Infoblox
CONTROL YOUR NETWORK

DEPLOYMENT GUIDE

Outbound API Integration with Rapid7 Nexpose

Contents

Introduction

Infoblox's Outbound REST API integration framework is a new way to updates to both IPAM data (networks, hosts, leases) and DNS threat data into additional ecosystem solutions. Infoblox and Rapid7 Nexpose together enable security and incident response teams to leverage the integration of 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 API notifications:

- Infoblox Grid running NIOS 8.1 or higher.
- Security Ecosystem license.
- Pre-configured services: DHCP, RPZ, Threat Analytics.
- Installed and configured Rapid7 Nexpose solution.
- Users credentials on Rapid7 Nexpose and NIOS.
- Network access from Grid Master or Grid Master Candidate (depending on the configuration) to Rapid7 Nexpose

Limitations

Know limitations:

- Rapid7 Nexpose does not allow modifying a site configuration if a scan for any asset included to this site is performing.
- Rapid7 Nexpose manages discovered assets only by an IP-address.
- Deletion of merged networks or ranges is not supported.
- Maximum 1000 sites are supported. Templates can delete a discovered asset if a site does not contain more than 1000 discovered assets.
- Provided templates do not support "MODIFY" action.

Best Practices

Outbound API templates can be found on the Infoblox community site. After registering an account, (https://community.infoblox.com) you can subscribe to the relevant groups and forums.

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 Infoblox's NIOS Administration guide about other best practices, limitations and any detailed information on how to develop notification templates.

Workflow

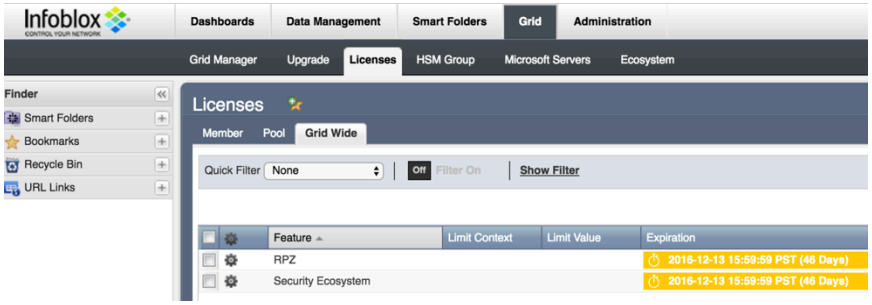
Use the following workflow in order to enable, configure and test outbound notifications:

- Install the Security Ecosystem license if it was not installed.
- Check that necessary services 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.

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 go to **Grid → Licenses → Grid Wide**.

Download templates from the Infoblox's community web-site

Outbound API notifications template is 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 guide.

Infoblox does not distribute any templates with the NIOS releases (out-of-box). Templates are available on the Infoblox community web-site. The templates for integration with Rapid7 are located in the Rapid7 group (https://community.infoblox.com/t5/Qualys/gp-p/Rapid7). Other templates are posted in "API & Integration" forum (https://community.infoblox.com/t5/API-Integration/bd-p/API_Integration).

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

Create Extensible Attributes

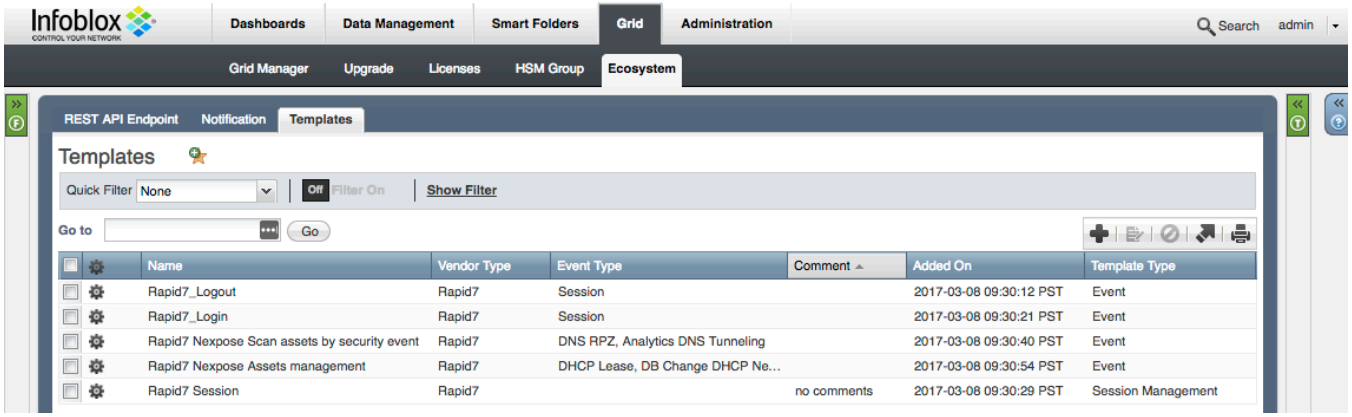
Rapid7 Nexpose outbound API notifications templates use different extensible attributes to adjust the templates behavior. You can download and use a sample php-script provided with the templates or create them manually. The extensible attributes are described in a table below.

Extensible Attribute	Description
R7_Sync	Defines if an object should be synced with Rapid7 Nexpose. 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 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 using a hostname. The hostname should be resolvable by Nexpose. Possible values: true, false

Add/upload templates

In order to upload/add templates go to **Grid → Ecosystem → Templates,** and press “**+**” or **“+ Add Template**” buttons.



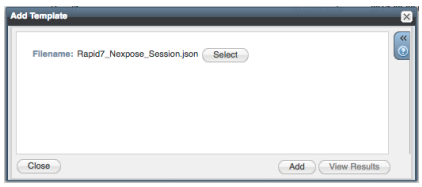
The “Add template” windows will open.

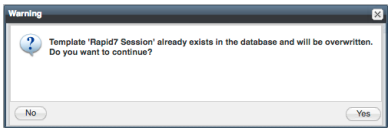
If the template was previously uploaded, check the “Overwrite the existing template” option.

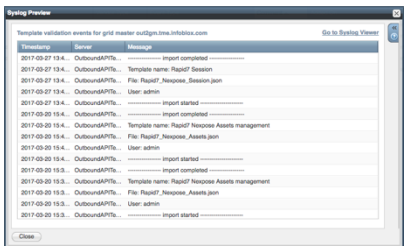
Press the “Select” button on the “Add template” window,

Press the “Select” button on the “Upload” window. The standard file selection dialog will be opened.

Select the file and press the “Upload” button on the “Upload” window.







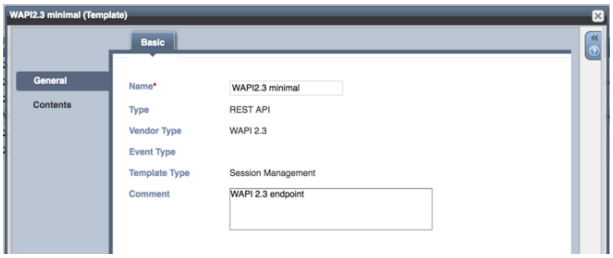
Press the “Add” button and the template will be added/uploaded.

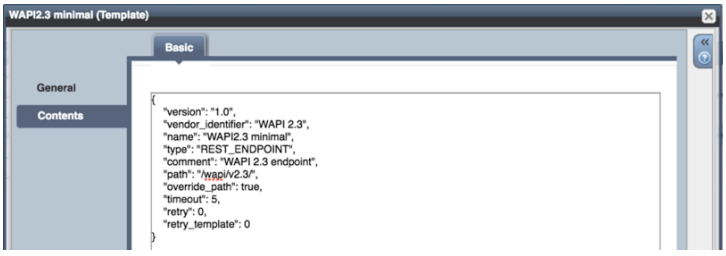
You can review the upload results in the syslog or by pressing “View Results” button.

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.



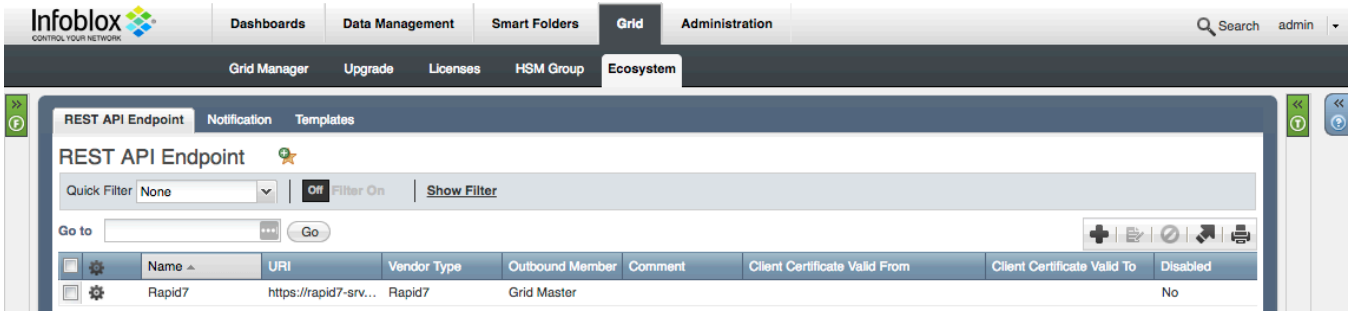


The template editor provides a simple interface to change a template, so it is recommended to use it only when making minimal changes. You can also edit, cut and paste template snippets from the text editor of your choice.

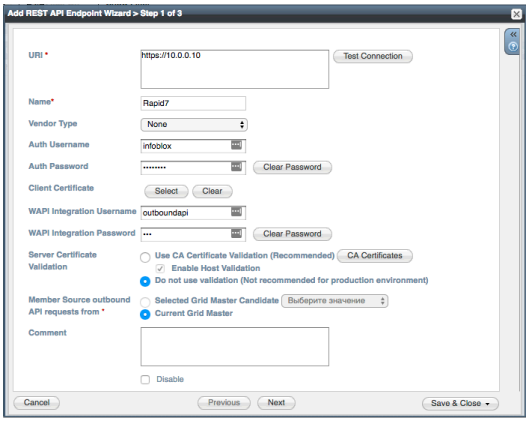
Please be aware that you cannot delete a template if it is used by an endpoint or by a notification.

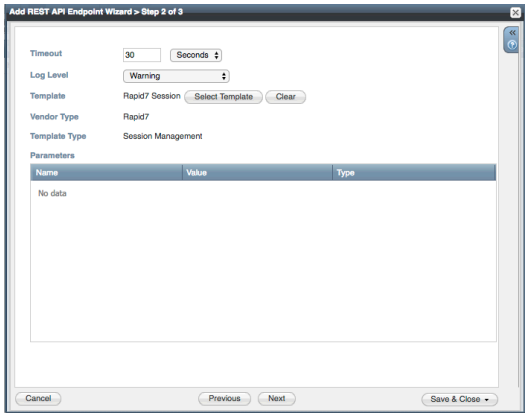
Add a REST API Endpoint

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 go to **Grid → Ecosystem → REST API Endpoints** and press "**+**" or "**+ Add REST API Endpoint**" buttons.





The "Add REST API Endpoint Wizard" window will open. The URI and Name fields are the required fields.

Specify "Auth Username", "Auth Password" (Rapid7 credentials), "WAPI Integration Username" and "WAPI Integration Password" (NIOS credentials).

For debug purposes (during initial configuration only) set Log Level to "Debug".

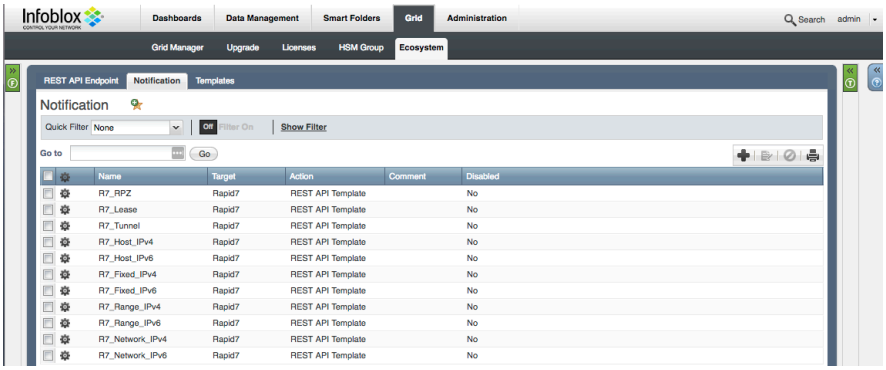
It is recommended to send notifications from a Grid Master Candidate if there is one available instead of Grid Master.

Please be aware that “Test Connection” only checks communication (establish TCP connection with a remote system) with the URI. It does not check the authentication/authorization credentials.

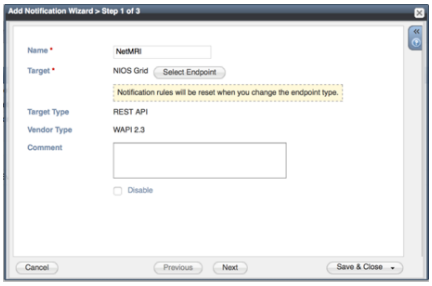
Add a Notification

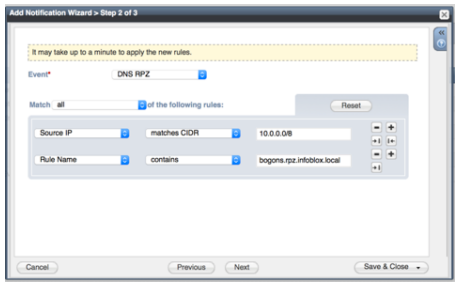
A notification is a link between a template, an endpoint, and an event. In the notification you define by which event triggers the notification, which template is executed and with which API endpoint the Grid will establish a connection to. The Rapid7 templates support all available notifications. In 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 go to **Grid → Ecosystem → Notification** and press “**+**” or **“+ Add Notification Rule**” buttons.





“Add Notification Wizard” window will open.

On the first step: input the notification’s name and select an endpoint (Target).

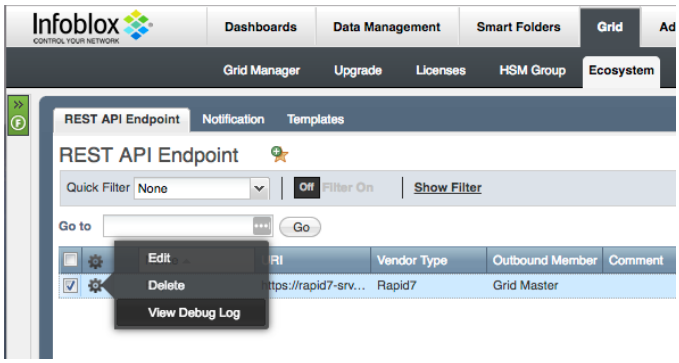
On the second step: select an event type and define a filter. From the performance perspective it is the best practice to make filter as narrow as possible.

On the third step select a relevant template and specify templates parameters if any required.

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.