Infoblox
NEXT LEVEL NETWORKING

DEPLOYMENT GUIDE

Integration with Rapid7 Nexpose/InsightVM

TABLE OF CONTENTS

Introduction

Infoblox's Outbound REST API integration framework is a new way to send both IPAM data (networks, hosts, leases) and DNS threat data to additional ecosystem solutions. This deployment guide is an update for Rapid7 Nexpose/InsightVM integration using Rapid7's REST API v3. Infoblox and Rapid7 Nexpose/InsightVM together enable security and incident response teams to leverage the integration between vulnerability scanners and DNS security to enhance visibility, manage assets, ease compliance and automate remediation. Thus, improving your security posture while maximizing your ROI in both products.

Prerequisites

The following are prerequisites for Outbound Notifications:

- Infoblox:
    - Infoblox Grid running NIOS 8.1 or higher.
    - Security Ecosystem license.
    - Pre-configured services: DNS, DHCP, RPZ, and Threat Analytics.
    - NIOS API user with the following permissions (access via API only):
        - All Host – RW.
        - All IPv4 DHCP Fixed Addresses/Reservations – RW.
        - IPv6 DHCP Fixed Addresses/Reservations – RW.
- Rapid7:
    - Installed and configured Rapid7 Nexpose/InsightVM solution.
    - Network access from Grid Master or Grid Master Candidate (depending on the configuration) to Rapid7 Nexpose/InsightVM.
    - Support Rapid7 REST API v3.
    - Users credentials on Rapid7 with the following permissions:
        - Specify Scan Targets.
        - Start Unscheduled Scans.
        - "Site Access" to Sites being used.

Limitations

Know limitations:

- Rapid7 Nexpose/InsightVM does not allow modification to a site configuration if a scan for any asset inside the site is performing.
- Rapid7 Nexpose/InsightVM manages discovered assets only by an IP-address.
- Deletion and modification events are not supported.
- Maximum 1000 sites are supported. Templates can delete a discovered asset if a site does not contain more than 1000 discovered assets.

Best Practices

Outbound Notification templates can be found on the Infoblox community site on the partners integration page. After registering an account, you can subscribe to the relevant groups and forums. If additional templates come out, they will be found on the community site.

For production systems, it is highly recommended to set the log level for an end-point to **"Info"** or higher (**"Warning"**, **"Error"**).

Please refer to the Infoblox NIOS Administrator's Guide about other best practices, limitations and any detailed information on how to develop notification templates. The NIOS Administrator's Guide can be found through the Help panel in your Infoblox GUI, or on the Infoblox Support Center.

Workflow

Use the following workflow in order to enable, configure and test outbound notifications:

- Rapid7:
    - Create API user
    - Create Sites
- Infoblox:
    - Install the Security Ecosystem license if not already installed.
    - Check that necessary services DNS, DHCP, RPZ, Threat Analytics are configured.
    - Create Extensible Attributes.
    - Create or download from Infoblox's community web-site session (Rapid7_Nexpose_Session.json), login (Rapid7_Nexpose_Login.json) and logout templates (Rapid7_Nexpose_Logout.json).
        - Add/upload login, logout and after that session template.
    - Create or download from Infoblox's community web-site notification templates (Rapid7_Nexpose_Assets.json, Rapid7_Nexpose_SecEvent.json).
    - Add/upload the notification templates.
    - Add a REST API Endpoint.
    - Add Notifications.
    - Emulate an event, then check the debug log and/or verify changes on the REST API Endpoint.

Before you get Started

Download Templates from the Infoblox's Community Web-site

Outbound Notification templates are an essential part of the configuration. Templates fully control the integration and steps required to execute the outbound notifications. Detailed information on how to develop templates can be found in the NIOS Administrator's guide.

Infoblox does not distribute any templates (out-of-the-box) with the NIOS releases. Templates **"Rapid7_Nexpose_SecEvent"** and **"Rapid7_Nexpose_Assets"** are available on the Infoblox community web-site. Templates for Rapid7 are located in the Rapid7 group. You can find other templates posted in the **"**API & Integration**"** forum.

Templates may require additional extensible attributes, parameters or WAPI credentials to be created or defined. The required configuration should be provided with a template. Don't forget to apply any changes required by the template before testing a notification.

Create Extensible Attributes

Rapid7 Nexpose/InsightVM Outbound Notification templates use different extensible attributes to adjust the templates behavior. You can download and use a sample php-script provided with the templates or create them manually. The extensible attributes are described in a table below.

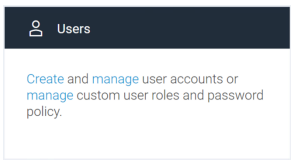
Table 1. Extensible Attributes

Extensible Attribute	Description
R7_Sync	Defines if an object should be synced with Rapid7 Nexpose/InsightVM. Possible values: true, false
R7_SyncedAt	Contains date/time when the object was synchronized, updated by the assets management template
R7_NetToSite	Defines if a network should be added to a site (as shown on the video). Possible values: true, false. If R7_NetToSite is false but R7_Sync is true, R7_SiteID will be updated.
R7_RangeToSite	Defines if a range should be added to a site. Possible values: true, false. If R7_NetToSite is false but R7_Sync is true, R7_SiteID will be updated.
R7_ScanOnEvent	Defines if an asset should be scanned if RPZ or DNS Tunneling events were triggered
R7_ScanOnAdd	Defines if an asset should be scanned immediately after creation
R7_ScanTemplate	Defines a Rapid7 Nexpose/InsightVM template which should be used for scans initiated by an Infoblox appliance. Possible values: default, full-audit, full-audit-without-web-spider etc (internal templates IDs). If set to “default” then a template configured for a site will be used.
R7_Site	Defines a Site name
R7_SiteID	Contains an internal site ID. Updated automatically. If the value was inherited from a top level, templates will bypass a few steps retrieving this ID. It should not be manually updated.
R7_LastScan	Contains a date when an asset was scanned last time by a request from Infoblox
R7_AddByHostname	Defines if a host should be synced with Rapid7 Nexpose/InsightVM using a hostname. The hostname should be resolvable by Nexpose/InsightVM. Possible values: true, false

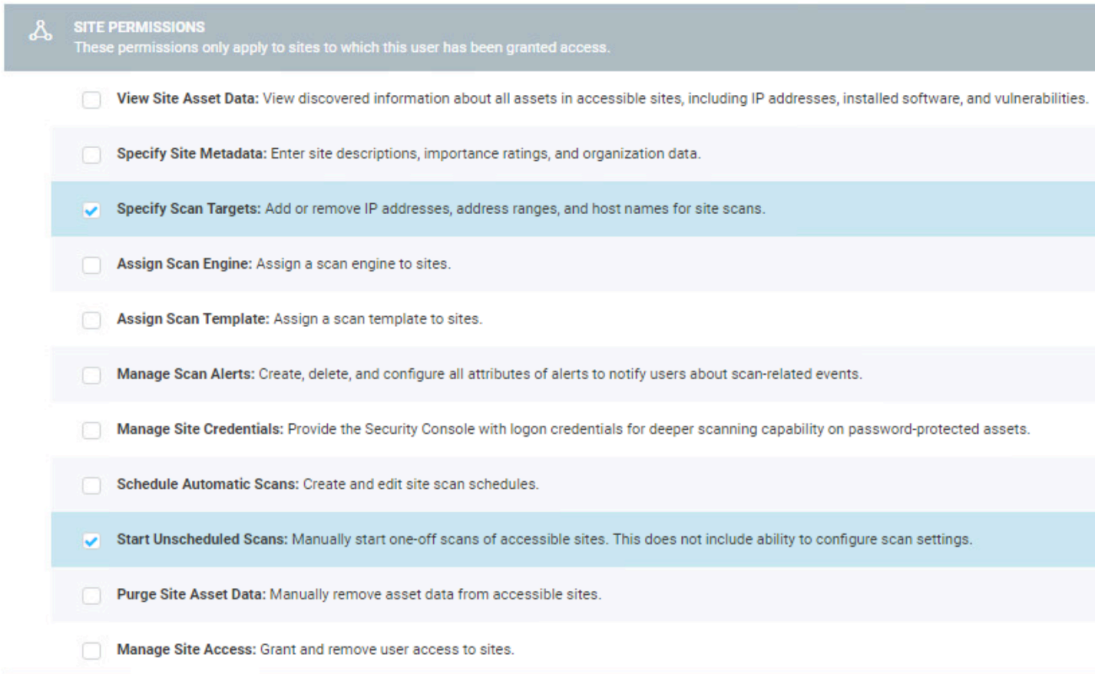
Rapid7 Nexpose/InsightVM Configuration

Configure API User

1. Navigate to **“Administration”** → **“Users”** and click the **“Create”** text.



2. Under the **“GENERAL”** tab enter in the basic user information for the user.
3. Under the **“ROLES”** tab select **“Specify Scan Targets”** and **“Start Unscheduled Scans”** under the **“SITE PERMISSIONS”**.

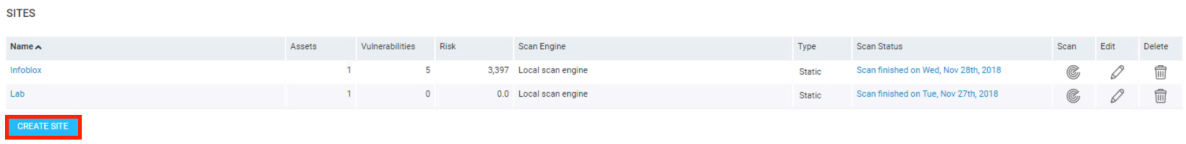


4. Under the **“SITE ACCESS”** tab select **“Create a custom list of sites that this user can access”** and click the **“SELECT SITES”** button and add the sites infoblox should have access to.

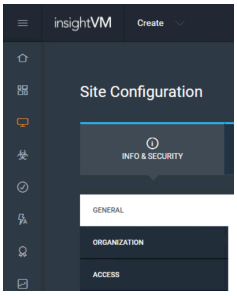
Create Sites

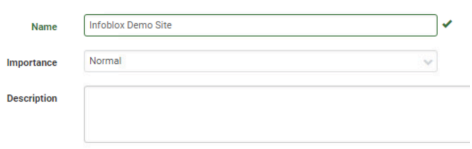
Creating a new site is optional If a site is already created and being used, however if a new site is needed use the following steps:

1. Navigate to the Home tab and click the **“CREATE SITE”** button.

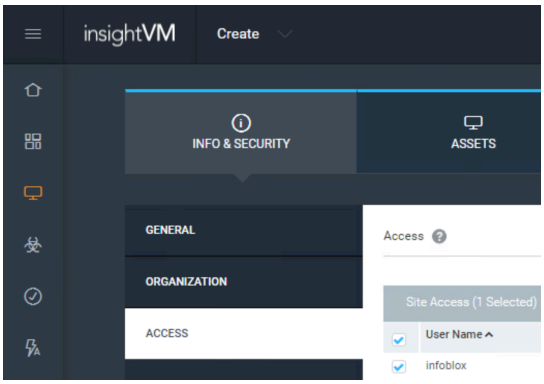


2. From **“INFO & SECURITY”** → **“GENERAL”** enter a name for the site that is not currently being used by other sites

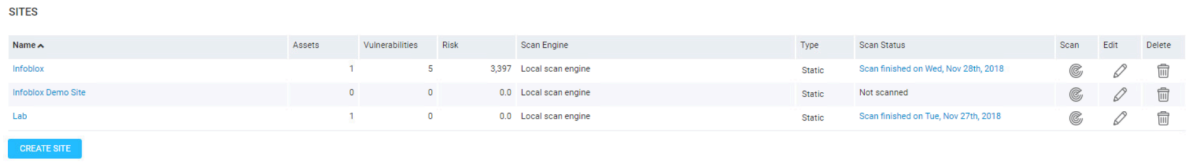




3. Under **“ACCESS”** choose the user account being used for access from Infoblox.



4. Click **“Save”** when finished.



Infoblox NIOS Configuration

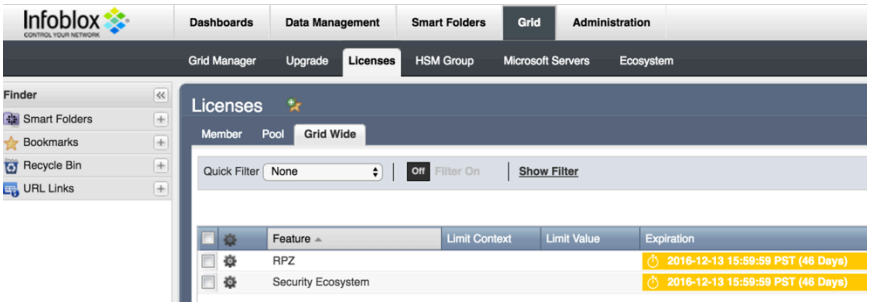
Infoblox Permissions

The Infoblox and Rapid7 integration requires a few permissions for the integration to work. Navigate to **“Administration”** → **“Administrators”** and add a **“Roles”**, **“Permissions”**, **“Groups”** and **“Admins”** to include permissions that are required for the integrations. When creating a new group, under the **“Groups”** tab, select the **“API”** interface under the **“Roles”** → **“Allowed Interfaces”** category.

Check if the Security Ecosystem License is Installed

Security Ecosystem License is a “**Grid Wide**” License. Grid wide licenses activate services on all appliances in the same Grid.

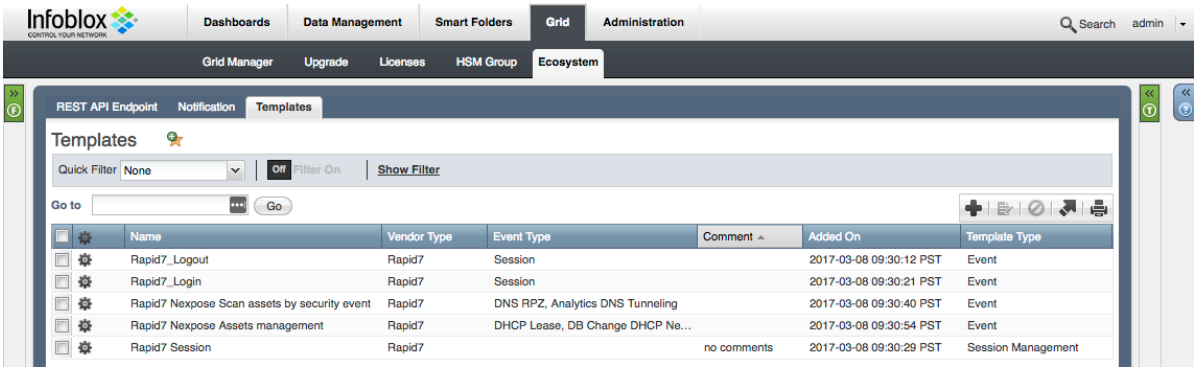
In order to check if the license was installed navigate to **“Grid”** → **“Licenses”** → **“Grid Wide”**.



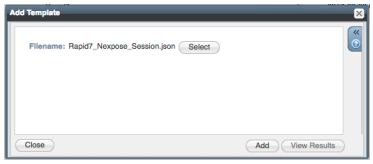
Add/Upload Templates

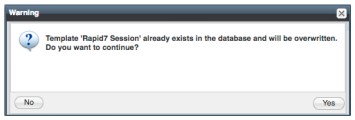
In order to upload/add templates:

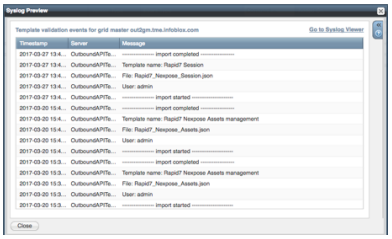
1. Navigate to “**Grid**” → “**Ecosystem**” → “**Templates**”, and press “**+**” or “**+ Add Template**” buttons.



2. Press the **“Select”** button on the **“Add template”** window.
3. If a template was previously uploaded, press **“Yes”** to overwrite the template.
4. **Upload** Press the **“Select”** button on the **“Upload”** window. The standard file selection dialog will be opened.
5. Select the file and press the **“Upload”** button on the **“Upload”** window.





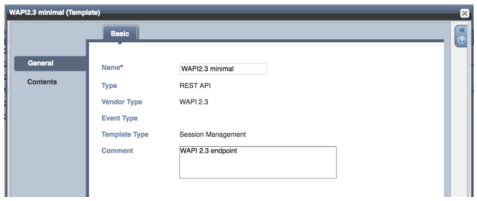


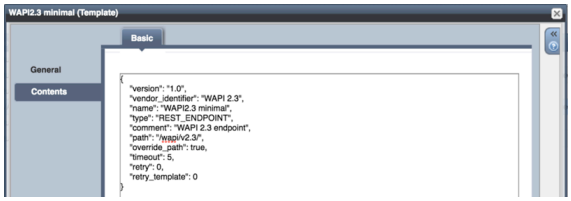
6. Press the **“Add”** button and the template will be added/uploaded.
7. You can review the uploaded results in the syslog or by pressing the **“View Results”** button.
8. There is no difference between uploading session management and action templates.

Modifying Templates

NIOS provides the facility to modify the templates via the web-interface:

1. Navigate to **“Grid”** → **“Ecosystem”** → **“Templates”**, and then press the gear icon next to the template you want to modify.
2. Press the **“Edit”** button to open up the **“Template”** window.





The template editor is a simple interface for making changes to templates. It is recommended to only use the template editor to make minor changes. You can also edit, cut and paste template snippets from a text editor of your choice.

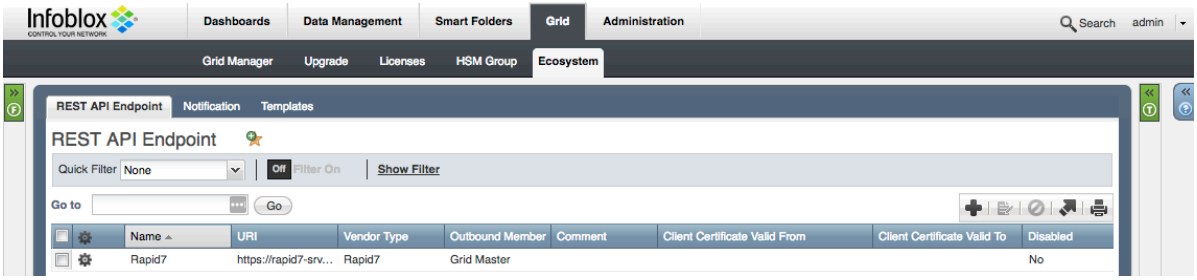
Note: You cannot delete a template if it is used by an endpoint or by a notification.

Add a REST API Endpoint

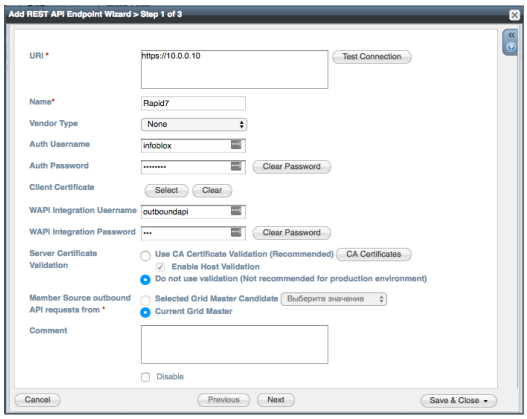
A **"REST API Endpoint"** is basically a remote system which should receive changes based on a notification and a configured template. A Grid, for example, can not only send notifications, it can also receive the notifications from itself (e.g. for testing purposes).

In order to add REST API Endpoints:

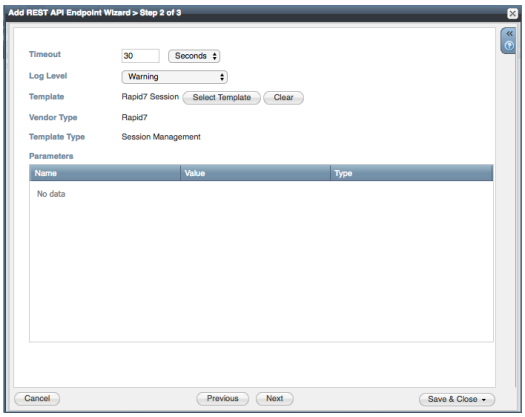
1. Navigate to **"Grid"** → **"Ecosystem"** → **"Outbound Endpoints"** and press **"+"** or **"+ Add REST API Endpoint"** buttons. The **"Add REST API Endpoint Wizard"** window will open.



2. The URI and Name for the appliance you are integrating with are required.
3. The URI should be the IP of the appliance you are integrating with, with the correct URI scheme.
4. Specify **"Auth Username"**, **"Auth Password"** (Rapid7 Nexpose/InsightVM Web Service account credentials), **"WAPI Integration Username"** and **"WAPI Integration Password"** (NIOS credentials).



5. (Optional) For debug purposes only: Under **"Session Management"**, set **"Log Level"** to **"Debug"**.



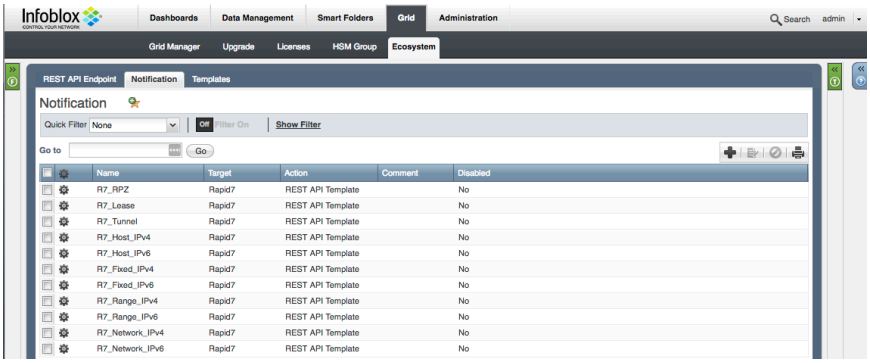
When possible, it is recommended to send notifications from a Grid Master Candidate instead of from the Grid Master.

Add a Notification

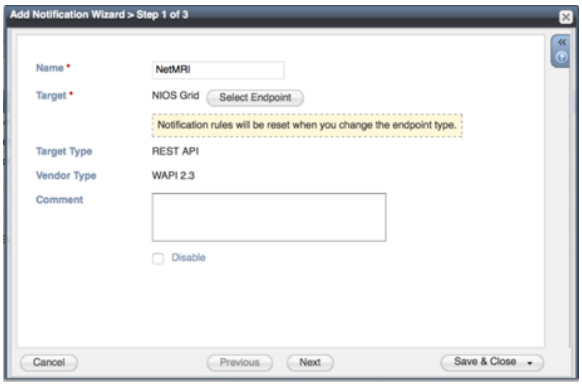
A notification is a link between a template, an endpoint, and an event. In the notification you define by which event triggers the notification, which template is executed and with which API endpoint the Grid will establish a connection to. The Rapid7 templates support all available notifications. In order to simplify the deployment, create only required notifications and use relevant filters. It is highly recommended to configure deduplication for RPZ events and exclude a feed automatically populated by Threat Analytics.

An endpoint and a template must be added before you can add a notification.
In order to add notifications:

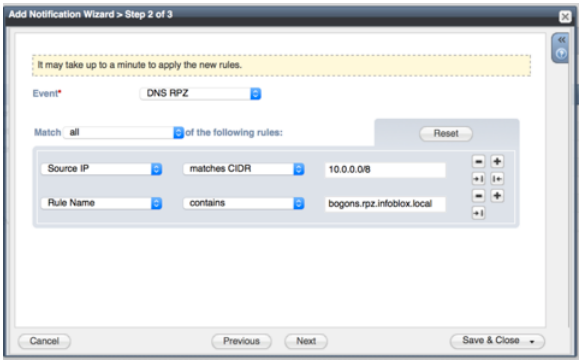
1. Navigate to **"Grid"** → **"Ecosystem"** → **"Notification"** and press **"+"** or **"+ Add Notification Rule"** then the **"Add Notification Wizard"** window will open.



2. Specify the notification's name and select an endpoint (Target), click **"Next"**.



3. Select an event type and define a filter. Note: For optimal performance, it is best practice to make the filter as narrow as possible. Click **"Next"**.

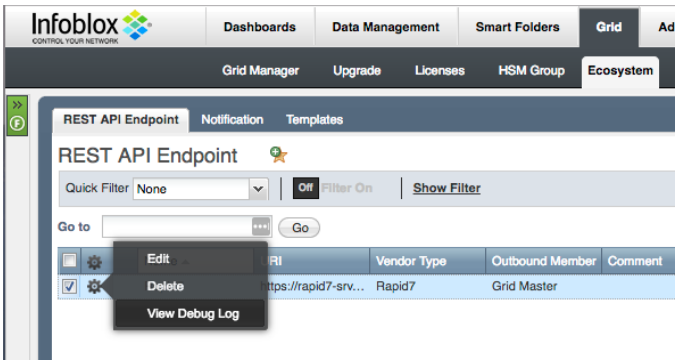


4. (For RPZ notifications only) Check **"Enable RPZ event deduplication"** and specify relevant parameters. Click **"Next"**.
5. Select a relevant template and specify the template's parameters if any are required. Click **"Save & Close"**.

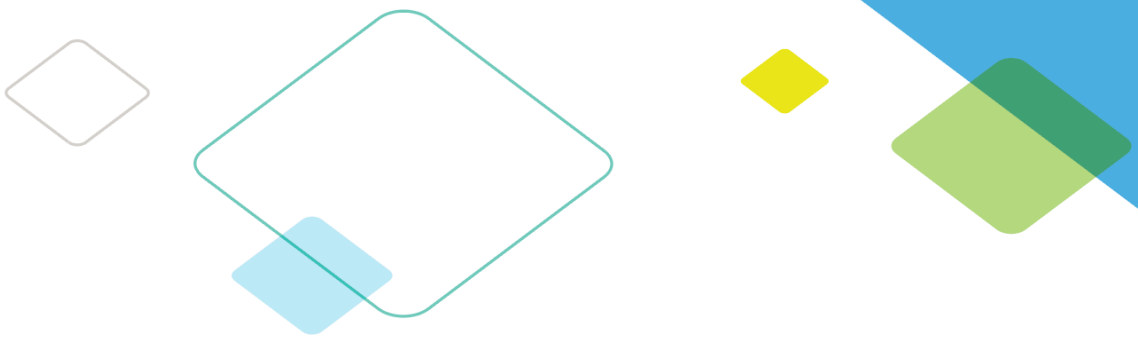
Check the Configuration

You can now emulate an event for which a notification was added (click on a gear icon next to the notification and select **"Test Rule"**). E.g create a host record or add a DHCP lease. If you have the debug log enabled, you can check it for any problems or errors.

To check a debug log for an endpoint, go to **Grid → Ecosystem → REST API Endpoints**, click on the gear icon and select **"View Debug Log"**.



Depend on a browser the debug log will be downloaded or opened in a new tab, you may need to check your popup blocker settings.



Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 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