

DEPLOYMENT GUIDE

Integration with ServiceNow

Outbound API

Contents

| | |
|----------------------------------------------------------------|-----------|
| Contents | 2 |
| Prerequisites..... | 3 |
| Known Limitations | 3 |
| Best Practices..... | 3 |
| Configuration | 4 |
| Workflow | 4 |
| Before you get Started..... | 4 |
| Download Templates from the Infoblox Community Web-Site | 4 |
| Create Extensible Attributes | 4 |
| Editing Instance Variables | 5 |
| Supported Notification | 5 |
| Adding Permissions | 6 |
| ServiceNow Configuration | 6 |
| Adding Categories and Subcategories | 6 |
| Adding and Removing Fields for Incidents..... | 7 |
| Adding and Removing Fields for Assets | 8 |
| Infoblox NIOS Configuration | 10 |
| Check if the Security Ecosystem License is Installed | 10 |
| Add/Upload Templates | 10 |
| Modifying Templates | 12 |
| Add a Rest API Endpoint | 13 |
| Add a Notification | 14 |
| Check the Configuration..... | 16 |
| Summary | 17 |
| Additional References | 17 |
| Annex | 18 |
| ServiceNow Incident Table Data Allocation | 18 |
| ServiceNow Asset Table Data Allocation..... | 18 |
| Infoblox Objects to ServiceNow Tables Association | 19 |

Introduction

Infoblox and ServiceNow: Modernizing the IT service management outlook

Consolidating your on-premise IT tools to a modern, easy-to-use service management solution in the cloud by:

- **Resolving Network Issues at light speed:**
Eliminate calls before they occur with self-service, proactively prevent issues by assessing product or service health in real time, and engage the right resources to fix issues fast.
- **Consumerize the Employee Network Experience:**
Provide a single place for network and security teams to quickly and easily get the services they need.
- **Build Business network and security decisions at light speed:**
Automate processes and orchestrate actions across the network enterprise, reuse components and integrations, and delegate application development with easy-to-use resources and drag-and-drop tools.
- **Eliminate network Service Outages:**
Proactively identify network and security issues and pinpoint disruptions with automated remediation.

Prerequisites

The following are the prerequisites required for the integration using Outbound API notifications:

- Infoblox:
 - NIOS 8.3 or higher.
 - Security Ecosystem License.
 - Outbound API integration templates.
 - Prerequisites for the templates (e.g. configured and set extensible attributes. For more details, refer to the Before you get started section.).
 - Pre-configured required services: DNS, DHCP, RPZ, Threat Analytics, Network Insight, Threat Protection, Network Discovery.
 - NIOS API user with the following permissions (access via API only):
 - All Host – RW.
 - All IPv4 DHCP Fixed Addresses/Reservations – RW.
 - All IPv6 DHCP Fixed Addresses/Reservations – RW.
 - All IPv4 Networks – RW.
 - All IPv6 Networks – RW.
- ServiceNow:
 - Kingston Version or later.
 - Incident Management (For the SNOW_Assets.json template).
 - CMDB (Configuration Management Database) (For the SNOW_SIR.json template).
 - Security Operations (For the SNOW_SIR.json template).

Known Limitations

The current templates support DNS Firewall(RPZ), Advanced DNS Protection (ADP), Network Discovery, Threat Insight (DNS Tunneling), Host IPv4, Host IPv6, Fixed address IPv4, Fixed address IPv6, Network IPv4, Network IPv6 and Discovery events only. If additional templates come out they will be found on the community site.

Best Practices

Outbound API 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.

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 portal.

Configuration

Workflow

- ServiceNow:
 1. Create an API user.
 2. Add categories and subcategories.
 3. Add Fields for assets and incidents.
- Infoblox:
 1. Install the Security Ecosystem license if it was not previously installed.
 2. Check that the necessary services and features, that include DNS, DHCP, RPZ ,Threat Analytics, Threat Protection, Discovery are properly configured and enabled.
 3. Create the required Extensible Attributes.
 4. Download (or create your own) notification templates (SNOW_Security.json, SNOW_Assets.json, SNOW_ADP.json, SNOW_Discovery.json and SNOW_SIR.json) from the Infoblox community web-site.
 5. Add the templates.
 6. Add a REST API Endpoint:
 7. Add Notifications.
 8. Emulate an event, check Rest API debug log and/or verify changes on the grid.

Before you get Started

Download Templates from the Infoblox Community Web-Site

Outbound API 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 are available on the Infoblox community web-site. Templates for the ServiceNow integration will be located in the "Partners Integrations". 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

For this integration, the following Extensible Attributes need to be created on the grid.

| Extensible Attributes | Description |
|--------------------------------------|------------------------------------------------------------------------------|
| ServiceNow_LastIncidentSentAt | Provides the last time an asset sent an incident to ServiceNow. |
| ServiceNow_Add_Incident | True or False. Defines if an object should create an incident on ServiceNow. |
| ServiceNow_Event_ID | Provides the Incident number of the last Incident sent to ServiceNow. |
| ServiceNow_SYS_ID | Provides the unique ID of the asset on ServiceNow. |

| | |
|--------------------------------------|----------------------------------------------------------------------------------------------------|
| ServiceNow_Sync | True or False. Defines if and asset should be added to ServiceNow when created. |
| ServiceNow_SyncedAt | Internal attribute. Provides the time that an asset was created on ServiceNow. |
| ServiceNow_Table | Internal attribute. Provides the ServiceNow table that an asset was added to. |
| ServiceNow_Location | Custom field. Determines the location field for the ServiceNow table upon creation. |
| ServiceNow_Discov_AddSecurInc | True or False. Defines if a Security incident should be created for a Discovery event. |
| ServiceNow_Discov_AllNew | True or False. Process and create incidents for discovery events of all devices or only unmanaged. |

Editing Instance Variables

ServiceNow templates use an instance variable to adjust the templates' behavior. Instance variables can be entered through the grid GUI at **"Grid" → "Ecosystem" → "Notification"** and then selecting the notification you created at **"Edit" → "Templates"**.

| Instance Variable | Description |
|-------------------|--------------------------------------------------------|
| Severity | 1, 2, or 3: Defines the severity of created incidents. |

Supported Notification

A notification can be considered as a "link" between a template, an endpoint and an event. In the notification properties, you define which event triggers the notification, which template is executed and with which API endpoint NIOS will establish the connection to. The ServiceNow templates support a subset of available notifications (refer to the limitations chapter in this guide for more details). In order to simplify the deployment, only create required notifications and use the relevant filters. It is highly recommended to configure deduplication for RPZ events and exclude a feed that is automatically populated by Threat Analytics.

| Notification | Description |
|----------------------------------|-----------------------------------------------|
| DNS RPZ | DNS queries that are Malicious or unwanted. |
| DNS Tunneling | Data exfiltration that occurs on the network. |
| Object Change Fixed Address IPv4 | Added/Deleted fixed/reserved IPv4 objects. |
| Object Change Fixed Address IPv6 | Added/Deleted fixed/reserved IPv6 objects. |
| Object Change Host Address IPv4 | Added/Deleted Host IPv4 object. |
| Object Change Host Address IPv6 | Added/Deleted Host IPv6 object. |

| | |
|----------------------------|--------------------------------|
| Object Change Network IPv4 | Added/Deleted IPv4 networks. |
| Object Change Network IPv6 | Added/Deleted IPv6 networks. |
| Security ADP | Advanced DNS Protection events |
| Network Discovery | Object Change Discovery Data |

Adding Permissions

The Infoblox and ServiceNow 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 which can be found in the prerequisites. When creating a new group, under the **“Groups”** tab, select the **“API”** interface under the **“Allowed Interfaces”** category. The NIOS API user is required to have the following permissions (access via API only):

- All Host – RW.
- All IPv4 DHCP Fixed Addresses/Reservations – RW.
- All IPv6 DHCP Fixed Addresses/Reservations – RW.
- All IPv4 Networks – RW.
- All IPv6 Networks – RW.

ServiceNow Configuration

Adding Categories and Subcategories

1. The ServiceNow endpoint configuration requires categories and subcategories that may not already be created. In order to add a category and subcategories: Navigate to **“Incidents” → “Create New”**, then right click on **“Category”** and click Configure Choices.

The screenshot shows the ServiceNow 'Incident' form. On the left is a navigation menu with options like 'Self-Service', 'Service Desk', 'Incident', 'Create New', 'Assigned to me', 'Open', 'Open - Unassigned', 'Resolved', 'All', 'Overview', 'Critical Incidents Map', and 'Administration'. The main form area is titled 'Incident New record'. It contains fields for 'Number' (INC0010069), 'Contact type' (None), 'State' (New), 'Impact' (3 - Low), 'Urgency' (3 - Low), 'Priority' (5 - Planning), 'Assignment group', and 'Assigned to'. A dropdown menu is open for the 'Category' field, showing options: 'Inquiry / Help', 'Configure Label', 'Configure Dictionary', 'Configure Styles', 'Configure Choices' (which is highlighted), 'Show Choice List', 'Show - 'category'', and 'Watch - 'category''. Below the form is a 'Related Search Results' section with a search bar.

2. At the bottom enter **“Network Security”** and click the **“Add”** button.
3. Click save to return to the **“Incident New record”** page.

Configuring Category Choices

Tailoring: incident.category
Incident

Available

Selected

Inquiry / Help
Software
Hardware
Network
Database
Network Security

Add
Remove

Move up
Move down

Save Cancel

Enter new item: Network Security Add

time(ms): 1195, Network: 12, server: 315, browser: 868

4. Right click on Subcategory and click Configure Choices.
5. At the bottom enter **"DNS RPZ"** then click the **"Add"** button, then enter **"DNS TUNNEL"** and click the **"Add"** button again.
6. Click save to return to the save the results.

Configuring Subcategory Choices

Tailoring: incident.subcategory
category: inquiry
Incident

Available

Selected

Tunnel
RPZ

Antivirus
Email
Internal Application
DNS RPZ
DNS TUNNEL

Add
Remove

Move up
Move down

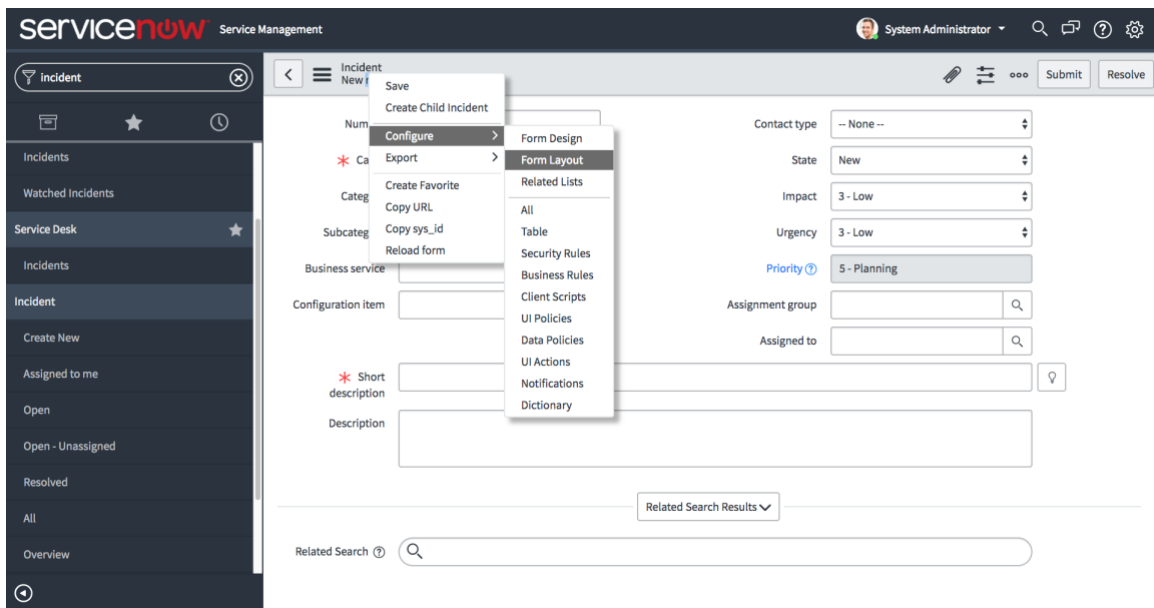
Save Cancel

Enter new item: DNS TUNNEL Add

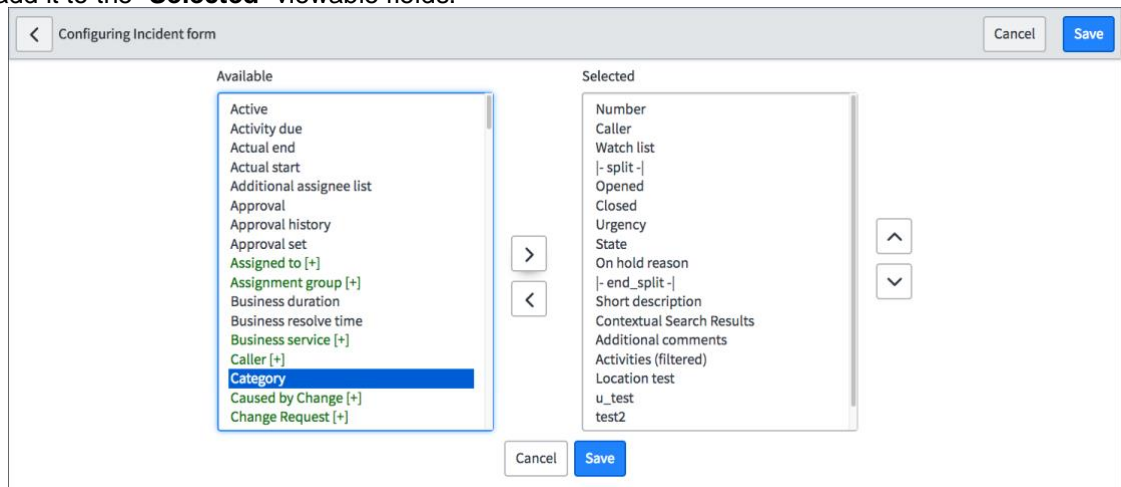
me(ms): 1208, Network: 13, server: 246, browser: 949

Adding and Removing Fields for Incidents

1. Navigate to **"Incident"** → **"Create New"** then right click on **"Incident New record"** and choose **"Configure"** → **"Form Layout"**.



2. Select the fields listed in the [ServiceNow Incident Table](#) under the “Annex”, then click the “>” button to add it to the “Selected” viewable fields.



3. In the same window type “Location” in the **Create new field** form under name, then click the “Add” button.

Form view and section

View name

Section

Create new field

Name

Type

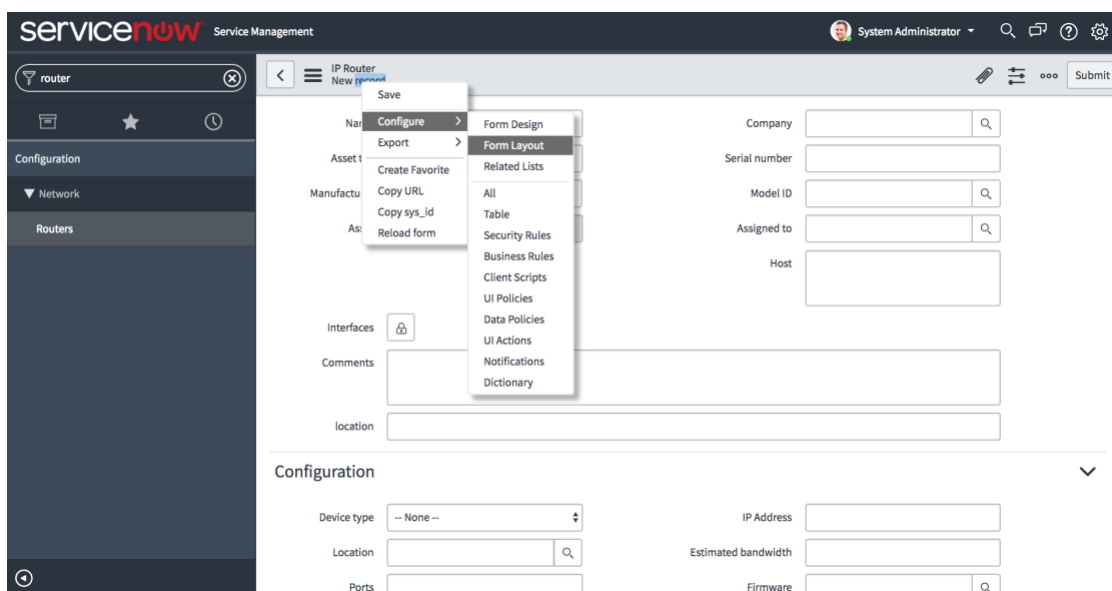
Field length

Add

4. Once you have added the fields you would like to view, click “Save”.

Adding and Removing Fields for Assets

1. Navigate to “Network” → “Routers” → “New” then right click on “IP Router New record”, then choose “Configure” → “Form Layout”.



2. Select the fields listed in the [ServiceNow Incident Table Data Allocation](#)

| Field Name | Purpose |
|-------------------|----------------------------------------------------------------------------|
| category | The category to which the incident belongs. |
| severity | 1, 2 or 3. Defines the severity of the created incident. |
| sys_id | ID automatically given to the incident. |
| description | Representation of the incident. |
| short_description | A short Representation of the incident. |
| subcategory | The subcategory to which the incident belongs. |
| opened_at | Time that the incident was opened. |
| sys_created_by | The person who created the incident. Automatically decided by credentials. |
| sys_created_on | Time that the incident was created. |
| sys_updated_by | Last person to update the incident. Automatically decided by credentials. |
| number | The Incident's number/ID. |
| sys_updated_on | Last time the incident was updated. |
| u_location | The location of the device that caused the incident. |

3. under the “**Annex**”, then click the “>” button to add it to the “**Selected**” viewable fields.

The screenshot shows a 'Create new field' dialog with two columns: 'Available' and 'Selected'. In the 'Available' column, 'Device type' is highlighted. In the 'Selected' column, several fields are listed, including 'Name', 'Asset tag', 'Manufacturer', 'Asset', 'Company', 'Serial number', 'Model ID', 'Assigned to', 'Host', 'Interfaces', 'Comments', and 'location'. An 'Add' button is located between the two columns, and a 'Save' button is at the bottom right.

4. In the same widow type “**Location**” in the Create new field form under name, then click the “**Add**” button.

Form view and section

Create new field

The screenshot shows two forms side-by-side. The 'Form view and section' form has 'View name' set to 'Default view' and 'Section' set to 'IP Router'. The 'Create new field' form has 'Name' set to 'location', 'Type' set to 'String', and 'Field length' set to 'Medium (100)'. An 'Add' button is located below the 'Create new field' form.

5. Once you have added the fields you would like to view, click “**Save**”.

Infoblox NIOS Configuration

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.

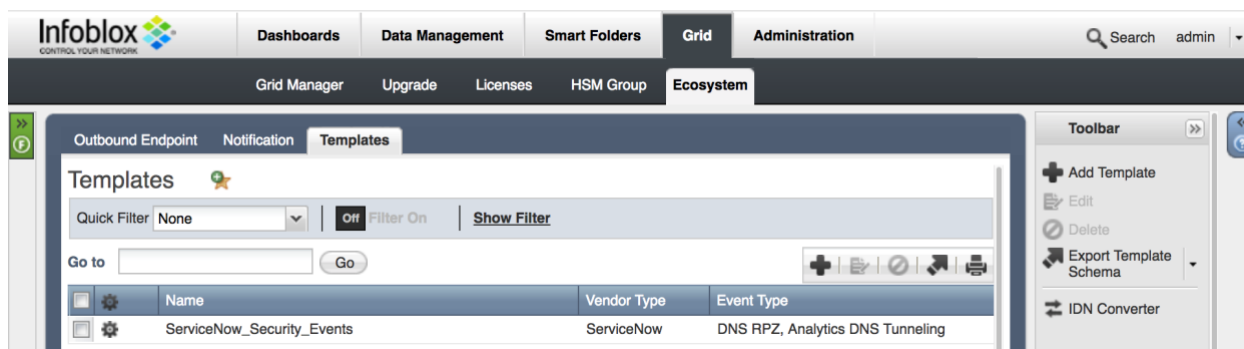
In order to check if the license was installed navigate to “**Grid**” → “**Licenses**” → “**Grid Wide**”.

The screenshot shows the Infoblox NIOS Configuration interface. The 'Grid' tab is selected in the top navigation bar. The 'Licenses' section is active, and the 'Grid Wide' tab is selected. A table lists the licenses, including 'RPZ' and 'Security Ecosystem', both with an expiration date of 2018-03-06 15:59:59 PST (48 Days).

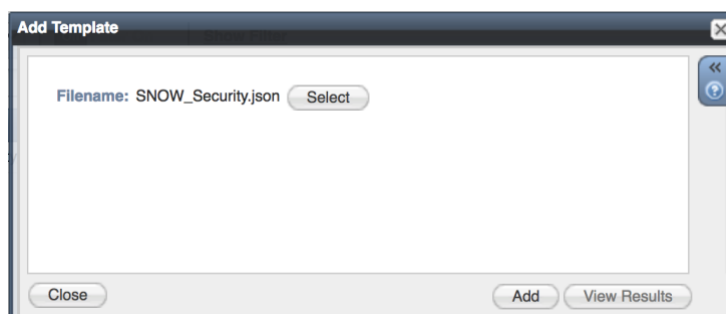
Add/Upload Templates

In order to upload/add templates:

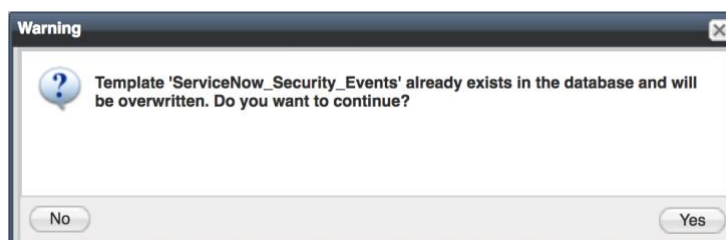
1. Navigate to “Grid” → “Ecosystem” → “Templates” and click on “+” or “+ Add Template” then the “Add template” window will open.



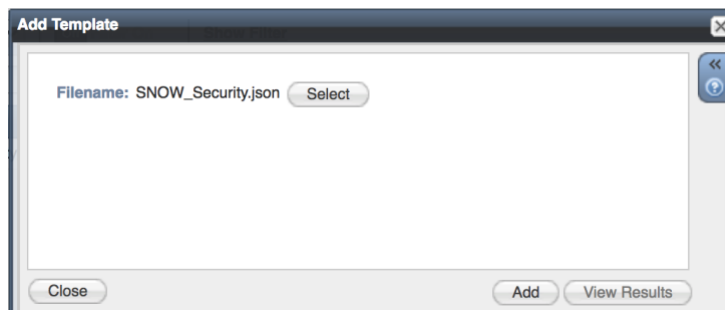
2. Press the “select” button on the “Add template” window.



3. If a template was previously uploaded, press “Yes” to overwrite the template.



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

Syslog Preview

Template validation events for grid master infoblox.localdomain [Go to Syslog Viewer](#)

| Timestamp | Server | Message |
|-------------------|------------------|-------------------------------------------|
| 2018-01-04 07:... | OutboundAPITe... | ----- import completed ----- |
| 2018-01-04 07:... | OutboundAPITe... | Template name: ServiceNow_Security_Events |
| 2018-01-04 07:... | OutboundAPITe... | File: SNOW_Security.json |
| 2018-01-04 07:... | OutboundAPITe... | User: admin |
| 2018-01-04 07:... | OutboundAPITe... | ----- import started ----- |
| 2018-01-04 07:... | OutboundAPITe... | ----- import completed ----- |
| 2018-01-04 07:... | OutboundAPITe... | Template name: ServiceNow_Security_Events |
| 2018-01-04 07:... | OutboundAPITe... | File: SNOW_Security.json |
| 2018-01-04 07:... | OutboundAPITe... | User: admin |
| 2018-01-04 07:... | OutboundAPITe... | ----- import started ----- |
| 2018-01-04 07:... | OutboundAPITe... | ----- import completed ----- |
| 2018-01-04 07:... | OutboundAPITe... | Template name: ServiceNow_Security_Events |
| 2018-01-04 07:... | OutboundAPITe... | File: SNOW_Security.json |
| 2018-01-04 07:... | OutboundAPITe... | User: admin |
| 2018-01-04 07:... | OutboundAPITe... | ----- import started ----- |

Close

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.

ServiceNow_Security_Events (Template)

Basic

General

Contents

Name* ServiceNow_Security_Even

Type REST API

Vendor Type ServiceNow

Event Type DNS RPZ, Analytics DNS Tunneling

Template Type Event

Comment Create an incident by a DNS security events

Cancel Save & Close

ServiceNow_Security_Events (Template)

Basic

General

Contents

```
{
  "version": "3.0",
  "name": "ServiceNow_Security_Events",
  "comment": "Create an incident by a DNS security events",
  "type": "REST_EVENT",
  "event_type": [
    "RPZ",
    "TUNNEL"
  ],
  "action_type": "Incidents",
  "content_type": "application/json",
  "vendor_identifier": "ServiceNow",
  "quoting": "XMLA",
  "instance_variables": [
    {
      "name": "Severity",
      "type": "INT",
      "value": "3"
    }
  ],
  "steps": [
    {
      "name": "check rpz or tunnel to assign query name",
      "operation": "CONDITION",

```

Cancel Save & Close

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.

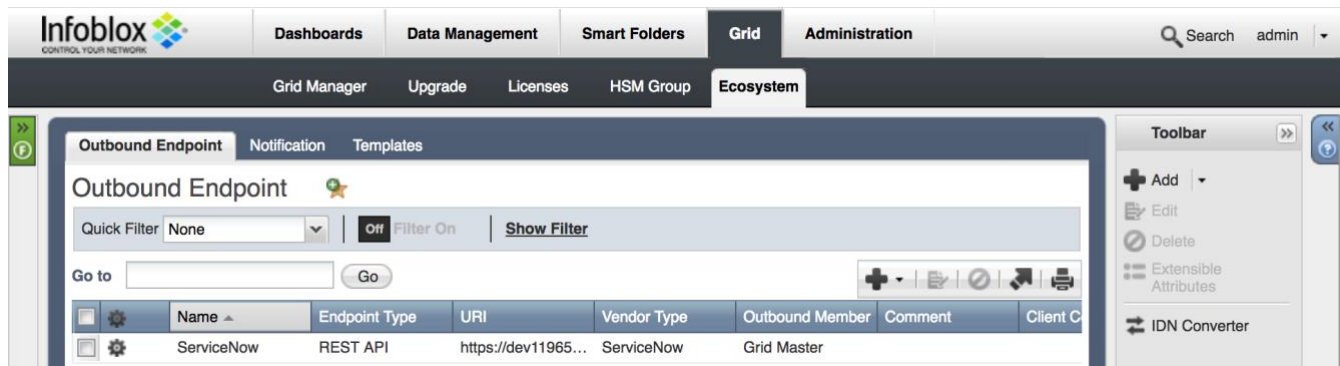
Note: You cannot delete a template if it is used by an endpoint or by a notification.

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 fields are required.
3. Specify **“Auth Username”**, **“Auth Password”** (ServiceNow Web Service account credentials), **“WAPI Integration Username”** and **“WAPI Integration Password”** (NIOS credentials).

4. (Optional) For debug purposes only: Under **“Session Management”**, set **“Log Level”** to **“Debug”**.

Timeout: 30 Seconds

Log Level: Debug

Template: Select Template Clear

Vendor Type

Template Type

Parameters

| Name | Value | Type |
|---------|-------|------|
| No data | | |

Cancel Previous Next Save & Close

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

Add a Notification

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.

Infoblox Dashboards Data Management Smart Folders Grid Administration

Grid Manager Upgrade Licenses HSM Group Ecosystem

Outbound Endpoint Notification Templates

Notification

Quick Filter: None Filter On Show Filter

Go to: Go

| Name | Target | Action | Disabled | Comment |
|-------------------|------------|-------------------|----------|---------|
| ServiceNow_Tunnel | ServiceNow | Outbound Template | No | |
| ServiceNow_RPZ | ServiceNow | Outbound Template | No | |

Toolbar: Add Notification Rule Edit Delete IDN Converter

2. Specify the notification’s name and select an endpoint (Target), click **“Next”**.

Name: ServiceNow_RPZ

Target: ServiceNow Select Endpoint

Target Type: REST API

Vendor Type: ServiceNow

Comment:

Disable

Cancel Previous Next Save & Close

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”**.

It may take up to a minute to apply the new rules.

Event* DNS RPZ

Match the following rule: Reset

Rule Name contains local.rpz

Cancel Previous Next Save & Close

4. (For RPZ notifications only) Check **“Enable RPZ event deduplication”** and specify relevant parameters. Click **“Next”**.

☒ Enable RPZ event deduplication

☒ Log all dropped events due to deduplication to the syslog

Select the fields to use for deduplication

Available: RPZ Policy, RPZ Type, Query Type, Network View, Network

Selected: Source IP, Query Name

Lookback Interval: 10 Minutes

Cancel Previous Next Save & Close

5. Select a relevant template and specify the template's parameters if any are required. Click **“Save & Close”**.

Template* ServiceNow_Security_Events Select Template Clear

Vendor Type ServiceNow

Template Type Event

Parameters

| Name | Value | Type |
|----------|-------|--------|
| Severity | 3 | Number |

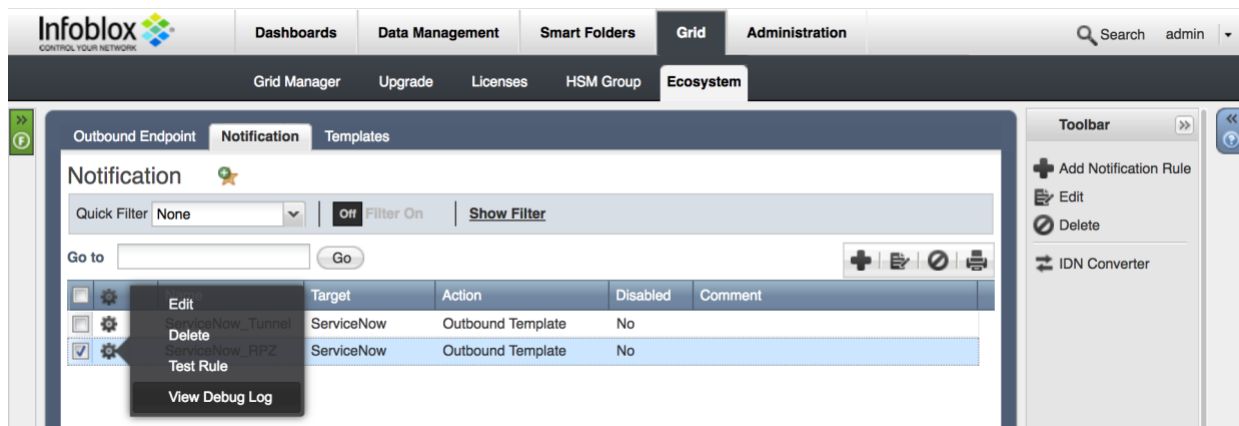
Cancel Previous Next Save & Close

Check the Configuration

You can emulate an event for which a notification was added by going to **“Dashboards”** → **“Status”** → **“Security”** then on the **“Dig Request”** panel, fill in the **“Domain Name to Query”** text box and click the **“Perform Dig”** button.

When performing the dig request above, make sure that the **“Domain Name to Query”** is blocked by your RPZ. To check this, navigate to **“Data Management”** → **“DNS”** → **“Response Policy Zone”**. You can export a RPZ feed or check the content of a local RPZ.

To check a debug log for an endpoint, go to **“Grid”** → **“Ecosystem”** → **“Notification”**, click on the gear wheel and select **“View Debug Log”**.



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

Summary

The integration solution from Infoblox and ServiceNow Modernizes your IT service management by providing a single place to manage and organize your security events and assets that are on the Infoblox devices.

Additional References

The Infoblox DDI activity pack manages the IP addresses used in a network by integrating DNS and DHCP. Custom Orchestration activities use Infoblox Web API (WAPI) REST web services to access the Infoblox GRID server.

https://docs.servicenow.com/bundle/jakarta-servicenow-platform/page/administer/orchestration-activities/concept/c_InfobloxDDIActivityPack.html

Annex

ServiceNow Incident Table Data Allocation

| Field Name | Purpose |
|-------------------|----------------------------------------------------------------------------|
| category | The category to which the incident belongs. |
| severity | 1, 2 or 3. Defines the severity of the created incident. |
| sys_id | ID automatically given to the incident. |
| description | Representation of the incident. |
| short_description | A short Representation of the incident. |
| subcategory | The subcategory to which the incident belongs. |
| opened_at | Time that the incident was opened. |
| sys_created_by | The person who created the incident. Automatically decided by credentials. |
| sys_created_on | Time that the incident was created. |
| sys_updated_by | Last person to update the incident. Automatically decided by credentials. |
| number | The Incident's number/ID. |
| sys_updated_on | Last time the incident was updated. |
| u_location | The location of the device that caused the incident. |

ServiceNow Asset Table Data Allocation

| Field Name | Purpose |
|-------------------|-----------------------------------------------------------------------------------------|
| sys_updated_on | Last time the incident was updated. |
| first_discovered | Time that an asset was created on Infoblox appliance. |
| sys_updated_by | Last person to update the asset. Automatically decided by credentials. |
| sys_created_on | Time that the asset was created. |
| sys_created_by | The person who created the incident. Automatically decided by credentials. |
| name | Name of the asset that's discovered. |
| short_description | Description of the asset that was discovered. |
| manufacturer | Vendor of the asset that is discovered. |
| vendor | Vendor of the asset that is discovered. |
| comments | Name of the operation system, model, and chassis serial number of the discovered asset. |
| ip_address | The IP of the Asset. |
| u_location | The location of the device that caused the incident. |

Infoblox Objects to ServiceNow Tables Association

| ServiceNow Table Name | Infoblox Objects |
|-----------------------|--------------------------------------|
| cmdb_ci_ip_router | Router devices. |
| cmdb_ci_ip_switch | Switch devices that are not routers. |
| cmdb_ci_ip_firewall | Firewall devices. |
| cmdb_ci_ip_server | Server device. |
| cmdb_ci_ip_lb | Load-balancer devices. |
| cmdb_ci_ip_phone | IP phone devices. |
| cmdb_ci_ip_device | Devices that are not supported. |
| cmdb_ci_ip_network | Networks created by Infoblox. |
| cmdb_ci_ip_address | Interfaces of devices. |
| incident | Security events. |