NetWitness® Platform

QRadar Integration Guide

NETWITNESS
Platform

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by RSA.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

June, 2024

Contents

NetWitness Platform Integration with IBM QRadar

IBM QRadar is an enterprise security information and event management (SIEM) product. It collects log data from an enterprise, its network devices, host assets and operating systems, applications, vulnerabilities, user activities and behaviors.

There are several NetWitness integrations with IBM QRadar. Currently, the following integration points are supported:

- Forwarding Alerts: NetWitness Platform to QRadar
- Qlink for NetWitness Platform
- NetWitness Platform Right Click to QRadar
- Right Click from QRadar to NetWitness Platform

Additionally, the source is supplied in this document, in the Appendix: Source Code section.

Forwarding Alerts: NetWitness Platform to QRadar

NetWitness Platform can forward Syslog CEF alerts to QRadar, both from Event Stream Analysis and the Reporting Engine. It is a two-step process.

1. NetWitness Platform needs to configure the alerts in CEF format to be sent to QRadar via syslog.
   - Use the Event Stream Analysis CEF template to forward from ESA: Event Stream Analysis CEF Template
   - Use the Reporting Engine Alert CEF template to forward from the Reporting Engine: Reporting Engine Alert Syslog CEF Template
2. Set up QRadar so it can parse these logs coming in from NetWitness Platform, rather than categorizing them as unknown.
   a. Install a single DSM.
   b. Add a Universal CEF log source on the QRadar console.
   c. Import the Netw QID map entries into QRadar.
   d. Configure event mapping for Universal CEF events.
   e. Add custom event properties.

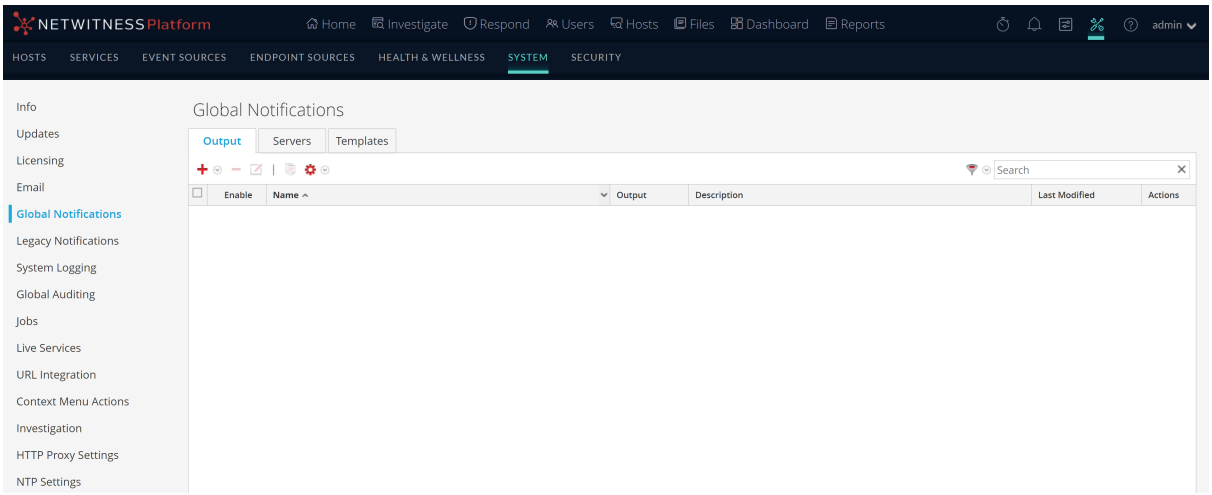
Event Stream Analysis CEF Template

In this section, you need to add a global notification output, server, and template, then set up an Alert to use them.

To add the global output, server and template:

1. Log in to the NetWitness Platform as an Administrator.
2. Go to  (Admin) > **System**.
3. In the options panel, select **Global Notifications**.

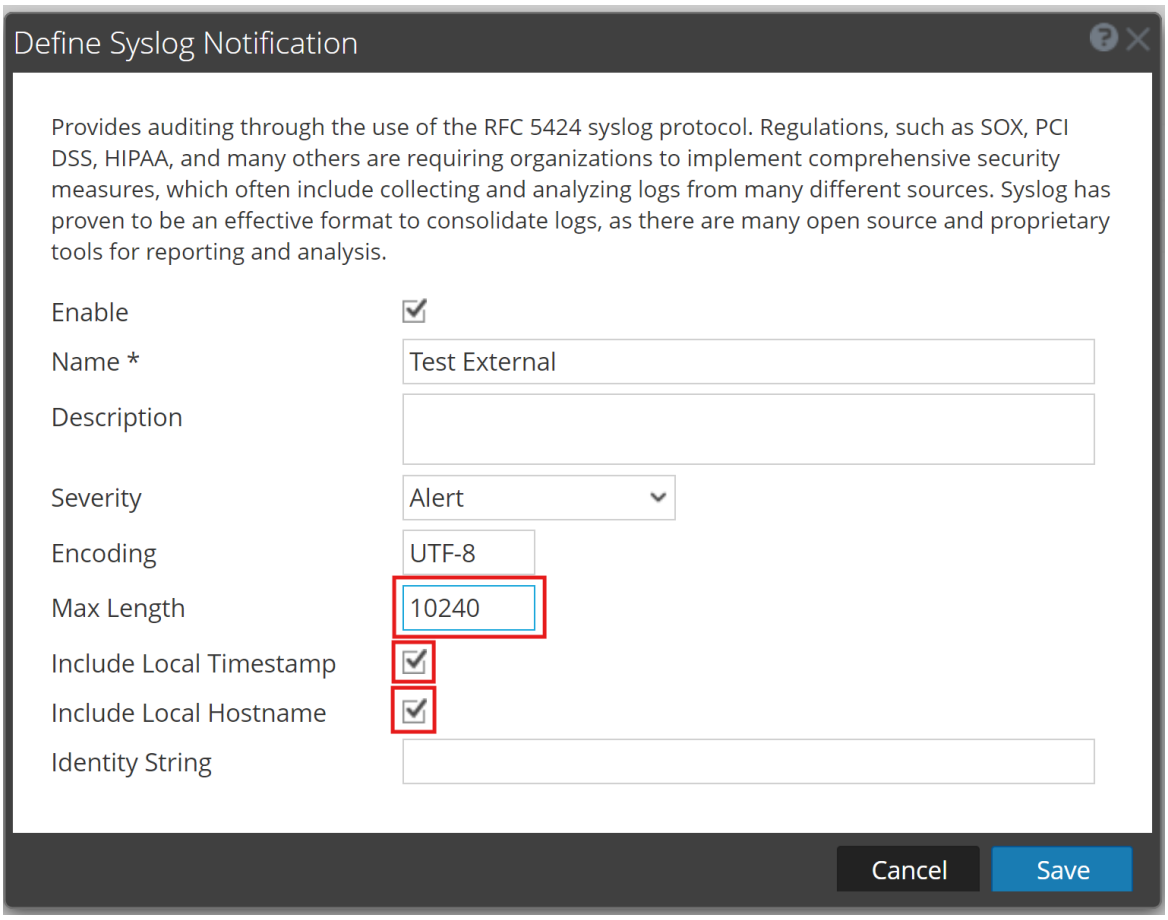
   The **Global Notifications** panel is displayed.



4. Add a Notification Output.

   a. From the **Output** tab, click  and choose Syslog from the drop-down menu.
   The **Define Syslog Notification** dialog box is displayed.

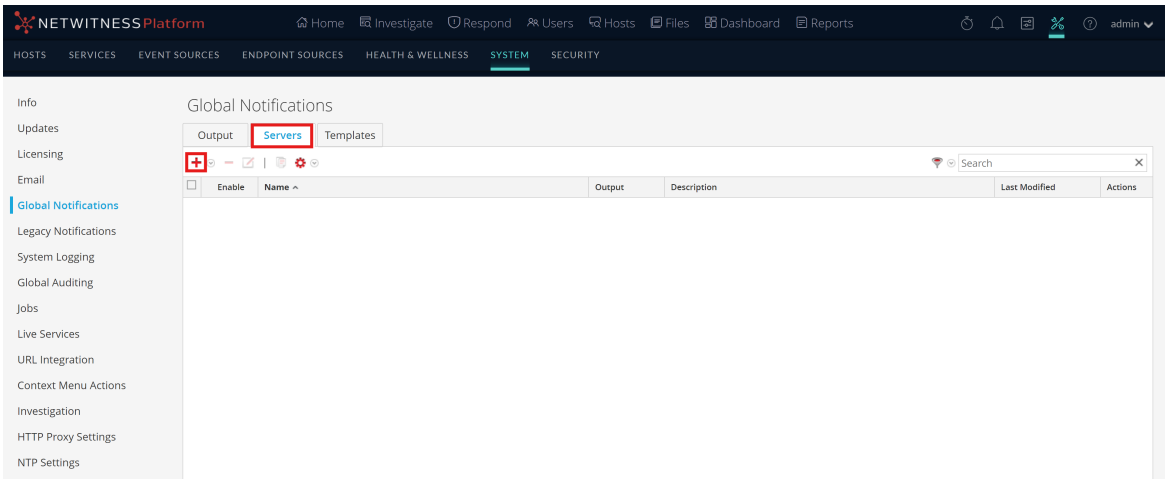
   b. Fill in the screen as it appears here:



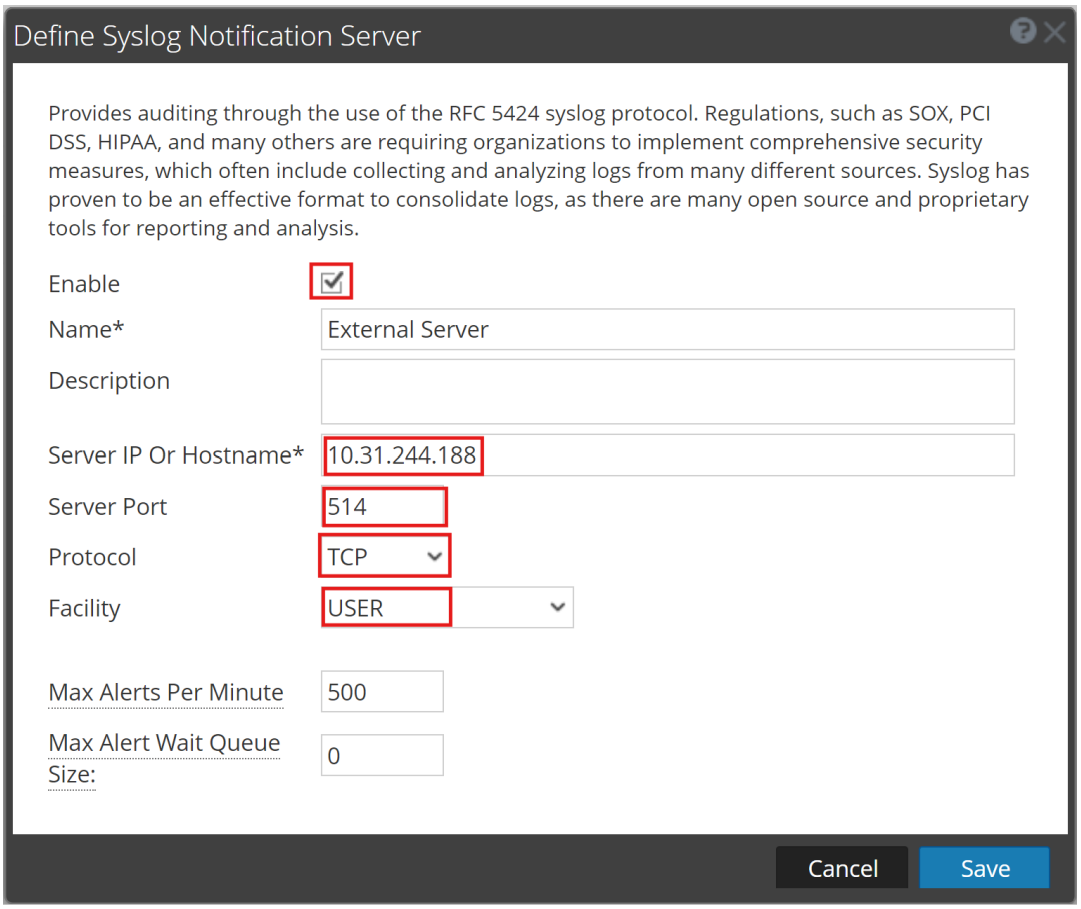
c. Click **Save**.

5. Add a Notification Server.

a. Select the **Servers** tab, click  , and choose Syslog from the drop-down menu.



b. Fill in the screen as it appears here:

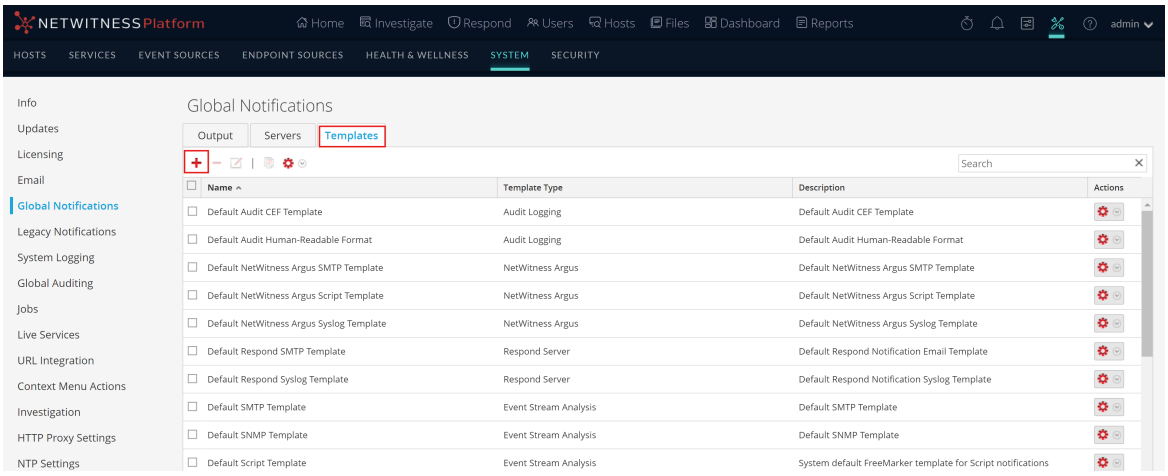


Note: The Server IP address should be the IP Address of your QRadar.

c. Click **Save**.

6. Add a Template.

a. Select the **Templates** tab and click  .



The **Define Template** dialog box is displayed.

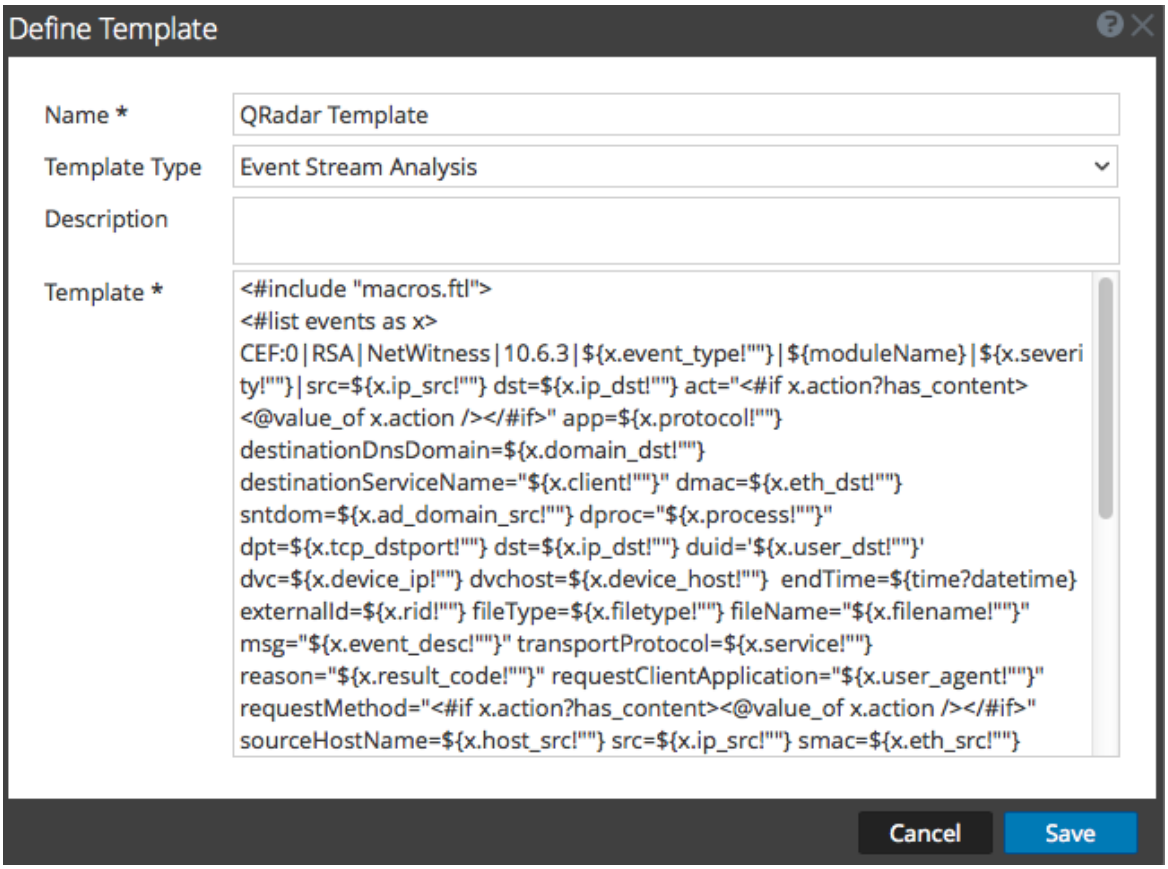
b. Enter a **Name** (such as QRadar Template).

c. From the **Template Type** drop-down menu, select **Event Stream Analysis**.

d. Copy and paste in the text listed below (or copy it from the file that you downloaded from NetWitness Community Link) into the Template text field:

```
#include "macros.ftl"
<#list events as x>
CEF:0|RSA|NetWitness|10.6.3|${x.event_
type!""}|${moduleName}|${x.severity!""}|src=${x.ip_src!""} dst=${x.ip_
dst!""} act="<#if x.action?has_content><@value_of x.action /></#if>"
app=${x.protocol!""} destinationDnsDomain=${x.domain_dst!""}
destinationServiceName="${x.client!""}" dmac=${x.eth_dst!""}
sntdom=${x.ad_domain_src!""} dproc="${x.process!""}" dpt=${x.tcp_
dstport!""} dst=${x.ip_dst!""} duid='${x.user_dst!""}' dvc=${x.device_
ip!""} dvchost=${x.device_host!""}  endTime=${time?datetime}
externalId=${x.rid!""} fileType=${x.filetype!""}
fileName="${x.filename!""}" msg="${x.event_desc!""}"
transportProtocol=${x.service!""} reason="${x.result_code!""}"
requestClientApplication="${x.user_agent!""}" requestMethod="<#if
x.action?has_content><@value_of x.action /></#if>"
sourceHostName=${x.host_src!""} src=${x.ip_src!""} smac=${x.eth_src!""}
sourceDnsDomain=${x.domain_src!""} suid='${x.user_src!""}'
type=${x.medium!""} deviceCustomDate1=${x.event_time!""}
deviceCustomDate1Label="Event Time" cs2=${time?datetime?iso_m_nz
("GMT+01")} cs2Label="Custom Time String plus 1 Hour"
cs1=${time?datetime?iso_m_nz("GMT-01")} cs1Label="Custom Time String
minus 1 Hour" cat="${x.event_cat_name!""}" spriv="${x.group!""}"
cs3="${x.alert_id!""}" cs3Label="Alert ID" cs4="${x.msg_id!""}"
cs4Label="Message ID" cs5="${x.risk_info!""}-${x.risk_suspicious!""}-
${x.risk_warning!""}" cs5Label="Risk Categories" cs6="${x.category!""}"
cs6Label="NW Category" suser='${x.ad_username_src!""}'
deviceExternalId=${x.did!""} dhost=<#if x.alias_host?has_
content><@value_of x.alias_host/></#if> spt=${x.tcp_srcport!""}
duser='${x.ad_username_dst!""}' fileSize=${x.size!""}
fileHash=${x.checksum!""} outcome="${x.ec_outcome!""}"
cn1=${x.sessionid!""} cn1Label="SessionID" </#list>
```

Your dialog box should look like this:

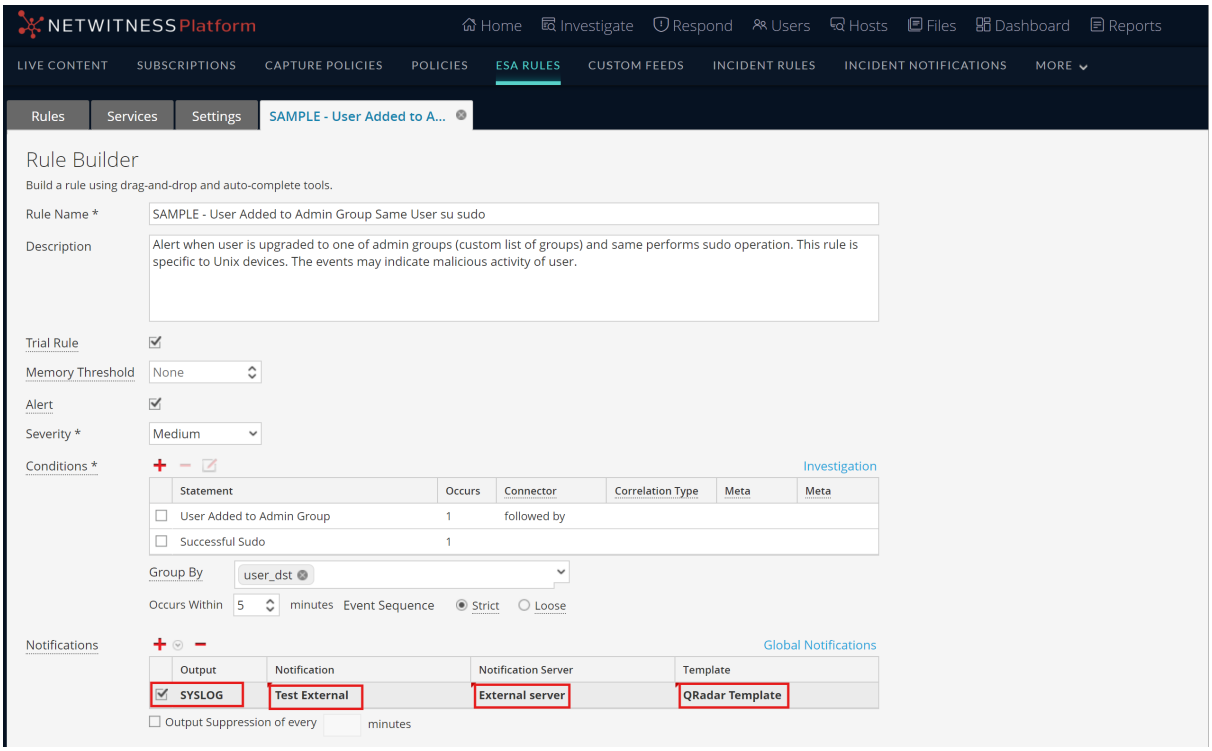


e. Click **Save**.

Next, configure your ESA Alert to use the new template.

To configure a rule to use the QRadar output, server, and template:

1. In the **NetWitness Platform** menu, select **(Configure) > ESA Rules**.
2. From the Rule Library, select a rule and click the **Edit** icon ( ).
   The Rule Builder screen appears.
3. In the Notifications section, click > **Syslog** to configure Syslog notifications for the rule.
   A notification row is added to the Notifications section.
4. Select the notification, notification server, and template that you created earlier.



5. Click **Save** to save your changes and close the Rule Builder screen.

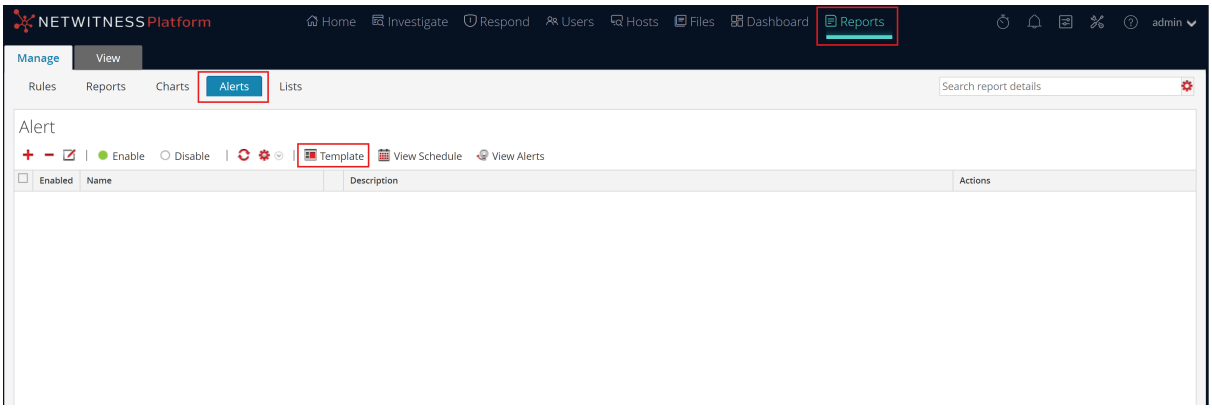
Note: Remember to re-deploy the rule to push the new notification templates

Reporting Engine Alert Syslog CEF Template

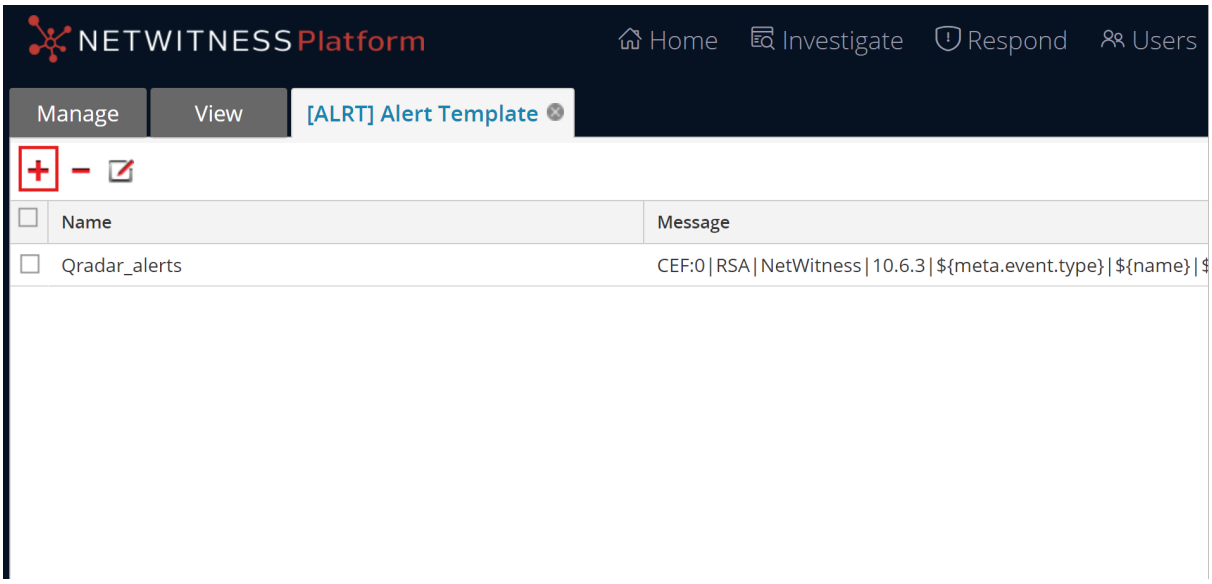
In this section, you need to add a Reporting Engine template, then set up an Alert to use it.

To add a Reporting Engine template:

1. Log in to the NetWitness Platform as an Administrator.
2. Go to **Reports > Alerts**.



3. Select **Template** and click + to create a new template.

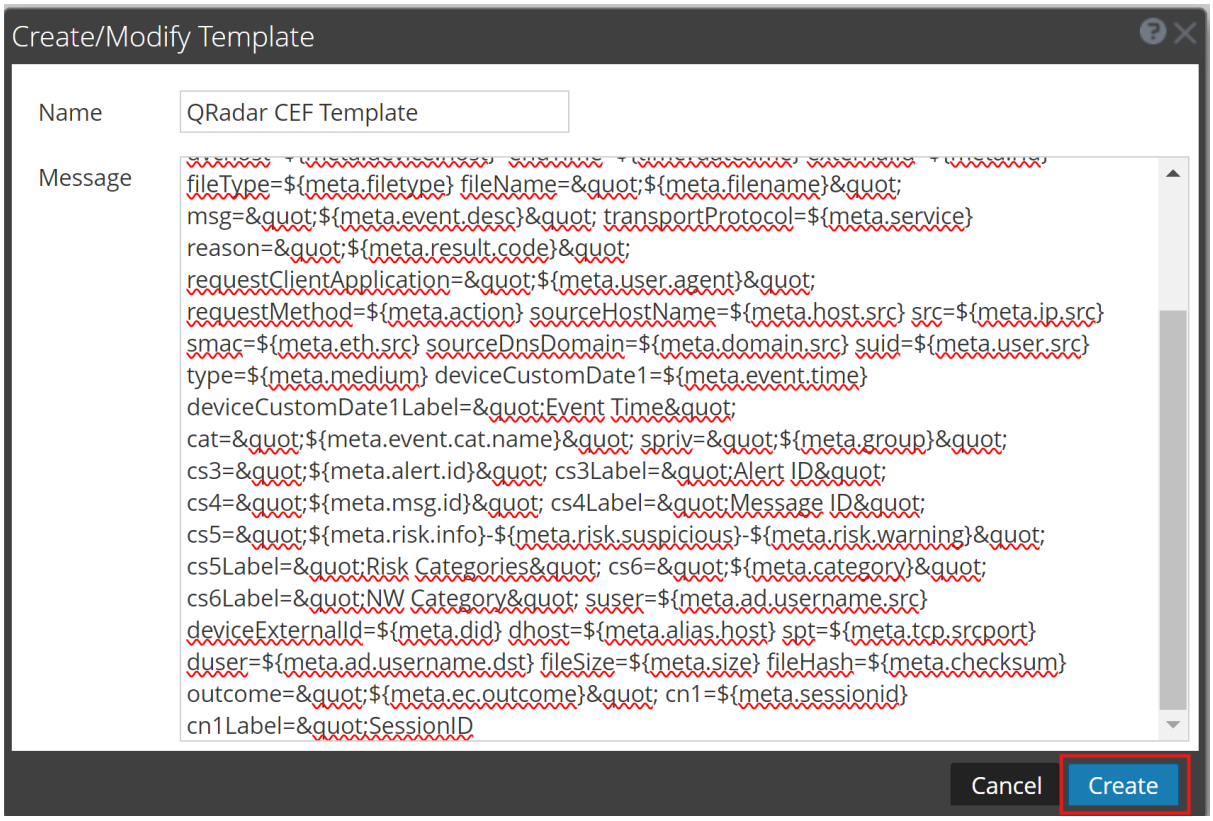


4. Name the template, for example **QRadar CEF Template**.
5. Copy and paste in the text listed below (or copy it from the file that you downloaded from NetWitness platform Link) into the Template text field:

```
CEF:0|RSA|NetWitness|10.6.3|${meta.event.type}|${name}|${meta.severity}|act
=${meta.action} app=${meta.protocol}
destinationDnsDomain=${meta.domain.dst}
destinationServiceName=&quot;${meta.client}&quot; dmac=${meta.eth.dst}
sntdom=${meta.ad.domain.src} dproc=&quot;${meta.process}&quot;
dpt=${meta.tcp.dstport} dst=${meta.ip.dst} duid=${meta.user.dst}
dvc=${meta.device.ip} dvchost=${meta.device.host}  endTime=${time?datetime}
externalId=${meta.rid} fileType=${meta.filetype}
fileName=&quot;${meta.filename}&quot; msg=&quot;${meta.event.desc}&quot;
transportProtocol=${meta.service} reason=&quot;${meta.result.code}&quot;
requestClientApplication=&quot;${meta.user.agent}&quot;
requestMethod=${meta.action} sourceHostName=${meta.host.src}
src=${meta.ip.src} smac=${meta.eth.src} sourceDnsDomain=${meta.domain.src}
suid=${meta.user.src} type=${meta.medium}
deviceCustomDate1=${meta.event.time} deviceCustomDate1Label=&quot;Event
Time&quot;  cat=&quot;${meta.event.cat.name}&quot;
spriv=&quot;${meta.group}&quot; cs3=&quot;${meta.alert.id}&quot;
cs3Label=&quot;Alert ID&quot; cs4=&quot;${meta.msg.id}&quot;
cs4Label=&quot;Message ID&quot; cs5=&quot;${meta.risk.info}-
${meta.risk.suspicious}-${meta.risk.warning}&quot; cs5Label=&quot;Risk
Categories&quot; cs6=&quot;${meta.category}&quot; cs6Label=&quot;NW
Category&quot; suser=${meta.ad.username.src} deviceExternalId=${meta.did}
```

```
dhost=${meta.alias.host} spt=${meta.tcp.srcport}
duser=${meta.ad.username.dst} fileSize=${meta.size}
fileHash=${meta.checksum} outcome=&amp;quot;${meta.ec.outcome}&amp;quot;
cn1=${meta.sessionid} cn1Label=&amp;quot;SessionID
```

Your dialog box should look like this:

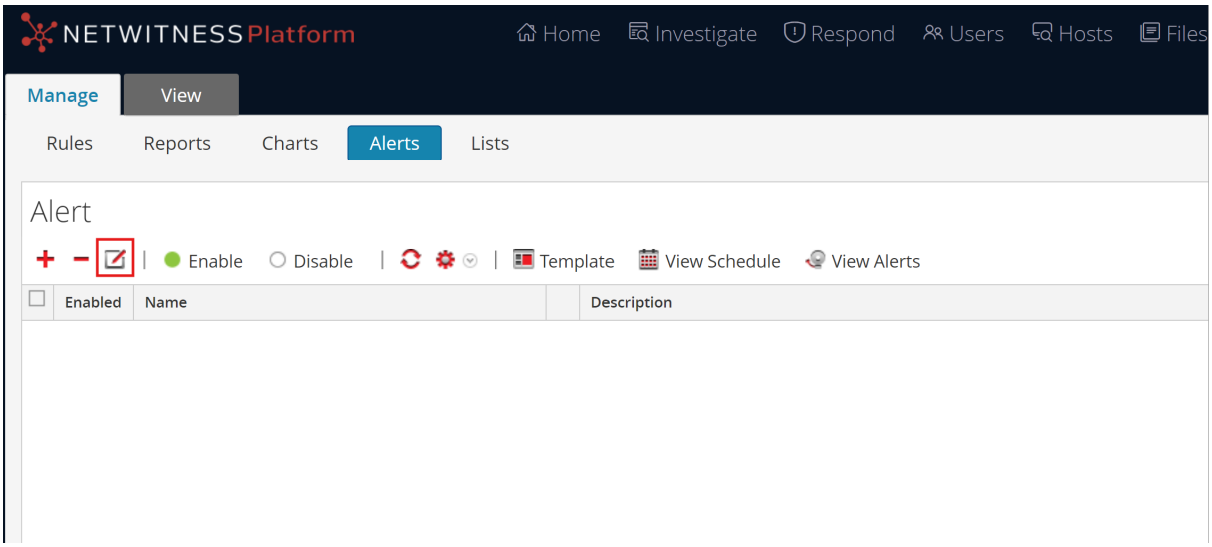


6. Click **Create**.

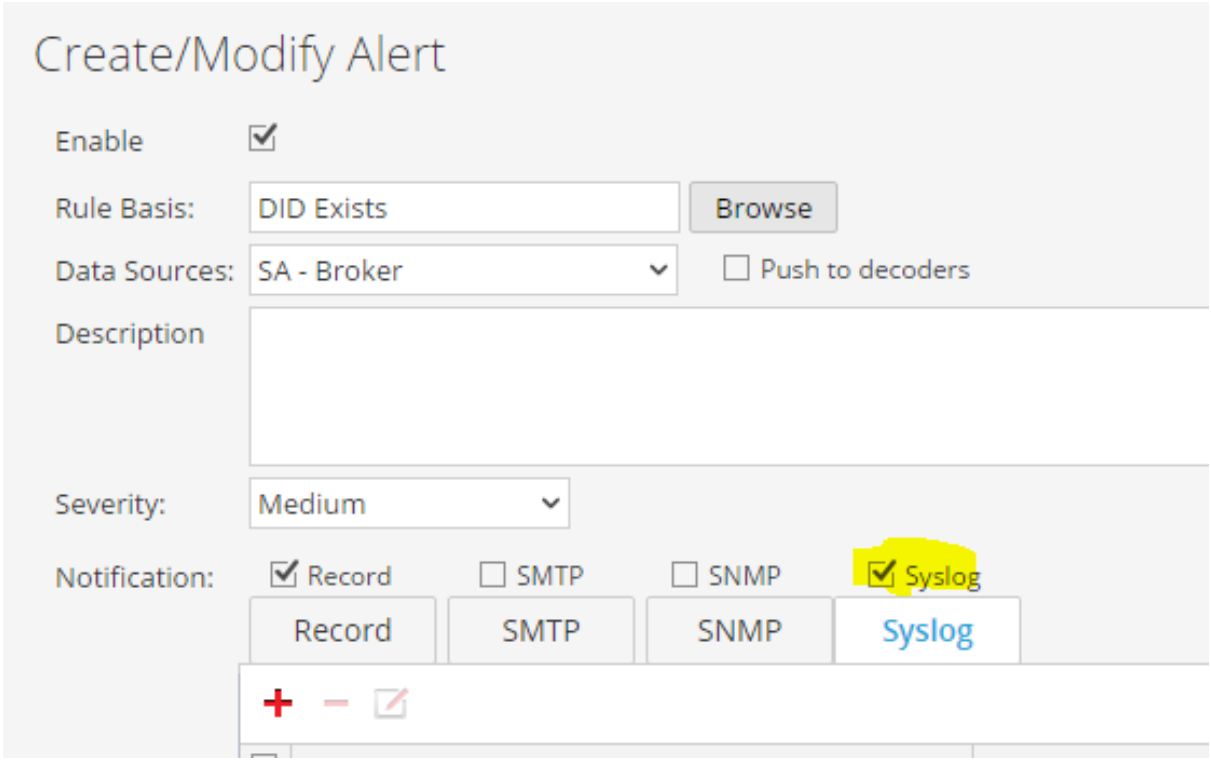
For each alert that you want to send to QRadar, you need to edit the Alert and configure it to send a Syslog Notification using the new template.

To configure a rule to use the QRadar Reporting Engine template:

1. In the **NetWitness Platform** menu, go to **Reports > Alerts**.



2. Select an alert and click the **Edit** icon ( ).
3. From the Rule Library, select a rule and click the **Edit** icon ( ).
   The Rule Builder screen appears.
4. In the Notification section, select **Syslog**.

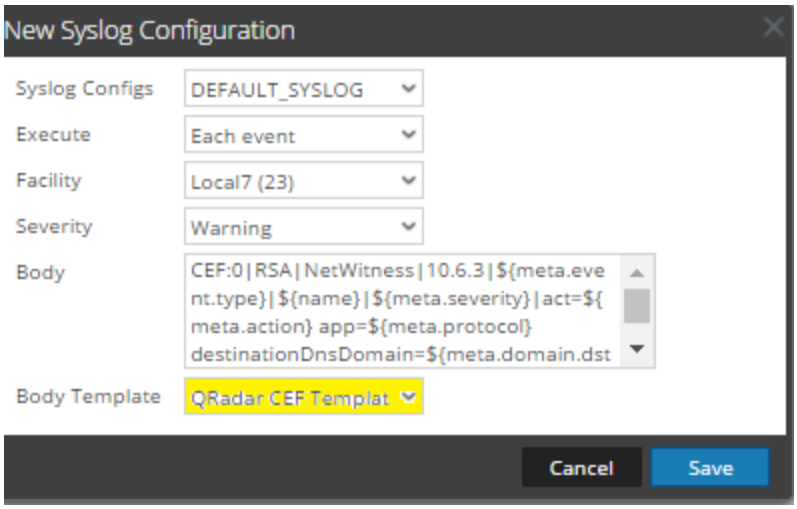


5. Click  .

   The New Syslog Configuration dialog box is displayed.

6. Enter parameters as follows.

   - For **Syslog Configs**, select your Syslog Destination. This Destination was configured under **Global Notifications**, in the Event Stream Analysis CEF Template section.
   - For **Body**, select the RE template you created earlier (Create RE template step).
   - For the remainder of the fields, accept the default values.



Repeat this procedure for each alert you want to export to QRadar.

QRadar configuration for accepting NetWitness platform Alerts

Typically, the Universal CEF DSM components are installed by default and are part of IBM's regular update schedule for DSM updates when the **automatic updates** setting is enabled. If the Universal CEF components are not installed, you need to install them. Download and install the most recent version of the following RPMs on your QRadar Console.

Install a single DSM

Note: The IBM support website contains individual DSMs that you can download and install using the command line.

1. Download the DSM file to your system hosting QRadar.
2. Using SSH, log onto QRadar as the root user (username is **root**).
3. Navigate to the directory that includes the downloaded file.
4. Type the following command:

– `rpm -Uvh` ***<filename>*** `i`

where ***<filename>*** is the name of the downloaded file. For example:

`rpm -Uvh DSM-UniversalCEF-7.2-953671.noarch.rpm`

or

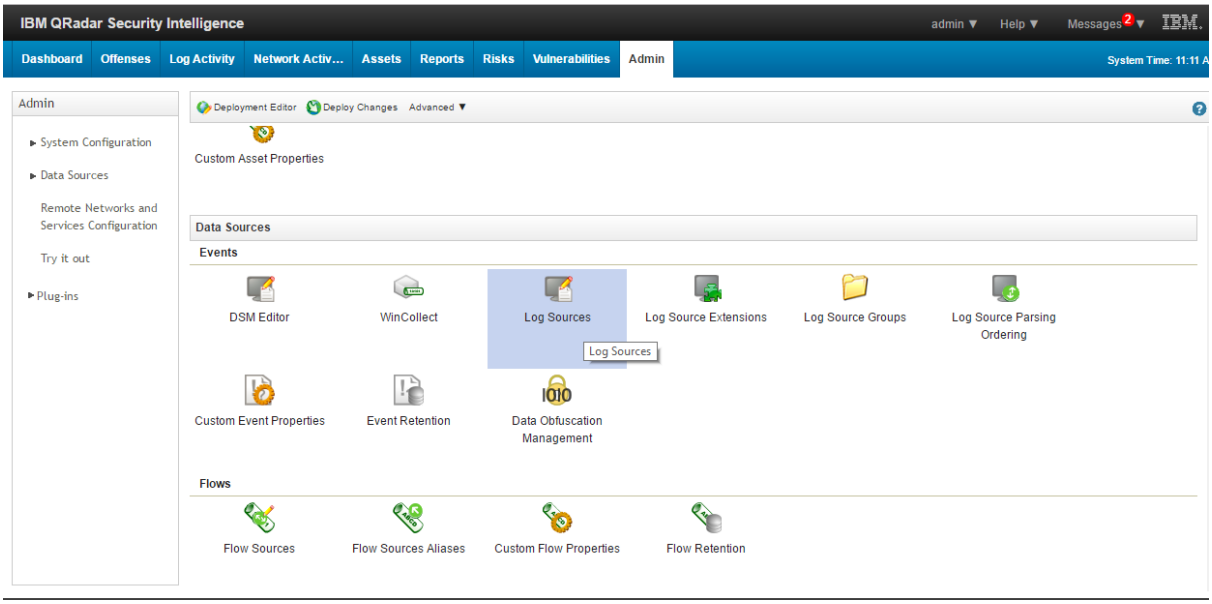
`rpm -Uvh DSM-UniversalCEF-7.2-953671.noarch.rpm`

5. Log in to QRadar: `https://`***<IP Address>*** `i`, where ***<IP Address>*** is the IP address of the QRadar console or event collector.
6. On the **Admin** tab, click **Deploy Changes**.

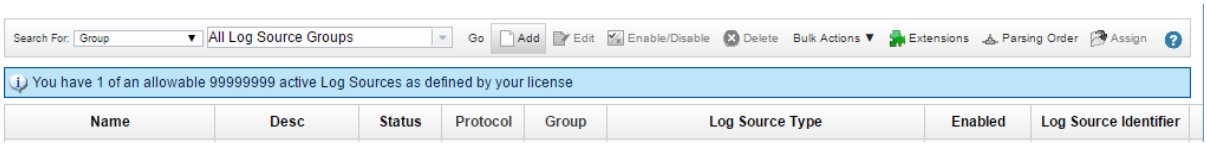
This completes the installation.

Add a Universal CEF log source on the QRadar console

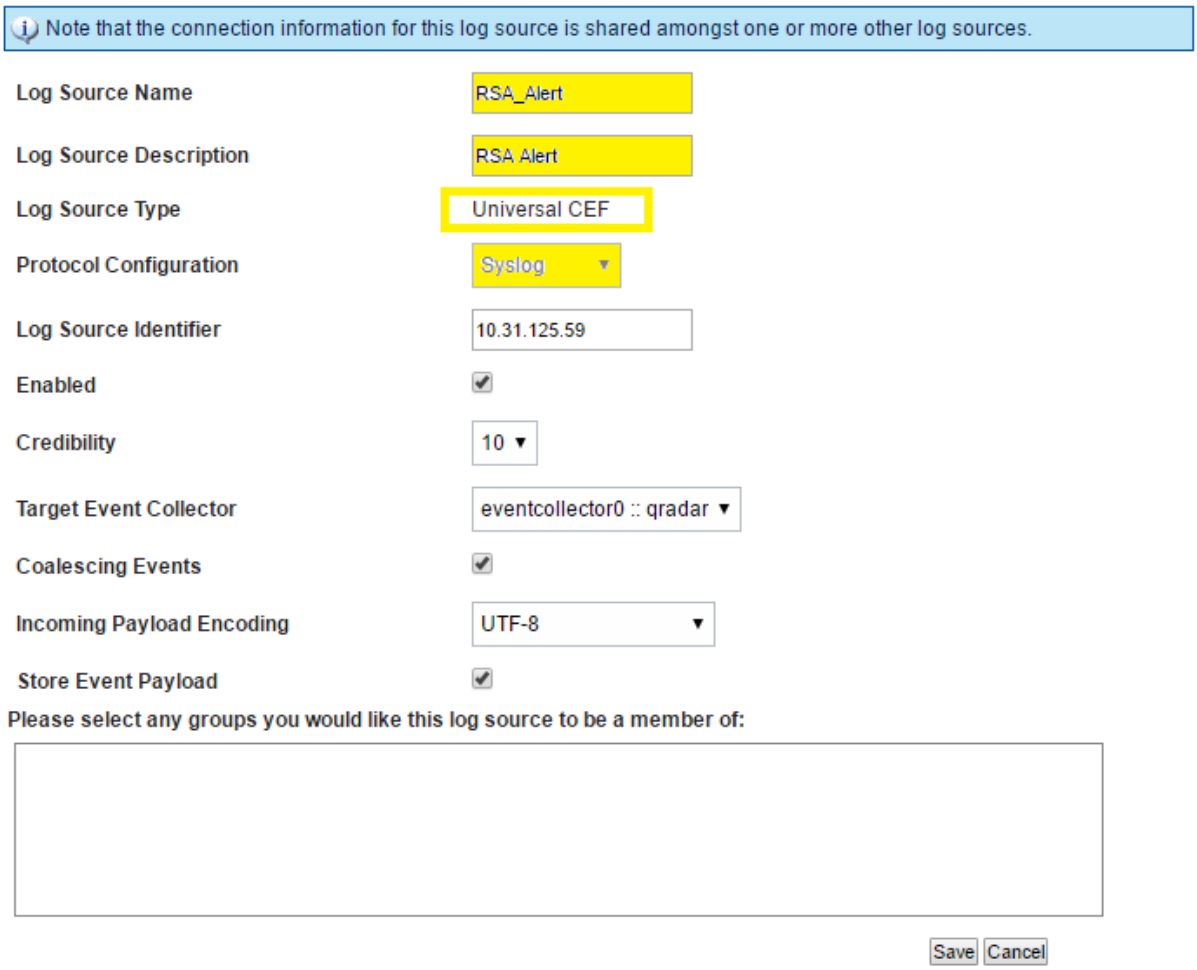
1. Log into the QRadar GUI with Administrative Credentials.
2. Navigate to the **Admin** tab, then click **Log Sources**.



3. Click **Add**.



4. Select log source as **Universal CEF** and fill in the details as rest as shown in the diagram.



5. Click **Save**.
6. Click **Deploy Changes**.

Import NetWitness platform QID map entries into QRadar

1. Create a text file named **RSA_QID.txt**.
2. Copy and paste the following entry into **RSA_QID.txt**:

   ```
   ,RSA NetWitness, ALERTS,3,8001
   ```

3. Using SSH, log in to QRadar SIEM as the root user (username is **root**).
4. Place the file on your system hosting QRadar in the following directory: `/opt`
5. Change to the following directory: `opt/qradar/bin`
6. To import the QID map file, execute the following command:

   ```
   ./opt/qradar/bin/qidmap_cli.sh –i –f /opt/RSA_QID.txt
   ```

Note: If any of the entries in the file cause an error, none of the entries in the file are enforced.

The output from the command should look similar to the following (this sample output has been truncated from the actual output):

```
importing from file: /opt/RSA_QID.txt
importing new: ,RSA NetWitness,ALERTS,3,8001
Created entry:
        qid: 2000005
        name: RSA NetWitness
        description: ALERTS
        severity: 3
        low level category id: 8001
        ratethreshold: 0
        catpipename: Golf
        rateshortwindow: 0
        ratelongwindow: 0
        reverseip: false
        rateinterval: 0
,RSA NetWitness,ALERTS,3,8001

Invoking operation: forceNotification ( )
Result: true

Invoking operation: forceNotification ( )
Result: true
```

7. Restart the QRadar **hostcontext** service:

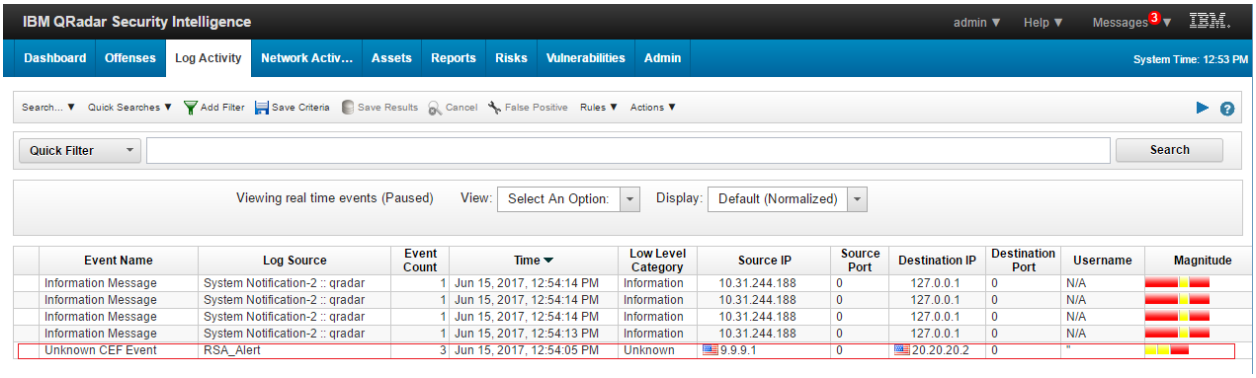
   ```
   /etc/init.d/service hostcontext restart
   ```

QID map file importing is complete.

Configure event mapping for Universal CEF events

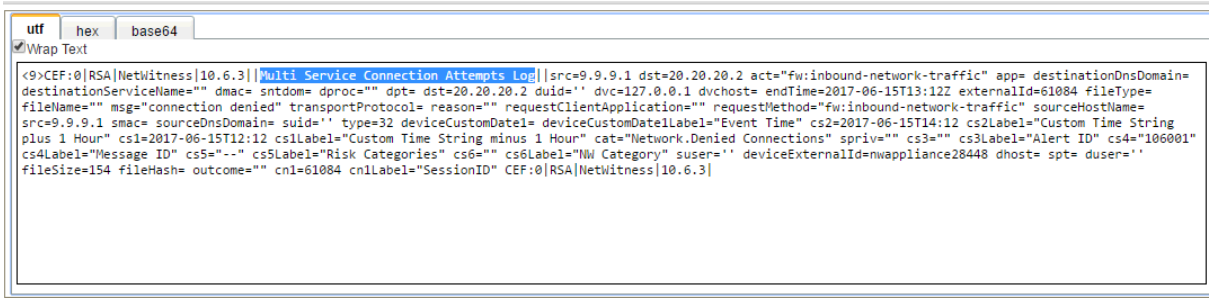
Note: The following procedure and details are reproduced here from IBM Support site: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.dsm.doc/t_dsm_guide_universal_cef_event_mapping.html

By default, the Universal CEF DSM categorizes all events as unknown. All Universal CEF events display a value of unknown in the Event Name and Low-Level Category columns on the Log Activity tab.

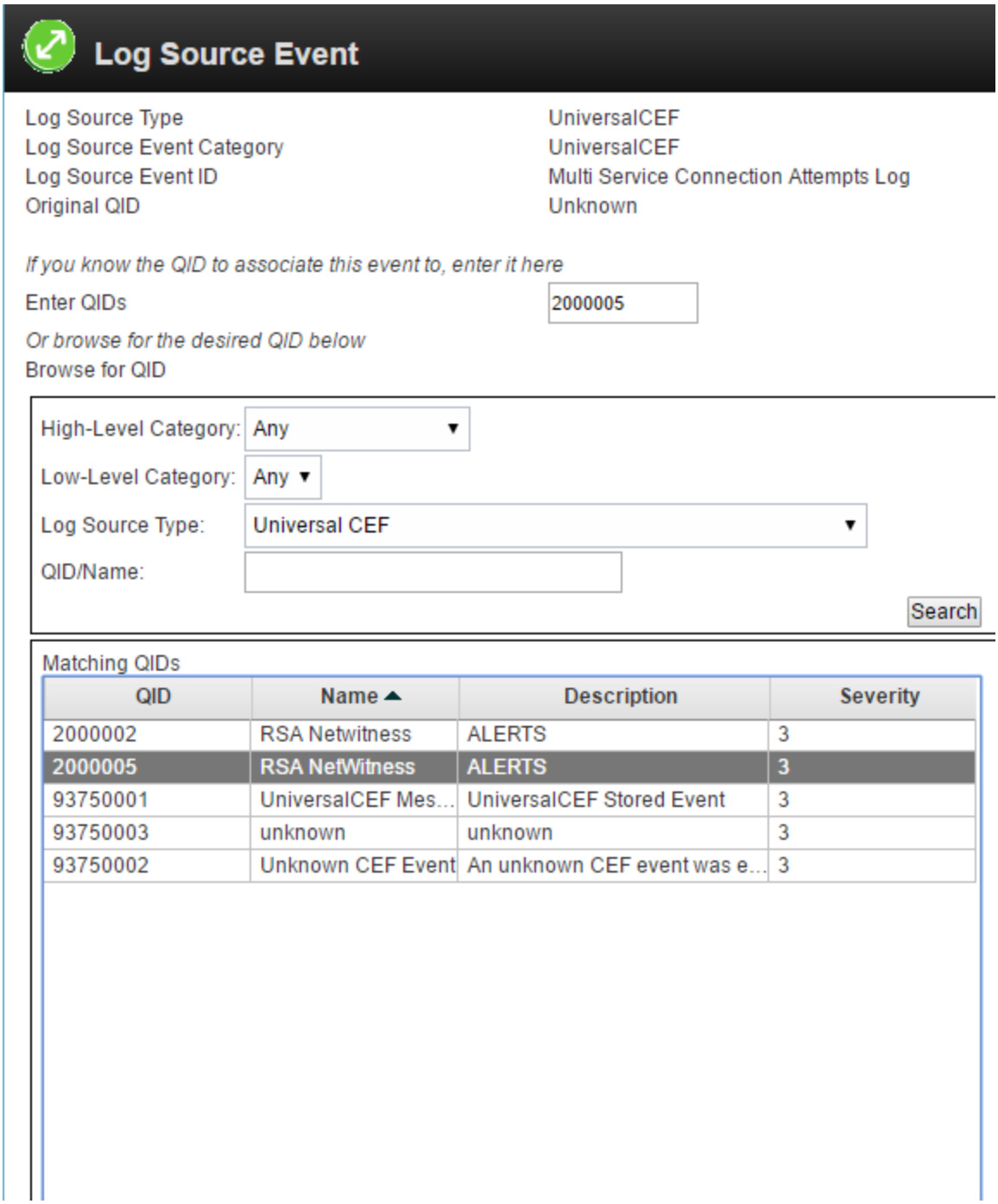


You must modify the QID map to individually map each event for your device to an event category in QRadar. Mapping events allows QRadar to identify, coalesce and track events from your network devices.

1. Log in to QRadar.
2. Click the **Log Activity** tab.
3. Click **Add Filter**.
4. From the first list, select **Log Source**.
5. From the **Log Source Group** list, select **Other**.
6. From the **Log Source** list, select your Universal CEF log source.
7. Click **Add Filter**.
8. From the **View** list, select **Last Hour**.
9. Optional: Click **Save Criteria** to save your existing search filter.
10. On the **Event Name** column, double-click an unknown event for your Universal CEF DSM.
11. Scroll to the Payload information at the bottom and highlight and copy the name of the event contained in the sixth field of the CEF header.



12. Click **Map Event**.
13. From the Browse for QID pane, paste the event name in the **QID/Name** search box.



14. Click **Search**.
15. Select the QID that you want to associate to your unknown Universal CEF DSM event and click **OK**.
16. Do this for all event types that come as Unknown from NetWitness Platform.

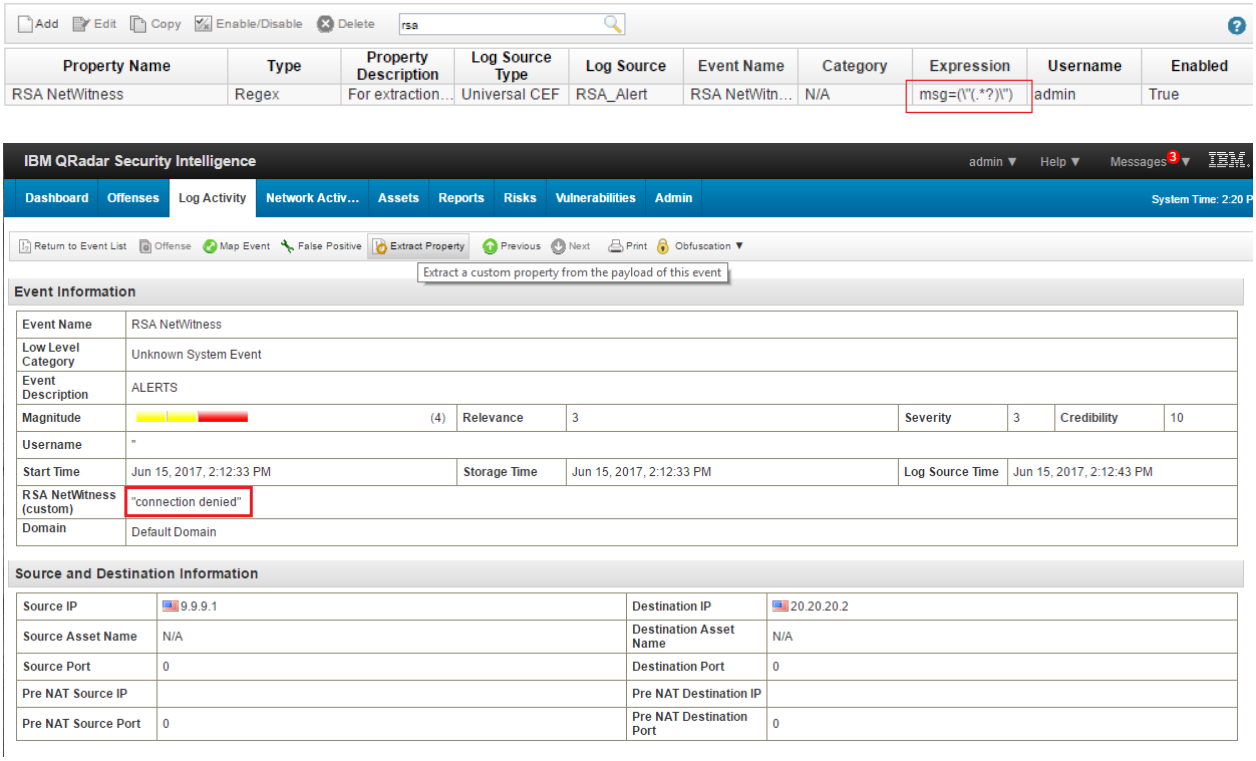
Event mapping is complete.

Add Custom Event Properties

If you need to extract information from the CEF that is not available in the standard set of properties, you can add custom event properties.

Navigate to Admin > Custom Event Properties to configure custom properties.

You can use this method to extract any key=value pair within the CEF syslog message.



Add | Edit | Copy | Enable/Disable | Delete | rsa

Property Name	Type	Property Description	Log Source Type	Log Source	Event Name	Category	Expression	Username	Enabled
RSA NetWitness	Regex	For extraction...	Universal CEF	RSA_Alert	RSA NetWitn...	N/A	msg=(\"(.*?)\")	admin	True

IBM QRadar Security Intelligence — admin ▼ | Help ▼ | Messages 3 ▼ | IBM

Dashboard | Offenses | Log Activity | Network Activ... | Assets | Reports | Risks | Vulnerabilities | Admin | System Time: 2:20 P

Return to Event List | Offense | Map Event | False Positive | Extract Property | Previous | Next | Print | Obfuscation ▼

Extract a custom property from the payload of this event

Event Information

Event Name	RSA NetWitness						
Low Level Category	Unknown System Event						
Event Description	ALERTS						
Magnitude	(4)	Relevance	3	Severity	3	Credibility	10
Username	-						
Start Time	Jun 15, 2017, 2:12:33 PM	Storage Time	Jun 15, 2017, 2:12:33 PM	Log Source Time	Jun 15, 2017, 2:12:43 PM		
RSA NetWitness (custom)	"connection denied"						
Domain	Default Domain						

Source and Destination Information

Source IP	9.9.9.1	Destination IP	20.20.20.2
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0

Qlink for NetWitness Platform

Introduction

The NetWitness Platform packet capture is frequently deployed alongside the IBM QRadar SIEM product to augment traditional Log or Flow event capture with deep visibility and NetWitness's market leading Network Forensics investigation capabilities.

QLink is a PHP script. Analysts can use it to pivot from Log or Flow events in QRadar to the NetWitness Platform Investigation screen, using source IP or destination IP data from a QRadar event as the starting drill-point into the NetWitness Platform packet capture dataset. It is possible to configure basic right-click actions without QLink: however, QLink enables focused timeQbased searches of the NetWitness Platform dataset, as opposed to broad, IPQ-only searches. QLink also addresses the following date-time challenges:

- QRadar outputs date-time variables in an epoch format, for example **1448281678752**. NetWitness Platform uses human-readable date-time format for inbound deep links, for example **2015Q11Q23T12:27Z**. Thus, tThe QRadar date-time format must be converted.
- QRadar appliances can be configured to run in a local time zone, whereas NetWitness Platform is always configured to use UTC with the administration interface applying a local timezone offset. QRadar date-time values must be adjusted to UTC, or else NetWitness Platform is queried for the wrong time period.
- QRadar date-time epoch values have millisecond resolution while the minimum time period for queries to NetWitness Platform is one minute. Thus, QRadar date-time range values must have second and millisecond values removed. The perceived loss of event time resolution is normally negated by the following point.
- QRadar provides start (event) time for Log events and a start to end time range for Flow events. However, analysts normally prefer to search NetWitness Platform data with a broader time range, so as to include additional activity and context around the event. To avoid repetitive clicking in the NetWitness Platform console to change time range values, QLink allows right-click actions that enlarge the range in preconfigured increments.

After date-time corrections are applied, QLink automatically redirects the analyst's browser to NetWitness Platform, making the right-click pivot transparent.

Deployment

You can deploy QLink to either your IBM QRadar appliance or a separate CentOS instance.

Deploy to IBM QRadar Appliance

The QLink script should be installed to `/opt/qradar/www/qlink.php` on the IBM QRadar appliance. The support status with IBM for this on-box location is not fully known, but other integration and utility scripts provided by IBM in the default QRadar installation image reside here.

Deploy to Separate CentOS Instance

Alternatively, it is a simple task to create a CentOS instance from a minimal ISO. You will need to install the **httpd** and **php** rpm packages, configure httpd to start automatically on boot, and configure the iptables firewall to permit inbound connections to the web server. Once you complete these steps, install QLink be to `/var/httpd/www`, then start the httpd service.

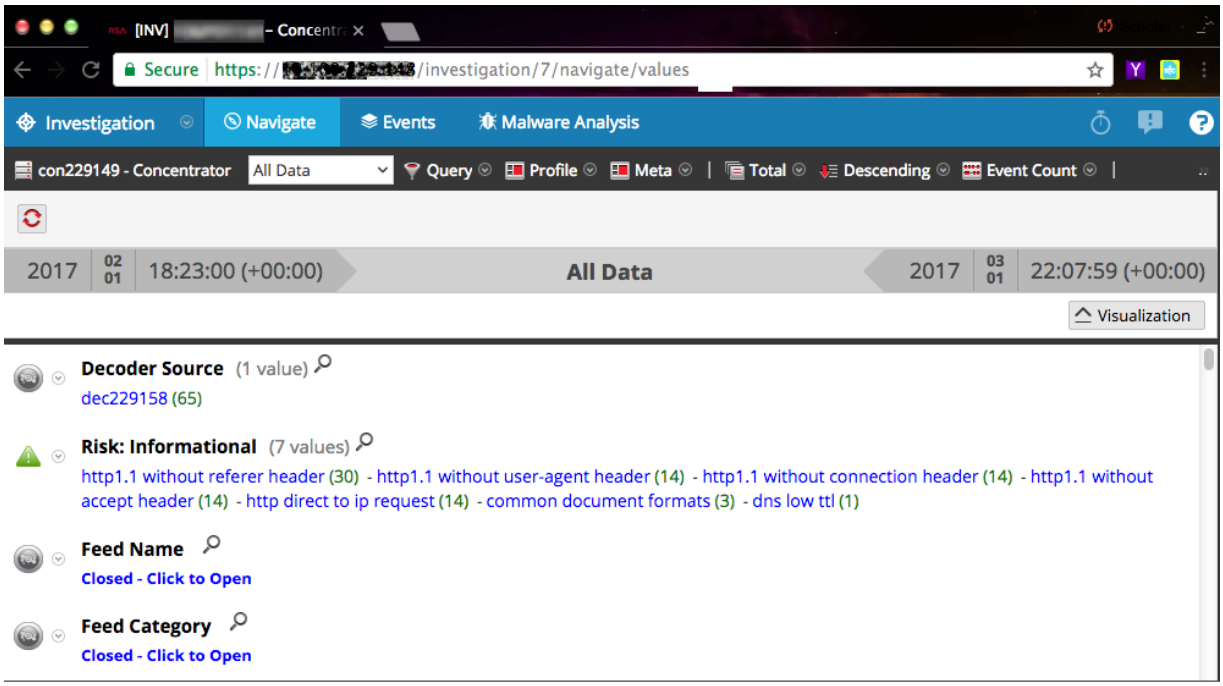
If you deploy QLink to a separate host, make sure to consider the sensitivity of the URL queries submitted to NetWitness Platform: NetWitness Platform encourages you to use SSL configuration to ensure queries are submitted from inside a secure session.

Please remember to check the `/etc/httpd/conf/httpd.conf` file. Place the `qlink.php` file in the folder mentioned under the **General Setup > DocumentRoot**.

Configuration

Once QLink has been deployed, three configuration items need to be set in the header of the script, and one in the footer of the script. The script has a number of clearly written comments to help you find these locations:

- **Header**: The FQDN or IP address of the NetWitness Platform server the script redirects to after transposing the deepQlink URL format from QRadar.
- **Header**: The node ID of the NetWitness Platform appliance in the GUI. This can be deduced from the Investigation screen. In the screenshot below, the ID value “7” can be seen in the URL bar.



- **Header**: The QRadar appliance time zone in PHP time zone format, as shown on the following website: http://php.net/manual/en/timezones.php. QLink uses Etc/UTC for the NetWitness Platform server time zone–this should not be changed.

- **Footer**: The script outputs text in a browser to show you the inbound and converted URLs during testing. To place the script into **autoQredirect** mode, you must comment out the echo statements that generate text, and uncomment the redirection function at the bottom of the script. The `/opt/qradar/conf/arielRightClick.properties` file holds configuration for QRadar right-click actions. It can be accessed via the QRadar SSH console. You can edit this file with a text editor (for example **vi**). In most installations, this file already exists. The example below shows default content.

Right-Click Properties File

The default content of the `arielRightClick.properties` file is available in the Appendix: Right-Click Properties Source Code.

Note: Comment lines begin with the pound sign (#).

Required Elements

The following elements must be included in the QLink URL:

- **query="<ip.src=$sourceIP$>"**. This is the query that you want to run against the NetWitness Platform dataset. The query must be enclosed in double quotes. Queries with multiple statements or logic that requires the use of spaces or complex characters such as **%&()|** must be URL Encoded (see http://www.w3schools.com/tags/ref_urlencode.asp) to ensure correct passing of the query in the URL. For example:

  `ip.src=192.168.10.2 && ip.dst=65.14.23.12` would be configured as:

  `query="ip.src=$sourceIP$%20%26%26%20ip.dst=$destinationIP$"`

- **stime=$variable$**. This determines the start of the time range for the NetWitness Platform search query. The **$startTime$** Ariel SDK variable is used for Log events, and **$firstPacketTime$** is used for Flow events.
- **etime=$variable$**. This determines the end of the time range for the NetWitness Platform search query. The **$endTime$** Ariel SDK variable is used for Log events, and **$lastPacketTime$** is used for Flow events. In Log events, **$endTime$** contains the same value as **$startTime$**, whereas in Flow events, the values are normally different, specifying a true time range.
- **timeRange="value"**. This is the time padding value used to expand the searched date-time range in the NetWitness Platform data set. By default, the range is 60 minutes.

Useful Elements

The following are useful elements of the the QRadar `arielRightClick.properties` file:

- **pluginActions=XXXX**. Each action must have a unique actionName, for example **XFE_URL_Lookup** as shown in the default example above. **pluginActions** must reference all configured rightQclick actionName values on a single line. The actionName is free text, but when applying many similar actions to the file, we suggest short, simple names with a logical structure to avoid confusion.

You can add comment lines to keep track of actions.

- **actionName.useFormattedValue=false**. Some online examples use this command.
- **actionName.arielProperty=sourceIP**. This configures actionName as an action when you right click on sourceIP events in the admin console. The QRadar console uses the same SDK variable in both Log and Flow events. Thus sourceIP rightQclick actions created for Log events are be visible when you right click sourceIP on Flow events; use text naming to differentiate the actions clearly. QRadar appears to support rightQclick actions on **sourceIP**, **destinationIP**, **sourcePort** and **destinationPort** only.
- **actionName.text=Investigate Event in RSA (ip.src)**. This sets the text description for the event in the admin console. NetWitness platform suggests simple, short statements for clarity.
- **actionName.url=https://qradar/qlink.php?query=XXXX**. This is the specially formatted URL used for the action. The URL points to the FQDN or IP of the QRadar admin console (or external web server) and path to the **qlink.php** script.

QLink Script Contents

The contents of the script are listed in the Appendix: QLink Configuration Script Source Code.

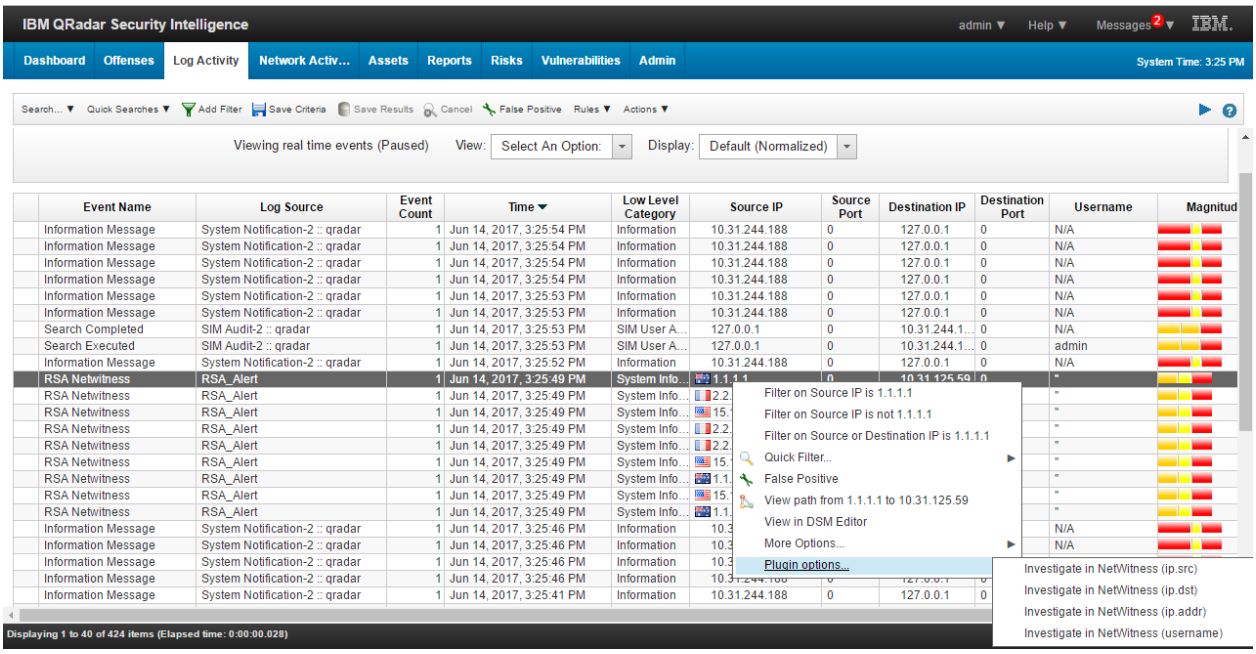
QRadar Admin Console

The following are screen shots show how the integration appears in the QRadar admin console.

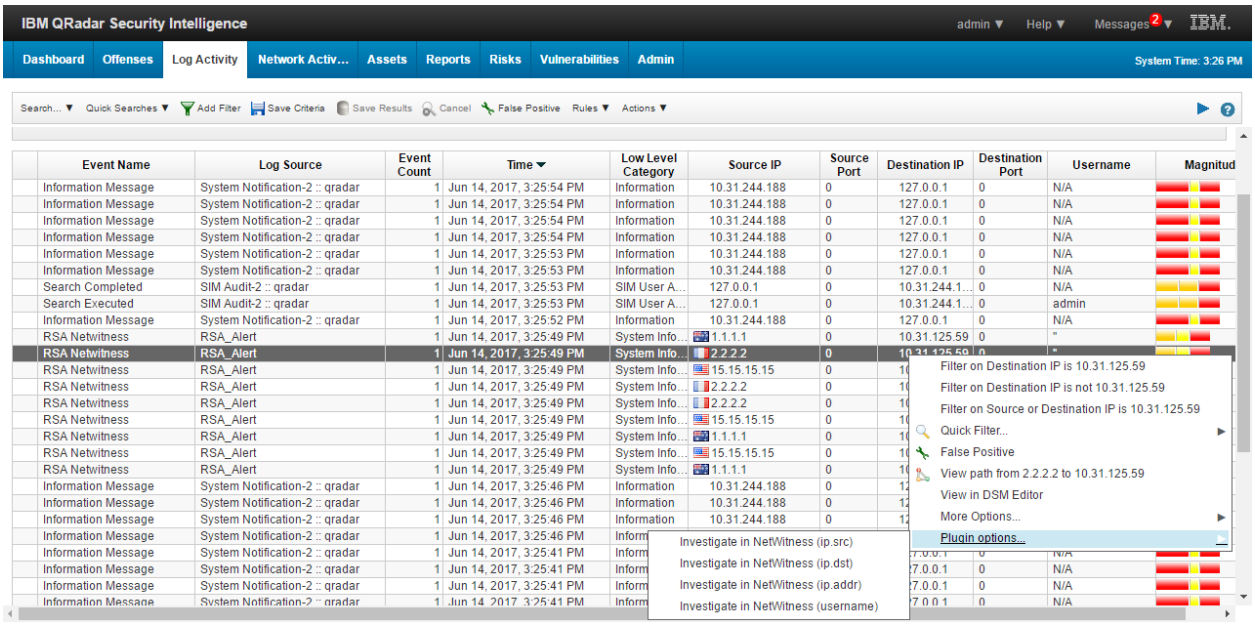
For Source IP and Destination IP right-click actions, the previous file provides options for investigating in NetWitness UI for the following:

- ip.src
- ip.dst
- ip.addr
- username: Since there is no right click on username by QRadar, this is a workaround. Provided the logs do have username, if not, null.

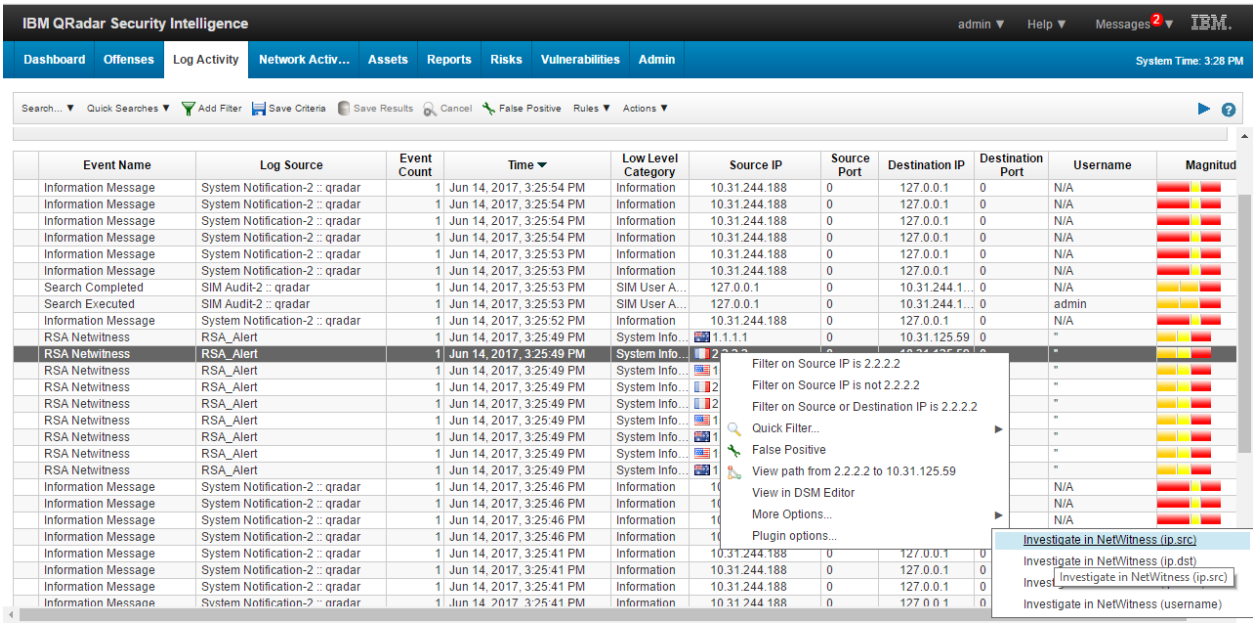
The following image shows **Right Click on Source IP**.



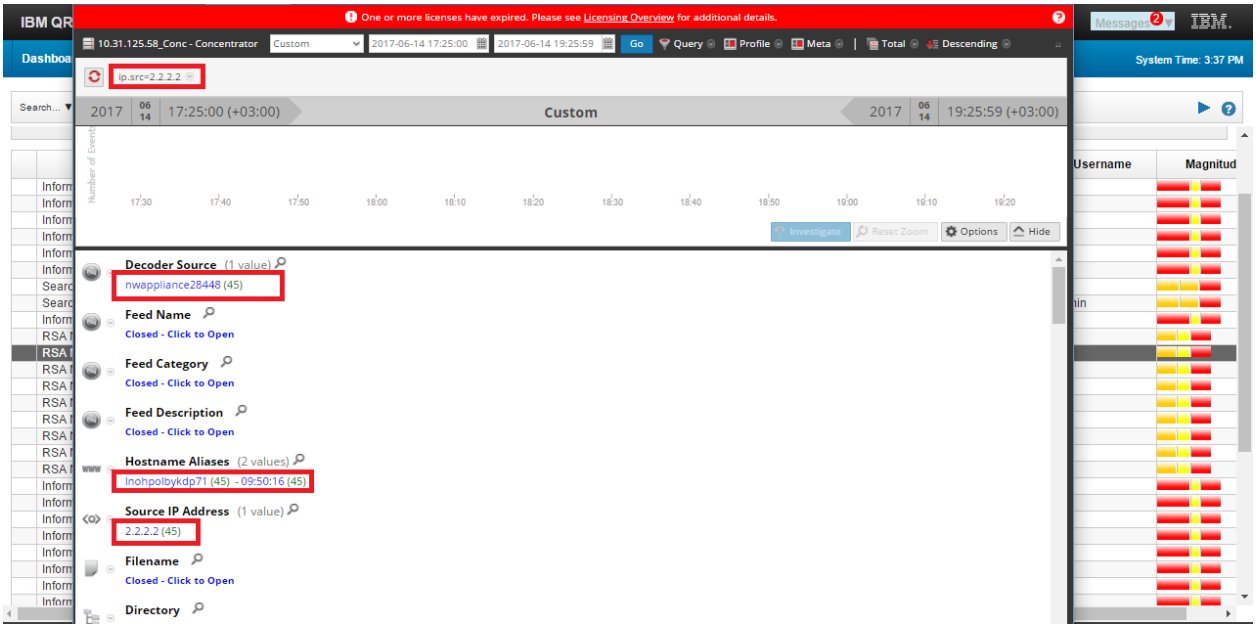
The following image shows **Right Click on Destination IP**.



The following image shows selecting **“Investigate in NetWitness (ip.src)” -1**.



The following image shows selecting **"Investigate in NetWitness (ip.src)" -2**.



For changes to take effect, you must run the service tomcat restart command. You can run this command through the Command-Line Interface (CLI) or by using the QRadar UI: **Admin > Advance > Restart Web Server**.

License and Support for QLink Configuration

The QLink script is not shipped with any form of license; you are simply free to use or modify it in any way to suit your needs. It is provided with no warranty or implied fitness for purpose, and is not supported by NetWitness platform Technical Support or NetWitness platform Professional Services. If you have questions on QLink, please post them to the NetWitness community forum where other QLink users may be able to offer assistance. The forum is located here:
https://community.rsa.com/community/products/netwitness

NetWitness Platform Right Click to QRadar

The integration where an analyst pivots from a meta field (for example IP address) in the NetWitness Platform Investigations console to IBM QRadar is not currently possible. NetWitness platform fully supports right-click actions being added to any meta element, but IBM does not expose a deep-linking URL structure to facilitate deep-link integrations by the means of right clicking and drilling into QRadar.

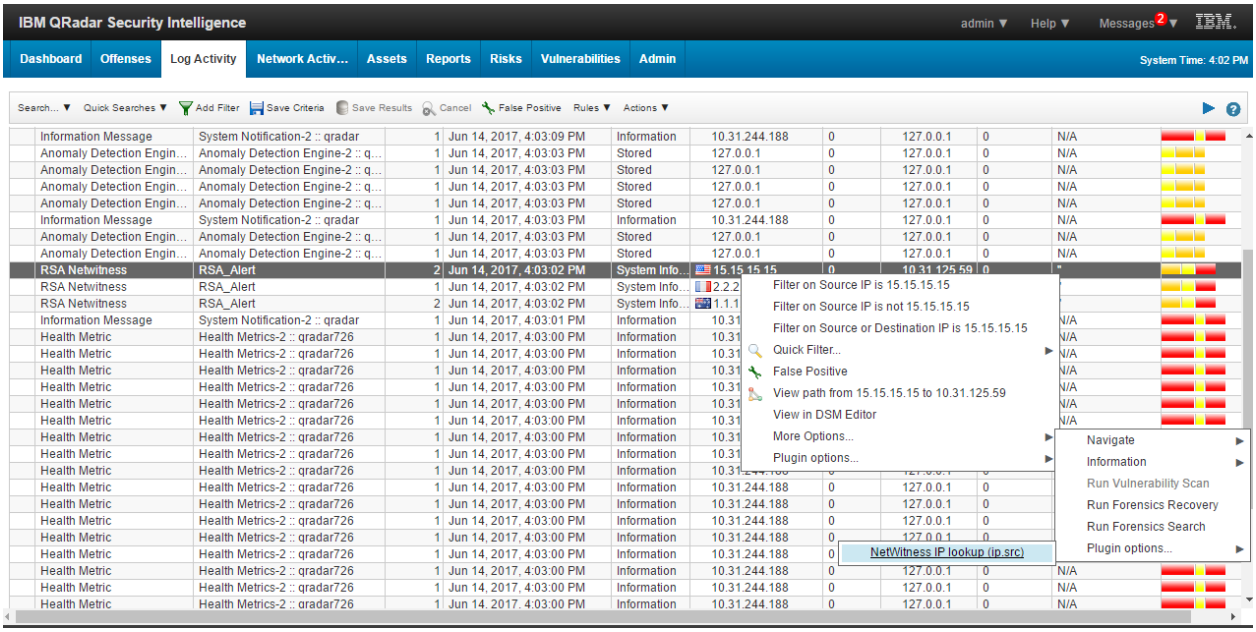
Right Click from QRadar to NetWitness Platform

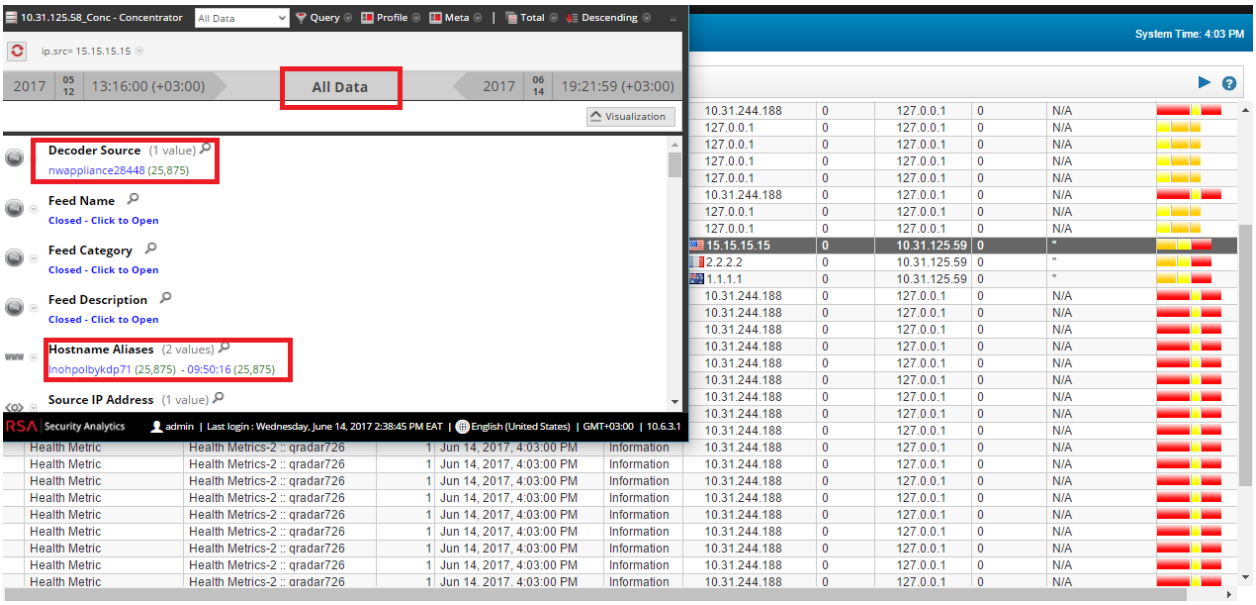
QRadar can also be configured for right-click integration with NetWitness Platform outside of the QLink script. You can create a right-click action by following the detailed documentation for supported versions on the IBM Website at this link:

http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.doc/t_CUSTOMIZING_THE_RIGHT_CLICK_MENU.html

This can be only be done on IP-based searches and do not have the time bound feature.

The following images show how the context menu behaves.





To get this behavior:

1. Open `/opt/qradar/conf/ip_context_menu.xml` in a text editor (such as vi).
2. Add the following line within the `<contextMenu></contextMenu>` element:

```
<menuEntry name="NetWitness IP lookup (ip.src)"
url="https://<Ip_of_
SA>/investigation/<DeviceID>/navigate/query/ip.src+%3D+%IP%"/>
```

3. Save the file and exit from your text editor.
4. Restart the tomcat service.

Additionally, you can also use the Threat Analytics Plugin for Google Chrome. The link to configure the Threat Analytics Plugin is located here: https://inside.dell.com/docs/DOC-182438.

Appendix: Source Code

The IBM QRadar package is delivered as a ZIP archive that contains the context actions code. You can find the package on the NetWitness Community downloads.

The code is to be used in QRadar system: add the code files to the desired folder and follow the steps mentioned below.

QLink Configuration Script Source Code

The file path is **/opt/qradar/www/qlink.php**

QLink Script Code

```
<?php
    ////////////////////////////////////////////////////////////////////////
    //
    // QLINK CONFIGURATION:
    //
    ////////////////////////////////////////////////////////////////////////
    //
    // set the NetWitness FQDN or IP address:
    $sahost = "<IP of SA>";
    //
    // set the NetWitness device ID (crib from SA 'Investigation' URLs)
    $sadevice = "<Go to the investigation page, use the number. For example
https://10.31.125.60/investigation/13/navigate use 13>";
    //
    // configure QRadar timezone, e.g. http://php.net/manual/en/timezones.php
    $dateTimeZoneIBM = new DateTimeZone('<check the timezone info from above and
then recheck using SSH into the QRadar box>');
    //
    ////////////////////////////////////////////////////////////////////////
    //
    // DO NOT TOUCH BELOW HERE!
    //
    ////////////////////////////////////////////////////////////////////////
    //
    // set NetWitness timezone to UTC by default, ONLY change if it is NOT in
UTC
    $dateTimeZoneRSA = new DateTimeZone('Etc/UTC');

    // calculate time in local timezones
    $dateTimeRSA = new DateTime("now", $dateTimeZoneRSA);
    $dateTimeIBM = new DateTime("now", $dateTimeZoneIBM);

    // calculate the timezone offset
    $offset = $dateTimeZoneIBM->getOffset($dateTimeRSA) - $dateTimeZoneRSA-
>getOffset($dateTimeRSA);

    // parse value pairs from the URL
    $ibm="https://".$_SERVER['HTTP_HOST'].$_SERVER['REQUEST_URI'];
```

```
    $ibm_parts = parse_url($ibm);
    $ibm_query_parts = parse_str($ibm_parts['query']);

    // remove quotes from query, stime, etime, fuzz
    $query = str_replace("\"", "", $query);
    $stime = str_replace("\"", "", $stime);
    $etime = str_replace("\"", "", $etime);
    $timeRange = str_replace("\"", "", $timeRange);


    // if no end time, use start time
    if ($etime == 0) {
        $etime = $stime;
    }

    // trim seconds from ibm epoch times
    $stime = substr($stime, 0, -3);
    $etime = substr($etime, 0, -3);

    // logic to determine what timezone offset maths to use
    if ($offset > 0) {
        // IBM timezone is ahead of RSA
        $stime = $stime - $offset - $timeRange;
        $etime = $etime - $offset + $timeRange;
    } elseif (0 > $time_offset) {
        // RSA timezone is ahead of IBM
        $stime = $stime + $offset - $timeRange;
        $etime = $etime + $offset + $timeRange;
    } else {
        // no timezone difference";
        $stime = $stime - $timeRange;
        $etime = $etime + $timeRange;
    }

    // output stime/etime in rsa format
    $stime = date('Y-m-d H:i', $stime);
    $stime = str_replace(" ", "T", $stime);
    $stime = $stime .= "Z";

    $etime = date('Y-m-d H:i', $etime);
    $etime = str_replace(" ", "T", $etime);
    $etime = $etime .= "Z";

    // build NetWitness URL
    $rsa = "https://" . $sahost . "/investigation/" . $sadevice
. "/navigate/query/" . $query . "/date/" . $stime . "/" . $etime;

    ////////////////////////////////////////////////////////////////////////////
    //
    // CONFIGURE TEXT-MODE/REDIRECTION-MODE BELOW HERE:
    //
    ////////////////////////////////////////////////////////////////////////////

    // uncomment for debugging
    //echo "query = " . $query . "<p>";
```

```
    //echo "ibm = " . $ibm . "<p>";
    //echo "rsa = " . $rsa;

    // uncomment to redirect browser after transformation
    header("Location: $rsa");
    die();
?>
```

Right-Click Properties Source Code

The file path is **/opt/qradar/conf/arielRightClick.properties**

Right-Click Properties Source Code

```
pluginActions=nwIPsrc0,nwIPsrc1,nwIPdst0,nwIPdst1,nwIPaddr0,nwIPaddr1,nwUsr,XFE_
URL_Lookup

#For IP search for ip.src from SourceIP
nwIPsrc0.useFormattedValue=false
nwIPsrc0.arielProperty=sourceIP
nwIPsrc0.text=Investigate in NetWitness (ip.src)
nwIPsrc0.url=https:
//10.31.244.188/qlink.php?query="ip.src=$sourceIP$"&stime="$startTime$"&etime="$
endTime$"&timeRange="3600"

# For IP search for ip.src from destinationIP
nwIPsrc1.useFormattedValue=false
nwIPsrc1.arielProperty=destinationIP
nwIPsrc1.text=Investigate in NetWitness (ip.src)
nwIPsrc1.url=https:
//10.31.244.188/qlink.php?query="ip.src=$destinationIP$"&stime="$startTime$"&eti
me="$endTime$"&timeRange="3600"

#For IP search for ip.dst from SourceIP
nwIPdst0.useFormattedValue=false
nwIPdst0.arielProperty=sourceIP
nwIPdst0.text=Investigate in NetWitness (ip.dst)
nwIPdst0.url=https:
//10.31.244.188/qlink.php?query="ip.dst=$sourceIP$"&stime="$startTime$"&etime="$
endTime$"&timeRange="3600"

# For IP search for ip.dst from destinationIP
nwIPdst1.useFormattedValue=false
nwIPdst1.arielProperty=destinationIP
nwIPdst1.text=Investigate in NetWitness (ip.dst)
nwIPdst1.url=https:
//10.31.244.188/qlink.php?query="ip.dst=$destinationIP$"&stime="$startTime$"&eti
me="$endTime$"&timeRange="3600"

#For IP search for ip.addr from SourceIP
nwIPaddr0.useFormattedValue=false
```

```
nwIPaddr0.arielProperty=sourceIP
nwIPaddr0.text=Investigate in NetWitness (ip.addr)
nwIPaddr0.url=https:
//10.31.244.188/qlink.php?query="ip.addr=$sourceIP$"&stime="$startTime$"&etime="
$endTime$"&timeRange="3600"

# For IP search for ip.addr from destinationIP
nwIPaddr1.useFormattedValue=false
nwIPaddr1.arielProperty=destinationIP
nwIPaddr1.text=Investigate in NetWitness (ip.addr)
nwIPaddr1.url=https:
//10.31.244.188/qlink.php?query="ip.addr=$destinationIP$"&stime="$startTime$"&et
ime="$endTime$"&timeRange="3600"

#For search on username
nwUsr.useFormattedValue=false
nwUsr.arielProperty=sourceIP,destinationIP
nwUsr.text=Investigate in NetWitness (username)
nwUsr.url=https:
//10.31.244.188/qlink.php?query="username=$userName$"&stime="$startTime$"&etime=
"$endTime$"&timeRange="3600"

# begin XFE integration
XFE_URL_Lookup.arielProperty=URL
XFE_URL_Lookup.text=X-Force Exchange Lookup
XFE_URL_Lookup.url=https://exchange.xforce.ibmcloud.com/#/url/$URL$
# end XFE integration

# Flow / destination + source / fuzz=1800
dsF1800.useFormattedValue=false
dsF1800.arielProperty=destinationIP
dsF1800.text=Investigate Flow in RSA (ip.dst & ip.src) +/Q 30 mins
dsF1800.url=https:
//192.168.1.181/qlink.php?query="ip.dst=$destinationIP$%20%26%26%20ip.src=$sourc
eIP$"&stime="$firstPacketTim
e$"&etime="$lastPacketTime$"&fuzz="1800"

# begin XFE integration
XFE_URL_Lookup.arielProperty=URL
XFE_URL_Lookup.text=XQForce Exchange Lookup
XFE_URL_Lookup.url=https://exchange.xforce.ibmcloud.com/#/url/$URL$
# end XFE integration
```