, refer to the *Infoblox NIOS Administrator Guide*.

4. Click **Next** to associate the RPZ feed with at least one external primary name server and a secondary name server:
   - Define name servers for the RPZ feed. An RPZ feed must have at least one RPZ source as an external primary name server and at least one Grid secondary name server. For external primary servers, specify the following (information that you have copied in a notepad):
     - **Name:** Type a resolvable domain name for the external primary server.
     - **Address:** Enter the name server IP address provided by Infoblox for the RPZ feed (US East/ US West).

— **Use TSIG:** To authenticate zone transfers between the local appliance and the external primary server using a TSIG (transaction signature), select this check box. Infoblox TSIGs use HMAC-MD5 hashes. These are keyed one-way hashes for message authentication codes using the Message Digest 5 algorithm. For details, see *RFC 1321, The MD5 Message-Digest Algorithm*, and *RFC 2104, HMAC: Keyed-Hashing for Message Authentication*.

- **Key name:** Type or paste the name of the TSIG key you want to use. This must be the same name as that of the TSIG key on the external primary server.
- **Key Algorithm:** Select **`hmac-md5`**.
- **Key Data:** Enter the TSIG string provided by Infoblox.
  Note that either the Grid name server or the DNS view must be recursive for RPZ feed. An RPZ feed must have at least one RPZ source as an external primary name server and at least one Grid secondary name server. You can associate a lead secondary with an RPZ feed. Note that a lead secondary may or may not have recursion enabled when it is used only for an RPZ feed. For information about all recursive name servers and how to specify name server groups, refer to the *Infoblox NIOS Administrator Guide*.

Note: Make sure that you provide a valid TSIG key string. The appliance cannot retrieve threat information for invalid TSIG keys.

5. Save the configuration and click **Next** to define extensible attributes. Click **Restart** if it appears at the top of the screen.

Infoblox Threat Intelligence Feed

The Infoblox Threat Intelligence Feed is categorized into pure malicious feeds and combination feeds. All the feeds listed below are set to return NXDOMAIN for items in the feed. Threat data changes are pushed every 20 minutes from the DNS servers and significant changes are typically made every two hours.

The following table lists the Infoblox Threat Intelligence feeds:

Table 3.1 Pure Malicious Feeds

Name	Description
Base (base.rpz.infoblox.local)	Enables protection against known hostnames that are dangerous as destinations, such as APT, Bot, Compromised Host/Domains, Exploit Kits, Malicious Name Servers, and Sinkholes along with bogon IP addresses.
Malware (antimalware.rpz.infoblox.local)	Enables protection against known malicious threats that can take action on or control of your system, such as Malware Command & Control, Malware Download, and active Phishing sites.
Ransomware (ransomware.rpz.infoblox.local)	Enables protection against ransomeware that restricts access to the computer system that it infects, and demands a ransom paid to the creator of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive, while some may simply lock the system and display messages intended to coax the user into paying.

Downloading RPZ Feed Rules

You can perform a zone transfer to transfer the rules from an external primary name server to the RPZ feed. You cannot modify these rules, but you can override the entire ruleset or an individual rule. However, if you import a zone to a local zone, you can edit the rules within a local zone. The feed zone supports NSIP and NSDNAME rules; however local RPZs do not support these rules. To download rules from an external primary name server:

1. From the **Data Management** tab, select the **DNS** tab -> **Response Policy Zones** tab, and then click the corresponding *RPZ Feed*.
2. In the **Export** dialog box, complete the following:
   - **Separator**: Select the separator used in the data file. The default value is **Comma**.
   - Click **Export**.

All the rules are transferred. You can download rules only if the lead secondary has completed at least one zone transfer from the external primary. You can either open the data file or save it to your computer. The rules are displayed for the selected RPZ feed in the *Rule* wizard.

After you have downloaded rules from an RPZ feed, you can test RPZ feed policies, as described in *Testing RPZ Feed Rules* on page 14.

Testing RPZ Feed Rules

After you have downloaded rules from an RPZ feed, you can test the downloaded policies by using the `dig` command and observing log messages that contain redirect or rewrite responses in the syslog. The NIOS appliance supports generation of RPZ log messages in CEF (Common Event Format). Note that non-RPZ messages cannot be generated in CEF. For information about CEF, refer to the *Infoblox NIOS Administrator Guide.*

You must enable the **rpz** option in the **Logging Category** of the *Grid DNS Properties* editor to receive RPZ related messages in the syslog.

To view RPZ log messages in the syslog, you can use the system filter **RPZ Logs** from the **Quick Filter** to filter the messages. Note that only messages in CEF are displayed.

To view RPZ log messages:

1. From the **Administration** tab, select the **Logs** tab -> **Syslog** tab.
2. From the drop-down list at the upper right corner, select the Grid member on which you want to view the syslog.
3. Click **Show Filters** to enable the filters. Select **RPZ Logs** from the **Quick Filter** drop-down list to narrow down the system messages you want to view.

The name server recursive cache makes a syslog entry when an RPZ functionality fails. The syslog message log format is as follows:

`rpz <TYPE> rewrite <QUERY> via <RPZ_RECORD><ERROR_MESSAGE>`

where: `<TYPE>` is one of following RPZ action types: QNAME, IP, NSIP, NSDNAME, CLIENT-IP;

`<QUERY>` is a query record to process;

`<RPZ_RECORD>` is an RPZ record that is used to perform an action to the query;

`<ERROR_MESSAGE>` is a message with error details. Example: `NS address rewrite rrset failed:, concatentate() failed:, NS db_find() failed:, stop on qresult in rpz_rewrite() failed:, stop on unrecognized qresult in rpz_rewrite() failed:`, etc.

To test RPZ feed policies:

1. Open a terminal console on your computer.
2. Type the command **`dig @<your DNS server IP> <queried domain>`**.
3. Go to the **Administration** tab -> **Logs** tab -> **Syslog** tab to view CEF log messages.