IBM Security QRadar
Version 7.2.1

SNMP Trap Configuration

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page 13.

CONTENTS

1 QRadar SNMP trap configuration

This technical note provides instructions for how to customize the SNMP configuration parameters that are displayed in the Custom Rules Wizard and modify the SNMP traps that the Custom Rule Engine sends.

Unless otherwise noted, all references to QRadar® refer to IBM® Security QRadar SIEM, IBM Security QRadar Log Manager, and IBM Security QRadar Network Anomaly Detection. References to flows do not apply to QRadar Log Manager.

SNMP trap overview

A Simple Network Management Protocol (SNMP) trap is an event or offense notification that QRadar can send to a configured SNMP host. In the Custom Rules Wizard, you can configure any rule to generate a rule response that sends an SNMP trap as a result of a rule's configured conditions being met.

The technical note is intended for system administrators experienced with SNMP and manipulating XML files. For more information on SNMP, go to the http://www.ietf.org/ website and type RFC 1157 in the search field.

You can customize the SNMP configuration parameters that are displayed in the Custom Rules Wizard and you can modify the SNMP traps that the Custom Rule Engine sends. QRadar provides two default traps, however, you can add custom traps or modify the existing traps to use new parameters.

Customizing the Custom Rules Wizard SNMP parameters

You can edit the SNMP trap parameter to customize information that is sent when a rule condition is met.

About this task

Use the Custom Rules Wizard to send SNMP traps if a rule meets the configured conditions. The SNMP trap parameters are only displayed in the Custom Rules Wizard if SNMP is enabled within the system settings.

For more information on the Custom Rules Wizard and QRadar system settings, see the *Administration Guide* for your product.

Procedure

Step 1 Using SSH, log in to QRadar as the root user.

Step 2 Navigate to the **/opt/qradar/conf** directory.

Step 3 Make back-up copies of the following files:

- **eventCRE.snmp.xml**
- **offenseCRE.snmp.xml**

Step 4 Choose one of the following options:

- To edit the SNMP parameters for event rules, open the **eventCRE.snmp.xml** file.
- To edit the SNMP parameters for offense rules, open the **offenseCRE.snmp.xml** file.

Step 5 Insert the following section into the file inside the <snmp> tag before the <creSNMPTrap> element, and update the labels as required:

Note: The label values in this code are for example purposes only. You must update the labels.

```
<creSNMPResponse name="snmp_response_1">
    <custom name="MyColor">
         <string label="What is your favorite color?"/>
    </custom>
    <custom name="MyCategory">
         <list label="Select a category">
               <option label="Label1" value="Category1"/>
               <option label="Label2" value="Category2"/>
         </list>
    </custom>
</creSNMPResponse>
```

Step 6 Save and exit the file.

Step 7 Copy the file from the **/opt/qradar/conf** directory to the /store/configservices/staging/globalconfig directory.

Step 8 Log in to the QRadar user interface.

Step 9 On the **Admin** tab menu, select **Advanced > Deploy Full Configuration**.

What to do next

Configure SNMP trap output.

Customizing SNMP trap output

SNMP allows QRadar to send traps that provide information when rule conditions have been met.

By default, QRadar adheres to the QRadar MIB. You can customize the output of the SNMP traps to adhere to any MIB.

About this task

When updating the variable binding information, include one of the following parameters:

Table 1-1 Value types for updating the variable binding information

Parameter	Description
string	Enables you to configure multiple values within the variable bindings.
integer32	Enables you to include a numerical value in the variable binding. For example: **name="ATTACKER_PORT" type="integer32">%ATTACKER_PORT%**
oid	Enables you to include OID information in the variable binding. For example: **OID="1.3.6.1.4.1.20212.2.46"**
ipAddress	Enables you to include IP address information in the variable binding. For example: **name="TARGET_IP" type="ipaddress">%TARGET_IP%**
gauge32	Enables you to include a numerical value range in the variable binding.
counter64	Enables you to include a numerical value that increments within a defined minimum and maximum range in the variable binding.

Procedure

Step 1 Using SSH, log in to QRadar as the root user.

Step 2 Navigate to the `/opt/qradar/conf` directory.

Step 3 Make back-up copies of the following files:

- `eventCRE.snmp.xml`
- `offenseCRE.snmp.xml`

Step 4 Choose one of the following options:

a To edit an event rule, open the **`eventCRE.snmp.xml`** file.

b To edit an offense rule, open the **`offenseCRE.snmp.xml`** file.

Step 5 To change the trap that is used for SNMP trap notification, update the following line with the appropriate trap OID:

```
-<creSNMPTrap version="3" OID="1.3.6.1.4.1.20212.1.1"
name="eventCRENotification">
```

Step 6 Update the variable binding information, as necessary. You can include one of the following values types from Table 1-1.

For each of the above options, you can include one of the following fields:

- **NATIVE** - Include a native event from QRadar. For the NATIVE value, you can include any of the following fields:
  - **LOCALHOST**
  - **DATE_AND_TIME**
  - **OFFENSE_ID**
  - **OFFENSE_DESCRIPTION**
  - **OFFENSE_LINK**
  - **MAGNITUDE**
  - **SEVERITY**
  - **CREDITIBILITY**
  - **RELEVANCE**
  - **CATEGORY_COUNT**
  - **TOP_CATEGORIES**
  - **TOP_CATEGORY_1**
  - **TOP_CATEGORY_2**
  - **TOP_CATEGORY_3**
  - **TOP_CATEGORY_4**
  - **TOP_CATEGORY_5**
  - **ATTACKER_COUNT**
  - **ATTACKER_IP**
  - **ATTACKER_USERNAME**
  - **ATTACKER_NETWORKS**
  - **TOP_ATTACKER_IPS**
  - **TOP_ATTACKER_IP_1**
  - **TOP_ATTACKER_IP_2**
  - **TOP_ATTACKER_IP_3**

- **TOP_ATTACKER_IP_4**
- **TOP_ATTACKER_IP_5**
- **TOP_ATTACKER_USERNAMES**
- **TOP_ATTACKER_USERNAME_1**
- **TOP_ATTACKER_USERNAME_2**
- **TOP_ATTACKER_USERNAME_3**
- **TOP_ATTACKER_USERNAME_4**
- **TOP_ATTACKER_USERNAME_5**
- **TARGET_COUNT**
- **TARGET_IP**
- **TARGET_USERNAME**
- **TARGET_NETWORKS**
- **TOP_TARGET_IPS**
- **TOP_TARGET_IP_1**
- **TOP_TARGET_IP_2**
- **TOP_TARGET_IP_3**
- **TOP_TARGET_IP_4**
- **TOP_TARGET_IP_5**
- **TOP_TARGET_USERNAMES**
- **TOP_TARGET_USERNAME_1**
- **TOP_TARGET_USERNAME_2**
- **TOP_TARGET_USERNAME_3**
- **TOP_TARGET_USERNAME_4**
- **TOP_TARGET_USERNAME_5**
- **ANNOTATION_COUNT**
- **TOP_ANNOTATION_1**
- **TOP_ANNOTATION_2**
- **TOP_ANNOTATION_3**
- **TOP_ANNOTATION_4**
- **TOP_ANNOTATION_5**
- **RULE_COUNT**
- **RULE_NAMES**
- **EVENT_COUNT**
- **EVENT_ID**
- **QID**

- **EVENT_NAME**
- **EVENT_DESCRIPTION**
- **CATEGORY_ID**
- **CATEGORY_NAME**
- **CATEGORY**
- **RULE_ID**
- **RULE_NAME**
- **RULE_DESCRIPTION**
- **RULE_NOTES**
- **SOURCE_IP**
- **SOURCE_PORT**
- **DESTINATION_IP**
- **DESTINATION_PORT**
- **PROTOCOL**
- **DATASOURCE_ID**
- **DATASOURCE_NAME**
- **CUSTOM_PROPERTY_NAME**

For more information on the native fields, access and open the snmp.help file located in the /opt/qradar/conf directory.

You can put any native field into a variable binding by surrounding the native field name with percentage (%) signs. Within the percentage signs, native fields must match the value type. For example, if the value type is **ipAddress**, you must use a native or custom variable that is an IP address. The **string** value type accepts any format.

- **TEXT** - Type the text that you want to include in the SNMP trap.
- **CUSTOM** - Type the custom SNMP trap information. This is information that you configured in **Customizing the Custom Rules Wizard SNMP parameters**. For example, if you used the default file information and wanted to include this information in the SNMP trap, you should include the following:

```
<variableBinding name="My Color Variable Binding"
OID="1.3.6.1.4.1.20212.3.1" type="string">My favorite color
is %MyColor%</variableBinding>
```

You can put any custom field into a variable binding by surrounding the native field name with percentage (%) signs. Within the percentage signs, custom fields must match the value type. For example, if the value type is **ipAddress**, you must use a native or custom variable that is an IP address. The **string** value type accepts any format.

For example, if you use the default information, the following SNMP trap is displayed if the rule conditions are met:

2006-07-11 16:06:44 NET-SNMP version 5.2.1 Started.

```
Cold Start: INFORM, SNMP v3, user admin, context
-SNMPv2-MIB::sysUPTime.0 - Timeticks: (555) 0:00:05.55
-SNMPv2-MIB::snmpTrapOID.0 = OID:
SNMPv2-SMI::enterprise.20212.200.0
-SNMPv2-SMI::enterprises:20212.100 = STRING: "Tue Jul 11
16:06:55 ADT 2006 QRADAR Custom Rule Engine Notification - Rule
'Network Scan' has fired. 172.168.1.42:32000 -> 10.100.100.25:80
6, Event Name: EmptyEventName, QID: 42, Category: 1004, Notes: A
scan of the network was detected"
```

Step 7 Save and exit the file.

Step 8 Copy the file from the **/opt/qradar/conf** directory to the /store/configservices/staging/globalconfig directory.

Step 9 Log in to the QRadar user interface.

Step 10 On the **Admin** tab menu, select **Advanced > Deploy Full Configuration**.

Adding a custom SNMP trap

You can create a new option for the SNMP trap selection in the Custom Rule Wizard. The trap names specified in the list box are configured in the master SNMP configuration file (snmp-master.xml).

About this task

To create a new trap, you need to create a new SNMP settings file, and then add the file name to the SNMP-master.xml file.

<include> elements have two attributes:

- **name** - The name of the trap you want to display in the list box.
- **uri** - The name of the custom SNMP settings file. For example:

  ```
  <include name="Custom_Event_Name" uri="customSNMPdef01.xml"/>
  ```

Procedure

Step 1 Using SSH, log in to QRadar as the root user.

Step 2 Navigate to the /opt/qradar/conf directory.

Step 3 Create an SNMP settings file for the new trap. Tip: Copy, rename, and modify one of the existing SNMP settings files.

Step 4 Make a back-up copy of the snmp-master.xml file.

Step 5 Open the snmp-master.xml file for editing.

Step 6 Add a new **<include>** element. The traps are displayed in the menu in the same order in which they are listed in the snmp-master.xml file.

Step 7 Save the snmp-master.xml file.

Step 8 Copy the file from the **/opt/qradar/conf** directory to the /store/configservices/staging/globalconfig directory.

Step 9 Log in to the QRadar user interface.

Step 10 On the **Admin** tab menu, select **Advanced > Deploy Full Configuration**.

Sending SNMP traps to a specific host

By default, SNMP traps are sent to the host identified in your host.conf file; however, you can customize the snmp.xml file to send SNMP traps to a different host.

Procedure

Step 1 Using SSH, log in to QRadar as the root user.

Step 2 Make back-up copies of the following files:

- **eventCRE.snmp.xml**
- **offenseCRE.snmp.xml**

Step 3 Choose one of the following options:

a To edit an event rule, open the **eventCRE.snmp.xml** file.

b To edit an offense rule, open the **offenseCRE.snmp.xml** file.

Step 4 Add the <trapConfig> tag into the file inside the <snmp> tag after the <creSNMPTrap> element:

```
<trapConfig>
     <!-- All attribute values are default -->
     <snmpHost snmpVersion="3" port="162" retries="2" timeout="500">HOST</snmpHost>
     <!-- Community String for Version 2 -->
     <communityString>COMMUNITY_STRING</communityString>
     <!-- authenticationProtocol (MD5 or SHA)securityLevel (AUTH_PRIV, AUTH_NOPRIV
     or NOAUTH_PRIV) -->
     <authentication authenticationProtocol="MD5"securityLevel="AUTH_PRIV">
     AUTH_PASSWORD </authentication>
     <!-- decryptionProtocol (DES, AES128, AES192 or AES256) --> <decryption
     decryptionProtocol="AES256"> DECRYPTIONPASSWORD </decryption>
     <!-- SNMP USER-->
     <user> SNMP_USER </user>
</trapConfig>
```

Update the attributes listed in the following table:

Table 1-2 Sending SNMP traps to a specific host

Option	Description
</snmpHost>	Identify the host to which you want to send SNMP traps.
<communityString>	Specify the commmunity string for the host.
<authentication>	Specify an authenticationprotocol, security level and password for the host.
<decryption>	Specify the decryption protocol and password for the host.
<user>	Specify the SNMP user.

Step 5 Save and exit the file.

Step 6 Copy the file from the **`/opt/qradar/conf`** directory to the `/store/configservices/staging/globalconfig` directory.

Step 7 Log in to the QRadar user interface.

Step 8 On the **Admin** tab menu, select **Advanced > Deploy Full Configuration**.

A NOTICES AND TRADEMARKS

What's in this appendix:

This section describes some important notices, trademarks, and compliance information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the

capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at *http:\\www.ibm.com/legal/copytrade.shtml*.