Course Exercises

IBM QRadar SIEM Advanced Topics

Course code BQ203 ERC 1.0

IBM Training

June 2018 edition

NOTICES

This information was developed for products and services offered in the USA.

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, MD-NC119
Armonk, NY 10504-1785
United States of America

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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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.

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.

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.

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 www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.

ITIL is a Registered Trade Mark of AXELOS Limited.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Contents

About these exercises

Virtual machines

The lab environment uses the following two virtual machines (VMs):

- QRadar - a virtual machine running IBM QRadar on Red Hat Enterprise Linux.
- Client - a virtual machine providing a graphical user interface.

Logging in to the Client VM

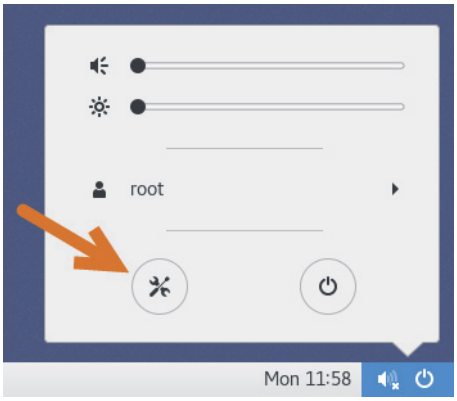
The operating system of the Client VM is configured to automatically log you in as **root** user without the need to enter a password. Screen lock is disabled. If you need to authenticate as **root** user, enter the following password:

`P@ssw0rd` the `'0'` is the digit zero

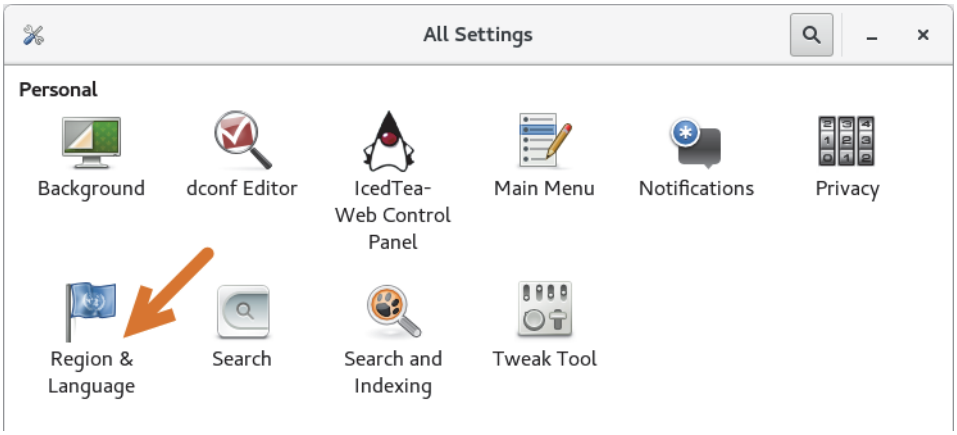
Changing the keyboard layout

If your keyboard does not use the US English layout, perform the following steps to configure the input source:

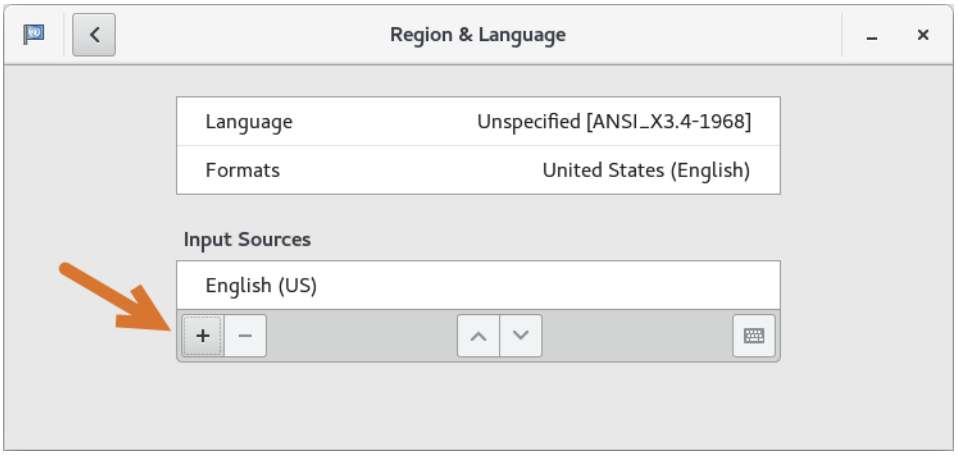
1. To open the System Menu, click the **bottom-right corner** of the desktop.
2. To open the System Settings, click the **screwdriver and wrench** icon.



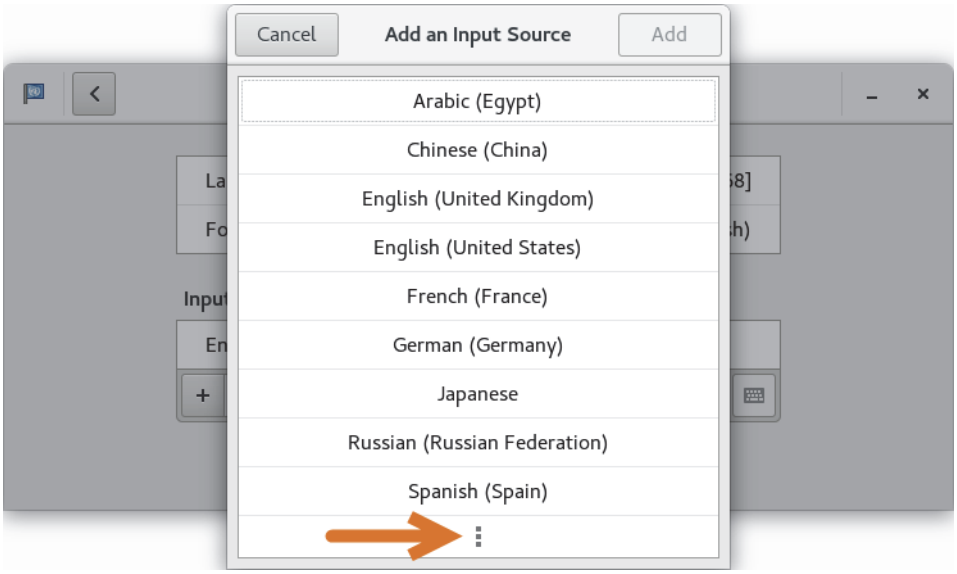
3. In the All Settings window, click the **Region & Language** icon.



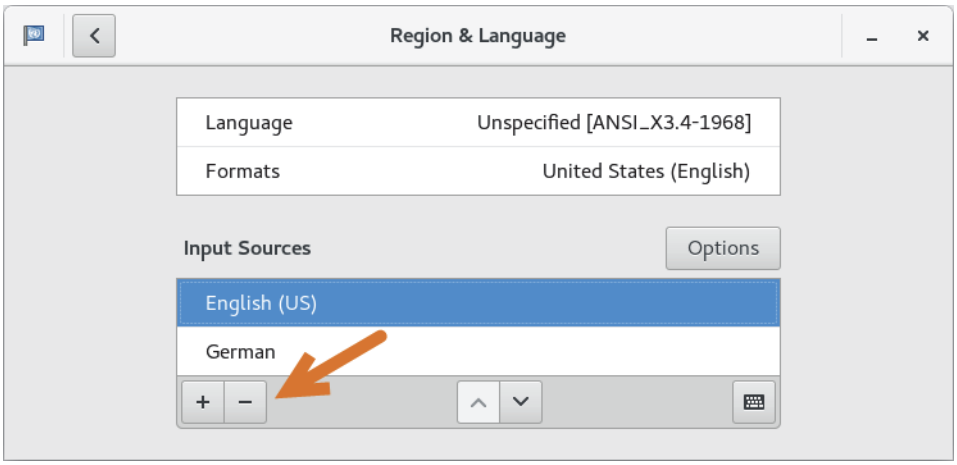
4. In the Region & Language window, click the **plus (+)** button.



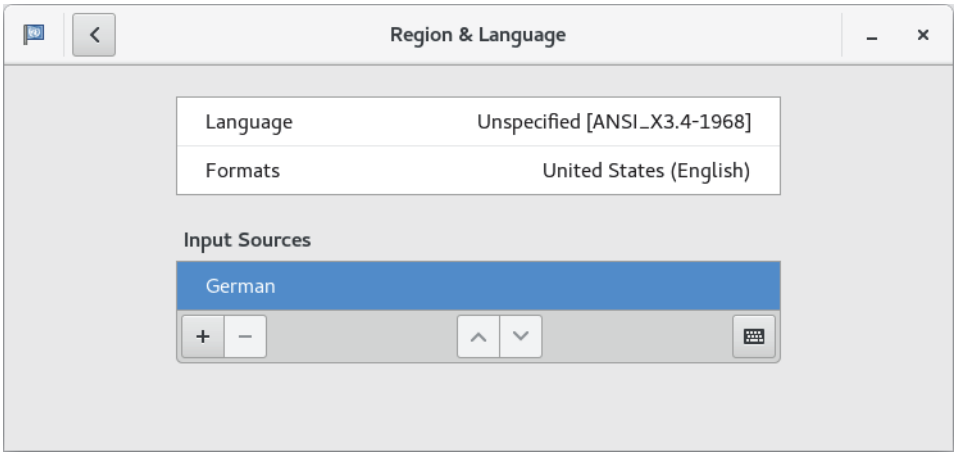
5. In the Add an Input Source window, select your keyboard layout. If your layout is not displayed, click the **three vertical dots** at the bottom.



6. Select the **English (US)** input source.
7. To remove the English (US) input source, click the **minus (-)** button.



8. Verify that the Input Sources list displays only your keyboard layout.



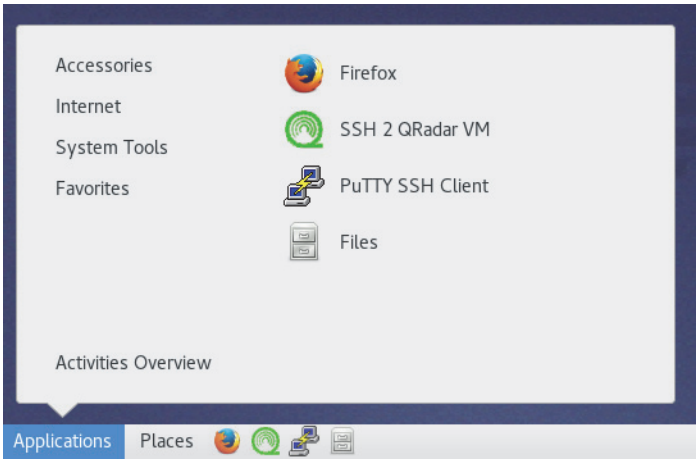
9. Close the *Region & Language* window.

Logging in to the QRadar user interface

To log in to QRadar, perform the following steps:

1. To start the web browser, click the **Firefox** icon on the bottom panel of the desktop.

You can also click **Applications** in the bottom-left corner of the desktop, and click the **Firefox** icon to open the web browser.



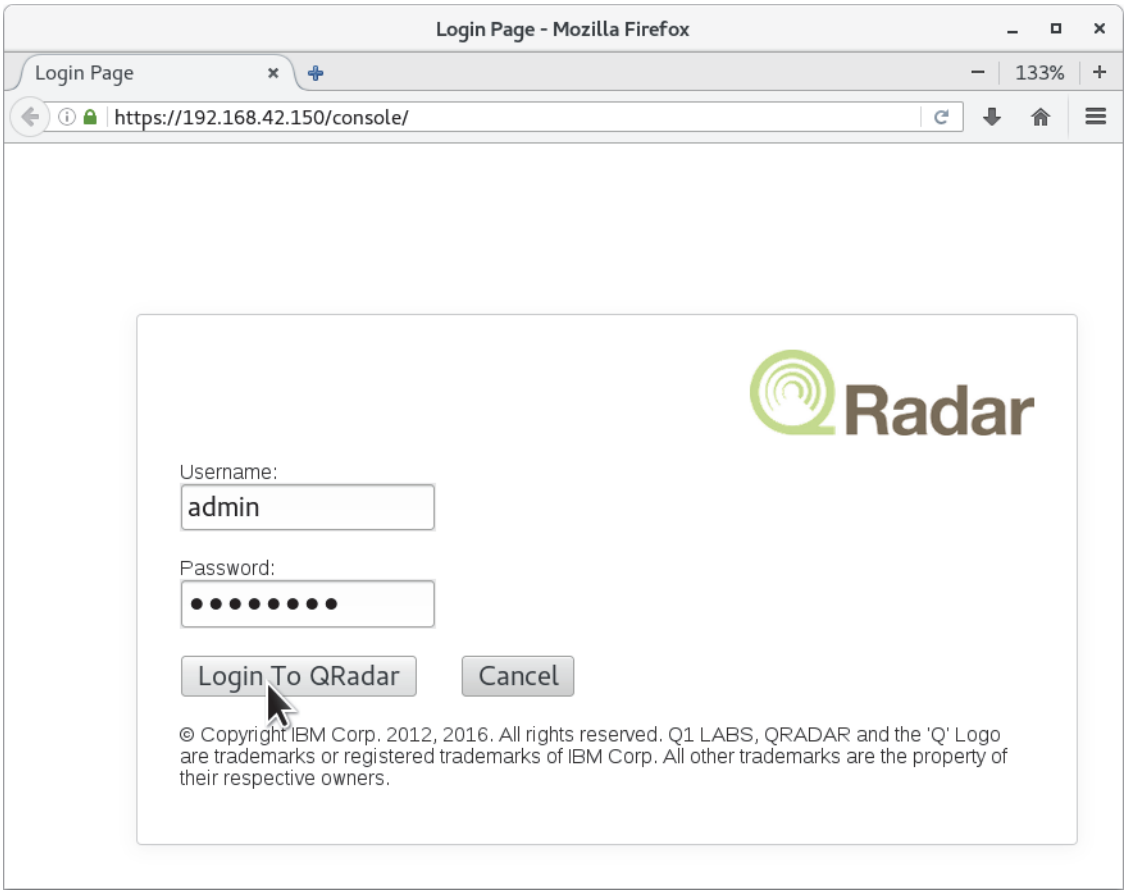
2. Firefox starts and loads the QRadar login page. If the login page does not open, QRadar is still in the process of starting. Wait at least one minute and click the **Home** icon in the upper-right corner of Firefox to try again.

3. On the QRadar login page, the **Username** and **Password** fields should already be populated. If they are not populated, enter the following credentials:

   Username: `admin`

   Password: `P@ssw0rd` the `'0'` is the digit zero

4. Click **Login To QRadar**.



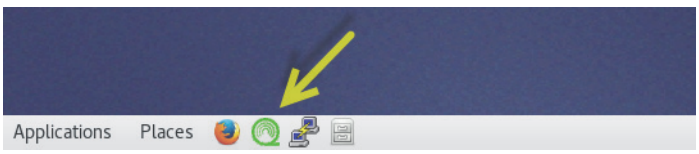
5. To zoom in, click the **plus (+)** symbol in the upper-right corner of Firefox.

   To zoom out, click the **minus (-)** symbol in the upper-right corner of Firefox.

Running commands on the QRadar VM

To run scripts that feed prepared sample data to QRadar, perform the following steps:

1. To open an SSH session to the QRadar VM, click the icon, that resembles the letter **Q** of QRadar, on the bottom panel.



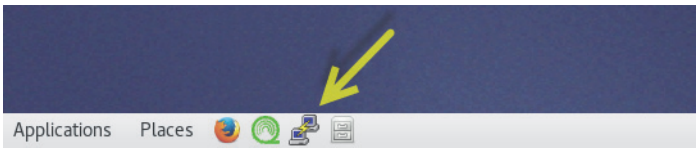
   You can also click **Applications** in the bottom-left corner of the desktop, and click the **Q** icon to open an SSH session to the QRadar VM.

   Unless you are logged in automatically, enter the following credentials:

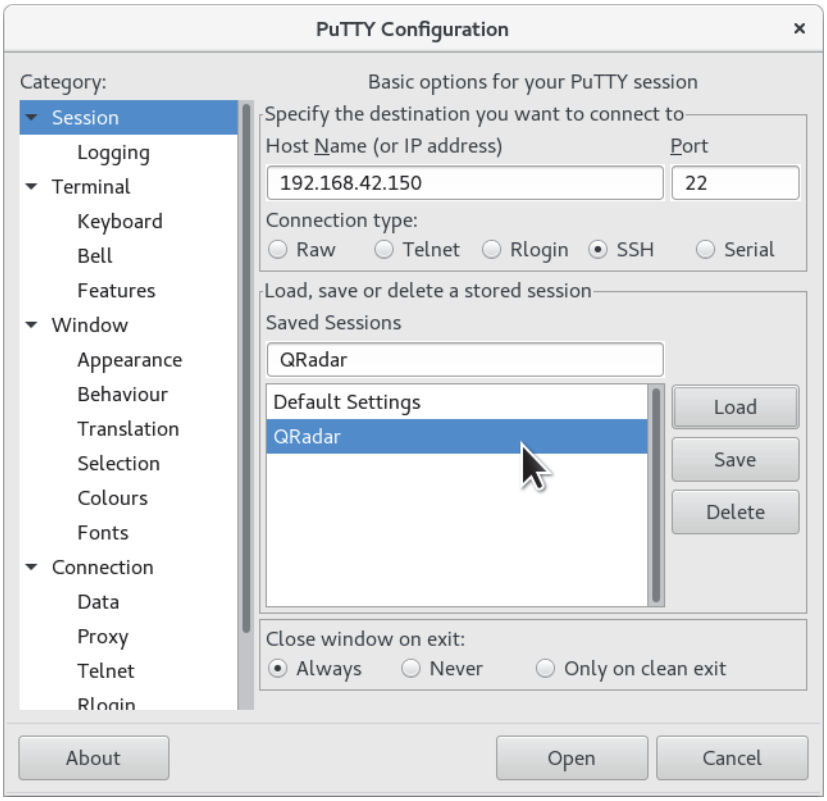
   Username: `admin`

Password: `P@ssw0rd` the `'0'` is the digit zero

2. Instead of using the OpenSSH client in a terminal, you can use PuTTY. To start PuTTY, click the **PuTTY** icon on the bottom panel or in the **Applications** menu.



In PuTTY, double-click the **QRadar** saved session to connect to the QRadar VM.



Unit 1 Log source types exercises

Your firewalls, proxies, user directories, and other IT systems record the footprints of attacks and policy violations as events in their log files. By themselves, these events might not raise any suspicion. To connect the dots between events, IBM QRadar SIEM can correlate these scattered events into offenses to alert you to suspicious activities.

After QRadar SIEM has received the original raw events and before the correlation can begin, QRadar SIEM parses and normalizes the IP addresses, user ID, and other fields from the original raw event to create a **normalized event**. It addition, QRadar SIEM names, rates, and categorizes each normalized event. QRadar SIEM uses the normalized events to correlate, for example, IP addresses from raw events that arrive in different formats from different sources.

Device Support Modules (DSM) enable QRadar SIEM to create normalized events from raw events. If QRadar SIEM receives raw events from a new source, each DSM analyses them in order to discover whether the DSM is built to create normalized events from the raw events of this type of software or network device. For many widely used software and network devices, QRadar SIEM provides DSMs. If QRadar SIEM does not provide a DSM for a source of raw events, you can configure QRadar SIEM to create proper normalized events suitable for correlation.

In this lab, QRadar SIEM receives raw events from a simplified physical access system. Because QRadar SIEM does not provide a DSM for this source, you use the DSM Editor to create a log source type for them. To parse and normalize properties, such as the username, from the raw events, you configure the new log source type with regular expressions. Furthermore, you create unique identifiers and mappings so that QRadar SIEM can name, rate, and categorize the events from the simplified physical access system. For verification you create a log source of the new log source type and replay raw events.

Note: For this exercise you can choose between two versions on how to perform it.

Version A is a bit more challenging. It is designed for experienced QRadar users who want to perform the exercises on their own with basic instructions what to do.

Version B is easier. It is designed for QRadar users with limited experience who want to perform the exercises step by step following more detailed instructions what **and** how to do it.

Hint: Feel free to use the version of your choice. You can anytime flip between the versions for instance when you get stuck in the harder version or if you consider the easier version is not challenging enough.

Version A Exercises

Exercise 1 a) Sending unknown events to QRadar SIEM

In this exercise, you send raw events from the physical access system to QRadar SIEM. None of the bundled DSMs can discover, parse, and normalize these raw events. You observe how QRadar SIEM displays events from unsupported sources.

1. Open a remote shell to the QRadar VM.
2. To feed the raw events prepared for this exercise to QRadar SIEM change into the labfiles directory (cd /labfiles) start the script sendPhysicalAccess.sh and let it run.
3. Log in to the QRadar user interface and watch the incoming events in the Log Activity tab.
4. What is the Event Name and the Low Level Category of the events?
5. What is the log source for these events?
6. Analyze the payload information of one event.
7. What is the log source identifier for this event?

Exercise 2 a) Using the DSM Editor to create a new log source type

QRadar SIEM does not provide a DSM for a source of these raw events. To configure QRadar SIEM for these events, start the DSM Editor and create a new log source type.

1. Open the DSM Editor from the **Admin** tab.
2. In the Select Log Source Type Window click **Create New**.
3. Enter “Physical Access” as Log Source Type Name and click **Save**.

Exercise 3 a) Adding a Physical Access log source

Using the Log Source Type Physical Access you can now add a Log Source of this type to configure QRadar to identify the raw events as coming from the physical access system.

1. Still on the **Admin** tab go to **Log Sources** and add a log source ot the type Physical Access.
2. To configure the new log source, enter the values from the following table.

Field / Option	Setting
Log Source Name	Physical Access Headquarter
Log Source Description	Physical Access Control System
Log Source Type	Physical Access
Protocol Configuration	Syslog
Log Source Identifier	10.0.120.12
Coalescing Events	Clear check mark

3. Click **Save** and Deploy Changes.

Hint: If clicking **Deploy Changes** does not have any effect, double-click the **Admin** tab. The double-click resets the tab to its default settings. Click **Deploy Changes** again.

4. After the change has been deployed check in the Log Activity tab to what log source the incoming events are assigned to.

Exercise 4 a) Starting the DSM Editor from the Log Activity tab

1. From the Log Activity tab select at least four events from the Physical Access Headquarter log source.

Hint: To be able to select events click on the “Pause” button on right side of the menu on the top.

2. From the actions menu at the top of the screen select DSM Editor.

3. What information is displayed in the upper right workspace?

Exercise 5 a) Configuring property parsing

The Workspace section of the DSM Editor contains the raw events as they were sent by the physical access system. Observe that the raw events contain the following information:

- Time stamp of the syslog message header
- IP address of the physical access system
- Time stamp recorded by the physical access system
- Location
- User ID
- Username
- Entrance
- Access decision
- Access direction

The more information QRadar SIEM can use, the better it can detect suspicious activities. Therefore, you would configure QRadar SIEM to parse and normalize all of the above information, if this would be a real physical access system. This lab parses and normalizes only three properties as examples.

The Log Activity Preview in the lower-right part of the DSM Editor displays property values parsed from the raw events in the Workspace. Perform the following steps to configure the Log Activity Preview to display only the example properties:

1. Click the **wrench** symbol and select the following properties: Event ID, Log Source Time, Username.
2. Scroll down and click **Update**.
3. What changed in the **Log Activity Preview**?
4. Start parsing the event properties on the left side of the DSM Editor.
5. Locate the **Username** from the **Properties** tab.
6. Click the **Username** property and select **Override system behavior**.
7. Enter `\tName:(.*?)\tEntrance:` as Regex.
8. What is displayed in the payload of the sample events?
9. What colour has he capture group?

10. To reuse the strings that the capturing group of the regular expression in Regex match, enter for Format String the following back reference: `$1`
11. Click OK to save the configuration of Username.
12. Parse the **Log Source Time** in the same manner.
13. For Regex use: `\s(\d{2}/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\tLocation:`
14. For Format string use: `$1`
15. For Date Format use: `dd/MMM/yyyy:HH:mm:ss`
16. The next steps deal with the most important property the **Event ID**

Each event informs about an action that a log source recorded as raw event. The example physical access system performs three actions:

- Access outbound granted
- Access inbound granted
- Access inbound denied

The purpose of the Event ID property is to identify these three actions. Therefore, each action needs to parse to a different string. To parse the Event ID property, perform the following steps:

17. Parse the Event ID
18. For Regex use:

```
\tAccess:(Granted|Denied)\tDirection:(In|Out)$
```

19. For Format string use:

```
Access:$2:$1
```

20. What is now displayed in the **Log Activity Preview**?
21. To save your configuration scroll to the bottom of the DSM Editor and click
22. **Save**.
23. Click **Cancel** to close the DSM Editor.

Exercise 6 a) Verifying the Log Source Extension for Log Source Type Physical Access

In the last exercise you have configured the property parsing for the log source type Physical Access. By doing this, QRdara SIEM created a Log Source Extension document and configured it as default for all log sources of this type.

1. Navigate to the Admin tab and click the **Log Source Extensions** icon.
2. To open the extension document, select **PhysicalAccessCustom_ext** and click **Edit** in the toolbar.
3. What information is familiar to you in the Extension Document?
4. For what Log Source Types is the extension set to default?
5. Navigate to the **Log Sources**.
6. Open the **Physical Access Headquarter** log source.
7. What changed since your last visit to that record?

Exercise 7 a) Verifying the Physical Access log source

After you have created and deployed the log source of type Physical Access, QRadar correctly identifies events originating from the physical access system. To verify that QRadar SIEM displays the events on the Log Activity tab with Physical Access Headquarter as log source and investigate further.

1. Do the properties you parsed in Exercise 5 show up correctly?
2. Why are Event Name and Low Level Category still unknown?
3. What times are displayed for Start time, Storage time and Log Source time?
4. What do the time stamps mean and why are they different?
5. Open a single event and click on **Map Event** to see the Event ID.
6. Close without change.

Exercise 8 a) Creating an event categorization and mapping

With the new log source Physical Access Headquarter, QRadar SIEM correctly identifies events received from the physical access system. The property configurations of its log source type Physical Access enable the log source to parse and normalize the raw events.

However, the event name is still unknown. So that QRadar SIEM understands which kind of action a raw event informs, the event ID needs to be mapped to an Event Categorization. An event categorization specifies an event name, event description, severity rating, and links to a high-level category (HLC) and a low-level category (LLC). To create an event categorization and event mapping, perform the following steps:

1. Still on the Log Activity tab, right-click an event from the Physical Access log source and select **View in DSM Editor**.
2. In the DSM Editor navigate to the **Event Mappings** tab.

The tab displays the following two default event mappings, that QRadar SIEM already created:

- The mapping with the event category **Stored** maps all events that the log source cannot parse. QRadar SIEM links such events to the low-level category **Stored**.
- The mapping with the event category **unknown** maps all events that the log source can parse but cannot map to an event categorization. QRadar SIEM links such events to the low-level category **Unknown**.

Do not change these two mappings.

3. To create a new Event mapping click the **plus** symbol
4. Enter for Event ID:

   ```
   Access:In:Granted
   ```

5. For Category enter:

   ```
   unknown
   ```

6. To create an event categorization and map it to the event ID, click **Choose Event**.
7. Scroll down and click **Create New QID Record** in the lower-left corner.
8. Create a new QID record with the following information
9. For **Name**, enter the following text:

   ```
   Physical Entry Permitted
   ```

10. Optionally enter a **Description**.
11. For **Log Source Type**, select **Physical Access**.

12. For **High Level Category**, select **Access**.
13. For **Low Level Category**, select **Access Permitted**.
14. For **Severity**, configure **3**.
15. To create the event categorization, click **Save**.
16. Select the **Physical Entry Permitted** event categorization.
17. Click **Ok**.
    The Create a new Event Categorizations window closes.
18. To create the mapping between the event ID and the event categorization, click **Create**.
    The Create a new Event Mapping window closes.
19. Click **Save**.
20. Click **Cancel** to close the DSM Editor.

Exercise 9 a) Verifying the event categorization and mapping

Verify on the **Log Activity** tab that the events informing about a granted physical entry are named, categorized and mapped.

Exercise 10 a) Creating more event categorizations and mappings

Create two more event categorizations and mappings (like in exercise 8) using the information from the below table:

Property	Exit Permitted	Entry Denied
Event ID	`Access:Out:Granted`	`Access:In:Denied`
Event Category	`unknown`	`unknown`
Event Name	`Physical Exit Permitted`	`Physical Entry Denied`
Log Source Type	Physical Access	Physical Access
High Level Category	Access	Access
Low Level Category	Access Permitted	Access Denied
Severity	2	6

Exercise 11 a) Creating a custom property

Create a custom property for the “Physical Entrance Name” like shown in the payload below:

```
<182>Jun 06 09:00:46 10.0.120.12 15/feb/2017:12:02:31   Location
:HDQ    ID:112  Name:Anthony Pease      Entrance:Main Entrance
Access:Granted  Direction:In
```

As matching a Regex consumes a lot of computational resources, limit the custom property to the high level category (HLC) **Access** and any LLC

Hint: Use the DSM Editor to create new custom properties by clicking the **plus** symbol followed by the **Create New** button. To selectively use the custom to HLC and LLC click the Edit button beside “Selectivity” in the Expression window of the Property Configuration.

Exercise 12 a) Filtering by a custom property in a search (optional)

Use the custom property you created to filter for events containing “Main Entrance” and “Alley Garage”.

You have configured QRadar SIEM for an uncommon log source. To stop feeding raw events to QRadar SIEM, press Ctrl-C in the terminal window or PuTTY.

This concludes the exercises.

Version B Exercises

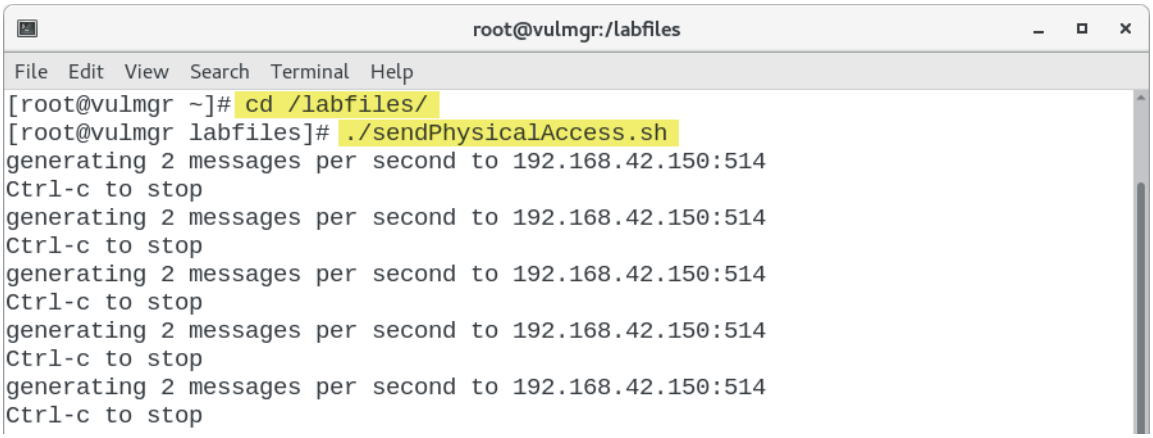
Exercise 1 b) Sending unknown events to QRadar SIEM

In this exercise, you send raw events from the physical access system to QRadar SIEM. None of the bundled DSMs can discover, parse, and normalize these raw events. You observe how QRadar SIEM displays events from unsupported sources.

1. To open a remote shell to the QRadar VM, use the procedure as outlined in Running commands on the QRadar VM.

2. To feed the raw events prepared for this exercise to QRadar SIEM, run the following commands:

   ```
   cd /labfiles
   ./sendPhysicalAccess.sh
   ```

   Do not close the terminal window.

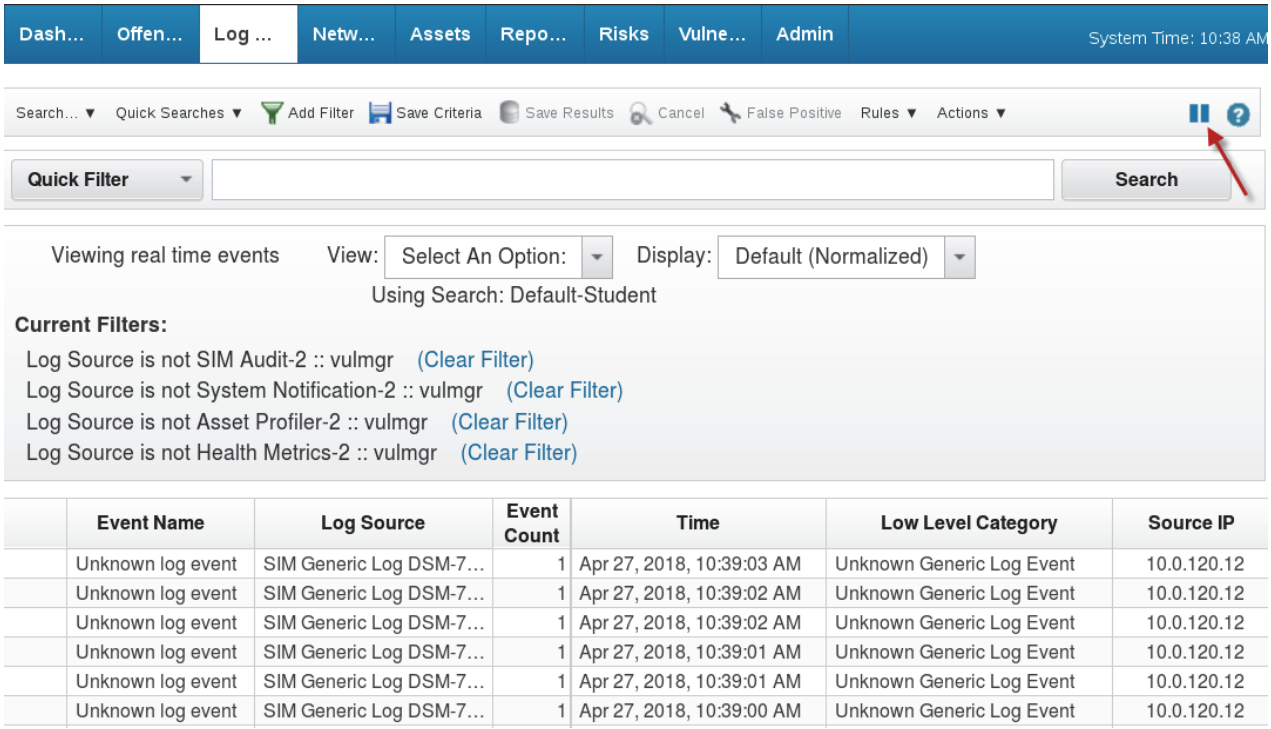
3. To log in to the QRadar user interface, use the procedure as outlined in Logging in to the QRadar user interface.

4. To watch the incoming events, double-click the **Log Activity** tab in the QRadar SIEM user interface. The double-click resets the tab to its default settings.

5. To pause the incoming events, click the **Pause** icon in the upper-right corner of the QRadar user interface.

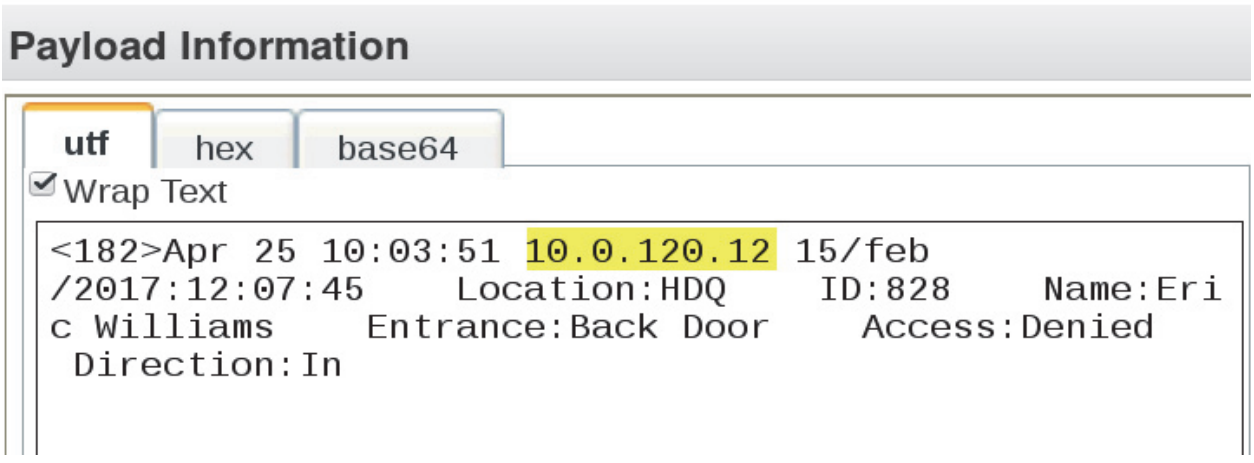
6. Observe the Event Name and Low Level Category. The Event Name is **Unknown log event** and the Low Level Category is **Unknown Generic Log Event**.

In addition, observe that the log source is **SIM Generic Log DSM-7**. This built-in log source processes events that QRadar SIEM cannot identify.



Event Name	Log Source	Event Count	Time	Low Level Category	Source IP
Unknown log event	SIM Generic Log DSM-7...	1	Apr 27, 2018, 10:39:03 AM	Unknown Generic Log Event	10.0.120.12
Unknown log event	SIM Generic Log DSM-7...	1	Apr 27, 2018, 10:39:02 AM	Unknown Generic Log Event	10.0.120.12
Unknown log event	SIM Generic Log DSM-7...	1	Apr 27, 2018, 10:39:02 AM	Unknown Generic Log Event	10.0.120.12
Unknown log event	SIM Generic Log DSM-7...	1	Apr 27, 2018, 10:39:01 AM	Unknown Generic Log Event	10.0.120.12
Unknown log event	SIM Generic Log DSM-7...	1	Apr 27, 2018, 10:39:01 AM	Unknown Generic Log Event	10.0.120.12
Unknown log event	SIM Generic Log DSM-7...	1	Apr 27, 2018, 10:39:00 AM	Unknown Generic Log Event	10.0.120.12

7. Double click on the first event to analyze the payload.



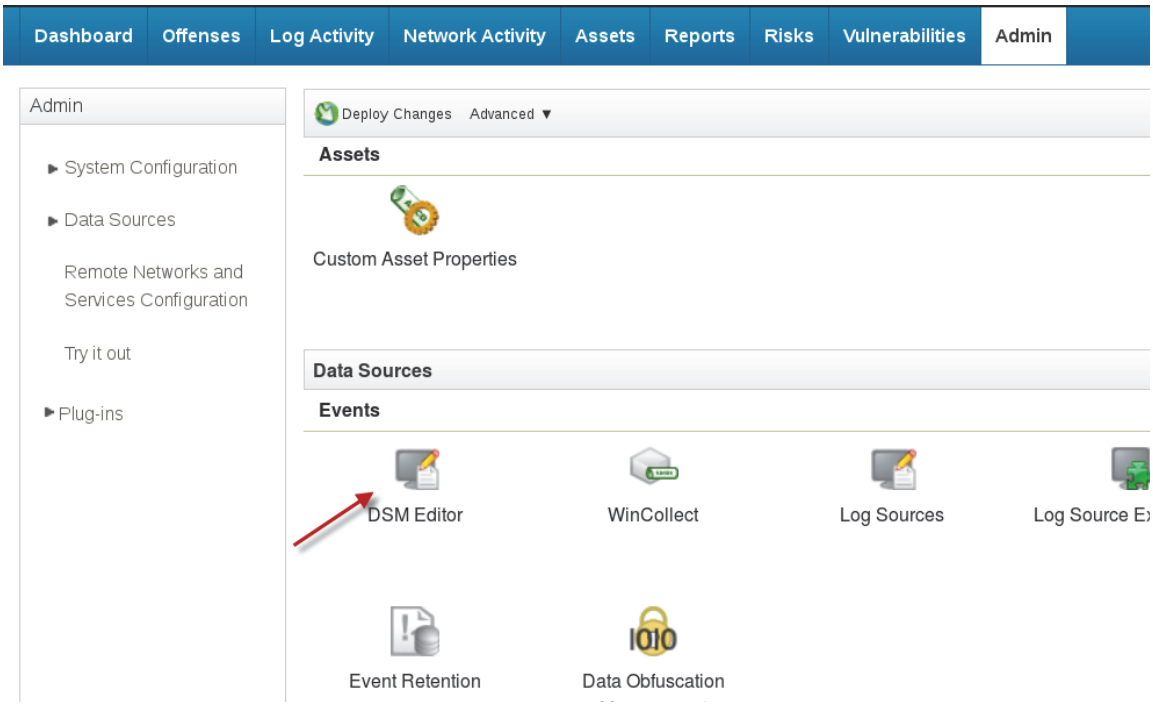
Note: The highlighted IP Address **10.0.120.12** behind the syslog timestamp is the IP address of the log source that sent the event to QRadar SIEM. Instead of the IP address, the syslog message header can contain the host name of the sender. QRadar SIEM refers to this IP address or host name as **log source identifier**. The combination of log source identifier, protocol configuration, and log source type uniquely identifies a log source.

Exercise 2 b) Using the DSM Editor to create a new log source type

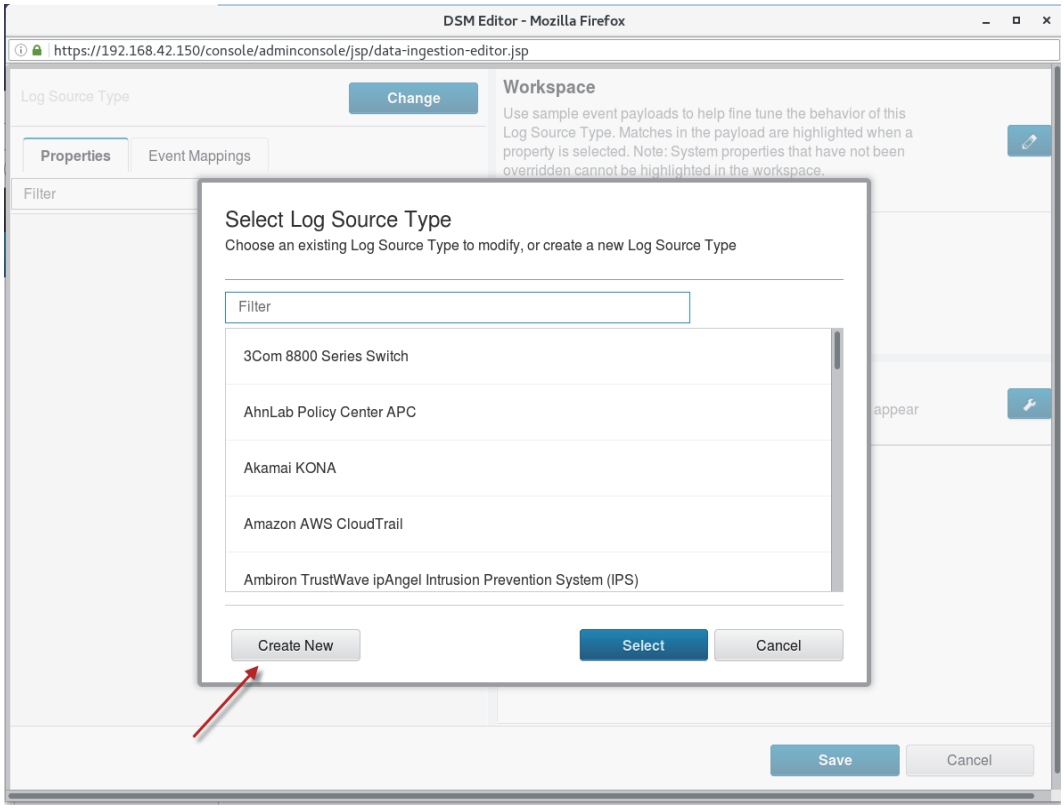
QRadar SIEM does not provide a DSM for a source of these raw events. To configure QRadar SIEM for these events, start the DSM Editor.

1. Navigate to the **Admin** tab.
2. In the left pane, click **Data Sources**.
3. To start the DSM Editor, click the **DSM Editor** icon.

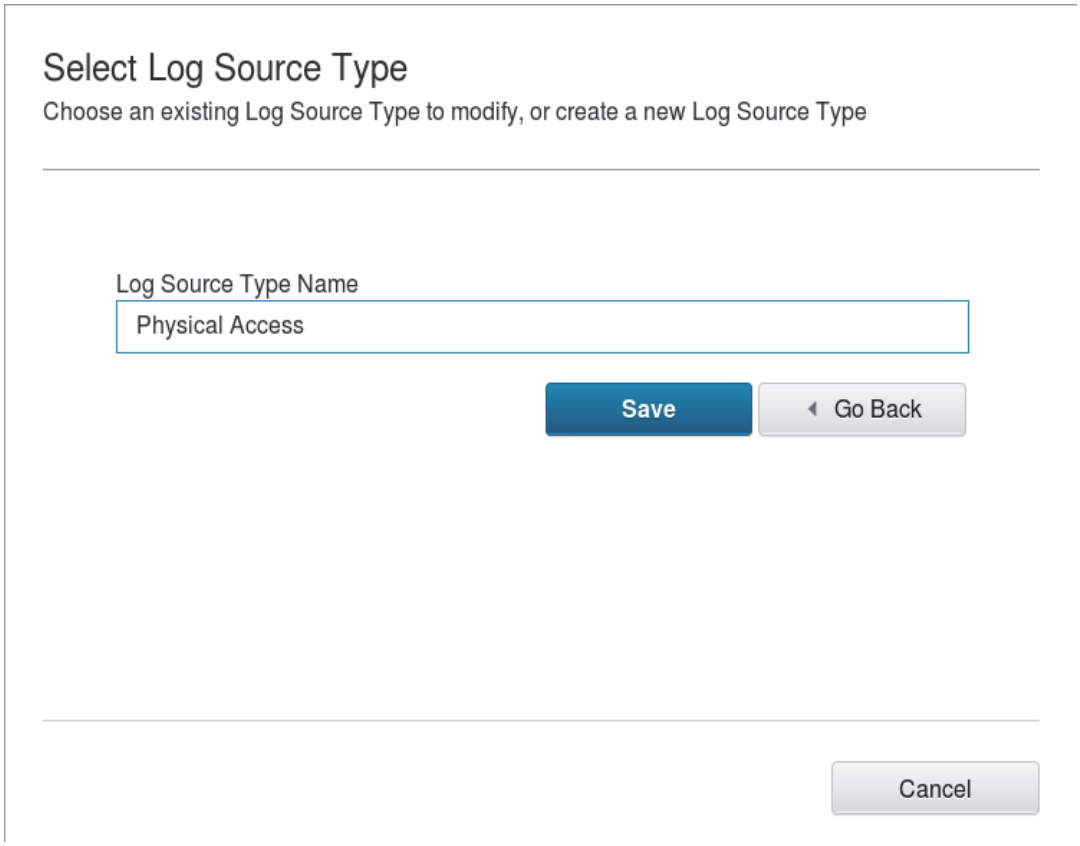
   The DSM Editor opens.



4. In the Select Log Source Type Window click **Create New**.



5. For **Log Source Type Name**, enter `Physical Access` and click **Save**.



6. Click **Cancel** to exit the DSM Editor**.**

Note: Now you have created a new Log Source Type. The DSM Editor provides more functionality we are going to use later.

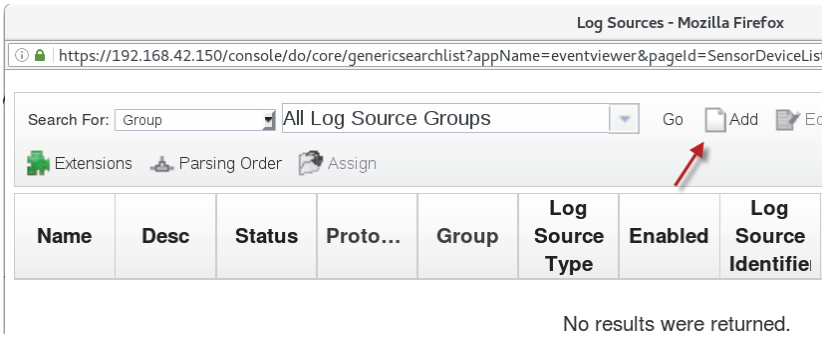
Exercise 3 b) Adding a Physical Access log source

Using the Log Source Type Physical Access you can now add a Log Source of this type to configure QRadar to identify the raw events as coming from the physical access system.

1. Still on the **Admin** tab, click the **Log Sources** icon.

   The Log Source window opens.

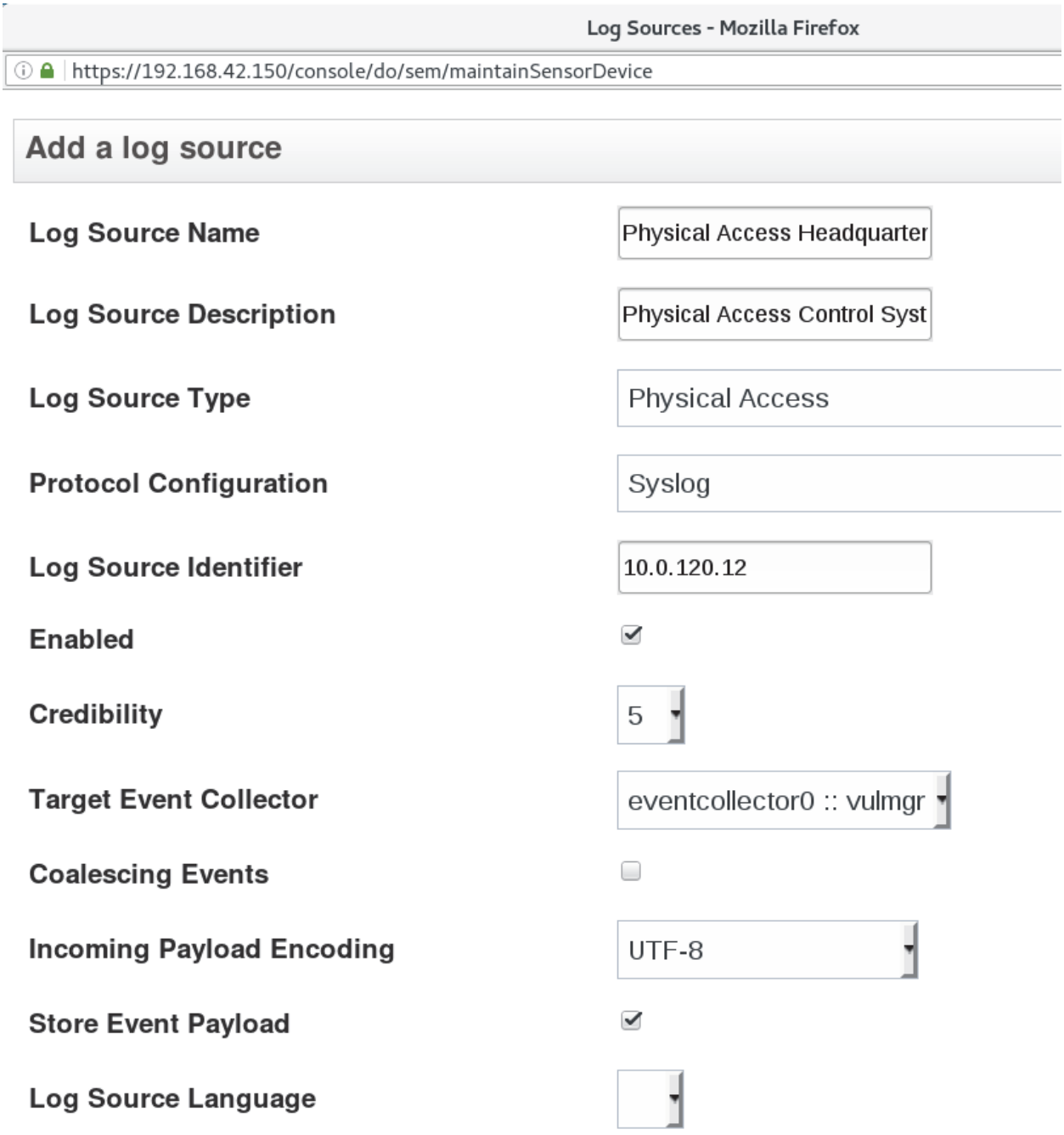
2. To create a new log source, click **Add**.



3. To configure the new log source, enter the values from the following table.

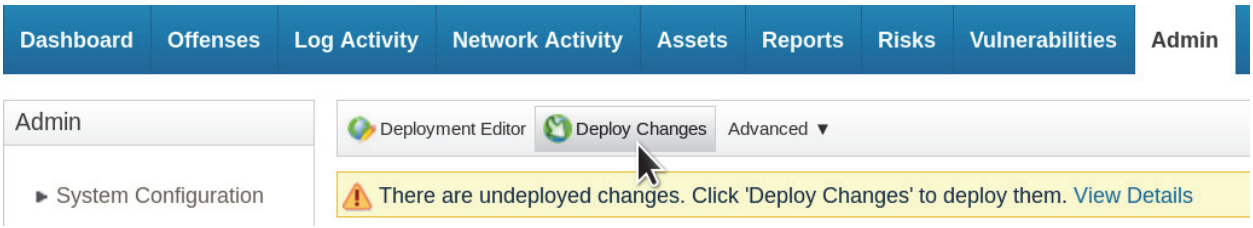
Field / Option	Setting
Log Source Name	Physical Access Headquarter
Log Source Description	Physical Access Control System
Log Source Type	Physical Access
Protocol Configuration	Syslog
Log Source Identifier	10.0.120.12
Coalescing Events	Clear check mark

4. Verify that your configuration resembles the following screen capture.



Note: The combination of log source identifier, protocol configuration, and log source type uniquely identifies the log source. For log source identifier, enter the IP address or host name from the syslog message header. However, usually you create only a few log sources manually, because QRadar discovers and configures log sources automatically for many common software and network devices.

5. To create the new log source, click **Save**.
6. Close the Log Sources window.
7. To update QRadar with the new log source, scroll to the top of the **Admin** tab and click **Deploy Changes**. The deployment may run for a few minutes.



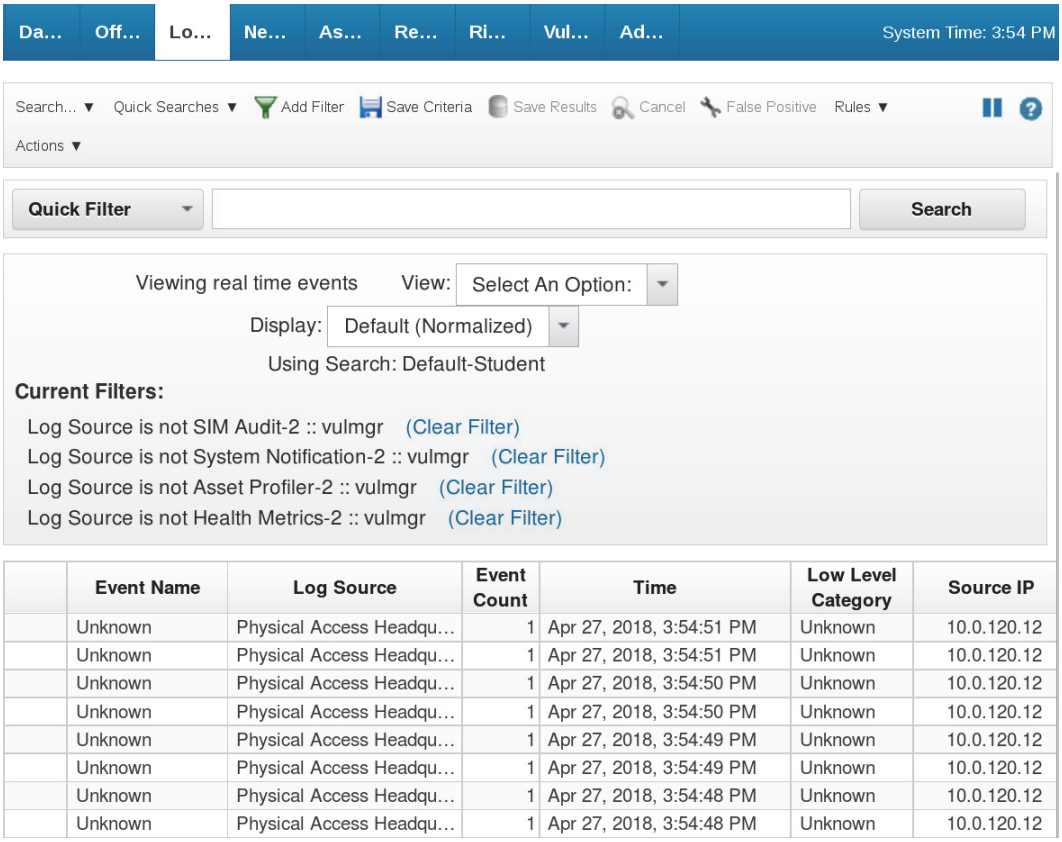
Hint: If clicking **Deploy Changes** does not have an effect, double-click the **Admin** tab. The double-click resets the tab to its default settings. Click **Deploy Changes** again.

8. After the change has been deployed, double-click the **Log Activity** tab. The double-click resets the tab to its default settings. Verify that the incoming events are now assigned to the log source **Physical Access Headquarter**.

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:39 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:39 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:38 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:37 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:37 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:36 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:36 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:35 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:35 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:34 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:34 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:33 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:33 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:32 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:32 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:31 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:31 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:30 PM	Unknown	10.0.120.12
Unknown	Physical Access Headquarter	1	Apr 27, 2018, 2:58:30 PM	Unknown	10.0.120.12
Unknown log event	SIM Generic Log DSM-7 :: vulmgr	1	Apr 27, 2018, 2:58:29 PM	Unknown Generic Log Event	10.0.120.12
Unknown log event	SIM Generic Log DSM-7 :: vulmgr	1	Apr 27, 2018, 2:58:29 PM	Unknown Generic Log Event	10.0.120.12
Unknown log event	SIM Generic Log DSM-7 :: vulmgr	1	Apr 27, 2018, 2:58:28 PM	Unknown Generic Log Event	10.0.120.12
Unknown log event	SIM Generic Log DSM-7 :: vulmgr	1	Apr 27, 2018, 2:58:28 PM	Unknown Generic Log Event	10.0.120.12
Unknown log event	SIM Generic Log DSM-7 :: vulmgr	1	Apr 27, 2018, 2:58:27 PM	Unknown Generic Log Event	10.0.120.12
Unknown log event	SIM Generic Log DSM-7 :: vulmgr	1	Apr 27, 2018, 2:58:27 PM	Unknown Generic Log Event	10.0.120.12

Exercise 4 b) Starting the DSM Editor from the Log Activity tab

1. Go back to the **Log Activity** tab by double clicking it. You can now see that QRadar detects the events from the newly created log source.

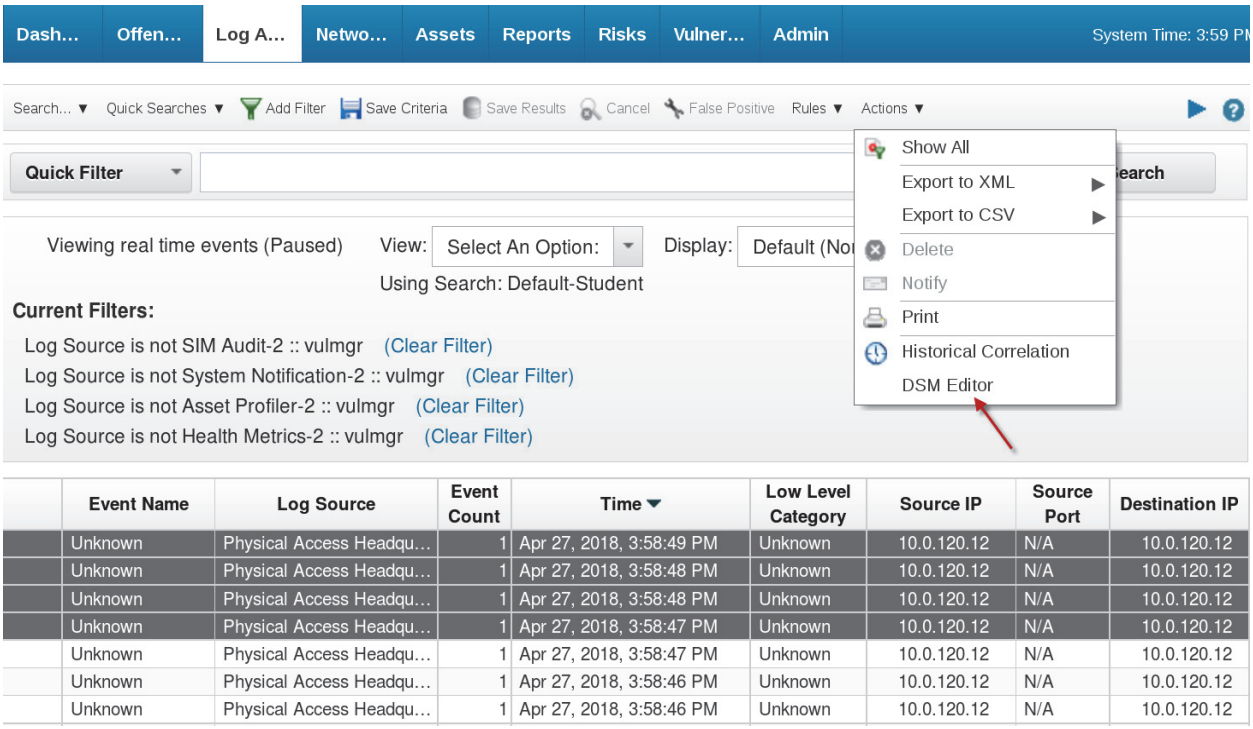


	Event Name	Log Source	Event Count	Time	Low Level Category	Source IP
	Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:54:51 PM	Unknown	10.0.120.12
	Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:54:51 PM	Unknown	10.0.120.12
	Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:54:50 PM	Unknown	10.0.120.12
	Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:54:50 PM	Unknown	10.0.120.12
	Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:54:49 PM	Unknown	10.0.120.12
	Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:54:49 PM	Unknown	10.0.120.12
	Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:54:48 PM	Unknown	10.0.120.12
	Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:54:48 PM	Unknown	10.0.120.12

2. Locate at least four events with the name **Unknown** and the log source P**hysical Access Headquarter**. To mark them, click each of the events while you hold down the Ctrl key.

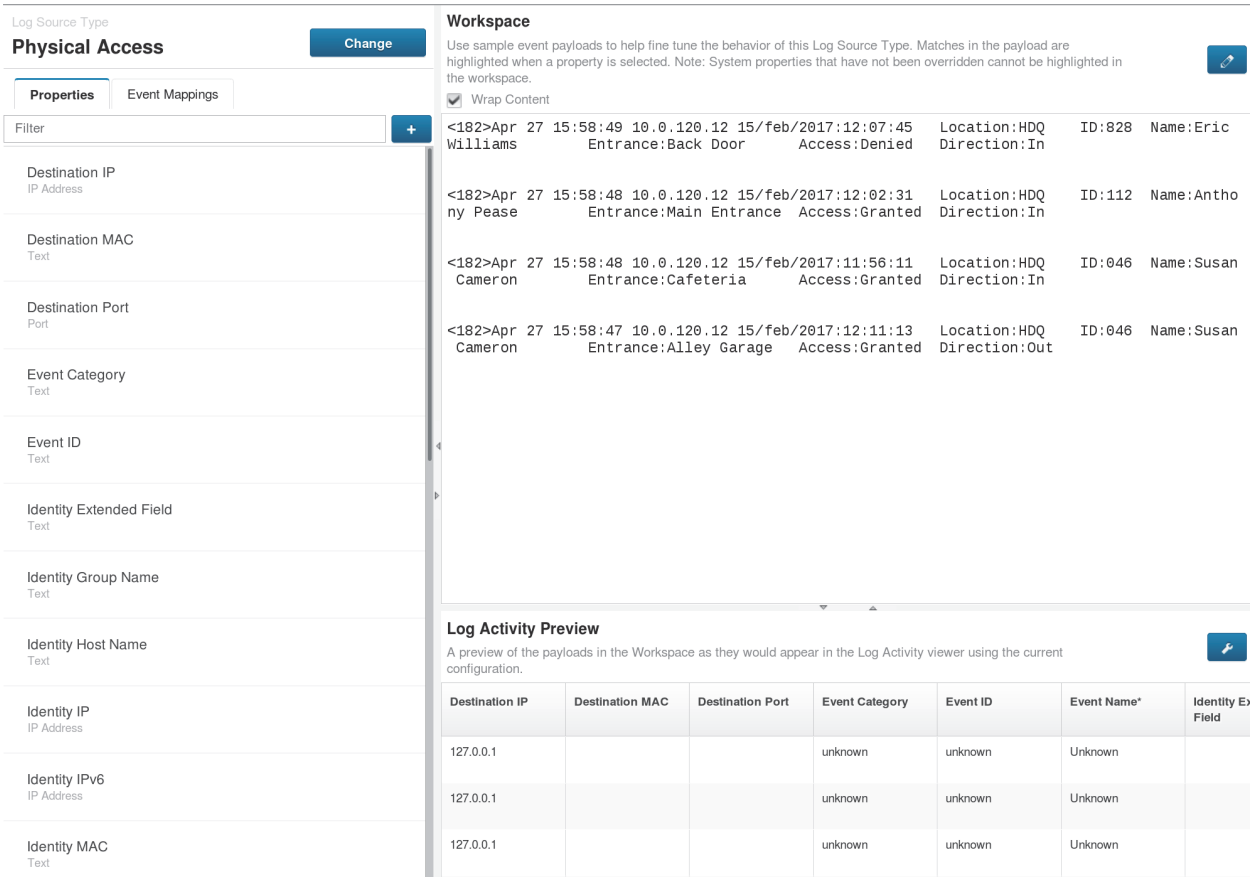
Hint: To be able to select events click on the “Pause” button on right side of the menu on the top.

3. From the **Actions** drop-down list, select **DSM Editor**.



Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP
Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:58:49 PM	Unknown	10.0.120.12	N/A	10.0.120.12
Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:58:48 PM	Unknown	10.0.120.12	N/A	10.0.120.12
Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:58:48 PM	Unknown	10.0.120.12	N/A	10.0.120.12
Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:58:47 PM	Unknown	10.0.120.12	N/A	10.0.120.12
Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:58:47 PM	Unknown	10.0.120.12	N/A	10.0.120.12
Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:58:46 PM	Unknown	10.0.120.12	N/A	10.0.120.12
Unknown	Physical Access Headqu...	1	Apr 27, 2018, 3:58:46 PM	Unknown	10.0.120.12	N/A	10.0.120.12

4. The DSM Editor window opens with all marked events in the upper-right Workspace.



Exercise 5 b) Configuring property parsing

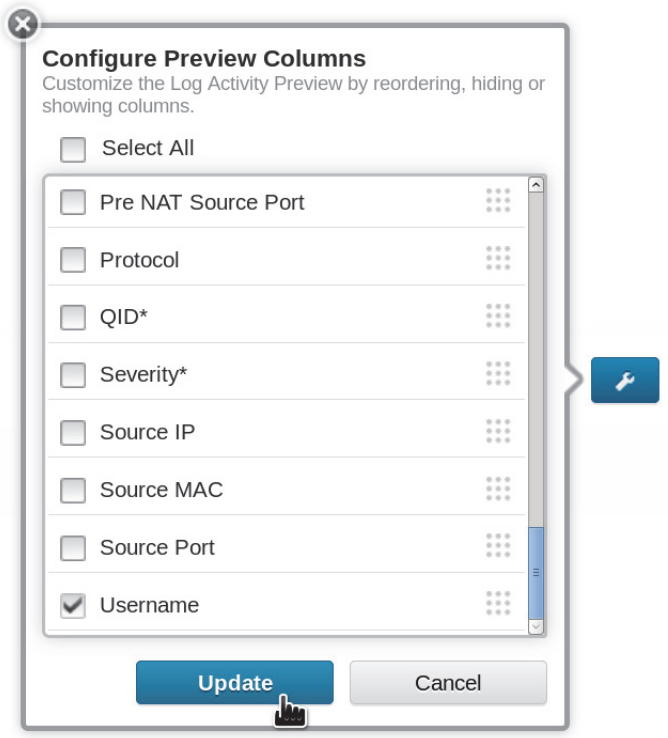
The Workspace section of the DSM Editor contains the raw events as they were sent by the physical access system. Observe that the raw events contain the following information:

- Time stamp of the syslog message header
- IP address of the physical access system
- Time stamp recorded by the physical access system
- Location
- User ID
- Username
- Entrance
- Access decision
- Access direction

The more information QRadar SIEM can use, the better it can detect suspicious activities. Therefore, you would configure QRadar SIEM to parse and normalize all of the above information, if this would be a real physical access system. This lab parses and normalizes only three properties as examples.

The Log Activity Preview in the lower-right part of the DSM Editor displays property values parsed from the raw events in the Workspace. Perform the following steps to configure the Log Activity Preview to display only the example properties:

1. Click the **wrench** symbol on the Log Activity Preview.
   The Configure Preview Columns window opens.
2. Enable **Select All**.
3. To deselect all properties, clear the **Select All** check box.
4. Select the following properties:
   – Event ID
   – Log Source Time
   – Username
5. Scroll down and click **Update**.
   The Configure Preview Columns window closes.



To parse the **Username** property, perform the following steps:

6. Locate the **Username** property on the **Properties** tab of the DSM Editor. Either scroll down until you find it, or use the **Filter** field so that the list only displays properties that match the letters you have entered.

7. Click the **Username** property.

   The Property Configuration expands.

8. Select **Override system behavior**.

Note: With **Override system behavior** selected, QRadar SIEM creates a **Log Source Extension (LSX)**. An LSX configures parsing and normalization for a log source. It can override the configuration of a bundled DSM if an IT system changes its log format and the bundled DSM has not been updated yet.
To display an LSX in XML format, navigate to the **Admin** tab and click the **Log Source Extensions** icon. To create an LSX without using the DSM Editor, upload a log source extension document in XML format.

9. For **Regex**, enter the following regular expression:

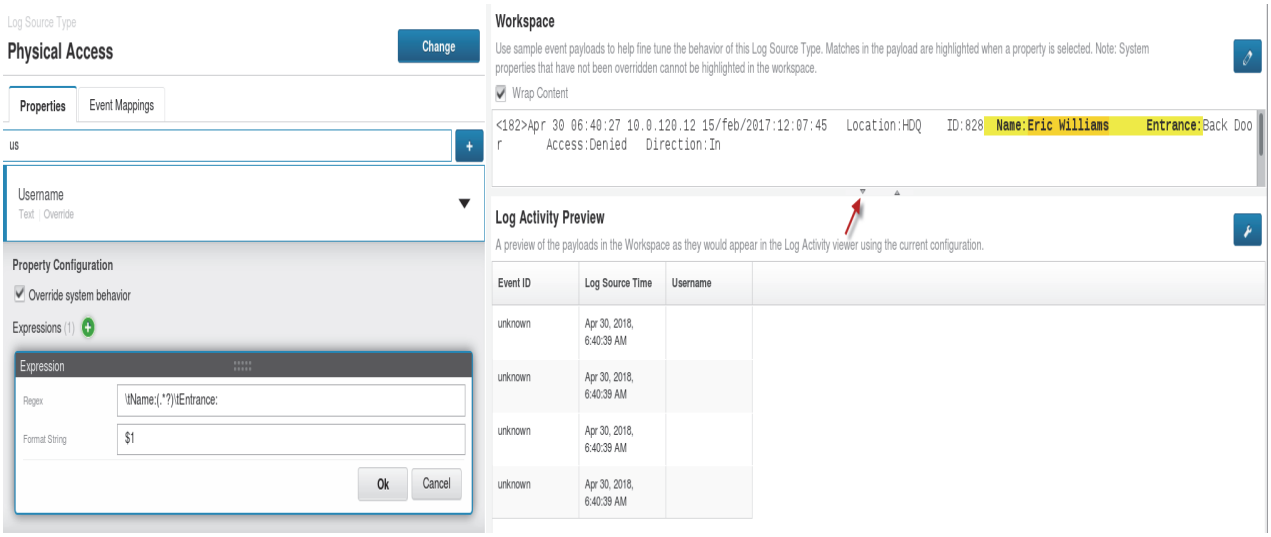
   `\tName:(.*?)\tEntrance:`

   The parentheses define a capturing group. Observe how the Workspace highlights the string that the capturing group matches, in an orange color. Any other characters that the regular expression matches outside the capturing group appear in a yellow color.

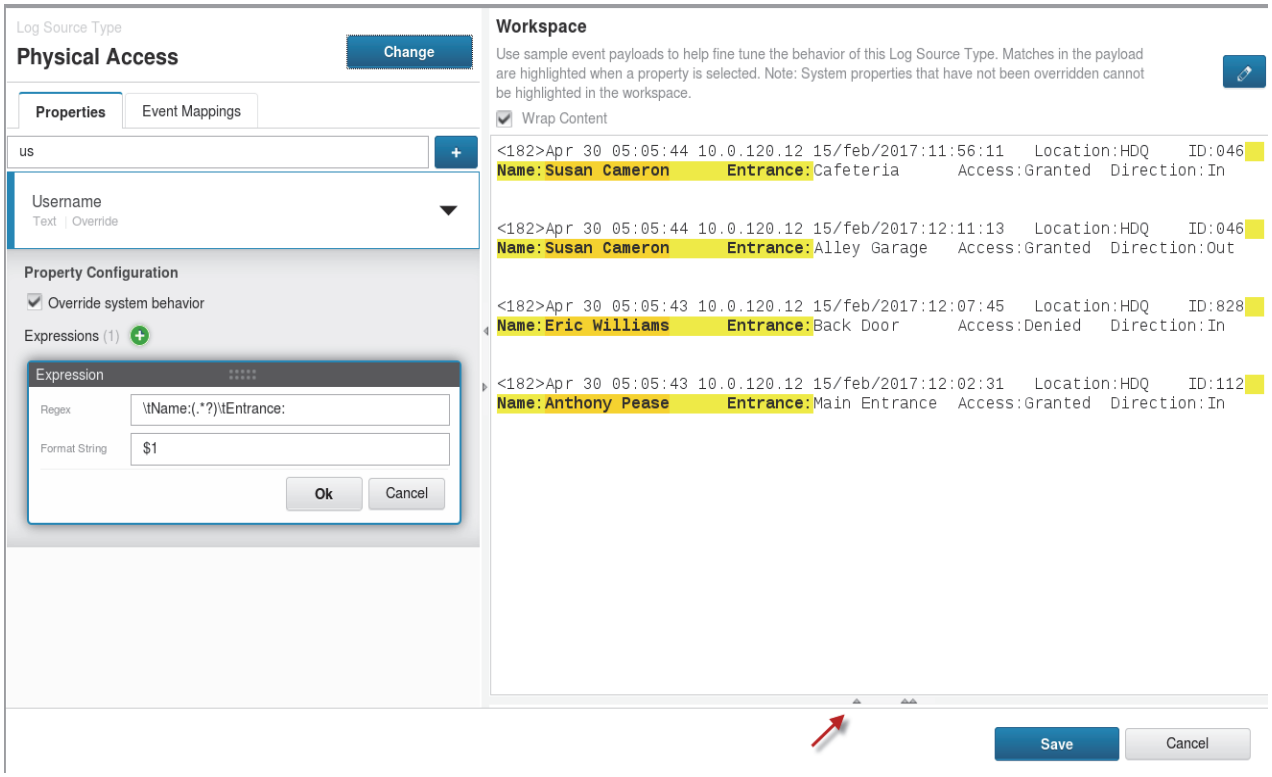
10. To reuse the strings that the capturing group of the regular expression in **Regex** match, enter for **Format String** the following backreference:

    `$1`

11. To verify that the regular expression matches the usernames of all raw events in the Workspace, click the button with the downward facing triangle at the bottom to the Workspace in order to enlarge it.



12. Verify that the Workspace highlights the username of each raw event.



13. To restore the DSM Editor to its default layout, click the button with the upward facing triangle at the bottom to the Workspace.

14. Click **Ok** for the Property Configuration of Username.

15. Verify that the **Username** column in the Log Activity Preview displays person names, such as Susan Cameron.

To parse the **Log Source Time** property, perform the following steps:

16. Locate the **Log Source Time** property on the **Properties** tab of the DSM Editor.

17. Click the **Log Source Time** property.

    The Property Configuration expands.

18. Select **Override system behavior**.

19. For **Regex**, enter the following regular expression:

    `\s(\d{2}/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\tLocation:`

20. To reuse the string that the capturing group of the regular expression in **Regex** matches, enter for **Format String** the following backreference:

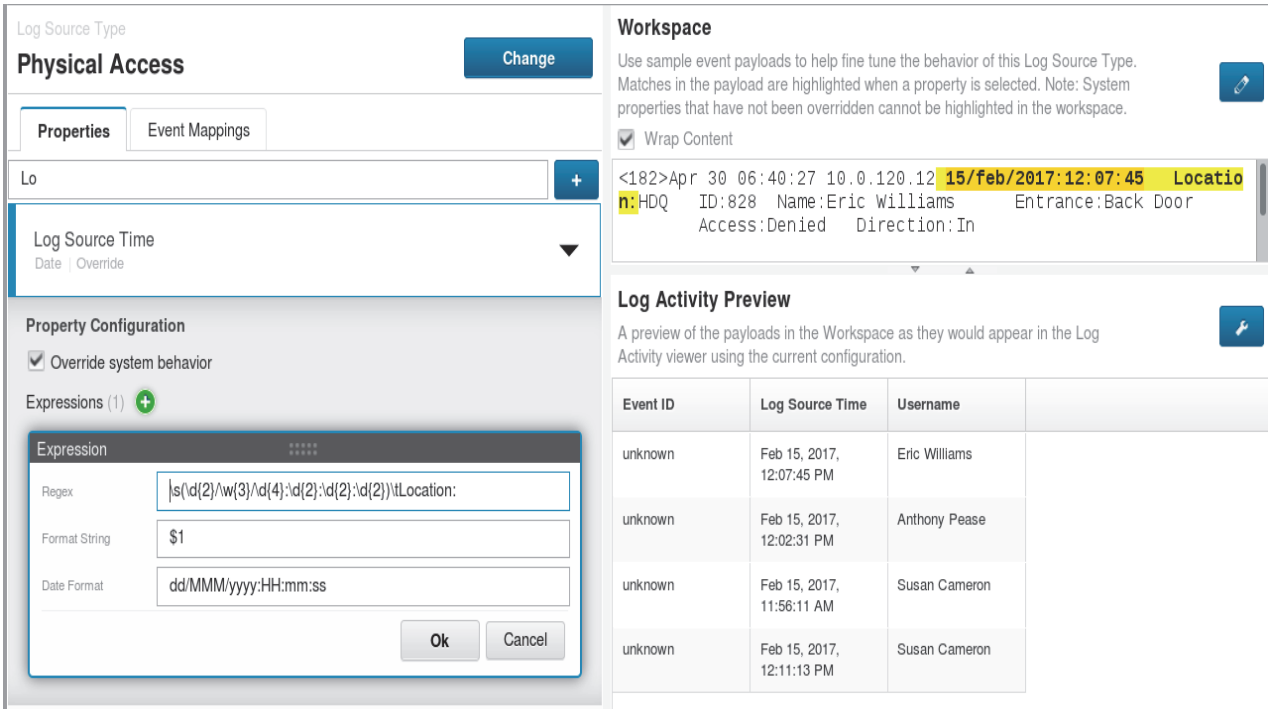
    `$1`

21. For **Date Format**, enter the following date format:

    `dd/MMM/yyyy:HH:mm:ss`

22. Click **Ok**.

23. Verify that the **Log Source Time** column in the Log Activity Preview displays the date Feb 15, 2017 and a time, such as: Feb 15, 2017, 12:11:13 pm.



Each event informs about an action that a log source recorded as raw event. The example physical access system performs three actions:

- Access outbound granted
- Access inbound granted
- Access inbound denied

The purpose of the **Event ID** property is to identify these three actions. Therefore, each action needs to parse to a different string. To parse the Event ID property, perform the following steps:

24. Locate the **Event ID** property on the **Properties** tab of the DSM Editor.

25. Click the **Event ID** property.

    The Property Configuration expands.

26. Select **Override system behavior**.

27. For **Regex**, enter the following regular expression:

    ```
    \tAccess:(Granted|Denied)\tDirection:(In|Out)$
    ```

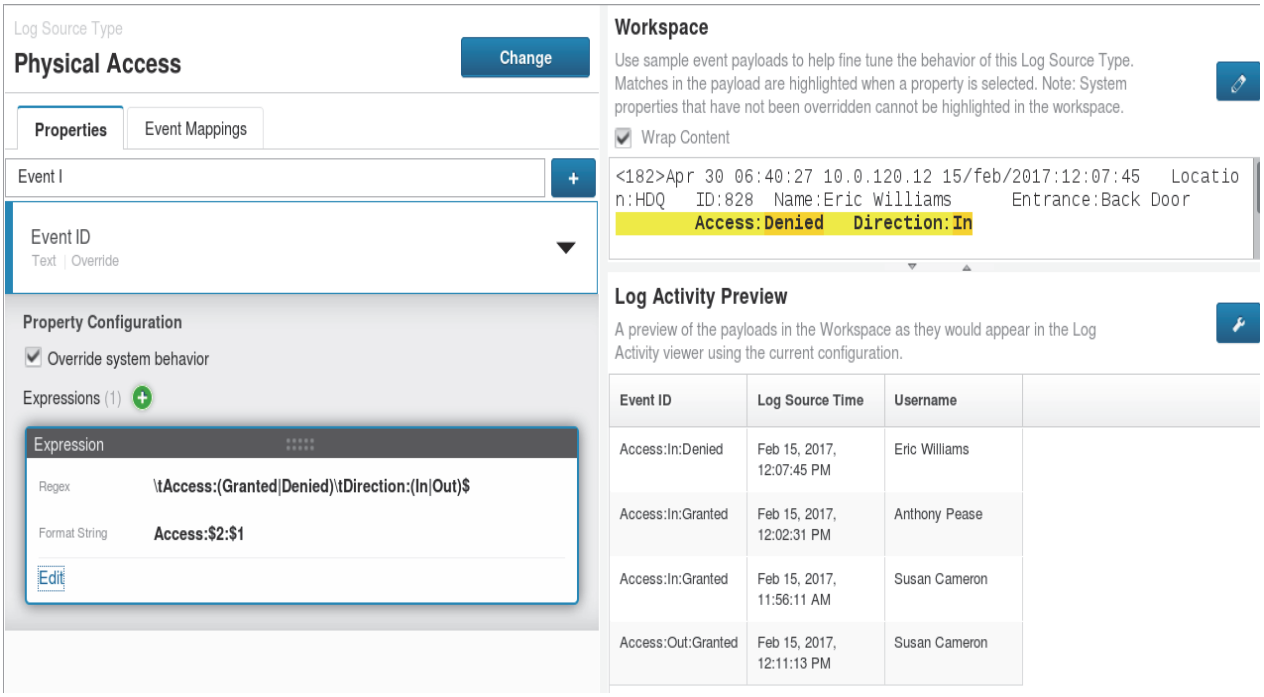
28. To reuse the strings that the capturing groups of the regular expression in **Regex** match, enter for **Format String** the following format string:

    ```
    Access:$2:$1
    ```

Note: The previous properties configured the format string with only one backreference. As this example shows, you can configure more than one backreference. In addition, you can configure character strings. They are always the same for all events and therefore do not help identifying the action that an event informs about. However, character strings can help document and structure the format strings.

29. Click **Ok**.

30. Verify that the **Event ID** column in the Log Activity Preview displays one or more of the following Event IDs:
    - Access:Out:Granted
    - Access:In:Granted
    - Access:In:Denied



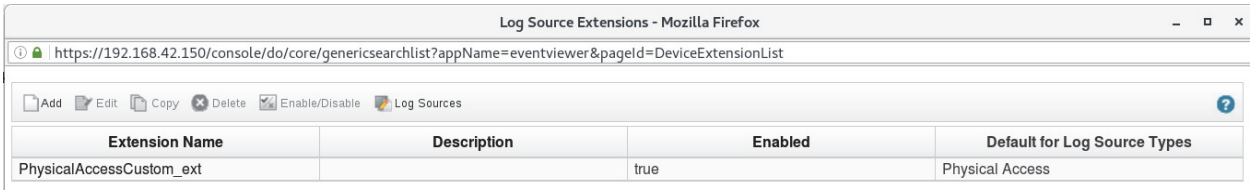
31. To save your configurations and close the DSM Editor, perform the following steps:
    a. Use the right-most scrollbar of the DSM Editor to scroll to the bottom.
    b. Click **Save**.
    c. Click **Cancel**.
    The DSM Editor closes.

Exercise 6 b) Verifying the Log Source Extension for Log Source Type Physical Access

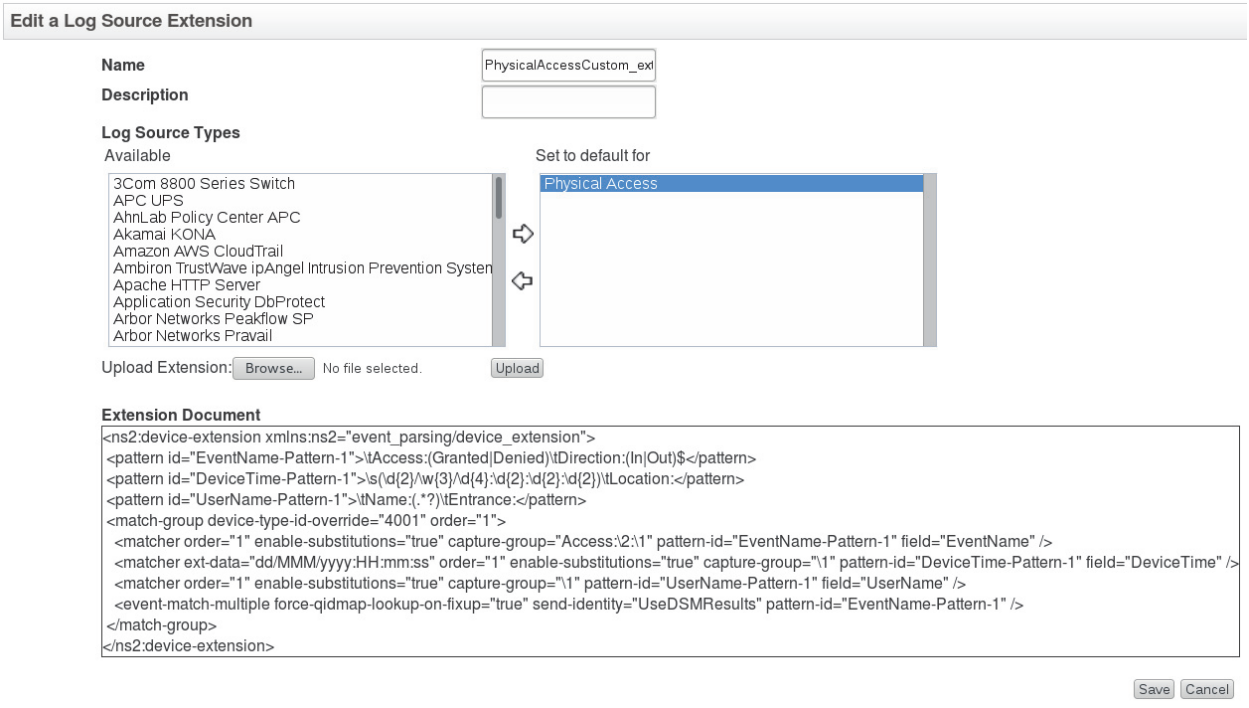
In the last exercise you have configured the property parsing for the log source type **Physical Access**. By doing this, QRdara SIEM created a Log Source Extension document and configured it as default for all log sources of this type.

1. Navigate to the **Admin** tab.
2. Click the **Log Source Extensions** icon to observe the extension.

   The Log Source Extensions window opens.

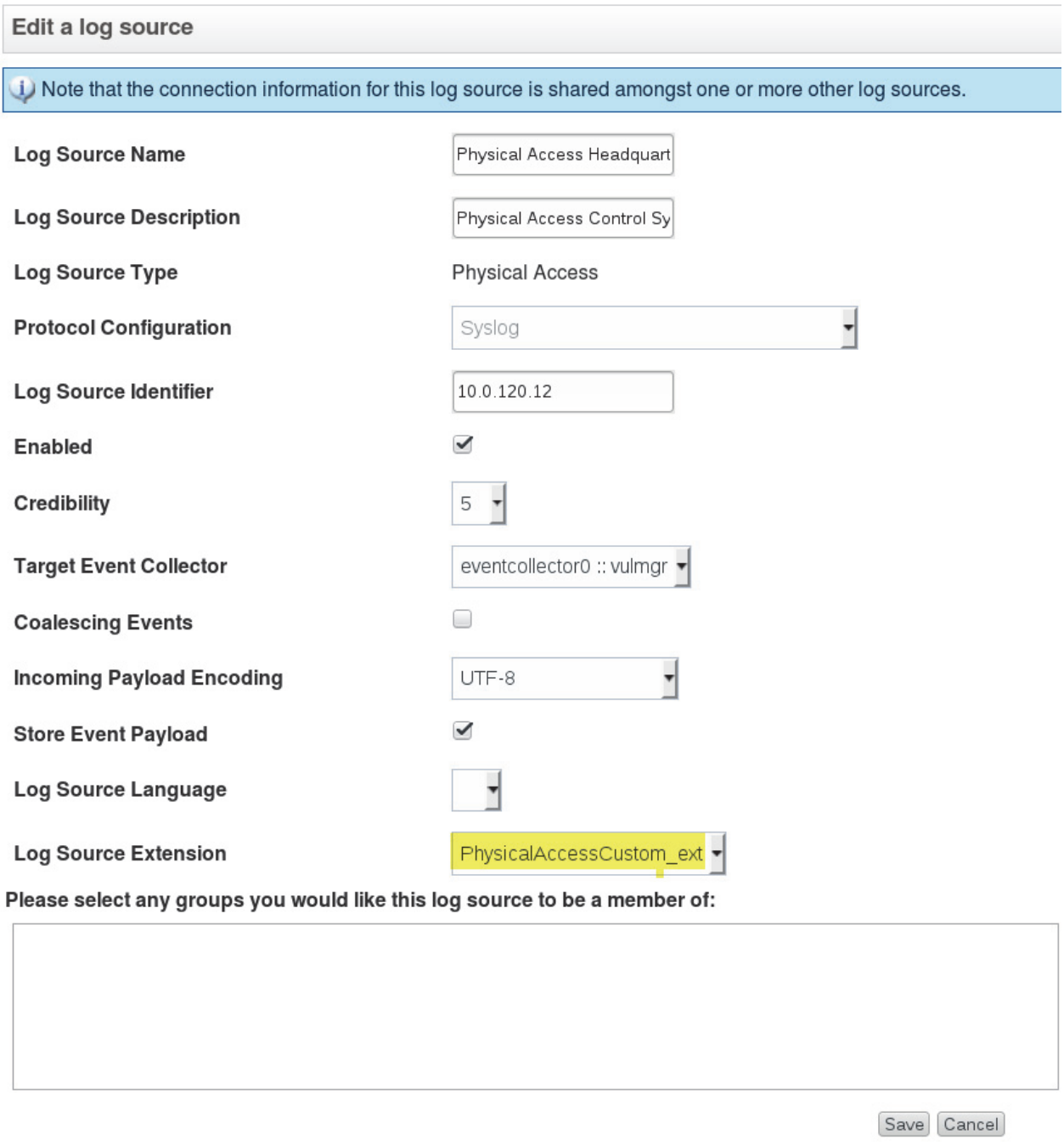


3. To open the extension document, select **PhysicalAccessCustom_ext** and click **Edit** in the toolbar.



4. Observe that the PhysicalAccessCustom_ext log source extension is set to default for the Physical Access log source type.

5. In the Extension Document, observe the regular expressions that you entered in the DSM Editor.
6. To close the window without any changes, click **Cancel** and close the browser window.
7. On the **Admin** tab, click the **Log Sources** icon.
   The Log Sources window opens.
8. To display the created log source, double-click the **Physical Access Headquarter** log source.
9. Observe that **PhysicalAccessCustom_ext** is now configured as log source extension.



10. To close the window without any changes, click **Cancel** and close the browser window.

Exercise 7 b) Verifying the Physical Access log source

After you have created and deployed the log source of type Physical Access, QRadar correctly identifies events originating from the physical access system. To verify that QRadar SIEM displays the events on the **Log Activity** tab with **Physical Access Headquarter** as log source and investigate further, perform the following steps:

1. To watch the incoming events, double-click the **Log Activity** tab in the QRadar SIEM user interface.
2. Verify that you see events with **Physical Access Headquarter** in the Log Source column.
3. To pause the incoming events, click the **Pause** icon in the upper-right corner of the QRadar SIEM user interface.
4. Observe that the **Event Name** and **Low Level Category** are still unknown.

	Event Name	Log Source	Event Count	Time ▾	Low Level Category
	Unknown	Physical Access Headquarter	1	May 1, 2018, 8:27:59 AM	Unknown
	Unknown	Physical Access Headquarter	1	May 1, 2018, 8:27:59 AM	Unknown
	Unknown	Physical Access Headquarter	1	May 1, 2018, 8:27:58 AM	Unknown
	Unknown	Physical Access Headquarter	1	May 1, 2018, 8:27:58 AM	Unknown
	Unknown	Physical Access Headquarter	1	May 1, 2018, 8:27:57 AM	Unknown

5. To verify that the usernames have been parsed correctly, scroll to the right until you find the **Username** column.
6. Observe that the **Source IP** and the **Destination IP** columns contain the IP address from the syslog message header that you configured as the log source identifier in a previous step. QRadar defaults to the log source identifier unless the raw events contain source and destination IP addresses and you configure parsing for them.

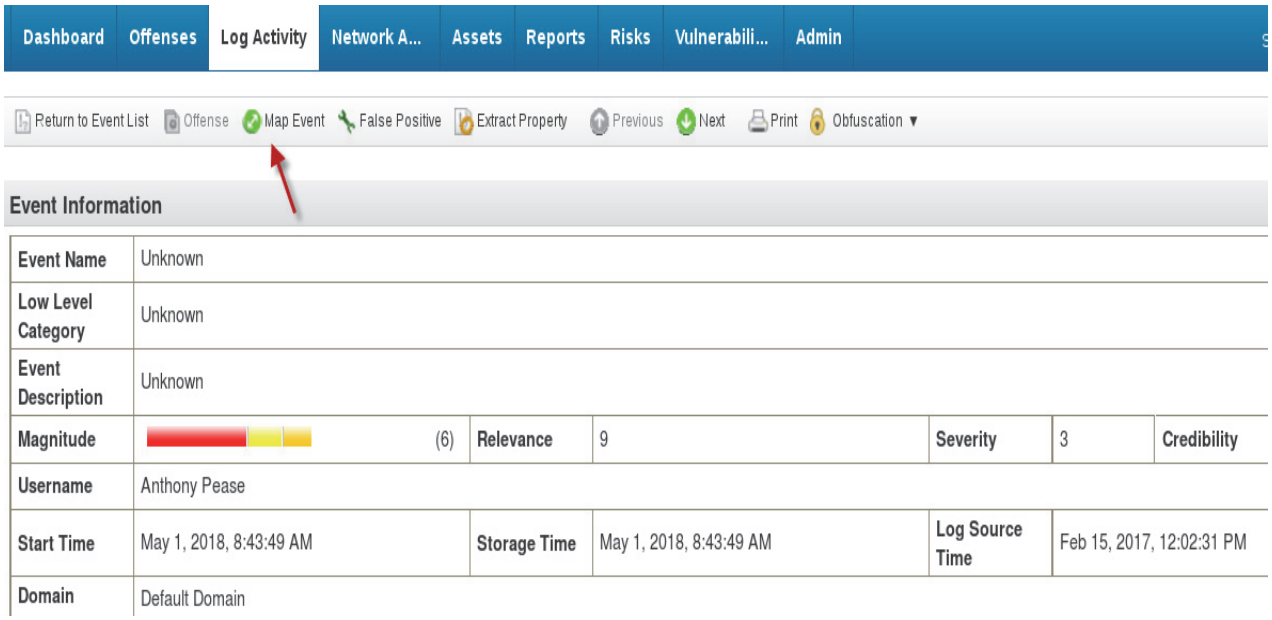
Note: For this lab's physical access system, the log source identifier is the same as the source IP address. Often the log source identifier of a log source is different from the source IP addresses of its events. For example, for a firewall feeding syslog to QRadar, use the IP address of the firewall as the log source identifier. This IP address differs from the source and destination IP addresses recorded in each firewall event, because they identify the origin and target of the connection attempts that the firewall allowed or blocked.

7. The **Time** column displays when an event collector started working with the newly arrived raw event that the displayed event represents. Elsewhere, the user interface and the documentation label this time as **Start Time**.

8. In a previous step, you configured parsing of the time stamp that the physical access system recorded in the raw event, which is called **Log Source Time** in QRadar. To display the log source time, double-click one event from the Physical Access Headquarter log source to open its details.

   If double-clicking does not open the event details, click the **Pause** icon and try again.

9. Locate the **Log Source Time** and verify that the date is Feb 15, 2017 and differs from the Start Time.



Note: The left-most time stamp in the Workspace of the DSM Editor is the time stamp of the syslog message header. The event collector uses it as log source time if parsing of the log source time is not configured or does not result in a valid time. If no valid time stamp is present in the syslog message header, the event collector uses the start time as log source time.

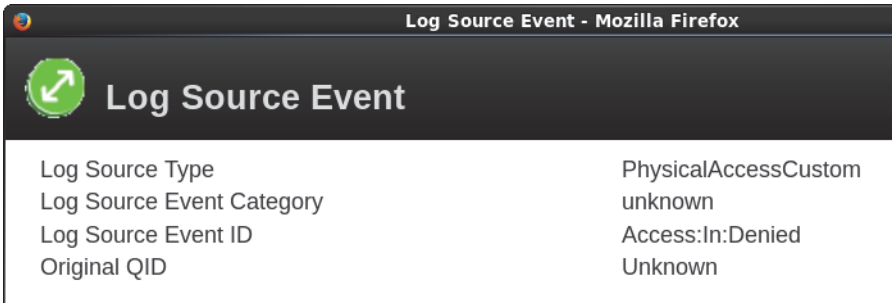
10. Observe the **Storage Time**. It records the time when QRadar has finished processing the event and writes it to disk. It is only relevant for troubleshooting.

Hint: For more information about times in QRadar, refer to the following technote: http://www.ibm.com/support/docview.wss?uid=swg21695264.

11. To display the Event ID, click **Map Event**.

    The Log Source Event window opens.

12. Observe the **Log Source Event ID**.



13. To close the Log Source Event window, click **Cancel**.

14. Click **Return to Event List**.

Exercise 8 b) Creating an event categorization and mapping

With the new log source **Physical Access Headquarter**, QRadar SIEM correctly identifies events received from the physical access system. The property configurations of its log source type **Physical Access** enable the log source to parse and normalize the raw events.

However, the event name is still unknown. So that QRadar SIEM understands which kind of action a raw event informs, the event ID needs to be mapped to an **Event Categorization**. An event categorization specifies an event name, event description, severity rating, and links to a high-level category (HLC) and a low-level category (LLC). To create an event categorization and event mapping, perform the following steps:

1. Still on the **Log Activity** tab, right-click an event from the **Physical Access** log source and select **View in DSM Editor**.

   If right-clicking does not open the menu with the DSM Editor, click the **Pause** icon and try again.

   The DSM Editor window opens.

2. Verify that the DSM Editor displays the log source type name **Physical Access** in the upper-left corner. If it does not, click **Change** to select the **Physical Access** log source type.

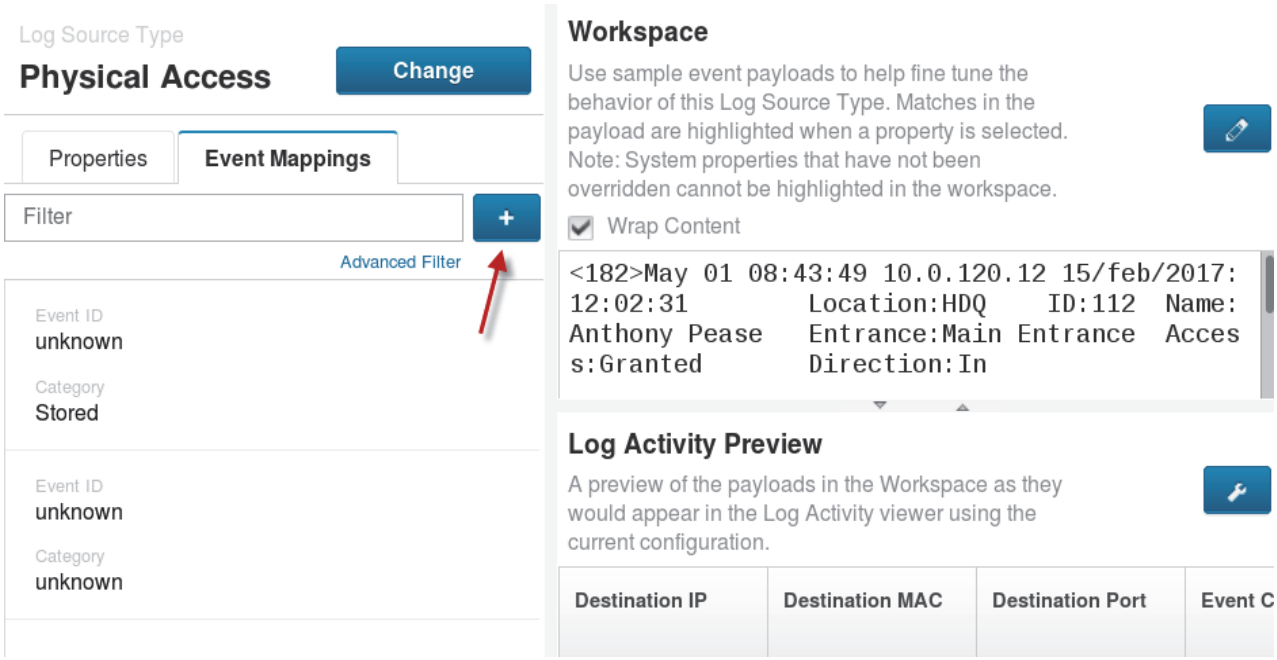
3. In the DSM Editor navigate to the **Event Mappings** tab.

   The tab displays the following two default event mappings, that QRadar SIEM already created:

   – The mapping with the event category **Stored** maps all events that the log source cannot parse. QRadar SIEM links such events to the low-level category **Stored**.

   – The mapping with the event category **unknown** maps all events that the log source can parse but cannot map to an event categorization. QRadar SIEM links such events to the low-level category **Unknown**.

Do not change these two event mappings.



4. Click the blue **plus** symbol.

   The Create a new Event Mapping window opens.

5. For **Event ID**, enter the following identifier:

   `Access:In:Granted`

6. For **Category**, enter the following text:

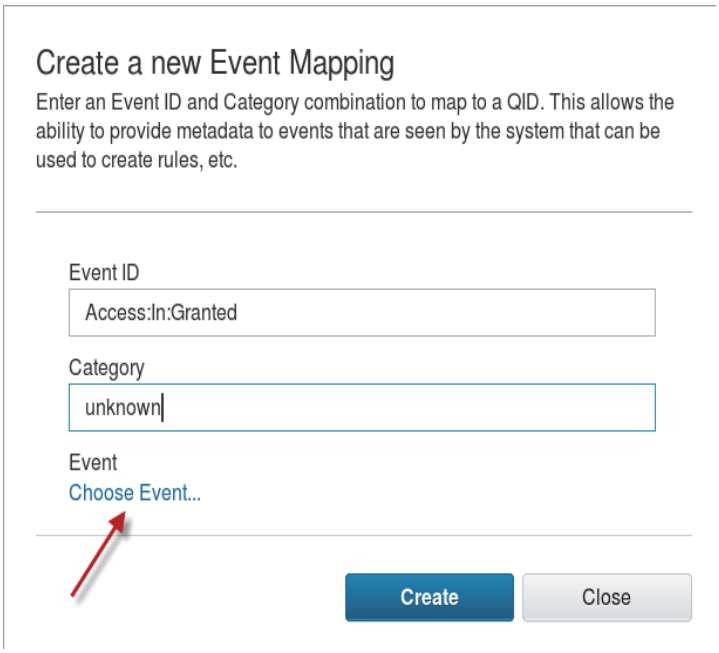
   `unknown`

Note: The Event **Category** is only indirectly related to the event categorization that configures the HLC and LLC of an event, in addition to the event name, event description, and severity rating. The event category is a character string that is parsed from the raw event using your configured regular expression, the same as with the event ID. To look up an event categorization, QRadar SIEM uses the combination of event ID, event category, log source type, and whether the event mapping is predefined or manual.

For many log sources, the event category is not relevant to identify event categorizations. For those, the event category is configured as a fixed character string such as *unknown*.

For events from Microsoft Windows, QRadar SIEM uses the event category. Example values include those in this list:
- Success Audit
- Failure Audit
- DNS
- Directory Service

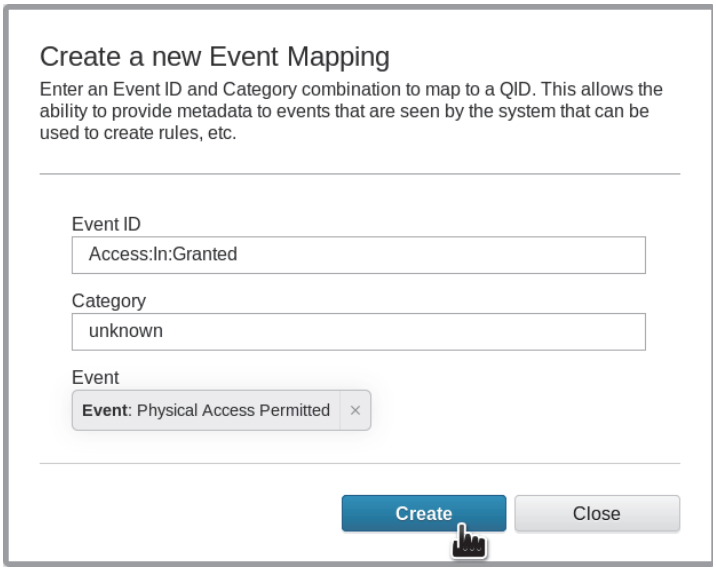
For events from Check Point, QRadar SIEM uses the event category, too. Example values include those in this list:
- CheckPoint
- SmartDefense
- Application Control
- CheckPointAntiMalware



8. To create an event categorization and map it to the event ID, click **Choose Event**.

The Event Categorizations window opens.

9. Scroll down and click **Create New QID Record** in the lower-left corner.
10. For **Name**, enter the following text:
    `Physical Entry Permitted`
11. Optionally enter a **Description**.
12. For **Log Source Type**, select **Physical Access**.
13. For **High Level Category**, select **Access**.
14. For **Low Level Category**, select **Access Permitted**.
15. For **Severity**, configure **3**.
16. To create the event categorization, click **Save**.
17. Select the **Physical Entry Permitted** event categorization.
18. Click **Ok**.
    The Create a new Event Categorizations window closes.
19. To create the mapping between the event ID and the event categorization, click **Create**.
    The Create a new Event Mapping window closes.



21. Click **Save**.
22. Click **Cancel**.
    The DSM Editor closes.

Exercise 9 b) Verifying the event categorization and mapping

To verify that the events informing about a granted physical entry are named, categorized, and mapped, perform the following steps:

1. To watch the incoming events, double-click the **Log Activity** tab in the QRadar SIEM user interface.
2. Verify that events appear with the **Physical Entry Permitted** event name and **Access Permitted** low-level category.

Event Name	Log Source	Ever Cou	Time ▼	Low Level Category
Physical Entry Permitted	Physical Access Headquarter	1	May 1, 2018, 10:03:16 AM	Access Permitted
Physical Entry Permitted	Physical Access Headquarter	1	May 1, 2018, 10:03:15 AM	Access Permitted
Unknown	Physical Access Headquarter	1	May 1, 2018, 10:03:15 AM	Unknown
Unknown	Physical Access Headquarter	1	May 1, 2018, 10:03:14 AM	Unknown
Physical Entry Permitted	Physical Access Headquarter	1	May 1, 2018, 10:03:14 AM	Access Permitted
Physical Entry Permitted	Physical Access Headquarter	1	May 1, 2018, 10:03:13 AM	Access Permitted
Unknown	Physical Access Headquarter	1	May 1, 2018, 10:03:13 AM	Unknown
Unknown	Physical Access Headquarter	1	May 1, 2018, 10:03:12 AM	Unknown
Physical Entry Permitted	Physical Access Headquarter	1	May 1, 2018, 10:03:12 AM	Access Permitted
Physical Entry Permitted	Physical Access Headquarter	1	May 1, 2018, 10:03:11 AM	Access Permitted
Unknown	Physical Access Headquarter	1	May 1, 2018, 10:03:11 AM	Unknown

Exercise 10 b) Creating more event categorizations and mappings

Repeat the steps of Exercise 8, “b) Creating an event categorization and mapping” to create event categorizations and event mappings for granted physical exit and denied physical entry. Navigate to the DSM Editor and use the values from the following table.

Property	Exit Permitted	Entry Denied
Event ID	`Access:Out:Granted`	`Access:In:Denied`
Event Category	`unknown`	`unknown`
Event Name	`Physical Exit Permitted`	`Physical Entry Denied`
Log Source Type	Physical Access	Physical Access
High Level Category	Access	Access

Property	Exit Permitted	Entry Denied
Low Level Category	Access Permitted	Access Denied
Severity	2	6

Verify that Physical Exit Permitted and Physical Entry Denied events appear as shown in the following screen capture.

Event Name	Log Source	Ever Cou	Time ▼	Low Level Category
Physical Entry Permitted	Physical Access Headquarter	1	May 1, 2018, 11:20:43 AM	Access Permitted
Physical Exit Permitted	Physical Access Headquarter	1	May 1, 2018, 11:20:42 AM	Access Permitted
Physical Entry Denied	Physical Access Headquarter	1	May 1, 2018, 11:20:42 AM	Access Denied
Physical Entry Permitted	Physical Access Headquarter	1	May 1, 2018, 11:20:41 AM	Access Permitted
Physical Entry Permitted	Physical Access Headquarter	1	May 1, 2018, 11:20:41 AM	Access Permitted
Physical Exit Permitted	Physical Access Headquarter	1	May 1, 2018, 11:20:40 AM	Access Permitted
Physical Entry Denied	Physical Access Headquarter	1	May 1, 2018, 11:20:40 AM	Access Denied
Physical Entry Permitted	Physical Access Headquarter	1	May 1, 2018, 11:20:39 AM	Access Permitted
Physical Entry Permitted	Physical Access Headquarter	1	May 1, 2018, 11:20:39 AM	Access Permitted
Physical Exit Permitted	Physical Access Headquarter	1	May 1, 2018, 11:20:38 AM	Access Permitted
Physical Entry Denied	Physical Access Headquarter	1	May 1, 2018, 11:20:38 AM	Access Denied
Physical Entry Permitted	Physical Access Headquarter	1	May 1, 2018, 11:20:37 AM	Access Permitted
Physical Entry Permitted	Physical Access Headquarter	1	May 1, 2018, 11:20:37 AM	Access Permitted
Physical Exit Permitted	Physical Access Headquarter	1	May 1, 2018, 11:20:36 AM	Access Permitted

Exercise 11 b) Creating a custom property

So far you have configured three properties that are built into QRadar SIEM. They cannot be deleted. In addition, custom event properties can extract more information. Searches, reports, and rules can use custom properties in the same way as built-in properties.

QRadar SIEM already comes with predefined custom properties. Extensions can add more custom properties. To browse, add, edit, and delete custom event properties, you can navigate to the **Admin** tab and click the **Custom Event Properties** icon.

In addition, the DSM Editor allows you to create and add existing custom event properties to a log source type. To create the **Physical Entrance Name** custom event property for the Physical Access log source type, perform the following steps:

1. Still on the **Log Activity** tab, right-click an event from the **Physical Access** log source and select **DSM Editor**.

   If right-clicking does not open the menu with the DSM Editor, click the **Pause** icon and try again.

   The DSM Editor window opens.

2. Verify that the DSM Editor displays the log source type name **Physical Access** in the upper-left corner. If it does not, click **Change** to select the **Physical Access** log source type.

3. Click the blue **plus** symbol.

   The Choose a Custom Property to Express window opens. It lists existing custom event properties.

4. Scroll down and click **Create New** in the lower-left corner.

   The Create a new Custom Property Definition form opens in the window.

5. For **Name**, enter the following text:

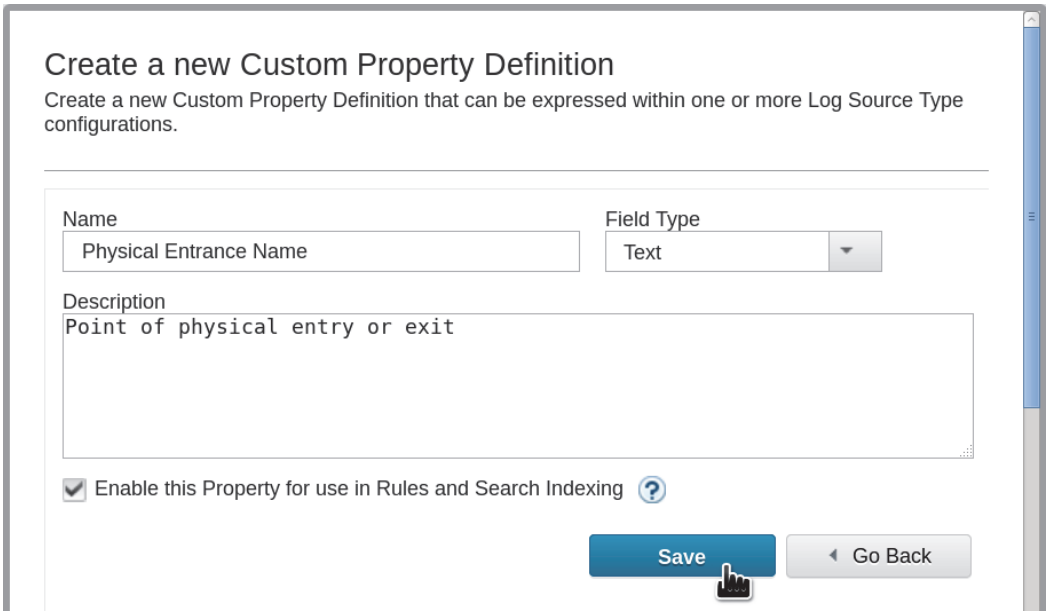
   ```
   Physical Entrance Name
   ```

6. For **Description**, enter the following text:

   ```
   Point of physical entry or exit
   ```

7. Select **Enable this Property for use in Rules and Search Indexing**.

Note: When you select this option, event collectors extract the property values from raw events immediately after they arrive, and event processors store them. Searches, reports, and rule tests can retrieve these values efficiently without extracting the property values again. Therefore, searches, reports, and rule tests consume fewer resources at the expense of higher resource consumption for event collection and storage of property values.



8. To create the custom property, click **Save**.

   The Choose a Custom Property to Express form opens in the window.

9. The new custom property **Physical Entrance Name** is selected. Scroll down and click **Select**.

   The Choose a Custom Property to Express window closes.

10. Click the **Physical Entrance Name** property.

The Property Configuration expands.

11. For **Regex**, enter the following regular expression:

    `\tEntrance:(.*?)\tAccess:`

12. For Capture Group, enter or select **1**.

13. Matching a regular expression consumes a lot of computational resources. Therefore, it is best practice to let QRadar SIEM compute the custom property for the smallest number of events possible. To limit the custom property to the high level category **Access**, perform the following steps:

    a. Next to **Selectivity**, click the **Edit** link.

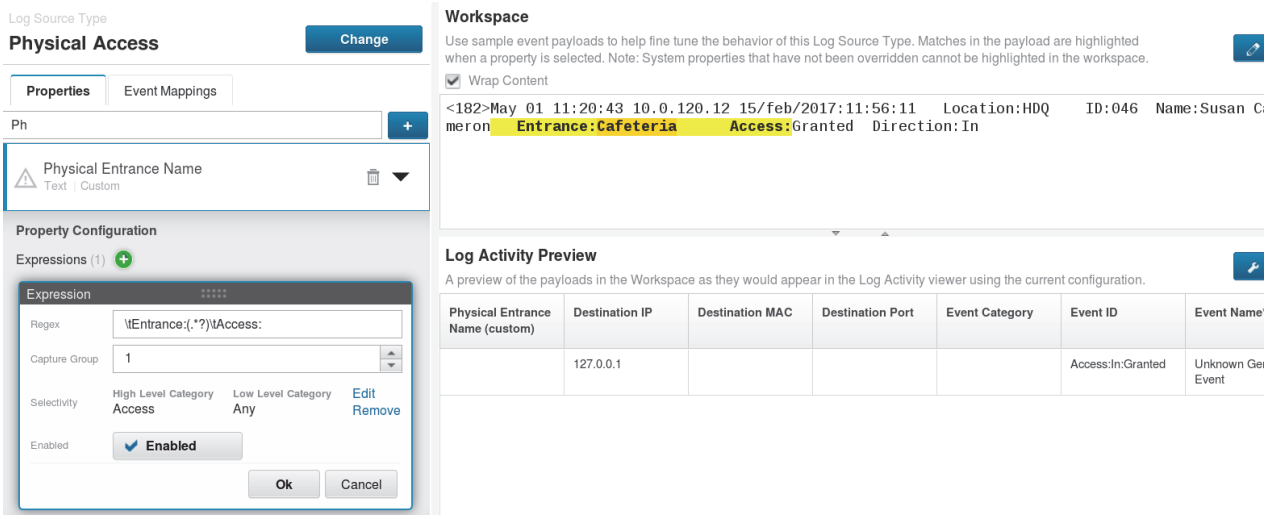
    The Selectivity window opens.

    b. For **High Level Category**, select **Access**.

    c. Click **Ok**.

    The Selectivity window closes.

14. Click **Ok** in the Property Configuration.



16. Click **Save**.

17. Click **Cancel**.

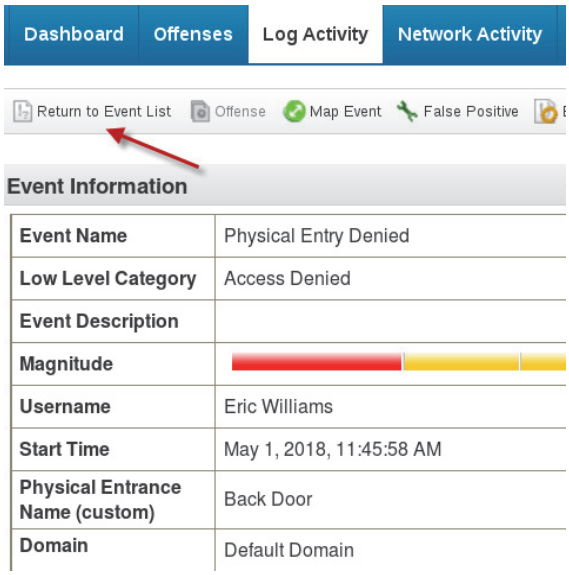
    The DSM Editor closes.

18. Double-click the **Log Activity** tab to reset it.

19. To pause the incoming events, click the **Pause** icon in the upper-right corner of the QRadar SIEM user interface.

20. Double-click one event from the Physical Access Headquarter log source to open its details.

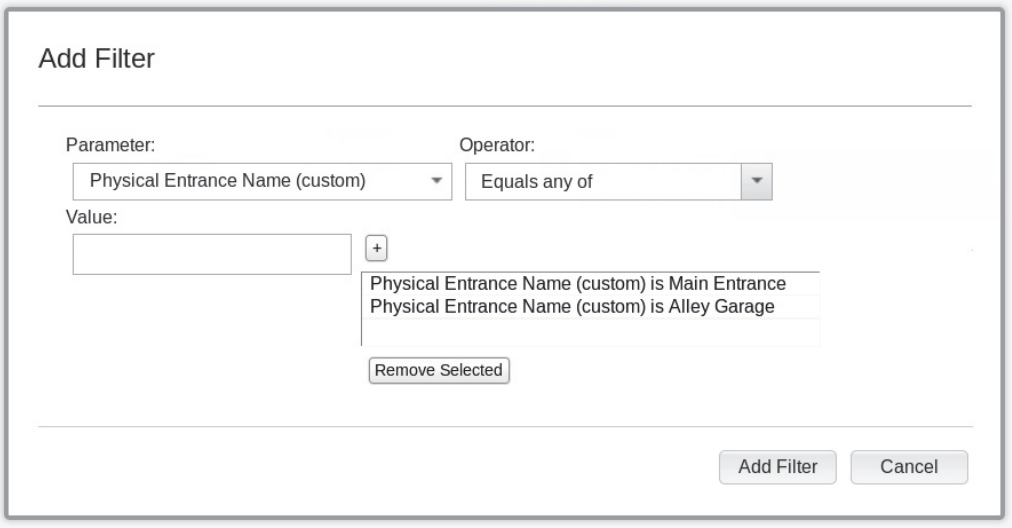
21. Verify that the details display the **Physical Entrance Name** custom event property.



23. Click **Return to Event List**.

Exercise 12 b) Filtering by a custom property in a search (optional)

You can optionally use the **Physical Entrance Name** custom property in a search.



From the **View** drop-down list on the **Log Activity** tab, select **Last Hour**.

You have configured QRadar SIEM for an uncommon log source. To stop feeding raw events to QRadar SIEM, press **Ctrl-C** in the terminal window or PuTTY.

This concludes the Version B exercises.

Unit 2 Leveraging reference data collections exercises

Reference data collections allow QRadar SIEM to maintain large amounts of information, such as IP addresses, port numbers, and user names. For example, use a reference set to maintain a watchlist of untrustworthy IP addresses to track suspicious activity.

Exercise 1 Using the REST API to manage reference data collections

This exercise illustrates how you can use the methods exposed by the REST API to create and manage reference data elements.

Task 1 Adding an element to a Reference Set using cURL

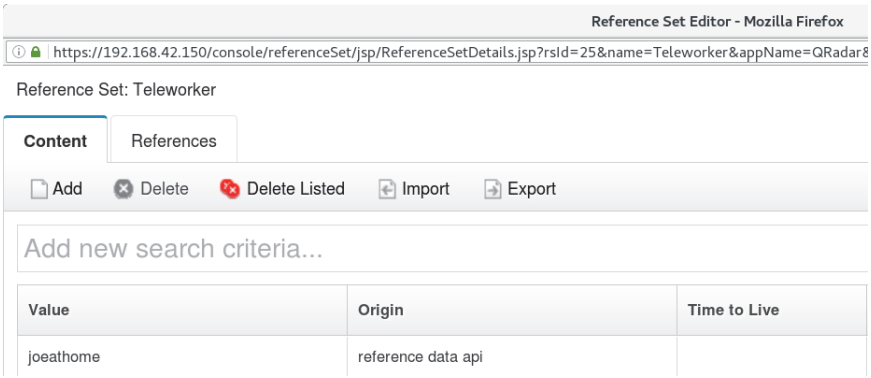
1. Open a remote shell to the QRadar VM.
2. In order to access the API, use the cURL utility. cURL is a command line tool for transferring data. To add a user account name into a reference set for remote employees, run the following command:

   ```
   curl -k --user admin:P@ssw0rd -X POST
   https://192.168.42.150/api/reference_data/sets/Teleworker?value=joeathome
   ```

3. Verify that the result closely matches the following screen capture.

```
[root@vulmgr ~]# curl -k --user admin:P@ssw0rd -X POST https://192.168.42.150/ap
i/reference_data/sets/Teleworker?value=joeathome
{"creation_time":1348244577718,"timeout_type":"LAST_SEEN","number_of_elements":1
,"name":"Teleworker","element_type":"ALN"}[root@vulmgr ~]#
```

4. Log in to the QRadar user interface.
5. To verify the addition of a new element into the reference set *Teleworker*, navigate to the **Admin** tab and click **Reference Set Management**.
6. From the Reference Set Management window, open the **Teleworker** set.

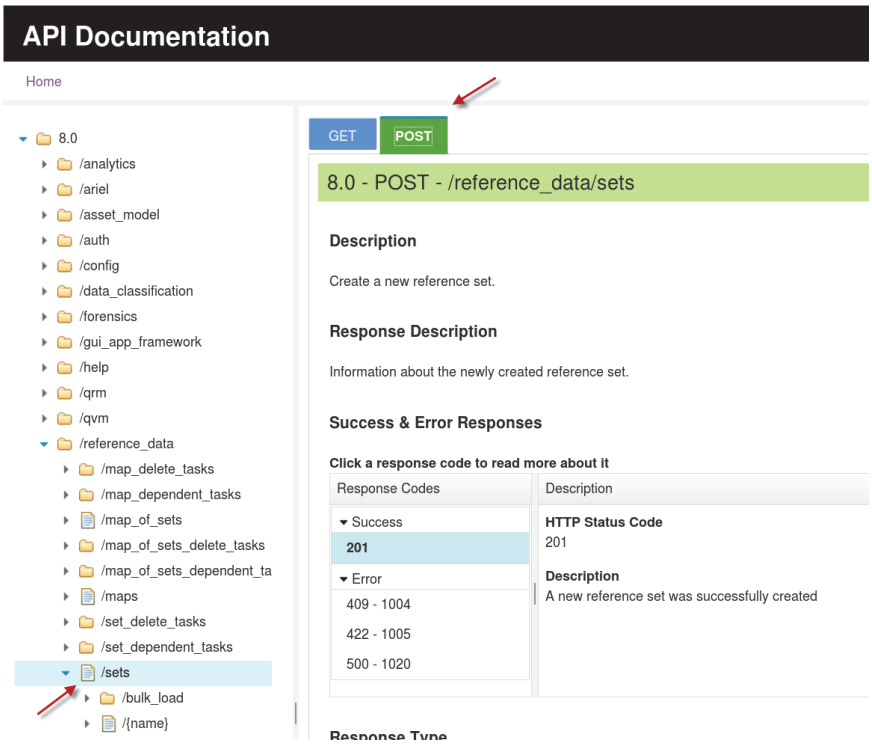


7. Note that the origin of the reference set element is from the REST API.

Task 2 Using the REST API via browser to manage reference sets

Note: No SSH connection or access to the QRadar GUI is necessary. The API calls that can be performed are defined by the REST API endpoints. To perform the API requests, the user needs specific Roles permissions and membership to a Security profile. For more information visit: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/kc_gen/toc-gen55.html

1. Open a second browser window in Firefox and enter the following URL:
   `https://192.168.42.150/api_doc`
2. Note that the URL contains the IP address of the QRadar Console.
3. The API Documentation site opens with several versions of the Rest API on the left-hand side.
4. To create a new Reference Set expand the folder with the latest version **8.0**.
5. Expand the folder `/reference_data` and click on `/sets`
6. The option **POST** on the upper right leads to the information about how to create a new reference set.

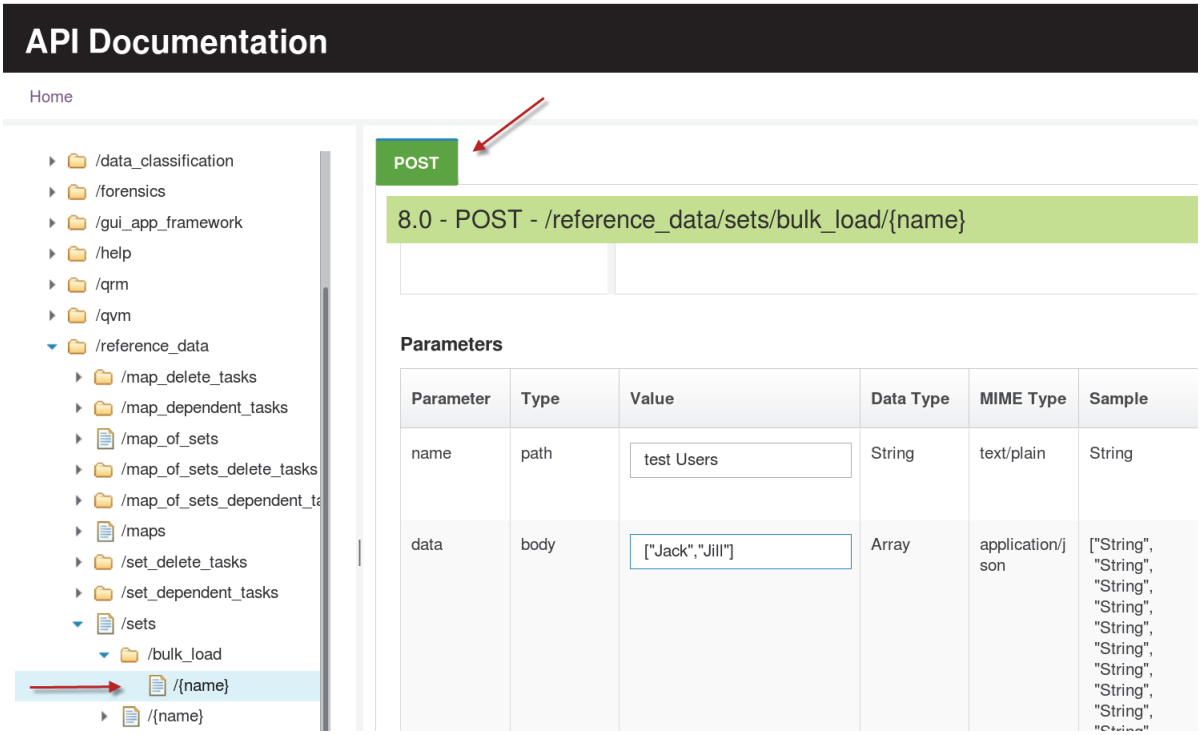


7. Scroll down to the parameters section and insert the following data in the required fields.

Parameters

Parameter	Type	Value	Data Type	MIME Type	Sample
element_type	query	ALN	String	text/plain	String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>
name	query	test Users	String	text/plain	String

8. To create the reference set click **Try It Out!** below the Parameters section.
9. Check the response code for success.
10. Add two elements in the created reference set by clicking **/name** and choosing the **POST** option.



11. Add **[“Jack”,”Jill”]** to the reference set **test Users.**

12. Click **Try It Out!** and check the response code for success.

13. Check the reference set in the QRadar user interface.

Note: Other types of reference data, such as maps, map of sets, and so on, can be managed accordingly.

Exercise 2 Using a reference map of sets

In this exercise, you use a reference map of sets in searches and custom rules.

Task 1 Creating a reference map

To create a reference map, perform the following steps:

1. Open an SSH session to the QRadar VM.
2. To create the reference map of sets, run the following commands:

```
cd /opt/qradar/bin
./ReferenceDataUtil.sh create PrivilegedAccess MAPOFSETS ALN
```

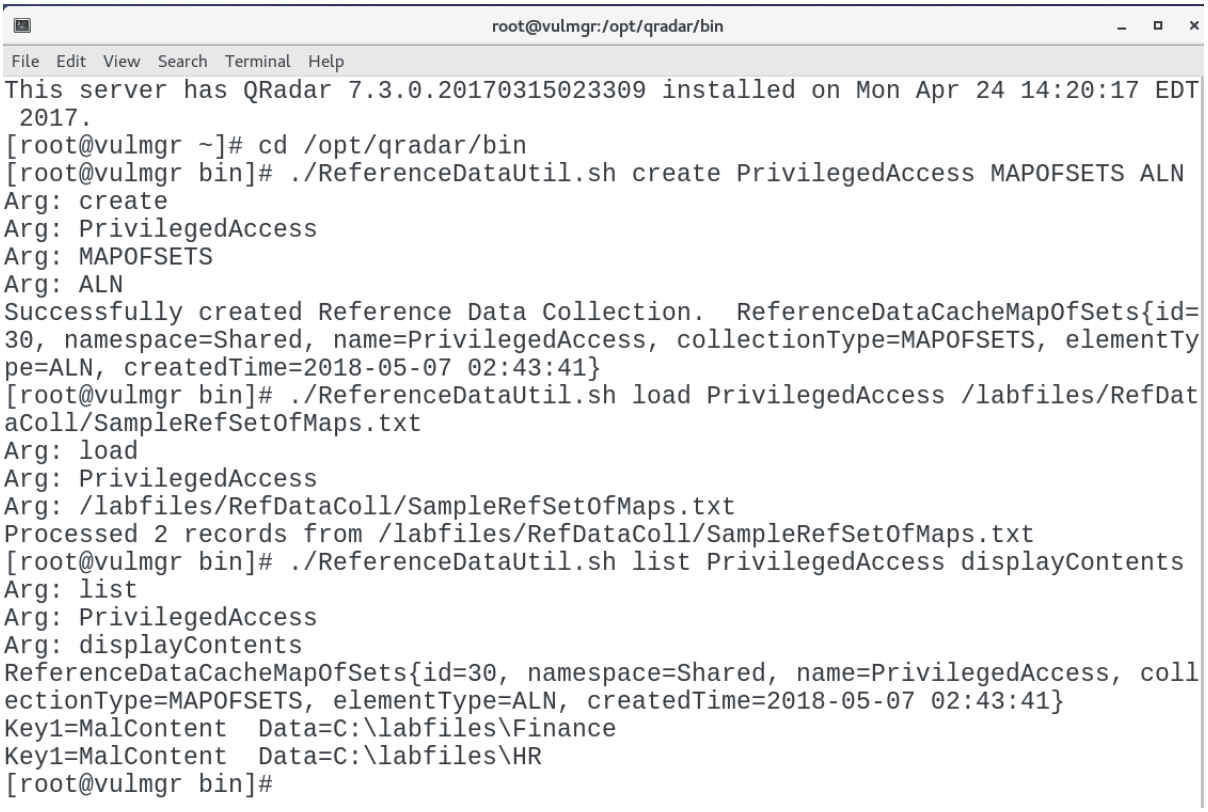
3. To populate the reference map of sets with elements, run the following command:

```
./ReferenceDataUtil.sh load PrivilegedAccess
/labfiles/RefDataColl/SampleRefMapOfSets.txt
```

4. To check the contents, run the following command:

```
./ReferenceDataUtil.sh list PrivilegedAccess displayContents
```

5. Verify that the contents of the reference map of sets look like the contents at the bottom of the following screen capture.



Task 2 Creating a log source

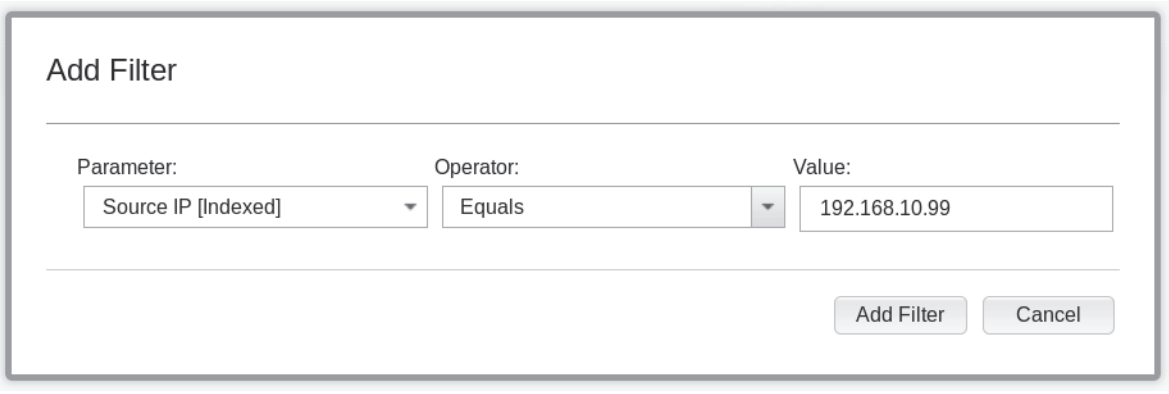
Follow these steps to create a log source for the Windows events that you will be analyzing:

1. In your SSH session on the QRadar VM, run the following commands:

```
cd /labfiles/RefDataColl
/opt/qradar/bin/logrun.pl -d 192.168.42.150 -u 192.168.10.99 -f
windows_audit.log 30
```

Note: `logrun.pl` is a utility shipped with QRadar that allows for the replay of raw events and is useful for testing.

2. Navigate to the **Log Activity** tab.
3. To display only events with the source IP address 192.168.10.99, perform the following steps:
   a. Click **Add Filter** on the toolbar.
   b. For **Parameter**, enter or select **Source IP [Indexed]**.
   c. For **Operator**, leave **Equals** selected.
   d. For **Value**, enter `192.168.10.99`
   e. Verify that your filter looks like the one in the following screen capture.



   f. Click **Add Filter**.

4. From the **View** drop-down list, select **Last 15 Minutes**. In the Log Source column, notice that QRadar SIEM discovered the log source type and created a log source object.

Event Name	Log Source	Even Coun	Time ▾	Low Level Category	Source IP
Microsoft Windows Security Event Log Message	WindowsAuthServer @ 192....	1	May 7, 2018, 3:28:1...	Stored	192.168.10.99
Microsoft Windows Security Event Log Message	WindowsAuthServer @ 192....	1	May 7, 2018, 3:28:0...	Stored	192.168.10.99
Microsoft Windows Security Event Log Message	WindowsAuthServer @ 192....	1	May 7, 2018, 3:28:0...	Stored	192.168.10.99
Success Audit: An attempt was made to access an object	WindowsAuthServer @ 192....	27	May 7, 2018, 3:28:0...	Information	192.168.10.99
Success Audit: An attempt was made to access an object	WindowsAuthServer @ 192....	1	May 7, 2018, 3:28:0...	Information	192.168.10.99
Success Audit: An attempt was made to access an object	WindowsAuthServer @ 192....	1	May 7, 2018, 3:28:0...	Information	192.168.10.99
Success Audit: An attempt was made to access an object	WindowsAuthServer @ 192....	1	May 7, 2018, 3:28:0...	Information	192.168.10.99
Unknown log event	SIM Generic Log DSM-7 :: v...	1	May 7, 2018, 3:28:0...	Unknown Generic Log Event	192.168.10.99
Unknown log event	SIM Generic Log DSM-7 :: v...	1	May 7, 2018, 3:28:0...	Unknown Generic Log Event	192.168.10.99
Unknown log event	SIM Generic Log DSM-7 :: v...	1	May 7, 2018, 3:28:0...	Unknown Generic Log Event	192.168.10.99
Unknown log event	SIM Generic Log DSM-7 :: v...	1	May 7, 2018, 3:28:0...	Unknown Generic Log Event	192.168.10.99
Unknown log event	SIM Generic Log DSM-7 :: v...	1	May 7, 2018, 3:28:0...	Unknown Generic Log Event	192.168.10.99
Unknown log event	SIM Generic Log DSM-7 :: v...	1	May 7, 2018, 3:28:0...	Unknown Generic Log Event	192.168.10.99

5. To open the details of the **Success Audit: An attempt was made to access an object** event, double-click it. Observe that a custom property **ObjectName** is displayed.

GroupID (custom)	N/A
ObjectName (custom)	C:\labfiles\Finance
ObjectType (custom)	File

6. The raw event, which is attached as a payload to the normalized event, contains the name of the accessed file as Object . Examine the structure of the file and the QID of the event.

Payload Information

utf | hex | base64

Wrap Text

```
<182>May 07 05:01:41 192.168.10.99 <13>Jul 10 23:27:28 securebox AgentDevice=WindowsLog    AgentLogFile=Securit
y    PluginVersion=7.2.2.984723    Source=Microsoft-Windows-Security-
Auditing    Computer=FSPDC.coe.ibm.com    OriginatingComputer=    User=    Domain=    EventID=4663    EventIDCo
de=4663    EventType=8    EventCategory=12800    RecordNumber=948263    TimeGenerated=1436563646    TimeWritten
=1436563646    Level=0    Keywords=0    Task=0    Opcode=0    Message=An attempt was made to access an object.
 Subject:  Security ID:  COE\MalContent  Account Name:  MalContent  Account Domain:  COE  Logon ID:  0x19467f
Object:  Object Server: Security  Object Type: File  Object Name: C:\labfiles
\Finance  Handle ID: 0x58  Process Information:  Process ID: 0xb9c  Process Name: C:\Windows\System32
\cmd.exe  Access Request Information:  Accesses: ReadData (or ListDirectory)       Access Mask: 0x1
```

Additional Information

Protocol	255	**QID**	5000850
Log Source	WindowsAuthServer @ 192.168.10.99	**Event Count**	1

7. By default, QRadar SIEM coalesces events for autodiscovered log sources. Because the payload field is not one of the fields tested for uniqueness during the coalescing process,

valuable data such as the path of the file being accessed can get lost. To disable coalescing for the Windows log source, perform the following steps:

a. Navigate to the **Admin** tab.

b. To open the Log Sources window, click the **Log Sources** icon.

c. Double-click the **WindowsAuthServer@192.168.10.99** entry.

d. Clear the **Coalescing Events** option.

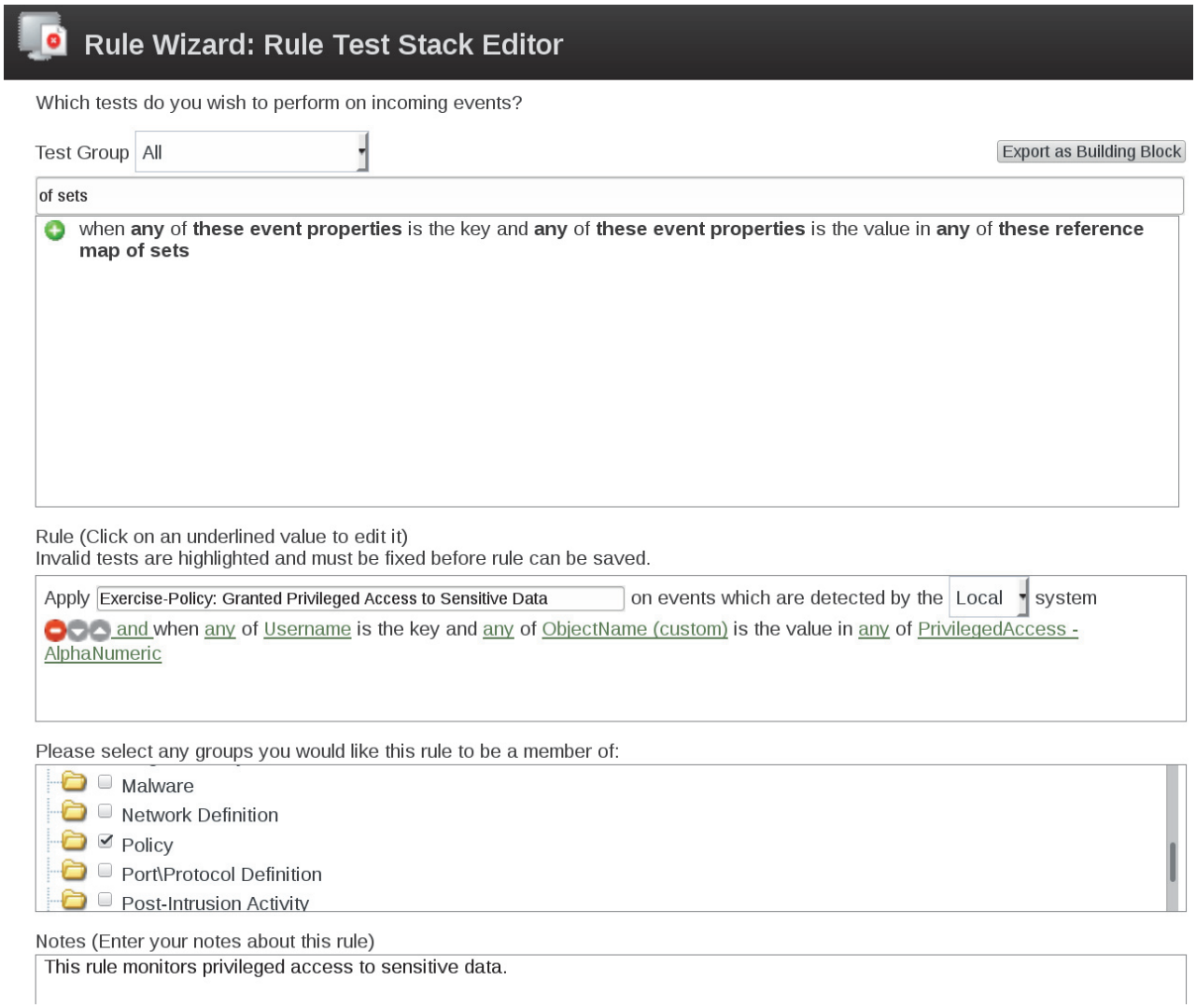
e. Click **Save**.

Task 3 Creating a custom rule to monitor privileged access to sensitive data

To create a custom rule to compare file access events with the existing reference map of sets, perform the following steps:

1. Navigate to the **Offenses** tab.
2. Click **Rules** in the left pane.
3. From the **Actions** drop-down list, select **New Event Rule**.
   The Rule Wizard opens.
4. If the Rule Wizard starts with its welcome page, read the introductory text and enable **Skip this page when running this rules wizard**. To navigate to the Rule Test Stack Editor, click **Next** twice.
5. For the custom rule name in the **Apply** field, enter the following name:
   `Exercise-Policy: Granted Privileged Access to Sensitive Data`
6. Locate and click the green **plus (+)** icon for the following test:
   when any of these event properties is the key and any of these event properties is the value in any of these reference map of sets
7. For the first these event properties parameter, select **Username**.
8. For the second these event properties parameter, select **ObjectName (custom)**.
9. For the these reference map of sets parameter, select **PrivilegedAccess**.
10. To assign the custom rule to the group Policy, scroll down in the list of groups and enable **Policy**.
11. To document the rule in the **Notes** field, enter the following text:
    `This rule monitors privileged access to sensitive data.`

12. Verify that your Rule Wizard looks like the following screen capture.



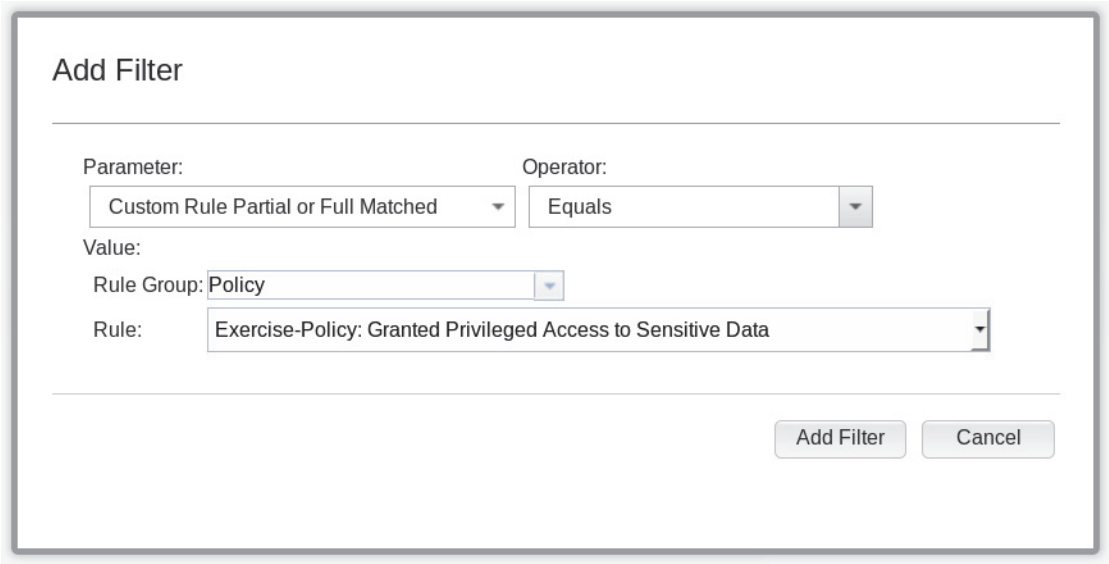
13. Do not configure an action or response.

14. Click **Finish**

Task 4 Creating a search

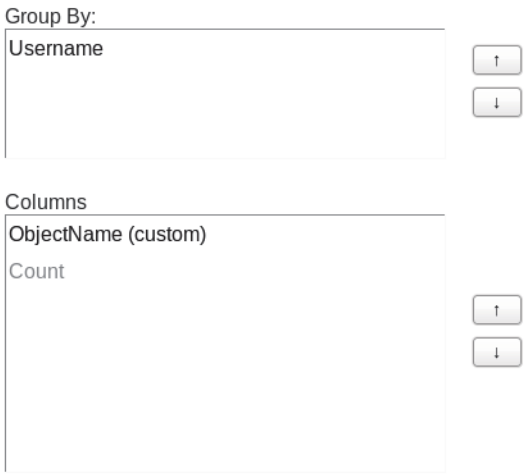
To create a search for events tagged by the custom rule, perform the following steps:

1. In the QRadar SIEM web interface, double-click the **Log Activity** tab. The double-click resets the tab to its default settings.
2. To add the **Custom Rule Partial or Full Matched Equals Exercise-Policy: Granted Privileged Access to Sensitive Data** filter, perform the following steps:
   a. Click **Add Filter** on the toolbar.
   b. In the **Parameter** drop-down list, select the **Custom Rule Partial or Full Matched** search parameter.
   c. For **Operator**, leave **Equals** selected.
   d. From the **Rule Group** drop-down list, select **Policy**.
   e. From the **Rule** drop-down list, select **Exercise-Policy: Granted Privileged Access to Sensitive Data**.
   f. Verify that your filter looks like the one in the following screen capture.



   g. Click **Add Filter**.
3. Edit the search and format the columns in the search results. Group the search results by **Username**. Include **ObjectName (custom)** in the search results. Order the search results by **Count** in descending order.

4. The following screen capture of the Column Definition shows only the mandatory columns. You can have more columns.

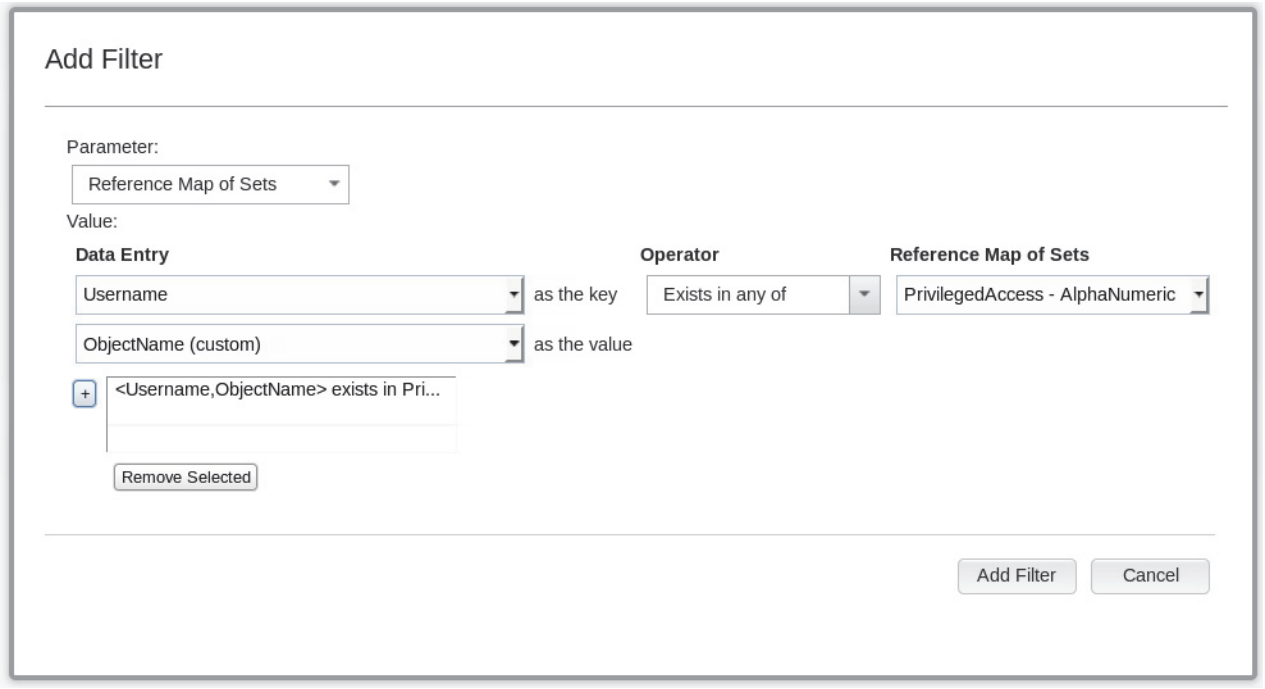


5. Save the search criteria under the name **Granted Privileged Access to Sensitive Data**.

Alternatively, you can create a search that uses directly the PrivilegedAccess reference map of sets instead of the rule. To create the alternative search, perform the following steps:

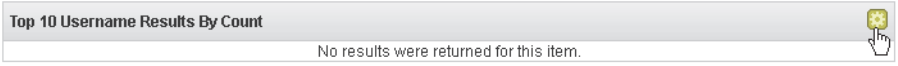
6. To reset the **Log Activity** tab to its default settings, double-click it.
7. To add a filter that uses the PrivilegedAccess reference map of sets, perform the following steps:
   a. Click **Add Filter** in the toolbar.
   b. In the **Parameter** drop-down list, select the **Reference Map of Sets** search parameter.
   c. From the **Data Entry** drop-down list **as the key**, select **Username**.
   d. From the **Data Entry** drop-down list **as the value**, select **ObjectName (custom)**.
   e. For **Operator**, leave **Exists in any of** selected.
   f. From the **Reference Maps of Sets** drop-down list, select **PrivilegedAccess**.
   g. Click the plus sign to add the filter.

h. Verify that your filter looks like the one in the following screen capture.

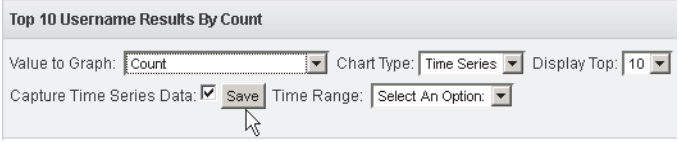


i. Click **Add Filter**.

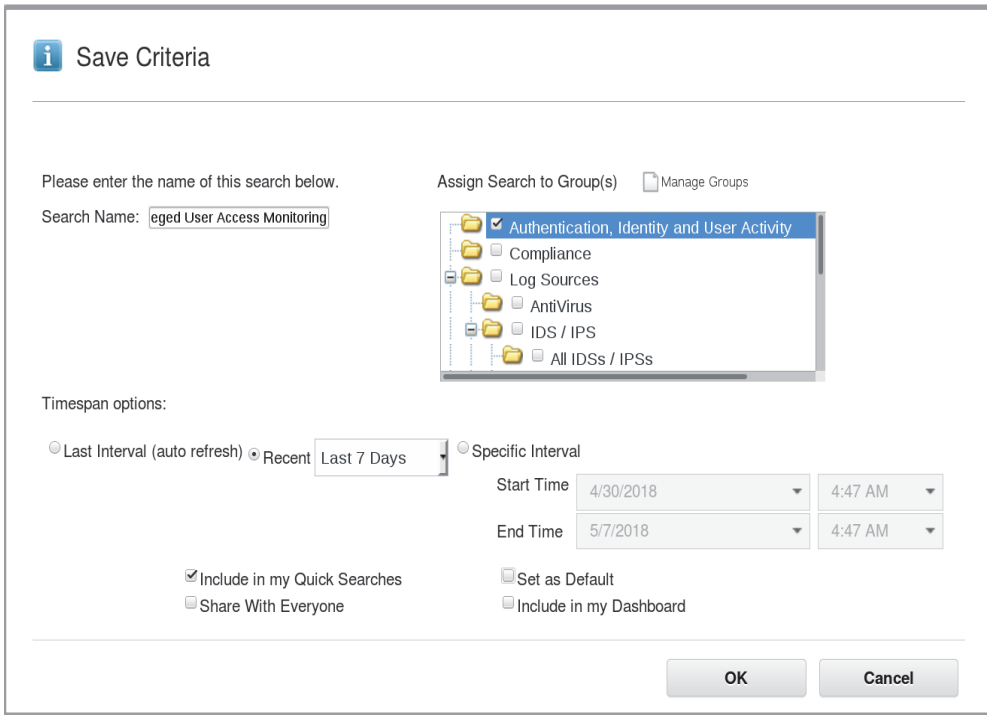
8. Edit the search and complete the following steps:
   a. For **Time Range**, enable **Recent** and select **Last 7 Days**.
   b. Under **Column Definition**, group the search results by **Username**.
   c. Add **ObjectName (custom)** to the search result columns.
   d. Order the search results by **Count** in descending order.
9. Click **Search**.
10. Configure the search to accumulate data.
    a. Click the **Configure** icon in the top-right corner of the **Top 10 Username Results By Count** chart.



    b. From the **Chart Type** drop-down list, select **Time Series**.
    c. Enable **Capture Time Series Data**.
    d. Verify that your configuration looks like the one in the following screen capture.



11. Click **Save**.
12. Name the search **Privileged User Access Monitoring**.
13. Assign the Search to the **Authentication, Identity and User Activity** group.



14. Double click the **Log Activity** tab to reset it.
15. Test both searches from your **Quick Searches** menu.

Task 5 Verifying the custom rule to monitor privileged access to sensitive data

1. In your SSH session on the QRadar VM, run the following commands:

```
cd /labfiles/RefDataColl
/opt/qradar/bin/logrun.pl -d 192.168.42.150 -u 192.168.10.99 -f
windows_audit.log 30
```

2. To reset the **Log Activity** tab to its default settings, double-click it.

3. From the **View** drop-down list, select **Last 5 minutes**. Verify that the list contains **Success Audit: An attempt was made to access an object** events.

Event Name	Log Source
Success Audit: An attempt was made to access an object	WindowsAuthServer @ 192.168.10.99
Success Audit: An attempt was made to access an object	WindowsAuthServer @ 192.168.10.99
Success Audit: An attempt was made to access an object	WindowsAuthServer @ 192.168.10.99
Success Audit: An attempt was made to access an object	WindowsAuthServer @ 192.168.10.99
Success Audit: An attempt was made to access an object	WindowsAuthServer @ 192.168.10.99
Success Audit: An attempt was made to access an object	WindowsAuthServer @ 192.168.10.99

4. Open the event details for any event and verify that the event triggered the **Exercise-Policy: Granted privileged access to sensitive data** rule.

Additional Information

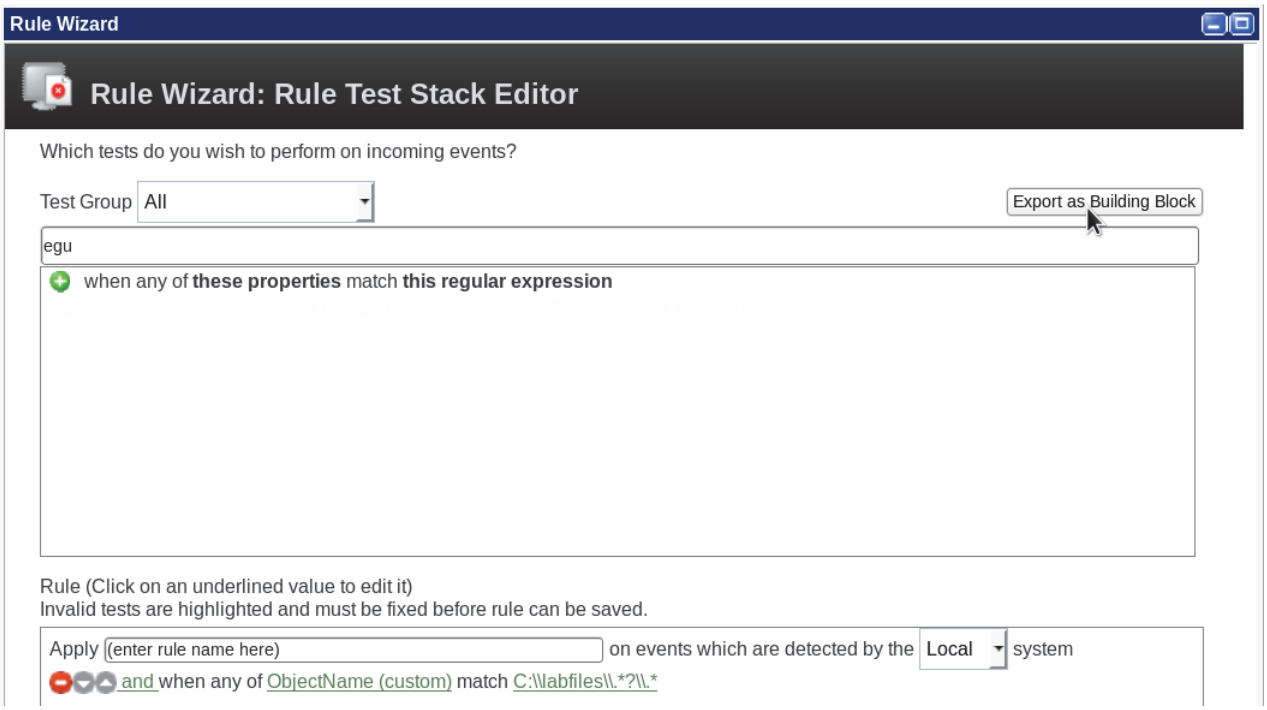
Protocol	255	**QID**	5000850
Log Source	WindowsAuthServer @ 192.168.10.99	**Event Count**	1
Custom Rules	Exercise-Policy: Granted Privileged Access to Sensitive Data Source Asset Weight is Low Destination Asset Weight is Low Context is Local to Local		

Task 6 Creating a custom rule to record access to sensitive data

When new sensitive data is created, company security policies require the file to be monitored for privileged user access. Assuming that the user who accesses the data is a privileged user, you can record who accesses the sensitive data. To create a building block and a custom rule, perform the following steps:

1. Navigate to the **Offenses** tab.
2. Click **Rules** in the left pane.
3. From the **Actions** drop-down list, select **New Event Rule**.
   The Rule Wizard opens.
4. Click **Next** twice.
5. To create a building block, perform the following steps:
   a. Locate and click the green **plus (+)** icon for the following test:
      when any of these properties match this regular expression
   b. For the these properties parameter, select **ObjectName (custom)**.
   c. For the this regular expression parameter, enter the following regular expression:
      `C:\\labfiles\\.*?\\.*`

6. Verify that your Rule Wizard looks like the following screen capture and click the button on the upper right **Export as Building Block**



Hint: The regular expression test consumes significant computational resources. In a production environment, precede the regular expression test with more efficient tests in order to minimize the number of events the regular expression has to be performed on.

7. For **Building Block Name**, enter the following name:

   `Exercise-BB:CategoryDefinition: Sensitive Data Accessed`

8. To create the building block, click **Save**.

   The window closes.

   Do not close the Rule Wizard.

9. To create another event rule, perform the following steps:

   a. For the custom rule name in the **Apply** field, enter the following text:

      `Exercise-Policy: Sensitive Data Accessed`

b. Locate and click the green **plus (+)** icon for the following test:
when an event matches any of the following rules

c. For the rules parameter, select **Exercise-BB:CategoryDefinition: Sensitive Data Accessed**.

d. Locate and click the green **plus (+)** icon for the following test:
when the event QID is one of the following QIDs

e. For the **QID** parameter, select **5000850**.

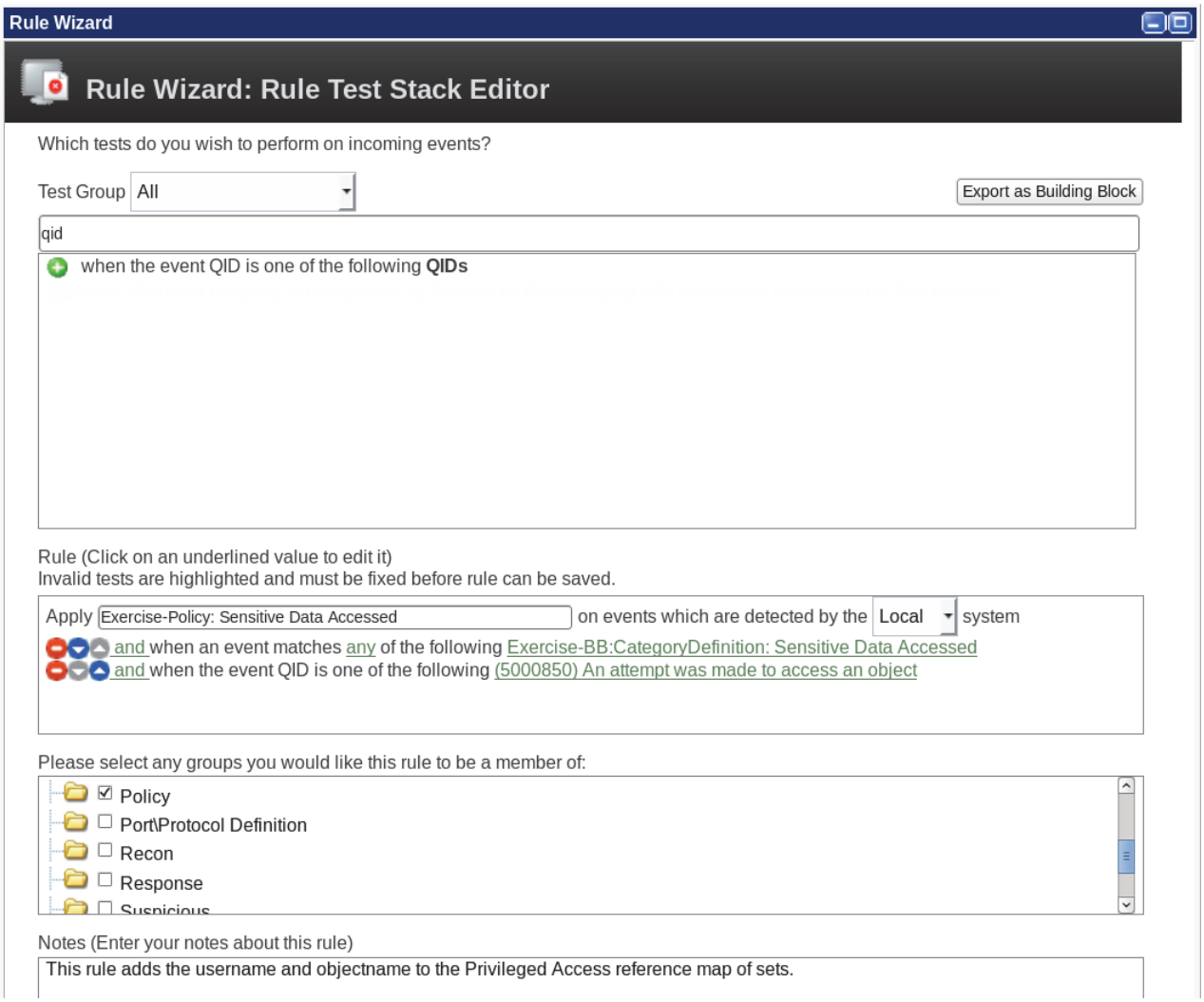
Hint: In the Browse or search for QID window, enter `5000850` in the **QID/Name** field and click **Search**.

f. To assign the custom rule to the group Policy, scroll down in the list of groups and enable **Policy**.

g. To document the rule in the **Notes** field, enter the following text:

```
This rule adds the username and objectname to the Privileged Access reference
map of sets.
```

10. Verify that your rule looks like the one in the following screen capture.

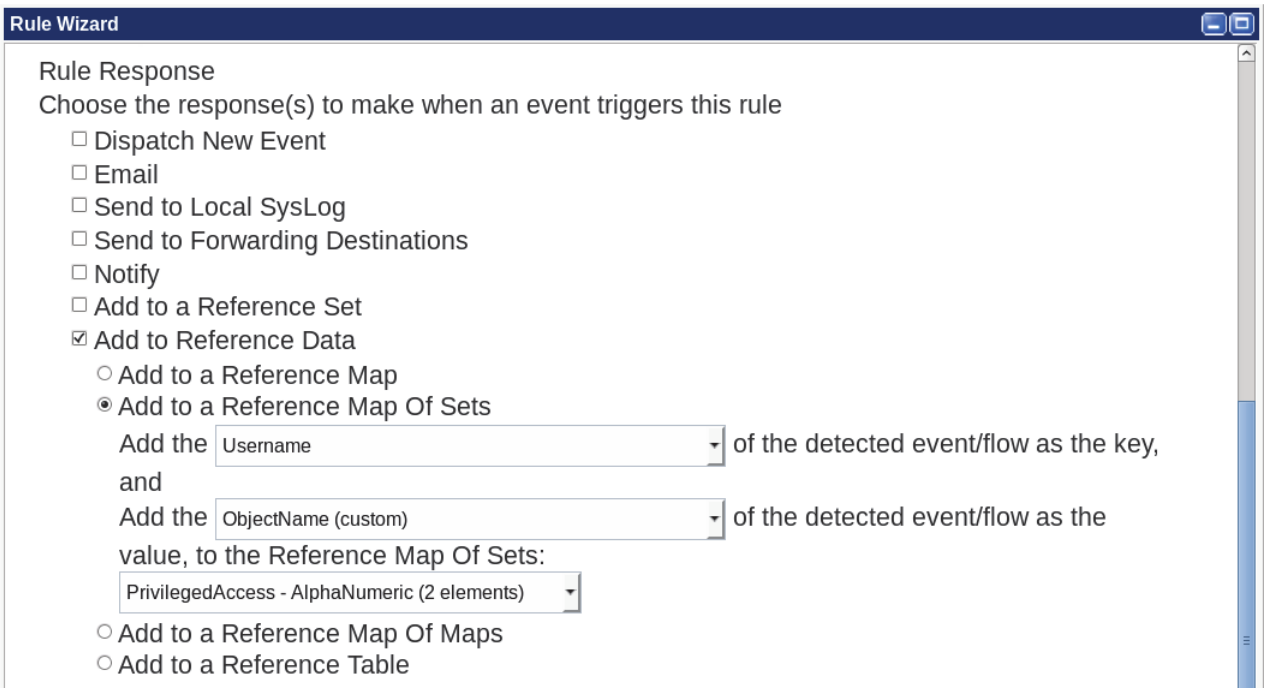


11. Click **Next**.

12. To configure the rule response, provide the settings from the following table.

Option	Setting
Add to Reference Data	Enable
Add to a Reference Map of Sets	Enable
Property to define as the key	Username
Property to define as the value	ObjectName(custom)
Reference Map of Sets	PrivilegedAccess

13. Verify that your rule response looks like the one in the following screen capture.



14. Click **Finish**.

Task 7 Testing the custom rule to record access to sensitive data

To test the custom rule, you must simulate file access on the monitored Windows server. The custom rule detects when a user accesses a file in the `C:\labfiles` directory and adds an element that contains the user name and the name of the file accessed in the PrivilegedAccess reference map of sets.

To test the custom rule, perform the following steps:

1. Navigate to the **Log Activity** tab.
2. From the **View** drop-down list, select **Real Time (Streaming)**.
3. In the **Quick Filter** search field, enter the following text:

   ```
   backdoor*
   ```

4. In your SSH session on the QRadar VM, run the following commands:

   ```
   cd /labfiles/RefDataColl
   /opt/qradar/bin/logrun.pl -d 192.168.42.150 -u 192.168.10.99 -f
   windows_backdoor.log 30
   ```

5. On the **Log Activity** tab, verify that **Success Audit: An attempt was made to access an object** events are displayed.

6. Pause the event stream, double-click any of the **Object Opened Successfully** events, and view the event detail.

7. Verify that the **ObjectName (custom)** property value is **C:\labfiles\Development\backdoor.txt**.

Event Information

Event Name	Success Audit: An attempt was made to access an object	
Low Level Category	Information	
Event Description	Success Audit: An attempt was made to access an object.	
Magnitude	(5)	**Relevance**
Username	BadActor	
Start Time	May 7, 2018, 5:22:21 AM	**Storage Time**
Accesses (custom)	N/A	
AccountDomain (custom)	N/A	
AccountID (custom)	N/A	
AccountName (custom)	BadActor	
ChangedAttributes (custom)	N/A	
EventID (custom)	4663	
GroupID (custom)	N/A	
ObjectType (custom)	File	
Object_Name_exercise (custom)	C:\labfiles\Development\backdoor.txt	

8. Verify that the event triggered the **Exercise-Policy: Sensitive Data Accessed** custom rule and **Exercises-BB:CategoryDefinition: Sensitive Data Accessed** building block.

Additional Information

Protocol	255	**QID**	5000850
Log Source	WindowsAuthServer @ 192.168.10.99	**Event Count**	1
Custom Rules	Exercise-BB:CategoryDefinition: Sensitive Data Accessed Exercise-Policy: Sensitive Data Accessed Exercise-Policy: Granted Privileged Access to Sensitive Data Source Asset Weight is Low Destination Asset Weight is Low Context is Local to Local		

9. To display the contents of PrivilegedAccess reference map of sets, run the following commands:

```
cd /opt/qradar/bin
./ReferenceDataUtil.sh list PrivilegedAccess displayContents
```

10. Verify that your output looks similar to the one in the following screen capture.

```
[root@vulmgr RefDataColl]# cd /opt/qradar/bin/
[root@vulmgr bin]# ./ReferenceDataUtil.sh list PrivilegedAccess displayContents
Arg: list
Arg: PrivilegedAccess
Arg: displayContents
ReferenceDataCacheMapOfSets{id=30, namespace=Shared, name=PrivilegedAccess, coll
ectionType=MAPOFSETS, elementType=ALN, createdTime=2018-05-07 02:43:41}
Key1=BadActor  Data=C:\labfiles\Development\backdoor.txt
Key1=MalContent  Data=C:\labfiles\Finance
Key1=MalContent  Data=C:\labfiles\HR
[root@vulmgr bin]#
```

11. Use the REST API to verify the reference data. In your SSH session, run the following command:

```
curl -k --user admin:P@ssw0rd -X GET
https://192.168.42.150/api/reference_data/map_of_sets/PrivilegedAccess | python
-mjson.tool
```

Note: Python is used in this command to properly format the JSON output.

12. Verify that your output resembles the one in the following screen capture.

You created a mechanism to automatically add new privileged access elements to the reference map of sets.

This concludes the exercises.

Unit 3 Developing custom rules exercises

In the exercises, you develop two different solutions for the same problem. You create custom rules, building blocks, custom event properties, and a reference set. The lab includes exploratory steps to narrow down approaches towards the two solutions.

Scenario: You suspect that occasionally unauthorized services run in your organization. QRadar SIEM creates asset profiles for hosts with services from analyzing network flows and events. But when you look for any unauthorized service or asset profile in QRadar, you cannot find any. Old events from the QRadar Asset Profiler suggest that a non-admin QRadar user deleted asset profiles shortly after QRadar SIEM created them automatically in order to hide the unauthorized service. Instead of investigating the old events further, you want to be alerted by an offense if a user deletes asset profiles shortly after they have been created.

Exercise 1 Considering the evidence

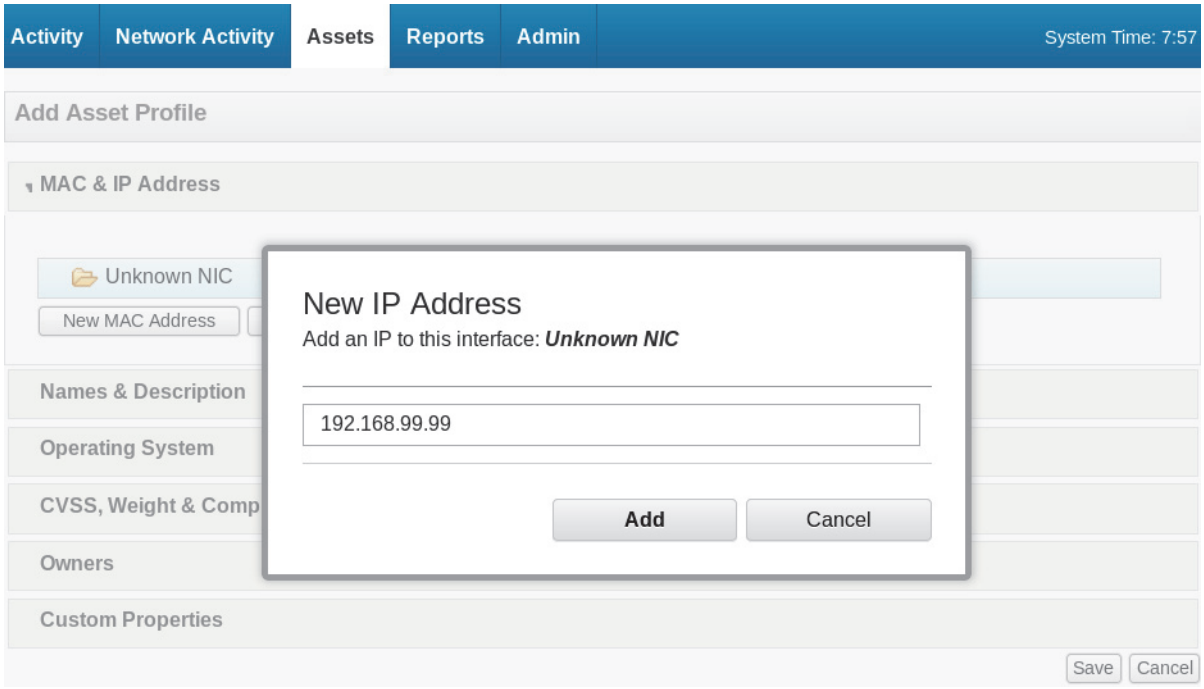
You want to detect when the same QRadar user deletes asset profiles that QRadar has created recently. The Asset Profiler of QRadar dispatches events when it creates and deletes asset profiles and their characteristics. These events carry the information necessary for your purpose.

Task 1 Creating and deleting asset profiles

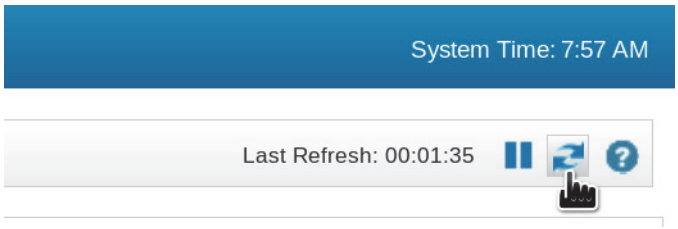
In order to determine how to detect when the same QRadar user deletes asset profiles that QRadar has created recently, learn which footsteps this activity leaves as events. Therefore, perform the following steps to create and delete an asset profile manually:

1. To log in to the QRadar web interface, start Mozilla Firefox. Use the procedure “Logging in to the QRadar user interface” on page vii.
2. Navigate to the **Assets** tab.
3. To create an asset profile, click **Add Asset** in the toolbar.

4. For **New IP Address**, enter `192.168.99.99` or any other address not used by an already existing asset profile.



5. To create the new IP address, click **Add**.
6. To create the new asset profile, click **Save**.
7. To refresh the listed asset profiles, click the **double arrow** icon in the upper-right corner of the QRadar SIEM user interface, or double-click the **Assets** tab. The double-click refreshes and resets the tab to its default settings.

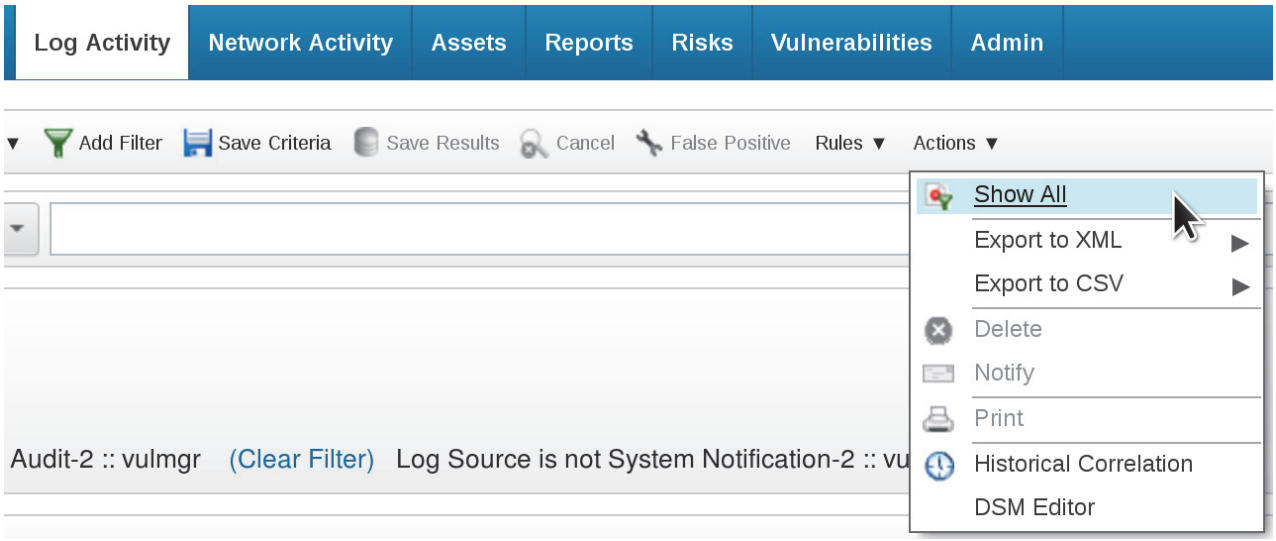


8. Locate the asset profile that you just created.
9. To delete the asset profile, select it and, from the **Actions** drop-down list, select **Delete Asset**.
10. To close the confirmation pop-up window, click **OK**.

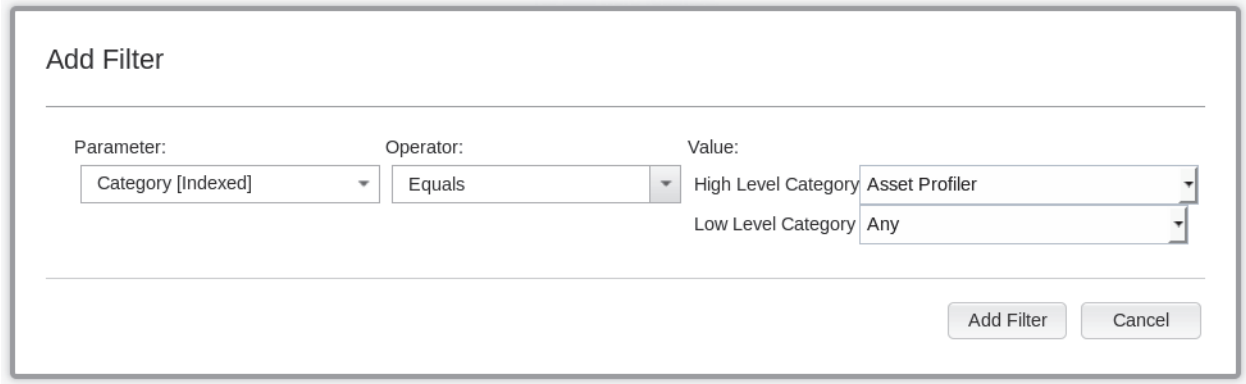
Task 2 Locating events from the Asset Profiler

The Asset Profiler of QRadar dispatched events to record your creation and deletion of an asset profile. To locate these events, perform the following steps:

1. Navigate to the **Log Activity** tab.
2. To clear all filters, from the **Actions** drop-down list, select **Show All**.



3. To display events from the last 15 minutes, in the **View** drop-down list, select **Last 15 minutes**.
4. To display only events in the Asset Profiler high level category, perform the following steps to create a filter:
   a. Click **Add Filter** in the toolbar.
   b. In the **Parameter** drop-down list, select the **Category [Indexed]** search parameter.
   c. In the **Operator** drop-down list, select **Equals**.
   d. In the **High Level Category** drop-down list, select **Asset Profiler**.
   e. To filter the events, click **Add Filter**.



As a result, the table on the **Log Activity** tab displays only asset-related events:

Current Filters:
High Level Category is Asset Profiler (Clear Filter)
▸ **Current Statistics**

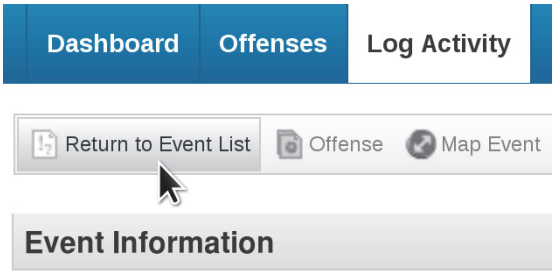
	Event Name	Log Source	Event Count	Time ▼	Low Level Category
	Asset Deleted	Asset Profiler-2 :: janus	1	Jun ...	Asset Deleted
	IP Address Created	Asset Profiler-2 :: janus	1	Jun ...	Asset IP Address Created
	Interface Created	Asset Profiler-2 :: janus	1	Jun ...	Asset Interface Created
	Asset Created	Asset Profiler-2 :: janus	1	Jun ...	Asset Created

These events record your creation and deletion of an asset profile. Any attempt to hide an unauthorized service by deleting asset profiles that QRadar created automatically leads to the same trail of evidence. Therefore, you have found the events that your custom rules and building blocks need to use.

Task 3 Exploring events and outlining a solution

Double-click the events of the Asset Profiler to navigate to their details. Their fields and payload lead you to the considerations below.

If you have navigated to the details of an event, click **Return to Event List** on the left in the toolbar in order to display the list of events from the Asset Profiler in the **Log Activity** tab.



Considerations:

- Asset Deleted event

  You need to detect the attempt to hide a temporary service when a QRadar user deletes an asset profile. Therefore, your rules need to watch Asset Deleted events.

- Temporary asset profiles

  Evidence for the attempt to hide an unauthorized service is that its asset information exists only temporarily in QRadar. The Asset Deleted event does not carry any lifetime information. To get the lifetime of an asset profile, you need to match a deletion event to the related creation event, and use the time of both events. To match events from the Asset Profiler concerning the same asset profile, use the asset ID. Two events concerning the same asset profile carry the same

asset ID in their payload. To extract the asset ID from the payload, you will create custom event properties later in this exercise.

- IP Address Created event

  For two reasons, you need to use the Asset IP Address event instead of the Asset Creation event:

  – It’s unlikely, but asset profiles can exist without an IP address. For this purpose, only asset profiles with IP addresses are relevant because an unauthorized service requires an IP address.

  – Asset profiles can have more than one IP address. In fact, the perpetrator could install the unauthorized service with a new IP address on an old host shortly before it is decommissioned. In this case, the asset profile was created a long time ago but the IP address exists only temporarily.

  For simplification, omit the case of a temporary port.

- Asset IP Address Deleted event

  When a QRadar user manually removes an IP address from an asset profile but does not delete the asset profile itself, QRadar SIEM dispatches an Asset IP Address Deleted event. For simplification, this exercise omits Asset IP Address Deleted events. When an entire asset profile is deleted, QRadar SIEM dispatches only an Asset Deleted event, not an Asset IP Address Deleted event.

- Same QRadar user

  Occasionally QRadar users might delete asset profiles shortly after their creation for legitimate reasons. To avoid false positives, you only need to be alerted by an offense if the same QRadar user deletes recently created asset profiles more than once. For this purpose, you need to extract the user name from the payload of Asset Deleted events using a custom event property later in this exercise.

Exercise 2 Creating custom event properties

To make the required information in the event payloads usable by custom rules and building blocks, create three custom event properties.

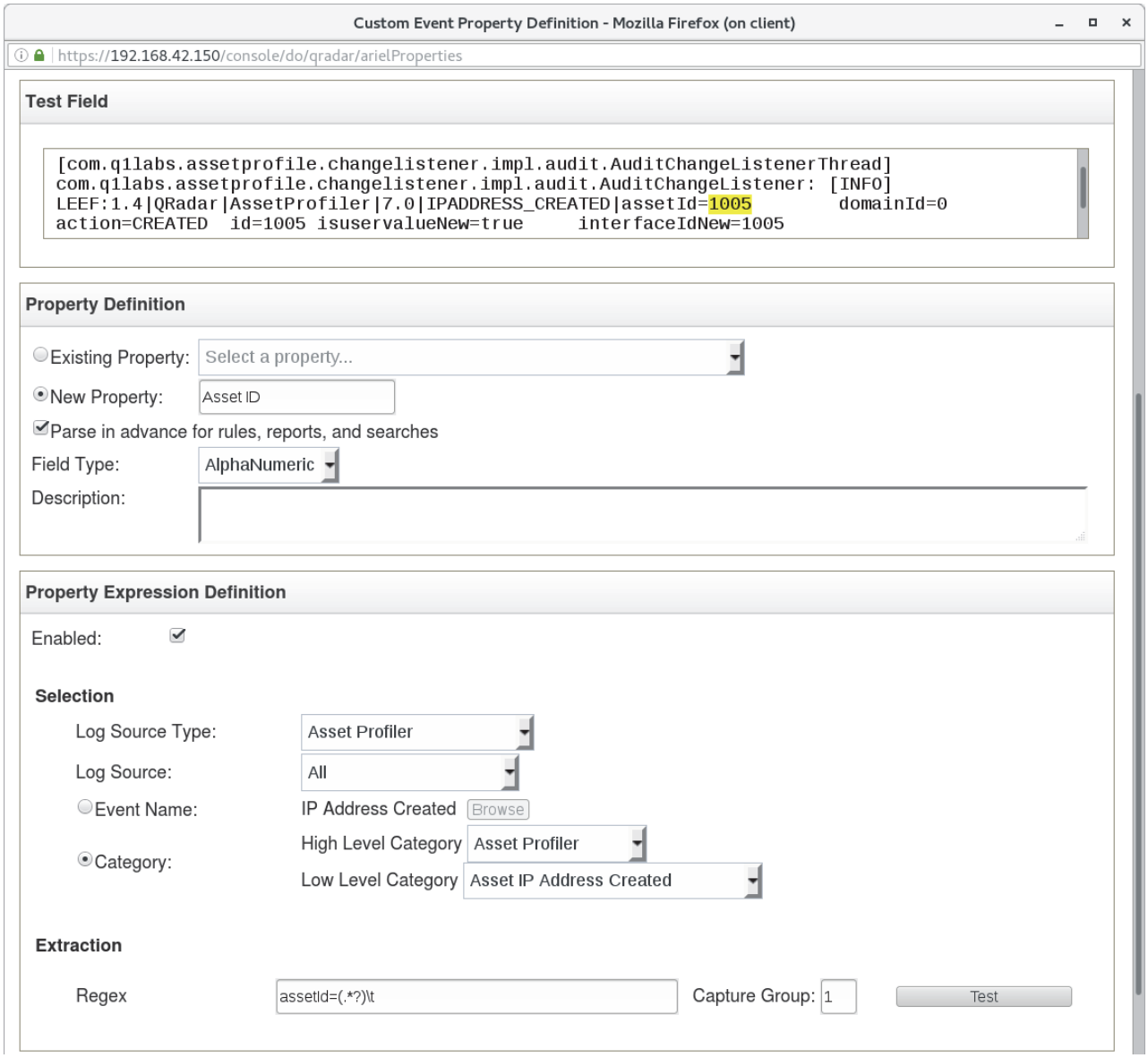
Task 1 Capturing Asset ID from IP Address Created events

To capture the asset ID from **IP Address Created** events in a custom event property, perform the following steps:

1. If you have navigated to the details of an event, click **Return to Event List** on the left in the toolbar in order to display the list of events from the Asset Profiler in the **Log Activity** tab.
2. To navigate to the details of an **IP Address Created** event, double-click it.
3. To open the Custom Event Property Definition window, click **Extract Property** in the toolbar.
4. In the Custom Event Property Definition window, scroll down to the Property Definition section and perform the following steps:
   a. Select **New Property**.
   b. For **New Property**, enter the following name:
      ```
      Asset ID
      ```
   c. Select **Parse in advance for rules, reports, and searches**.

5. Scroll down to the Property Expression Definition section and perform the following steps:
   a. Select **Category**.
   b. For **RegEx**, enter the following regular expression:

      ```
      assetId=(.*?)\t
      ```



6. Click **Save**.

   The Custom Event Property Definition window closes.

7. The **Log Activity** tab still displays the details of the **IP Address Created** event. To display the list of events from the Asset Profiler again, click **Return to Event List** on the left in the toolbar.

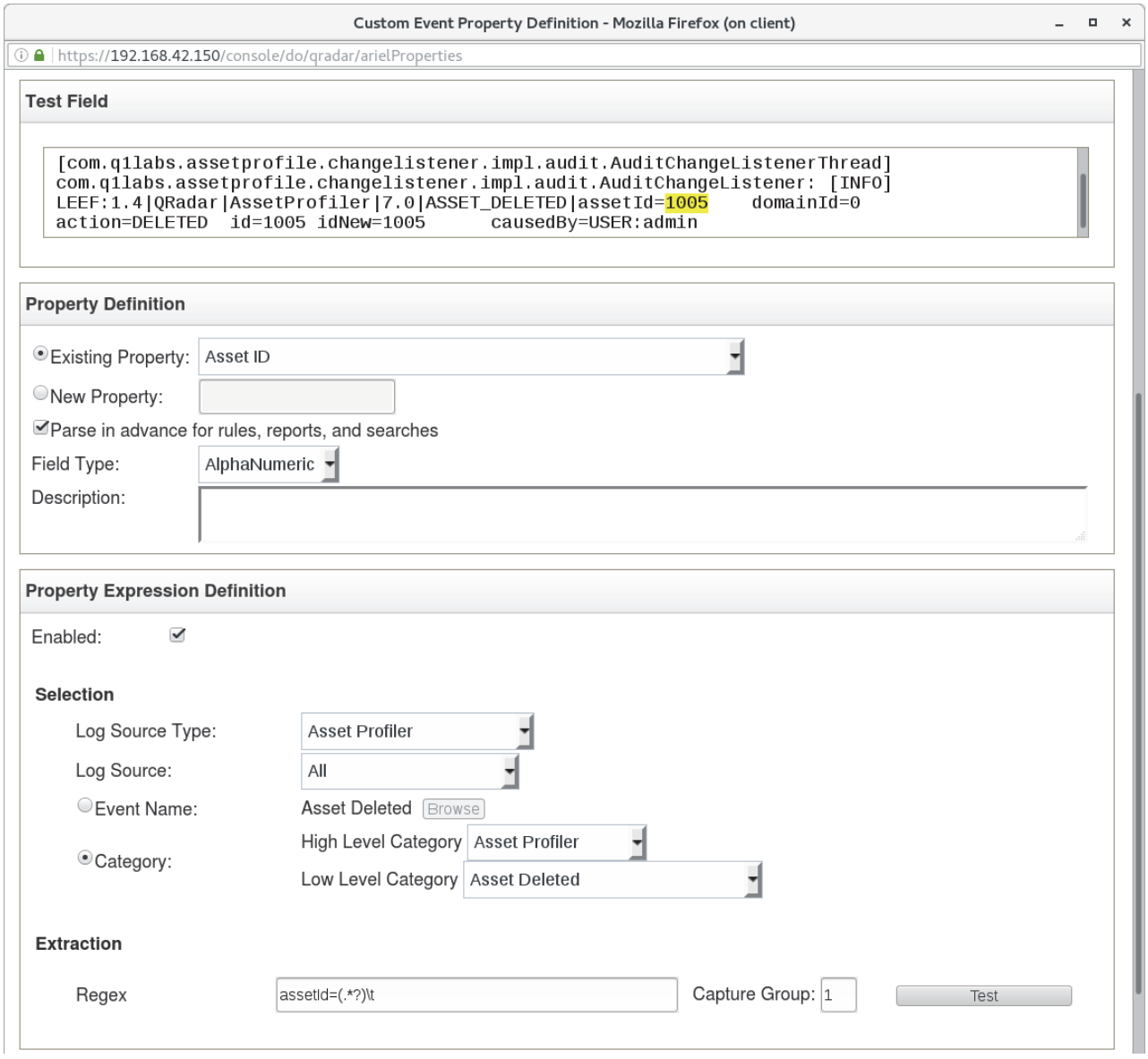
Task 2 Capturing Asset ID from Address Deleted events

To capture the asset ID from **Asset Deleted** events in a custom event property, perform the following steps:

1. Still on the **Log Activity** tab with the filter on the high-level category Asset Profiler, double-click an **Asset Deleted** event to navigate to its details.
2. To open the Custom Event Property Definition window, click **Extract Property** in the toolbar.
3. In the Custom Event Property Definition window, scroll down to the Property Definition section and perform the following steps:
   a. Select **Existing Property**.
   b. For Existing Property, select **Asset ID**.
   c. Select **Parse in advance for rules, reports, and searches**.

4. Scroll down to the Property Expression Definition section and perform the following steps:
   a. Select **Category**.
   b. For **RegEx**, enter the following regular expression:

      ```
      assetId=(.*?)\t
      ```



5. Click **Save**.

   The Custom Event Property Definition window closes.

   The **Log Activity** tab still displays the details of the **Asset Deleted** event. Do not navigate away.

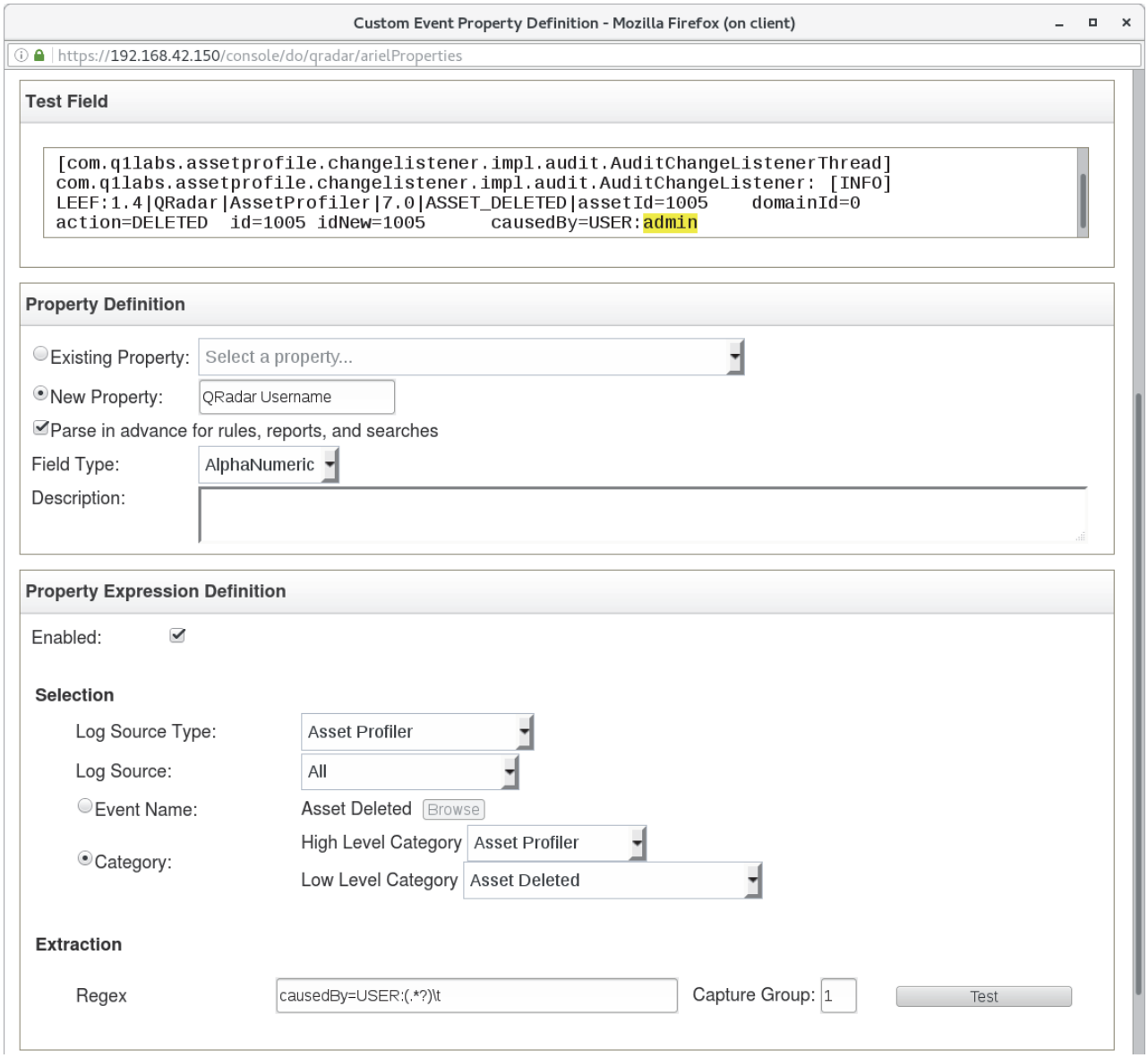
Task 3 Capturing QRadar Username from Address Deleted events

To capture the user name of the QRadar user who deletes an asset profile from each **Asset Deleted** event, perform the following steps to create a custom event property:

1. To open the Custom Event Property Definition window, click **Extract Property** in the toolbar.
2. In the Custom Event Property Definition window, scroll down to the Property Definition section and perform the following steps:
   a. Select **New Property**.
   b. For **New Property**, enter the following name:
      `QRadar Username`
   c. Select **Parse in advance for rules, reports, and searches**.

3. Scroll down to the Property Expression Definition section and perform the following steps:
   a. Select **Category**.
   b. For **RegEx**, enter the following regular expression:

      `causedBy=USER:(.*?)\t`



4. Click **Save**.

   The Custom Event Property Definition window closes.

Exercise 3 Creating a first solution using two building blocks and one custom rule

You need to detect when a QRadar user deletes an asset profile shortly after it has been created with an IP address. Your test needs to look for an Asset Deleted event that occurs shortly after an IP Address Created event does with the same asset ID. To test for such a sequence of events, QRadar provides function tests. These function tests take custom rules or building blocks as parameters.

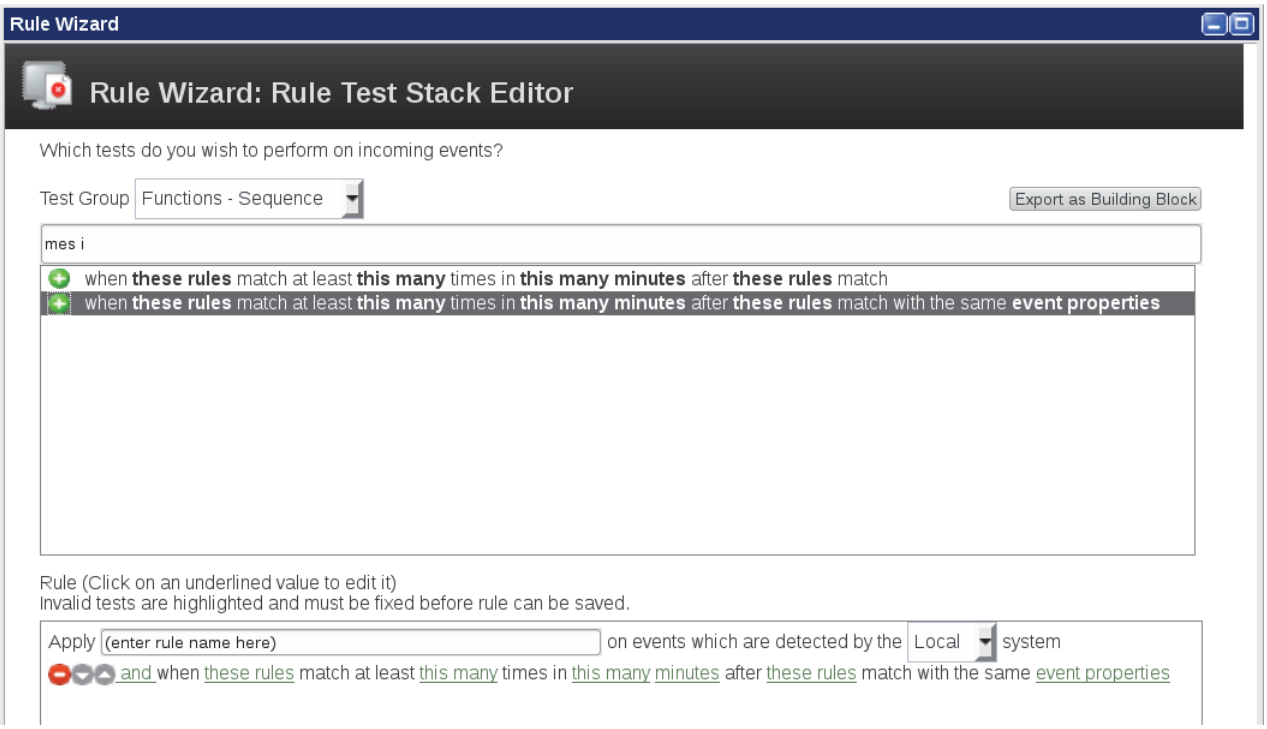
Task 1 Exploring and choosing sequence function test

To choose a sequence function test, perform the following steps:

1. Navigate to the **Offenses** tab.
2. Click **Rules** in the left pane.
3. From the **Actions** drop-down list, select **New Event Rule**.
   The Rule Wizard opens.
4. If the Rule Wizard starts with its welcome page, read the introductory text and select **Skip this page when running this rules wizard**. To navigate to the Rule Test Stack Editor, click **Next** twice.
5. For **Test Group**, select **Functions - Sequence**.
6. You need the Custom Rules Engine (CRE) to create an offense if an Asset Deleted event occurs a certain time after an IP Address Created event occurs with the same asset ID. To choose a sequence function test for this purpose, browse the sequence function tests listed.

Hint: To locate the required sequence function test, enter the following text in the **Type to Filter** field:

```
mes i
```



Notice the **these rules** placeholders. This sequence function test expects custom rules or building blocks as parameters. Therefore, you need to create building blocks before you can create the custom rule that creates the intended offense.

Task 2 Creating a building block to tag Asset Deleted events

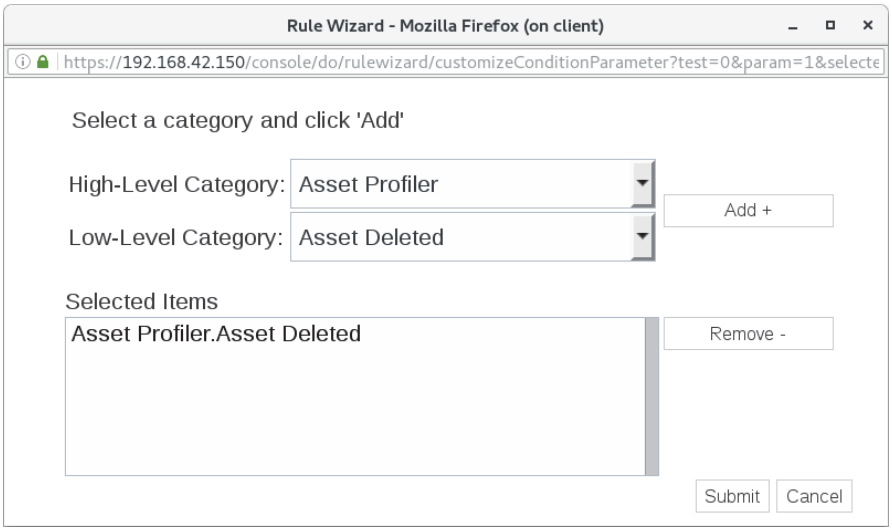
To create a building block to test for the **Asset Deleted** event category, perform the following steps:

1. Do not close the Rule Wizard. Use the opened Rule Wizard to create the required building blocks. If you added the sequence function test in the previous step, click the red **minus (-)** icon next to the sequence function test to remove it.
2. For **Test Group**, select **Event Property Tests**.
3. To locate the required event property test, enter in the **Type to Filter** field the following text:

   `categ`
4. Click the green **plus (+)** icon next to the following test:

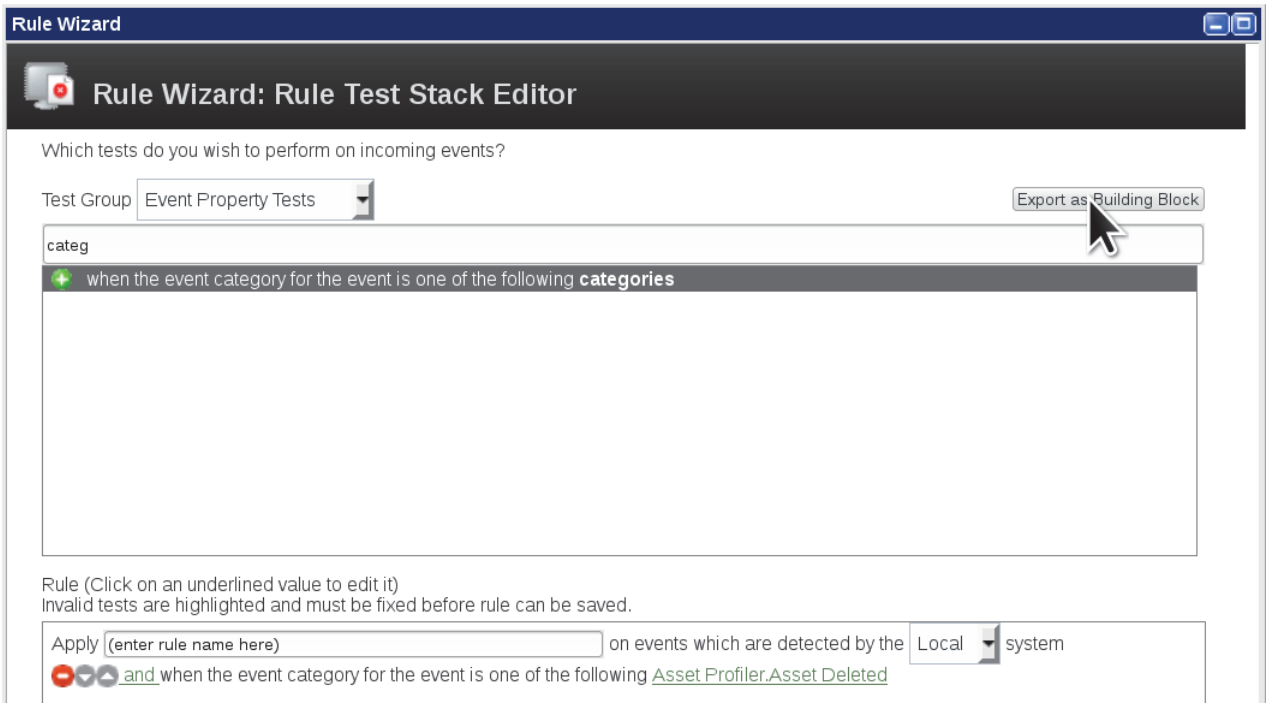
   when the event category for the event is one of the following categories
5. The underlined green term categories is a parameter. To open a window to select the categories that you want to test for, click categories.
6. For **High-Level Category**, select **Asset Profiler**.
7. For **Low-Level Category**, select **Asset Deleted**.

8. Click **Add**.



9. To add the category to the test, click **Submit**.
   The window closes.

10. Verify that your Rule Test Stack Editor looks like the following screen capture.



11. To open a window to create a building block with the event category test, click **Export as Building Block**.

Note: To easily distinguish predefined rules and building blocks from your own development, it is a best practice to establish a naming convention. Many users choose to use the name of their organization or department as a prefix connected with a dash (-). This exercise uses the prefix `Exercise-`.

12. For **Building Block Name**, enter the following name:

    `Exercise-BB:CategoryDefinition: Asset Deleted`

13. To create the building block, click **Save**.

    The window closes.

    Do not close the Rule Wizard.

Task 3 Creating a building block to tag IP Address Created events

To create the second building block to test for the **Asset IP Address Created** event category, perform the following steps in the still-open Rule Wizard:

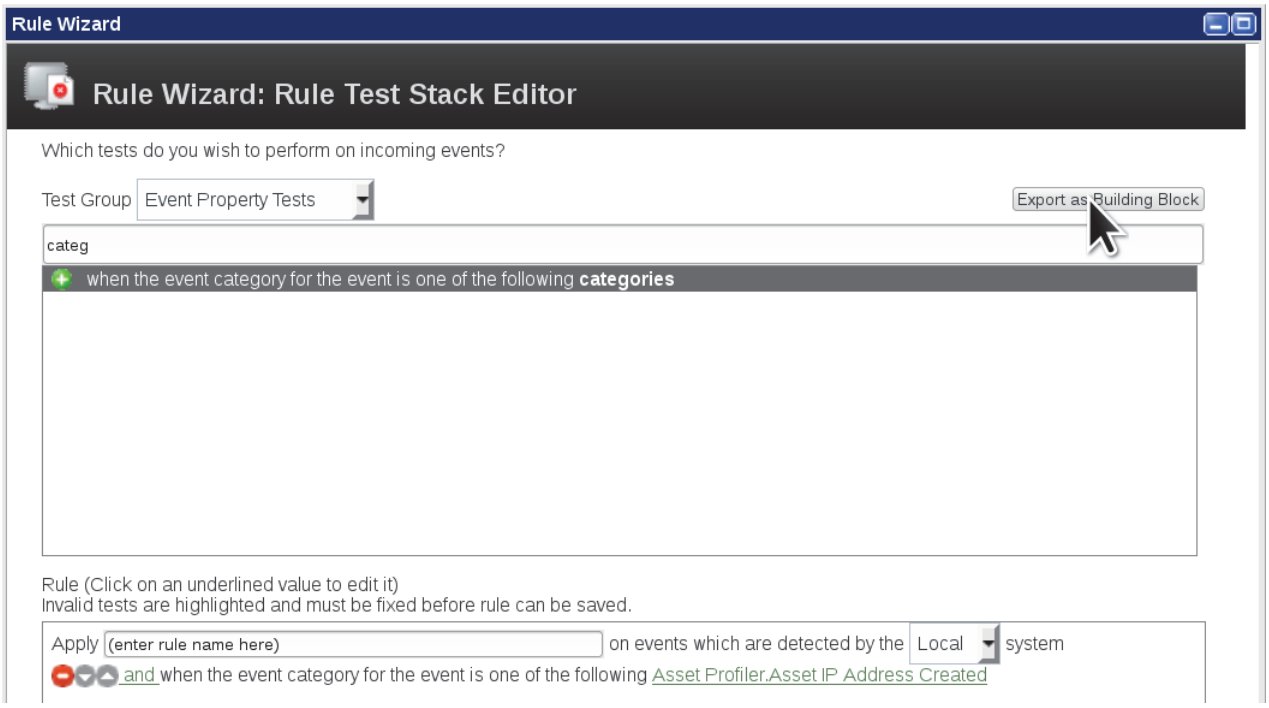
1. If not still selected, for **Test Group**, select **Event Property Tests**.
2. Click the green **plus (+)** icon next to the following test:

   when the event category for the event is one of the following categories
3. To open a window to select the categories that you want to test for, click categories.
4. For **High-Level Category**, select **Asset Profiler**.
5. For **Low-Level Category**, select **Asset IP Address Created**.

6. Click **Add**.

7. To add the category to the test, click **Submit**.
   The window closes.

8. Verify that your Rule Test Stack Editor looks like the following screen capture.



9. To open a window to create a building block with the event category test, click **Export as Building Block**.

10. For **Building Block Name**, enter the following name:

    `Exercise-BB:CategoryDefinition: Asset IP Address Created`

11. To create the building block, click **Save**.

    The window closes.

12. To close the Rule Wizard, click **Cancel**.

13. To close the confirmation pop-up window, click **OK**.

Task 4 Creating a group for your custom rules and building blocks

To more easily locate the custom rules and building blocks that you create for your organization, pool them in a group. Unless the **Exercise** group already exists, perform the following steps to create it:

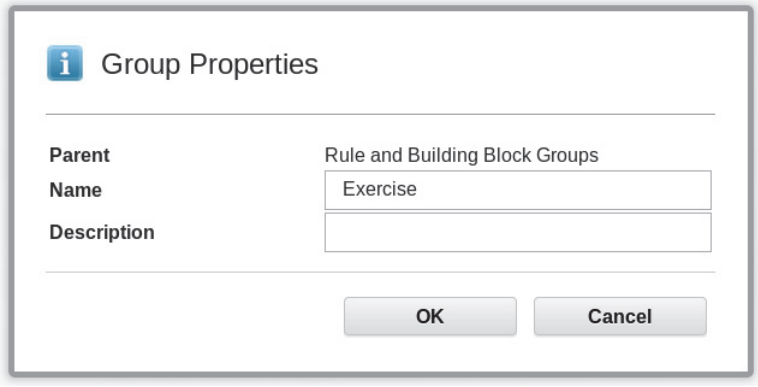
1. Still in Rules on the **Offenses** tab, click **Groups** in the toolbar to open the Rule and Building Block Groups window.

2. If you find a group with the name **Exercise**, close the Rule and Building Block Groups window and continue with Task 5, “Adding building blocks to your group,” on page 3-78.

3. To create a group, click **New Group**.

   The Group Properties window opens.

4. In the Group Properties window, enter `Exercise` for **Name**.



5. To create the group, click **OK**.

   The Group Properties window closes.

6. Close the Rule and Building Block Groups window.

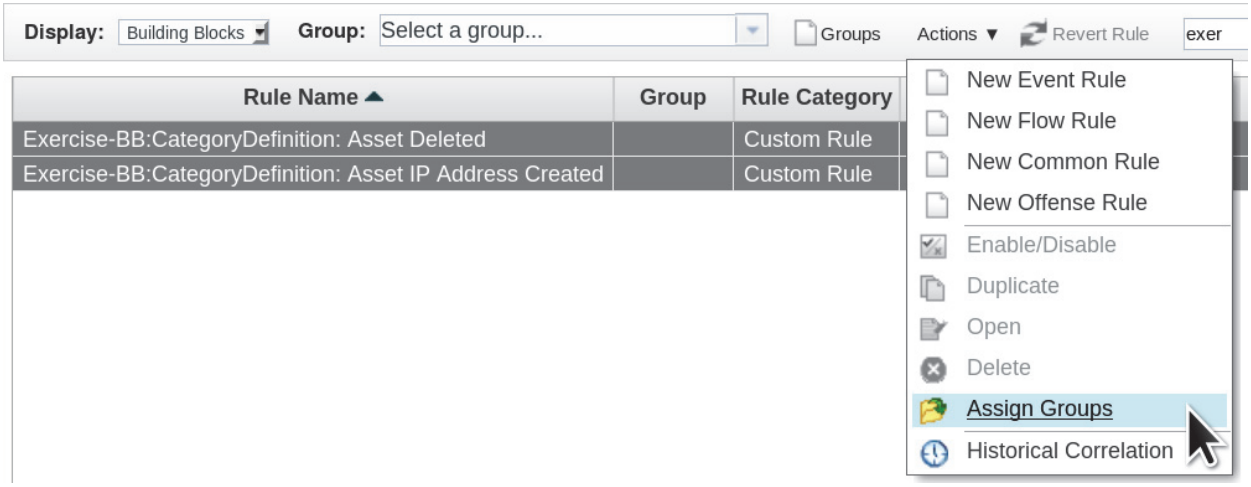
Task 5 Adding building blocks to your group

You can add new custom rules to a group while you create them in the Rule Wizard. Unlike custom rules, you can add building blocks to a group only after you have created them and finished the Rule Wizard. To add your two new building blocks to the **Exercise** group, perform the following steps:

1. Still in Rules on the **Offenses** tab, in the **Display** drop-down list in the toolbar, select **Building Blocks** to list all building blocks.

2. To locate the building blocks that you created, in the **Search Rules** field, enter `exer` and press **Enter**.

3. To open the Choose Group window, select both of your building blocks and, from the **Actions** drop-down list, select **Assign Groups**.



4. To assign groups in the Choose Group window, select the **Category Definitions** and **Exercise** groups. Click **Assign Groups**.

   The Choose Group window closes.

Note: When you need to locate all custom rules and building blocks that you have developed, first in the **Display** drop-down list, select **Rules** or **Building Blocks**, and then select **Exercise** in the **Group** drop-down list.

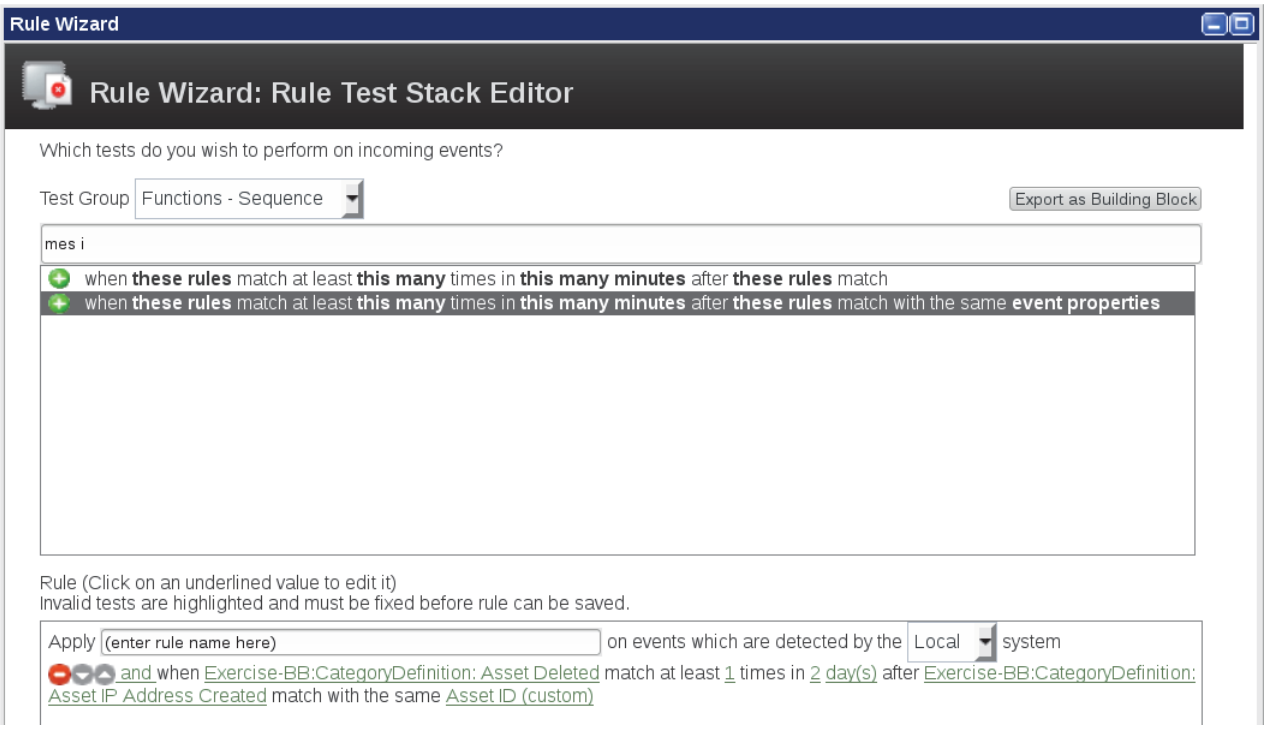
Task 6 Creating a custom rule to detect a possible policy violation

To create the custom rule with the sequence function test that you located in the beginning of this exercise, perform the following steps:

1. Still in Rules on the **Offenses** tab, from the **Actions** drop-down list, select **New Event Rule**.
   The Rule Wizard opens.
2. For **Test Group**, select **Functions - Sequence**.
3. To locate the required sequence function test, enter in the **Type to Filter** field the following text:
   `mes i`
4. Click the green **plus (+)** icon next to the following test:
   when these rules match at least this many times in this this many minutes after these rules match with the same event properties
5. To configure the test, click the green underlined parameters and provide the values from the following table.

Parameter	Setting
these rules	Exercise-BB:CategoryDefinition: Asset Deleted
this many	1
this many	2
minutes	day(s)
these rules	Exercise-BB:CategoryDefinition: Asset IP Address Created
event properties	Asset ID (custom)

6. Verify that your Rule Test Stack Editor looks like the following screen capture.



Task 7 Testing for two events with the same QRadar Username

To fire the custom rule only if the same QRadar user deletes two profiles, add to the custom rule a counter function test. Perform the following steps:

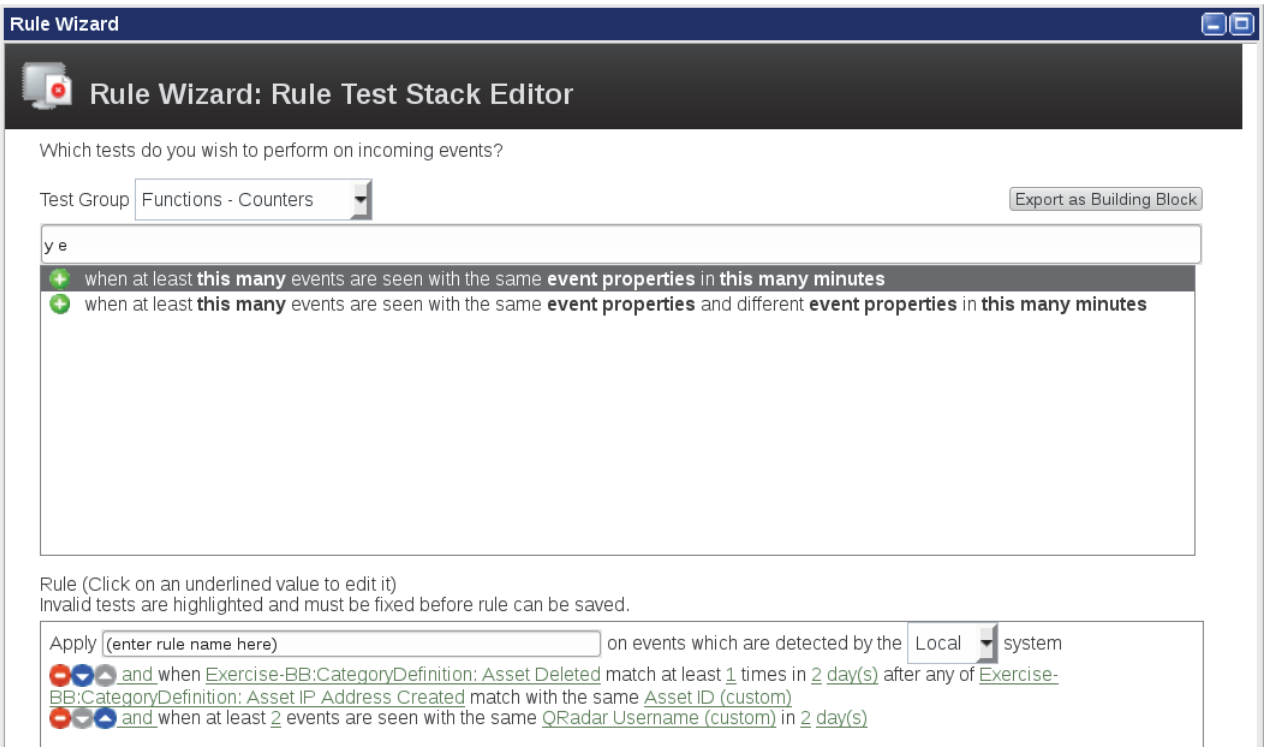
1. Still in the Rule Test Stack Editor, for **Test Group**, select **Functions - Counters**.
2. To locate the required counter function test, enter in the **Type to Filter** field the following text:

   `y e`
3. Click the green **plus (+)** icon next to the following test:

   when at least this many events are seen with the same event properties in this many minutes
4. To configure the test, click the green underlined parameters and provide the values from the following table.

Parameter	Setting
this many	2
event properties	QRadar Username (custom)
this many	2
minutes	day(s)

5. Verify that your Rule Test Stack Editor looks like the following screen capture.



6. For the custom rule name in the **Apply** field, enter the following name:

   `Exercise-Policy: Temporary Asset Profiles`

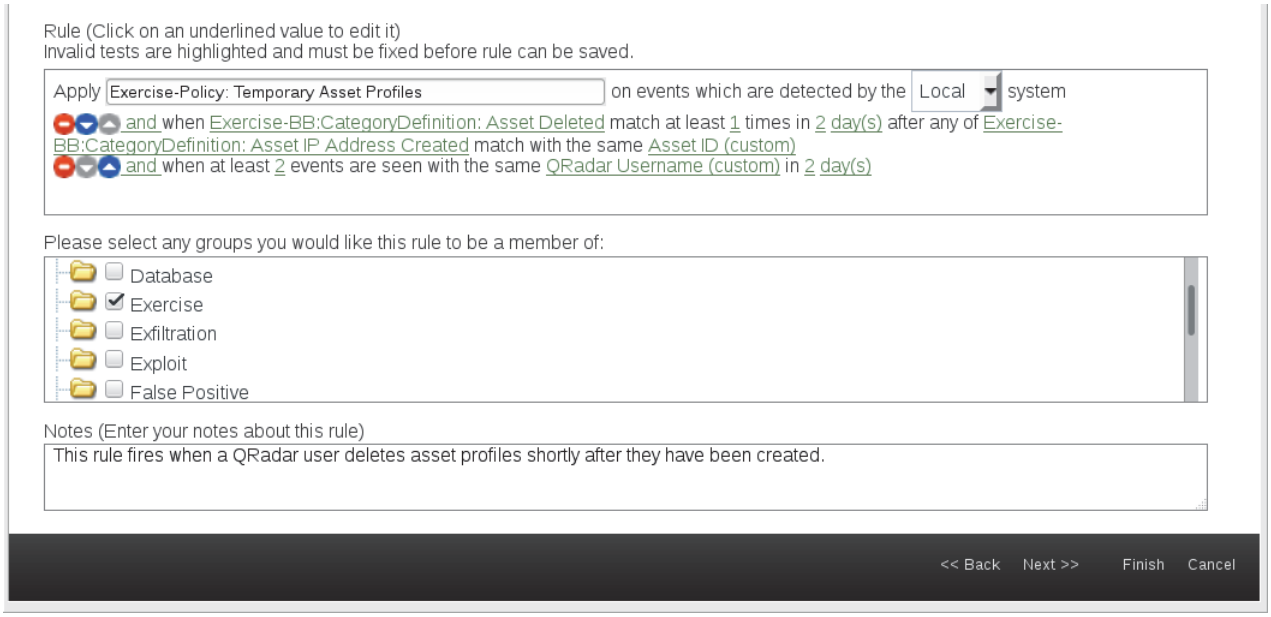
Note: This exercise uses the prefix `Exercise-` to distinguish the predefined custom rules from your own development to detect policy violations.

7. To assign the custom rule to the **Exercise** group, scroll down in the list of groups and select **Exercise**.

8. To document the custom rule in the **Notes** field, enter the following text:

   `This rule fires when a QRadar user deletes asset profiles shortly after they have been created.`

9. Verify that your Rule Wizard looks like the following screen capture.



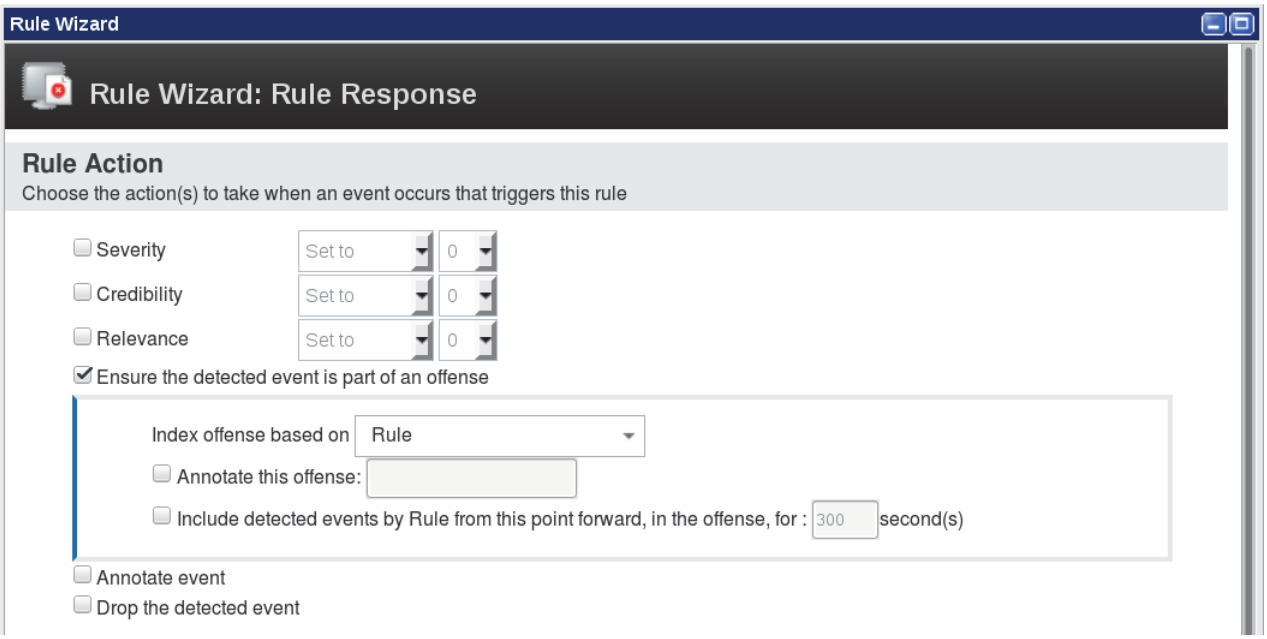
Important: The QRadar Username custom event property is limited to Asset Deleted events. Therefore, the second test only evaluates to true when the same QRadar user deletes two asset profiles.
However, regardless of the order, the CRE performs both tests because both are stateful. Therefore, the counters of the tests can reach their trigger values for unrelated asset profile creations and deletions. For example, the first test reaches its trigger value already when user A deletes one asset profile that is younger than two days. When user B deletes two older asset profiles, the custom rule fires although there is no indication that user B tries to hide an unauthorized service.

Task 8 Configuring rule responses

To have an offense created for the possible policy violation that the custom rule tests for, perform the following steps:

1. To navigate to the Rule Response, click **Next**.
2. Under Rule Action, select **Ensure the detected event is part of an offense**.
3. For **Index offense based on**, select **Rule**.

4. Verify that your Rule Wizard looks like the following screen capture.

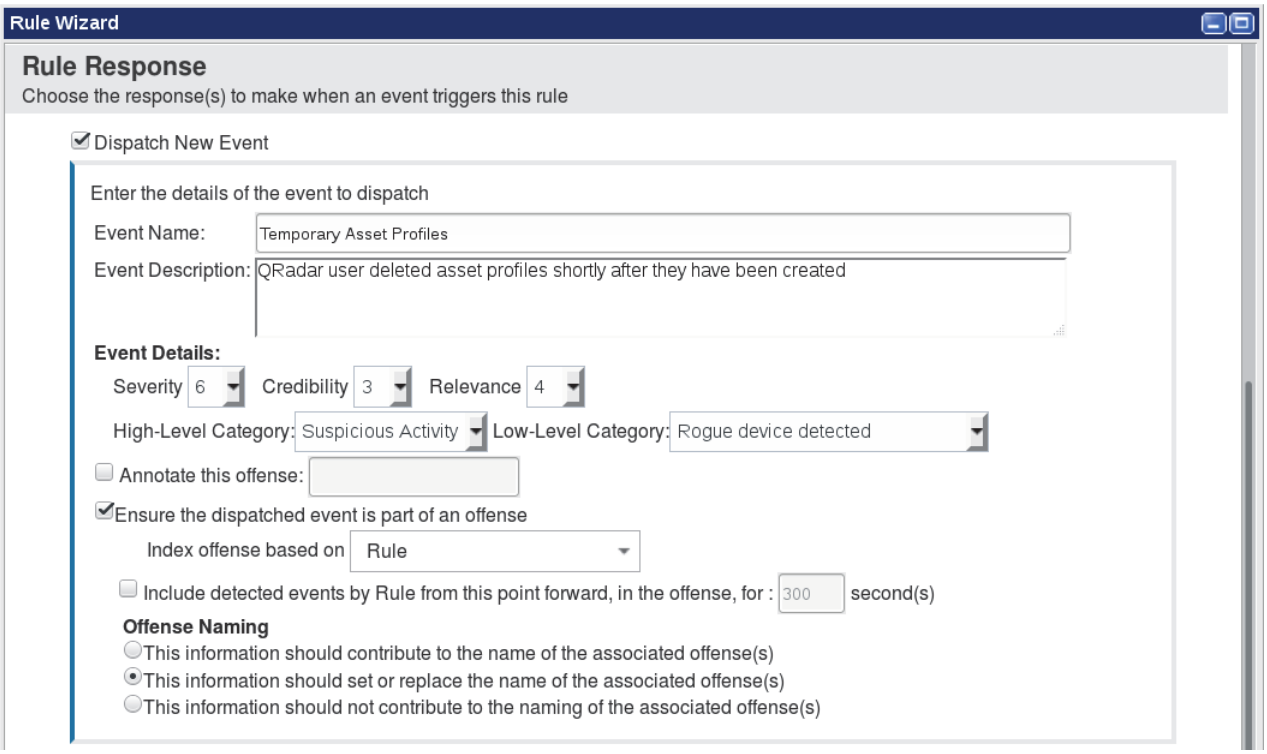


5. Still on the Rule Response page of the Rule Wizard, under Rule Response, select **Dispatch New Event**. Subsequently, the rule responses expand to many options under Dispatch New Event.

6. To configure the rule response under Dispatch New Event, provide the settings from the following table.

Option	Setting
Event Name	`Temporary Asset Profiles`
Event Description	`QRadar user deleted asset profiles shortly after they have been created`
Severity	6
Credibility	3
Relevance	4
High-Level Category	Suspicious Activity
Low-Level Category	Rogue device detected
Ensure the dispatched event is part of an offense	Select
Index offense based on	Rule
Offense Naming	This information should set or replace the name of the associated offense(s)

7. Verify that your Rule Wizard looks like the following screen capture.



8. To navigate to the Rule Summary, click **Next**.
9. To create the rule, click **Finish**.

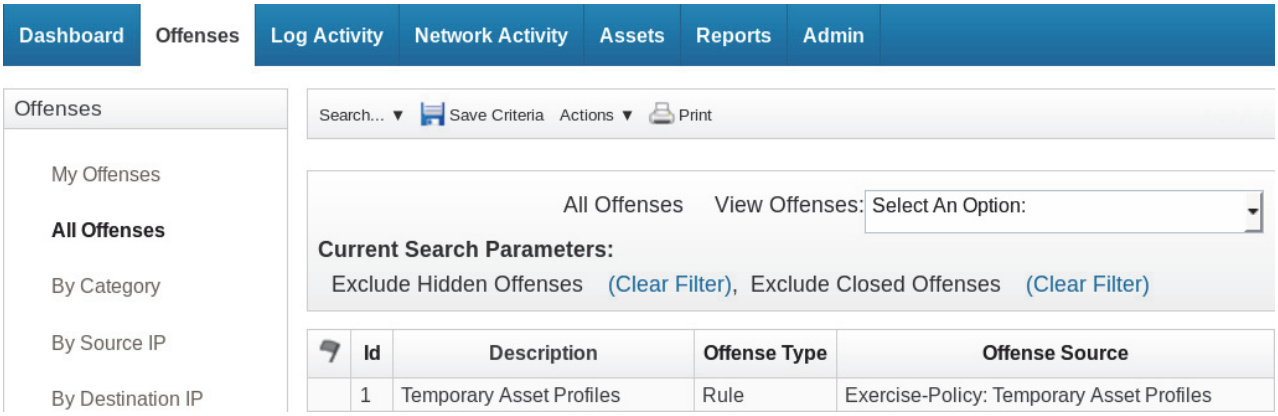
   The Rule Wizard closes.

Task 9 Verifying the solution

To verify whether your development creates an offense, create two asset profiles and delete them right away.

1. Repeat Step 2 on page 61 through Step 10 on page 62 two times.
2. To locate the new offense, navigate to the **Offenses** tab.
3. It might take up to two minutes until QRadar SIEM displays the new offense. To refresh the listed offenses, click the **double arrow** icon in the upper-right corner of the QRadar SIEM user

interface, or double-click the **Offenses** tab. The double-click refreshes and resets the tab to its default settings.



Exercise 4 Creating a second solution using one reference set and two custom rules

In this exercise, you follow an alternative approach to detect short-lived asset profiles. Instead of the sequence function test, you use a reference set.

Task 1 Creating a custom rule to add to reference set

To create a custom rule that fires when an asset profile receives a new asset IP address, perform the following steps:

1. Navigate to the **Offenses** tab.
2. Click **Rules** in the left pane.
3. From the **Actions** drop-down list, select **New Event Rule**.
   The Rule Wizard opens.
4. For **Test Group**, select **Event Property Tests**.
5. To locate the required event property test, enter in the **Type to Filter** field the following text:
   `categ`
6. Click the green **plus (+)** icon next to the following test:
   when the event category for the event is one of the following categories
7. To open a window to select the categories that you want to test for, click categories.
8. For **High-Level Category**, select **Asset Profiler**.

9. For **Low-Level Category**, select **Asset IP Address Created**.
10. Click **Add**.

11. To add the category to the test, click **Submit**.

    The window closes.

Note: In the previous exercise, you created a building block with the same test. You can test for a match of this building block instead of a match for the category. A test on the category consumes about the same amount of resources as a test on a building block. Therefore, reusing the building block is not a benefit in this case.

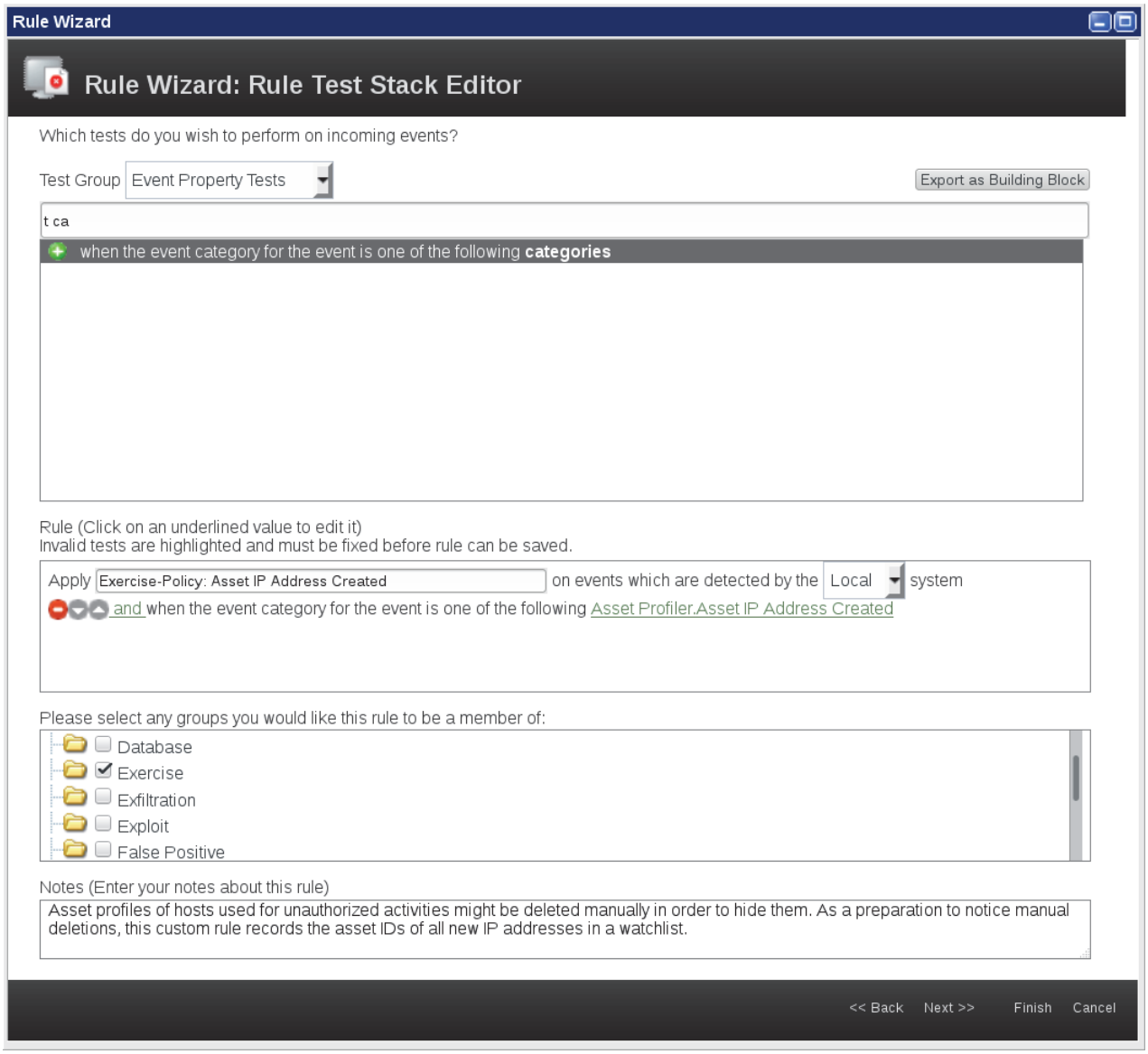
12. For the custom rule name in the **Apply** field, enter the following name:

    ```
    Exercise-Policy: Asset IP Address Created
    ```

13. To assign the custom rule to the **Exercise** group, scroll down in the list of groups and select **Exercise**.
14. To document the custom rule in the **Notes** field, enter the following text:

    ```
    Asset profiles of hosts used for unauthorized activities might be deleted
    manually in order to hide them. As a preparation to notice manual deletions,
    this custom rule records the asset IDs of all new IP addresses in a watchlist.
    ```

15. Verify that your Rule Test Stack Editor looks like the following screen capture.

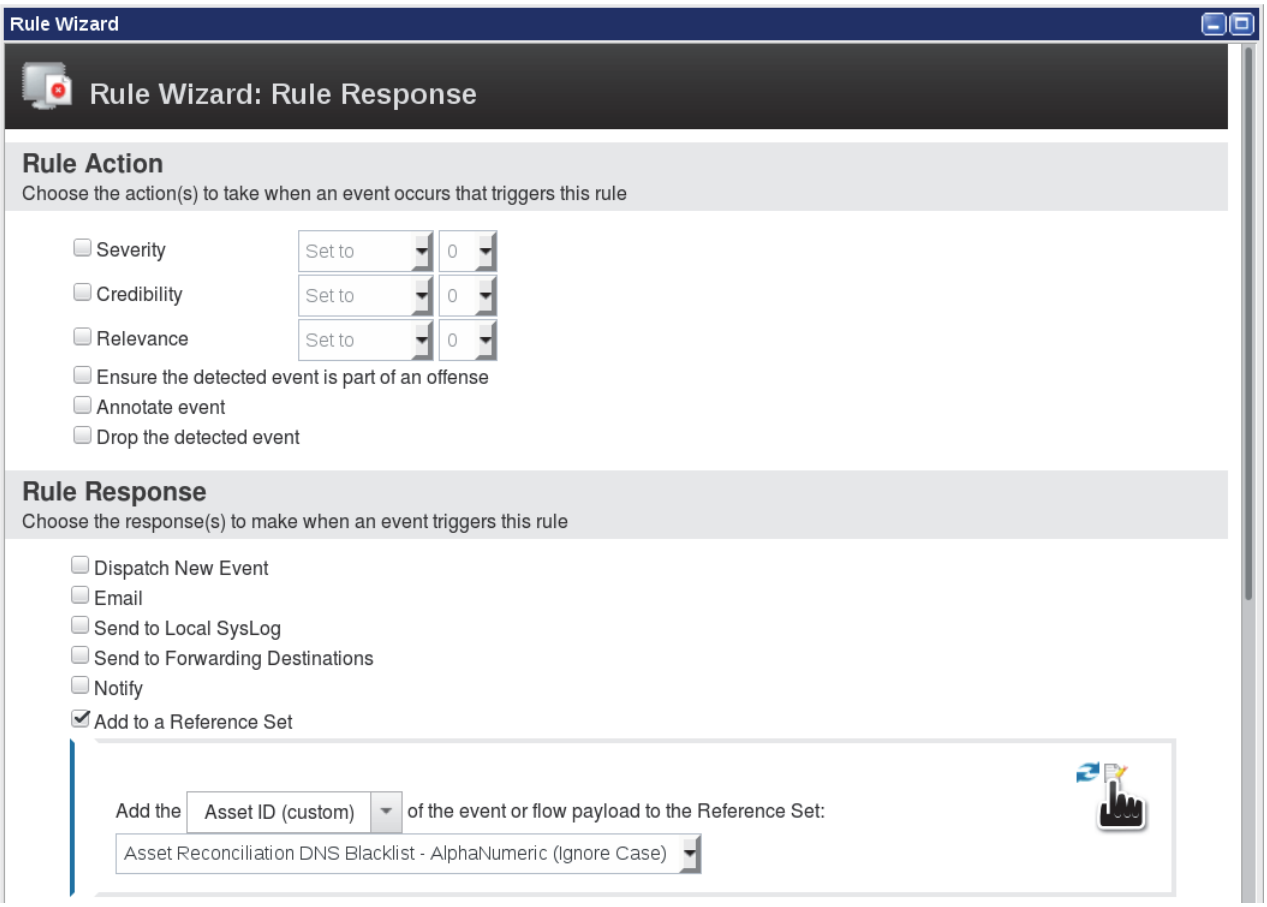


Task 2 Configuring rule responses

To create a new reference set and, if the custom rule fires, add the asset ID to it, perform the following steps:

1. To navigate to the Rule Response, click **Next**.
2. Select **Add to a Reference Set**.
3. For **Add the**, select **Asset ID (custom)**.

4. To create a reference set, click the **Configure Reference Sets** icon.



The Reference Set Management window opens, after you clicked the Configure Reference Sets icon.

5. Click **Add**.

   The New Reference Collection window opens.

6. In the New Reference Set window, follow these steps to create the reference set:
   a. For **Name**, enter the following name:

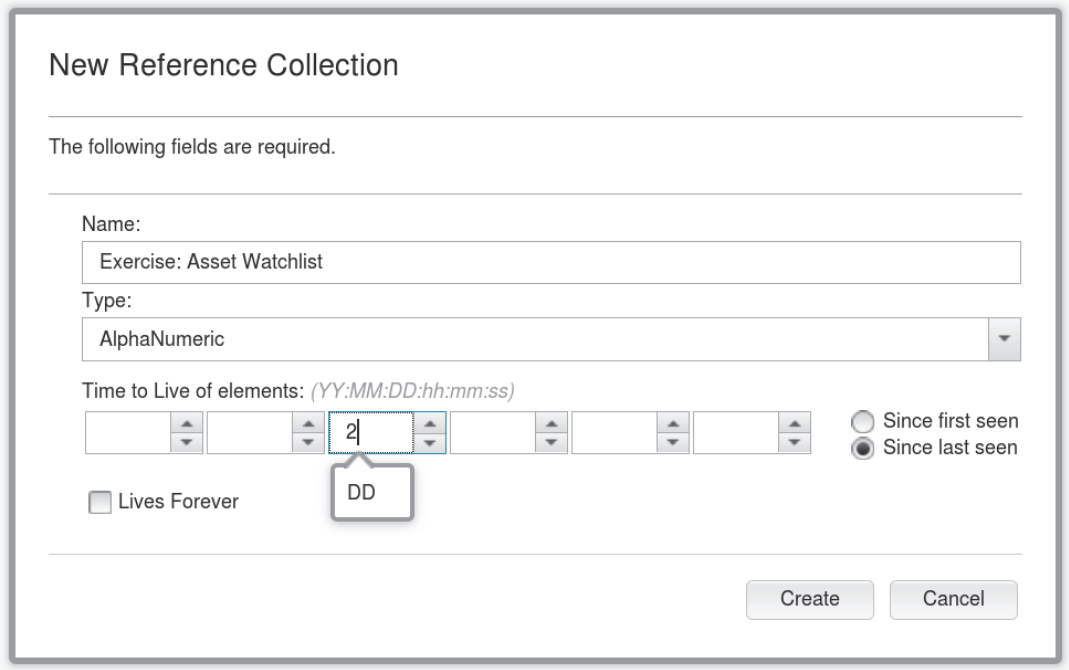
      `Exercise: Asset Watchlist`

   b. Clear the **Lives Forever** check box.

   c. For **Time to Live of elements**, enter `2` in the field for the number of days.

   d. Select **Since last seen**.

QRadar SIEM can detect an additional IP address for an asset profile whose asset ID is already stored in the reference set. In this case, the time to live for this asset ID needs to start from zero again. Therefore, choose **Since last seen**.

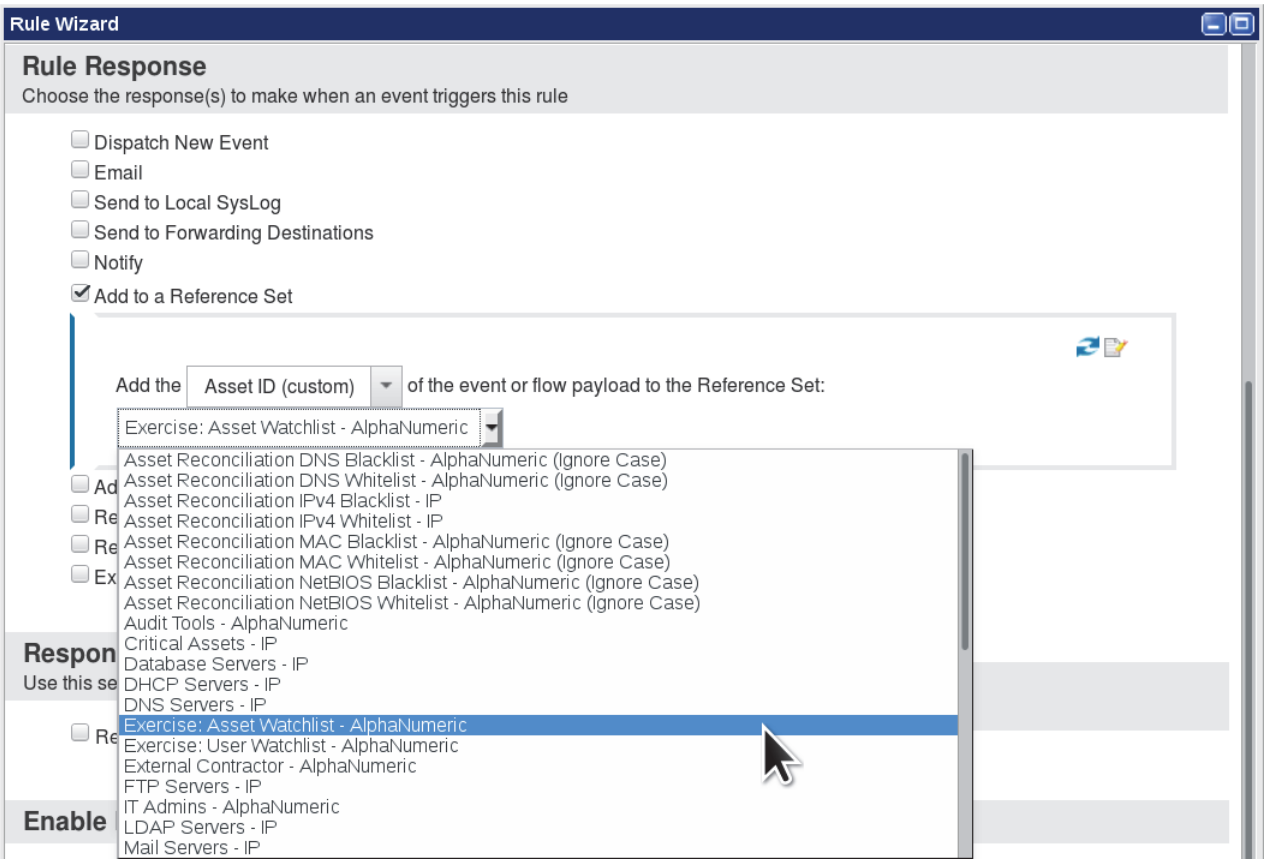


e. To create the reference set, click **Create**.

   The New Reference Collection window closes.

7. Close the Reference Set Management window.

8. Verify, that QRadar SIEM has automatically selected the **Exercise: Asset Watchlist - AlphaNumeric** for **of the event of flow payload to the Reference Set** new reference set.



9. To navigate to the Rule Summary, click **Next**.

10. To create the custom rule, click **Finish**.

    The Rule Wizard closes.

Task 3 Creating a custom rule to detect a possible policy violation

To create the custom rule that uses a reference set to detect when the same QRadar user deletes recently created asset profiles more than once, perform the following steps:

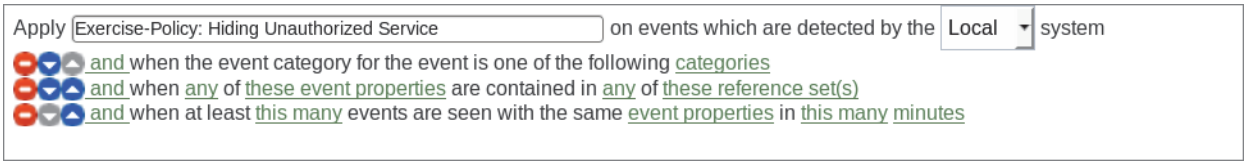
1. Still in Rules on the **Offenses** tab, from the **Actions** drop-down list, select **New Event Rule**.

   The Rule Wizard opens.

2. For the custom rule name in the **Apply** field, enter the following name:

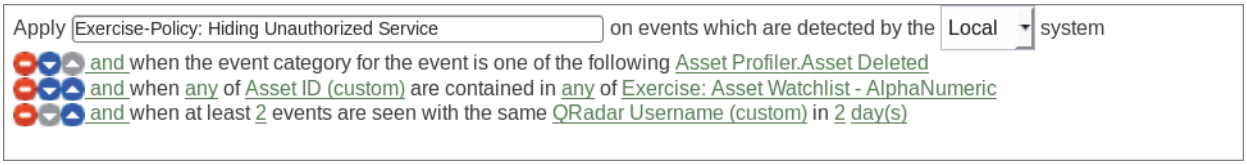
   `Exercise-Policy: Hiding Unauthorized Service`

3. Add three tests so that the Rule Test Stack Editor looks like the following screen capture. The following table helps to find the three tests.



Test Group	Type to Filter	Test
Event Property Tests	`categ`	when the event category for the event is one of the following categories
Event Property Tests	`ned`	when any of these event properties are contained in any of these reference set(s)
Functions - Counters	`n with the same event properties i`	when at least this many events are seen with the same event properties in this many minutes

4. Configure the three tests so that the Rule Test Stack Editor looks like the following screen capture. To configure the test, click the green underlined parameters and provide the values from the following table.



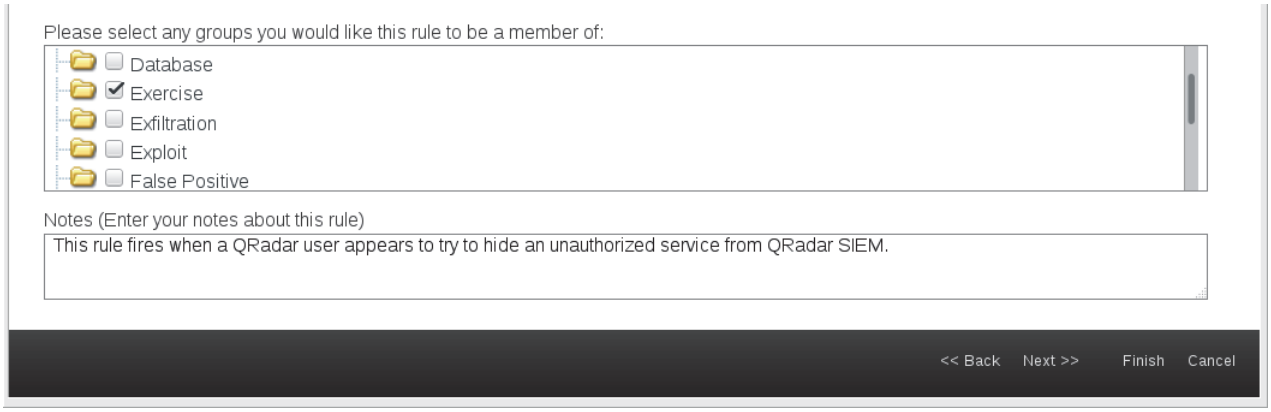
Parameter	Setting
categories	Asset Profiler.Asset Deleted
these event properties	Asset ID (custom)
reference set(s)	Exercise: Asset Watchlist - AlphaNumeric
this many	2
event properties	QRadar Username (custom)
this many	2
minutes	day(s)

5. Still in the Rule Test Stack Editor, to assign the custom rule to the group Exercise, scroll down in the list of groups and select **Exercise**.

6. To document the custom rule in the **Notes** field, enter the following text:

   `This rule fires when a QRadar user appears to try to hide an unauthorized service from QRadar SIEM.`

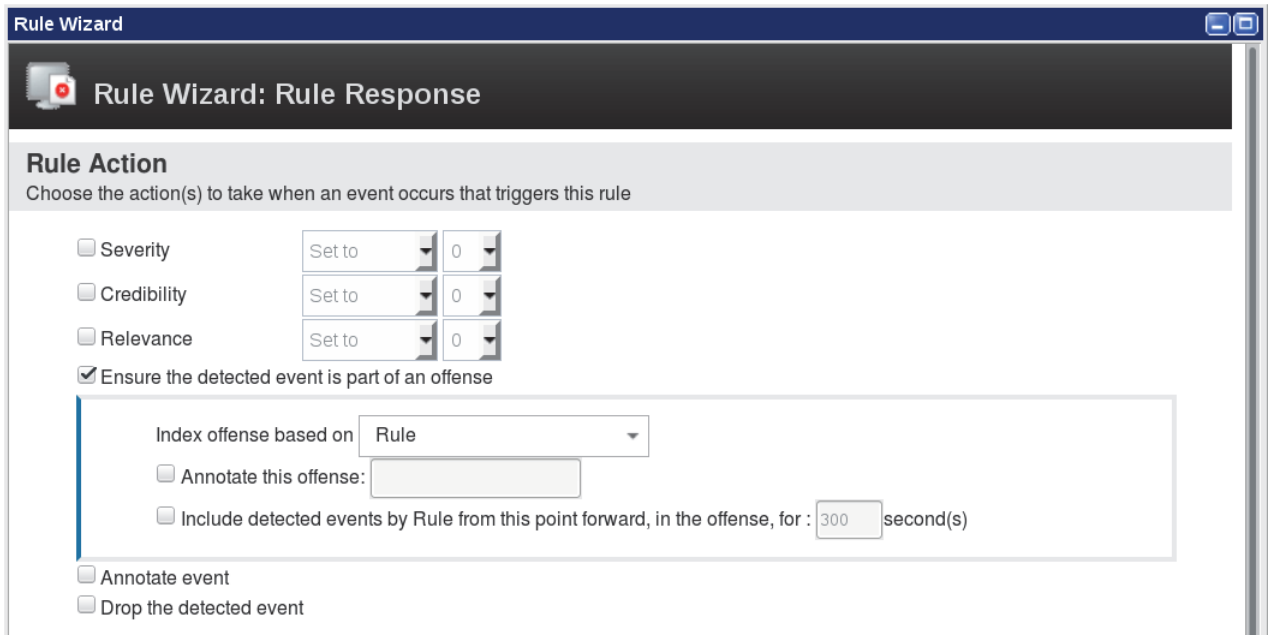
7. Verify that your Rule Test Stack Editor looks like the following screen capture.



Task 4 Configuring rule responses

To have an offense created for the possible policy violation that the custom rule tests for, perform the following steps:

1. To navigate to the Rule Response, click **Next**.
2. Complete the Rule Response page so that it looks like the following two screen captures. The response of this custom rule is very similar to the response of the last custom rule in the previous exercise. If necessary, revisit Step 2 on page 82 through Step 6 on page 83.

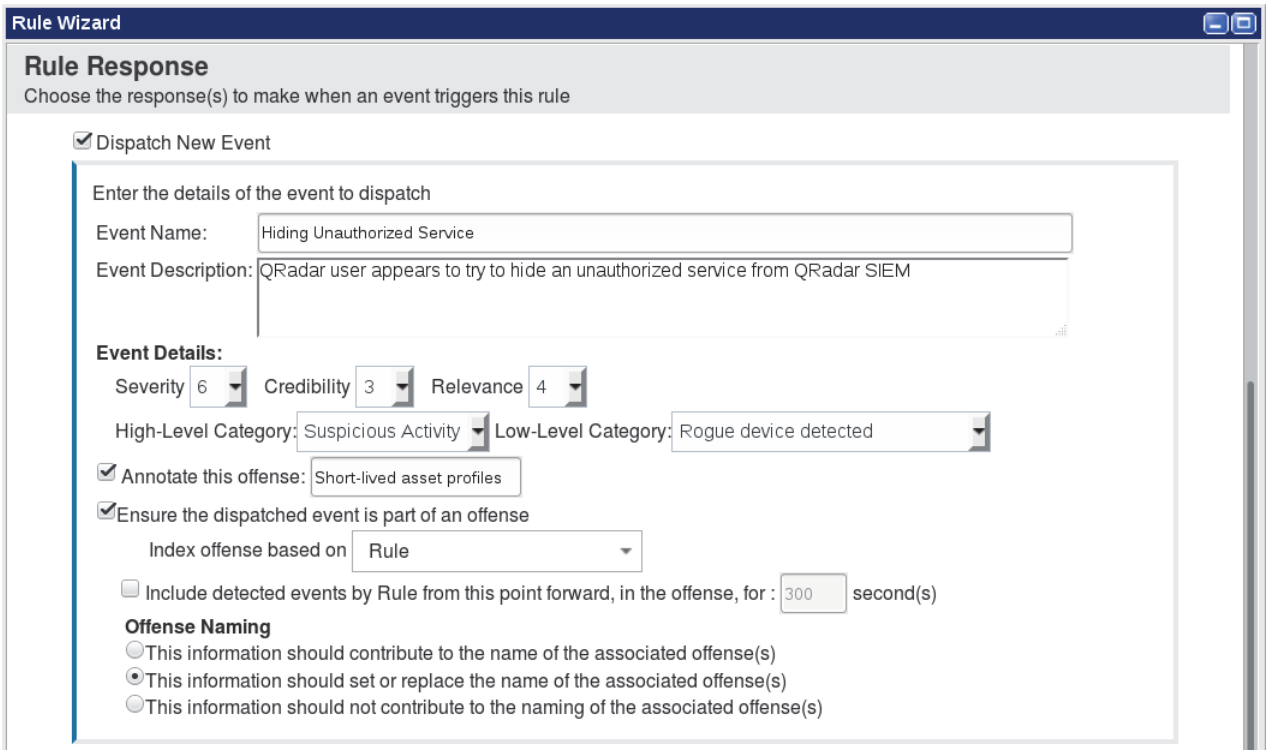


3. If you would enter the same values for both rules, you could not easily distinguish which rule created the events and offenses. Therefore, enter the following values in order to make events and offenses from the two rules distinguishable:
   - For **Event Name**, enter the following name:

     `Hiding Unauthorized Service`
   - For **Event Description**, enter the following description:

     `QRadar user appears to try to hide an unauthorized service from QRadar SIEM`
   - Optionally select **Annotate this offense** and enter the following text:

     `Short-lived asset profiles`



4. To navigate to the Rule Summary, click **Next**.
5. To create the custom rule, click **Finish**.

   The Rule Wizard closes.

Task 5 Disabling the custom rule from the previous solution

Optionally, before you verify whether your development creates an offense, disable the custom rule that you created in the previous exercise. Building blocks cannot be disabled, and anyway do not affect your verification because they do not create offenses.

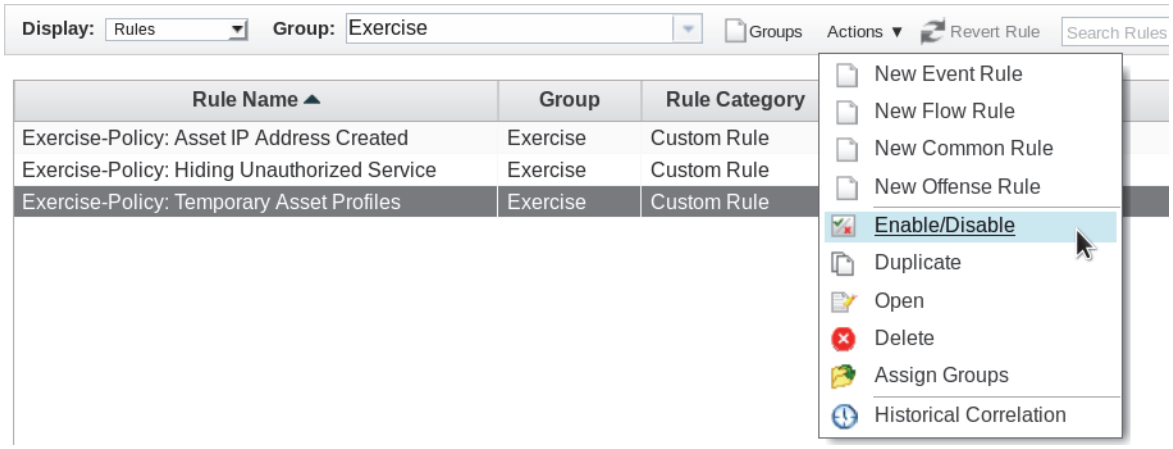
Note: As a best practice, always have only one custom rule create an offense for the indicator that you need to monitor.

To disable the custom rule from the previous exercise, perform the following steps:

1. Still in Rules on the **Offenses** tab, in the **Group** drop-down list in the toolbar, select **Exercise**.
   The table displays the custom rules in the group.

Note: The table displays the custom rules in the group, but not the building blocks. If you need to display the group's building blocks but not the custom rules, in the **Display** drop-down list, select **Building Blocks**.

2. Select the **Exercise-Policy: Temporary Asset Profiles** custom rule.
3. From the **Actions** drop-down list, select **Enable/Disable**.



4. To close the confirmation pop-up window, click **OK**.

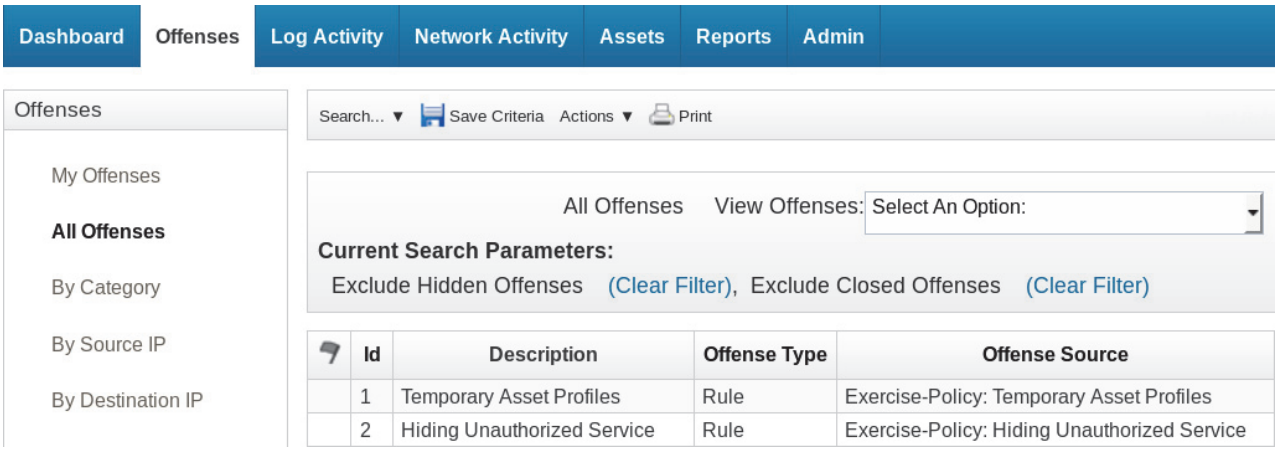
Task 6 Verifying the solution

Verify that your development creates an offense. Create two asset profiles and delete them.

1. Repeat Step 2 on page 61 through Step 10 on page 62 two times.

Attention: After creating the first asset profile, wait at least one minute before deleting it. In the meantime, you can create the second asset profile. Delete it after at least one minute, too. Otherwise the custom rule might not fire because it can take up to one minute until an added element appears in a reference set.

2. To locate the new offense, navigate to the **Offenses** tab.
3. It might take up to two minutes until QRadar SIEM displays the new offense. To refresh the listed offenses, click the **double arrow** icon in the upper-right corner of the QRadar SIEM user interface, or double-click the **Offenses** tab.



Exercise 5 Considering which solution to choose

The two solutions are more similar than they appear at first glance, because for the sequence test of the first solution, the CRE maintains an equivalent of the reference set that the second solution uses. Therefore, the key mechanism is the same for both solutions, just hidden under the hood for the first solution.

Both solutions create an offense to alert you when a QRadar user deletes two asset profiles shortly after they have been created. Unlike the second solution, the first solution can create false positive offenses as explained in Step 9 on page 82. Therefore, choose the second solution.

This concludes the exercises.

Unit 4 Custom action script exercises

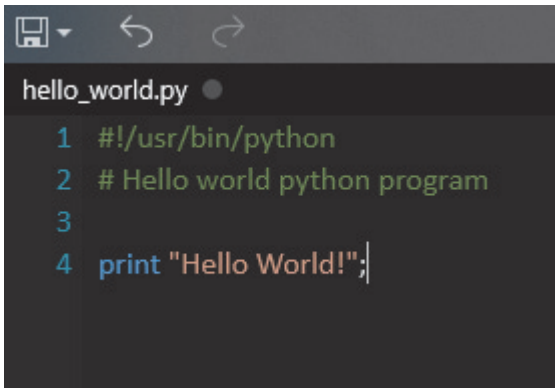
In the subsequent exercises, you are introduced to QRadar custom action scripts (CAS). Your hands-on experience with using the CAS functionality includes:

- Creating a test Hello World python script
- Defining the CAS during script upload
- Testing the CAS via Test Execution within the QRadar SIEM console
- Creating fixed and network event properties to test CAS parameters

Exercise 1 Create Hello World

In the following Hello World exercise, you create a python script that is executed as a custom action script in QRadar.

1. Open a text editor.
2. Type the following lines into the document:

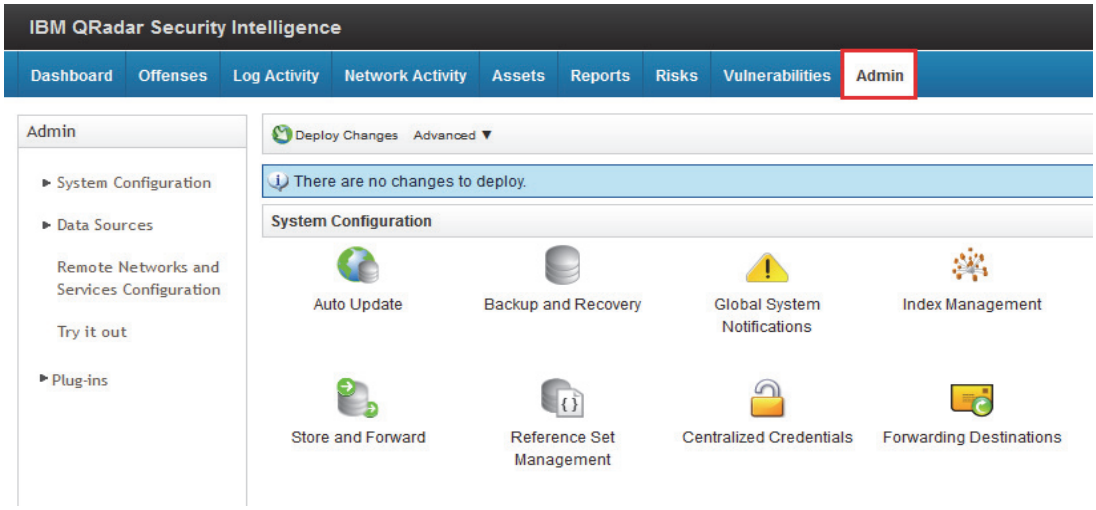


3. Save the file as `hello_world.py`

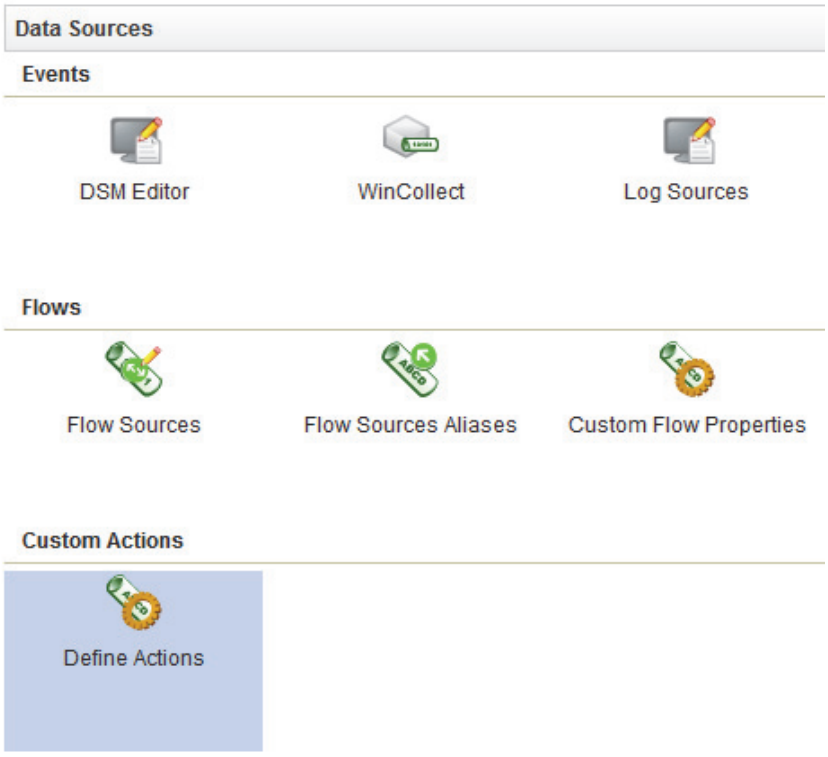
Exercise 2 Define custom action script

In the following steps, you add and define the script in QRadar as a custom action script.

1. Log in to QRadar.
2. Navigate to the **Admin** tab.



3. Scroll down to the **Data Sources** section at the bottom of the page. Then, under **Custom Actions**, select **Define Actions**.



A Custom Actions window opens.

4. In the pop-up window, click **Add**. A Define Custom Action window opens.
5. Define the custom action as shown in the following table:

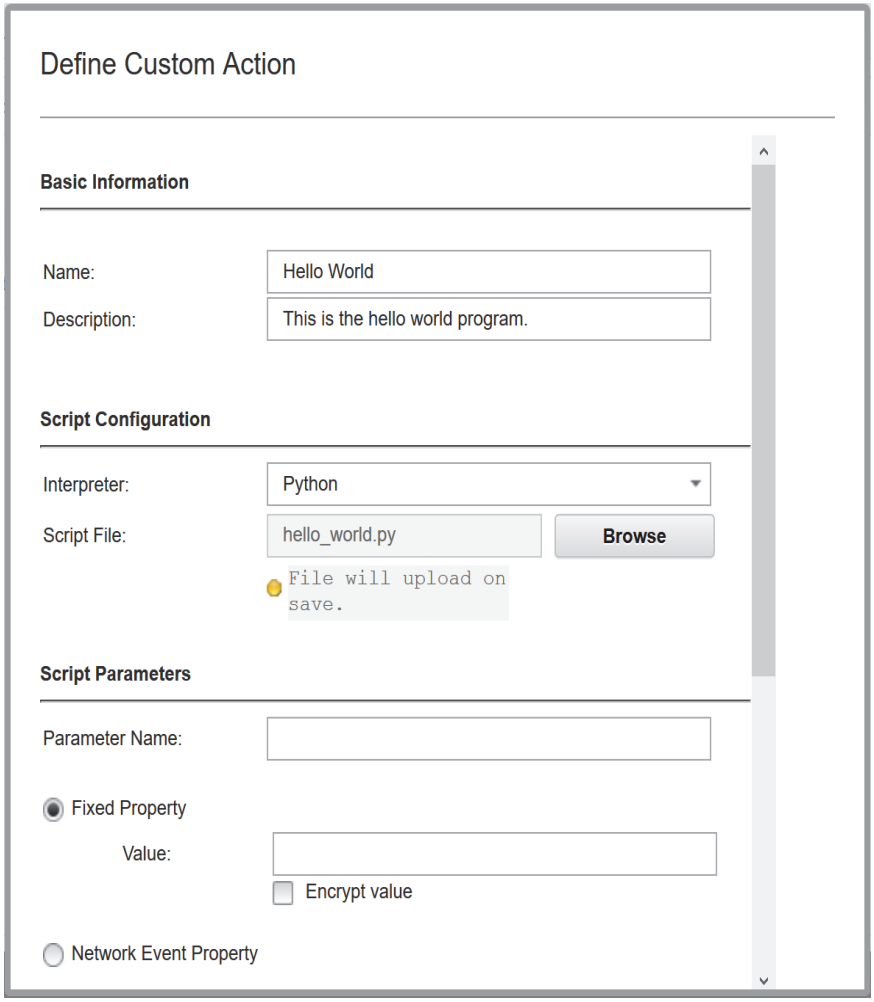
Field / Option	Setting
Name	Hello World
Description	This is a hello world program.

6. Select the drop-down value **Python** for the Interpreter.

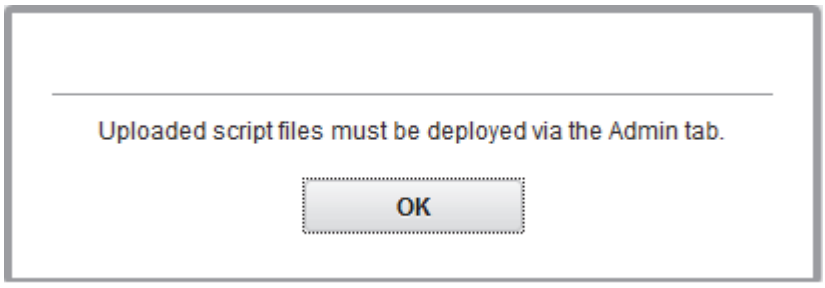
Note: The QRadar Interpreter can handle the following coding applications: Bash, Perl, and Python.

7. Click **Browse**.
8. Locate the `hello_world.py` on the desktop and select **Open**.

Add the `hello_world.py` to the Script Configuration. The Define Custom Action window should look similar to the screen below.



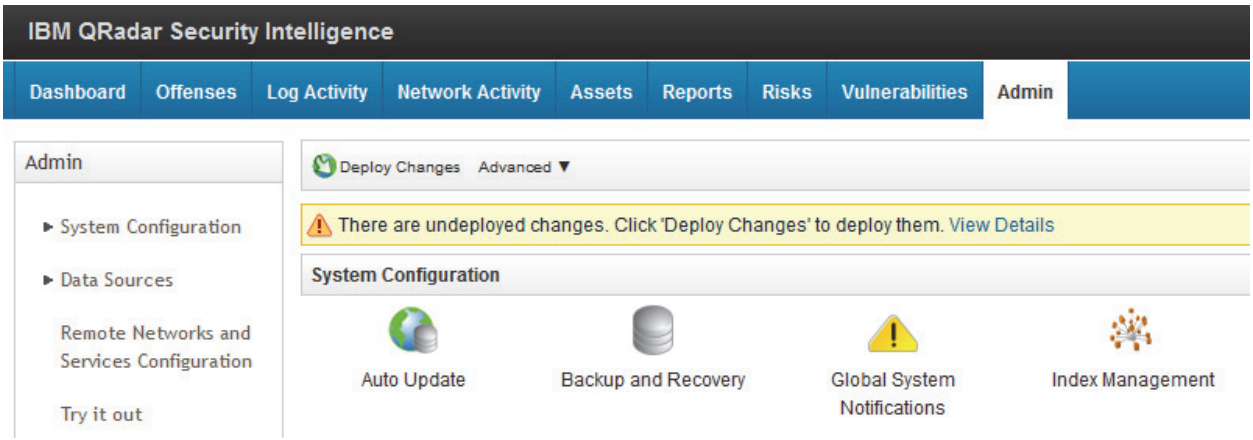
9. Scroll to the bottom of the Define Custom Action window and click **Save**.
10. Click **OK** on the **Uploaded script...** message.



Exercise 3 Test custom action script

In the following exercise, you will test your newly created python script and execute it as a custom action script in QRadar.

1. Check for **Deploy Changes** on the **Admin** tab by clicking on the tab once again to refresh the screen.

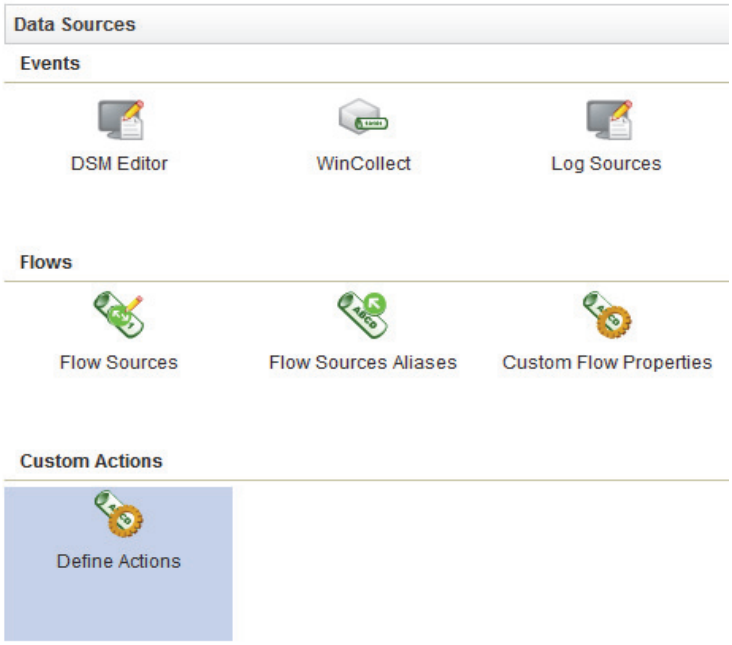


The system automatically checks for undeployed changes and displays a message.

2. Click **Deploy Changes**.

Note: Please be patient. It may take a few minutes to deploy the changes.

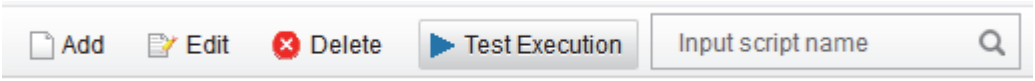
3. Scroll down to the bottom of the page and under **Data Sources** - **Custom Actions**, select **Define Actions**.



A Custom Actions window opens.

4. In the pop-up window, select the **Hello World** script.
   The Hello World record will be highlighted in blue.

5. Click **Test Execution**.

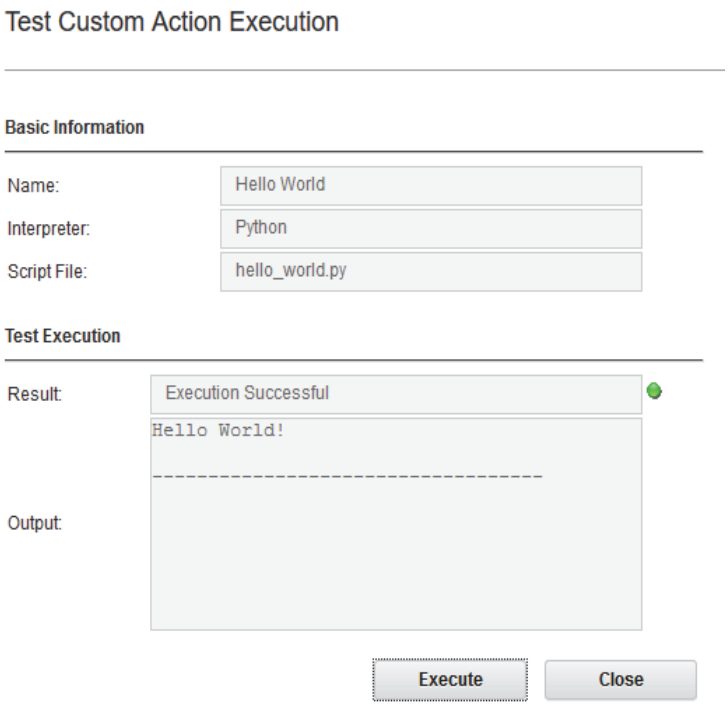


A Test Custom Action Execution window opens.

6. Click **Execute**.
   The **Execute** button will change to **Executing** as the code runs.

Important: When executing a custom action script, it will automatically time out after 15 seconds. QRadar enforces this to prevent long transaction times for scripts.

7. Verify the test results are successful as depicted below. Then close the window.



Exercise 4 Create and define parameters

In the following Python Sample exercise, you will create a python script that will print parameters when executed as a custom action script in QRadar.

1. Open your editor of choice.
2. Type the following lines into the document:

```
Python_sample.py
1 # Python script which prints out any arguments passed to it.
2 import sys
3
4 print("Executing example script")
5 print("Found parameters " + str(sys.argv))
```

3. Save the files as `python_sample.py`
4. Log in to QRadar.
5. Navigate to the **Admin** tab.

6. Scroll down to the bottom of the page and under **Data Sources** - **Custom Actions**, select **Define Actions**.

   A Custom Actions window opens.

7. In the pop-up window, Click **Add**.

   The Define Custom Action window opens.

8. Define the custom action as shown in the following table:

Field / Option	Setting
Name	Python Sample
Description	This is a python script which prints out any arguments passed to it.

9. Select the drop-down value of **Python** for the Interpreter.
10. Click **Browse**.
11. Locate the `python_sample.py` on the desktop and select **Open**.

    Add `python_sample.py` to the Script Configuration.

12. Add the following **Script Parameters** with the settings as shown below. Click **Add** after each parameter setting.

Name	Type	Value
console_ip	Fixed Property	1.2.3.4
offense_source_ip	Network Event Property	sourceip

13. After all parameters have been added, scroll to the bottom of the Define Custom Action window and click **Save**.
14. Click **OK** on the **'Uploaded script...'** message.

Exercise 5 Test parameters

In the following exercise, you will test your newly created python script and execute it as a custom action script in QRadar.

1. Check for **Deploy Changes** on the **Admin** tab by clicking on the tab once again to refresh the screen.

   The system automatically checks for undeployed changes and displays a message.

2. Click **Deploy Changes**.

Note: Please be patient. It may take a few minutes to deploy the changes.

3. Scroll down to the bottom of the page and under **Data Sources** - **Custom Actions**, select **Define Actions**.

   A Custom Actions window opens.

4. In the pop-up window, select the **Python Sample** script.

   The Python Sample record will be highlighted in blue.

5. Click **Test Execution**.

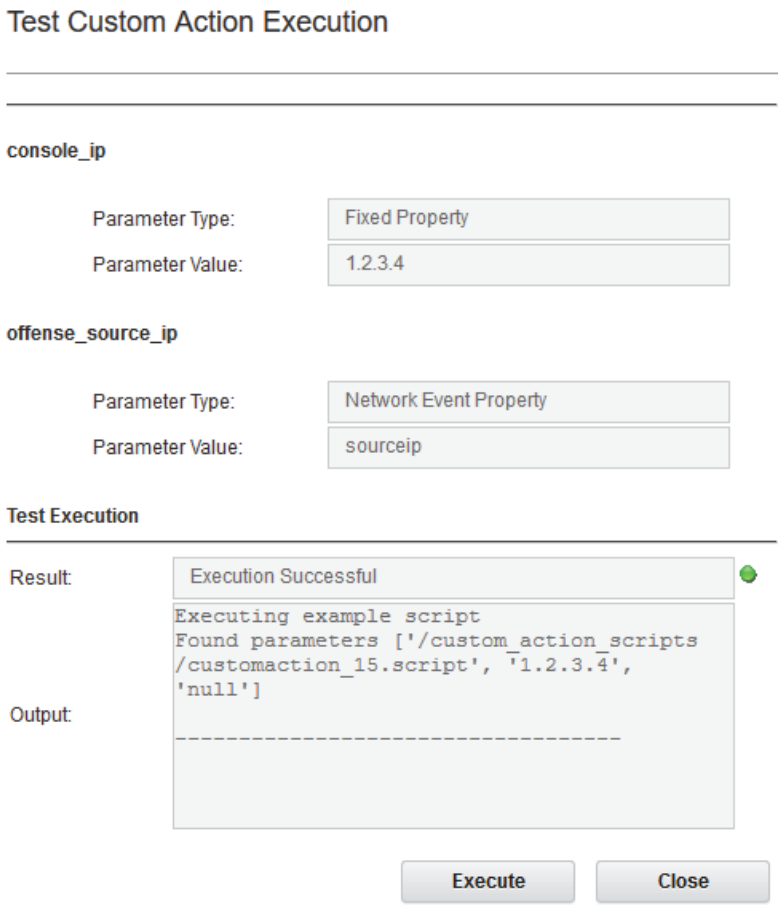
   A Test Custom Action Execution window opens.

6. Click **Execute**.

   The **Execute** button will change to **Executing** as the code runs.

Important: When executing a custom action script, it will automatically time out after 15 seconds. QRadar enforces this as to prevent long transaction times for scripts.

7. Verify the test results are successful as shown below. Then close the window.



Note: In your output, you may have a different script number referenced (e.g. customaction_xx.script). This is the id assigned by QRadar to the script in custom actions. 1.2.3.4 is a fixed parameter value and the sourceip is a null value by default until the script has been invoked from an event rule. Remember, if the script is executed by the “Test Execution” GUI mechanism, then all ‘Network Event Property’ parameters will be set to ‘null’.

Important: For more information on Custom Actions Samples scripts, see the sample code in **GitHub** (https://github.com/ibm-security-intelligence/api-samples/tree/master/custom_actions) and to practice more advanced CAS scripts, refer to the integration CAS examples mentioned under **Additional References** in the course unit.

This concludes the exercises.

Unit 5 Developing anomaly detection rules exercises

In these exercises, you develop an anomaly detection rule of type *Anomaly.* It tests for the deviation of the number of events matching a grouped search from the weighted moving average. The rule fires in the exercise because the sample data spikes above the deviation percentage configured in the anomaly rule.

Exercise 1 Preparing for the anomaly rule

For each anomaly detection rule, a grouped search provides the time series data, that the Anomaly Detection Engine (ADE) uses to detect a statistical deviation. In this exercise, you create a grouped search. To confirm, that your search works as intended, you feed sample data to QRadar SIEM. After QRadar SIEM has discovered the log source type of the sample data, it automatically creates a log source.

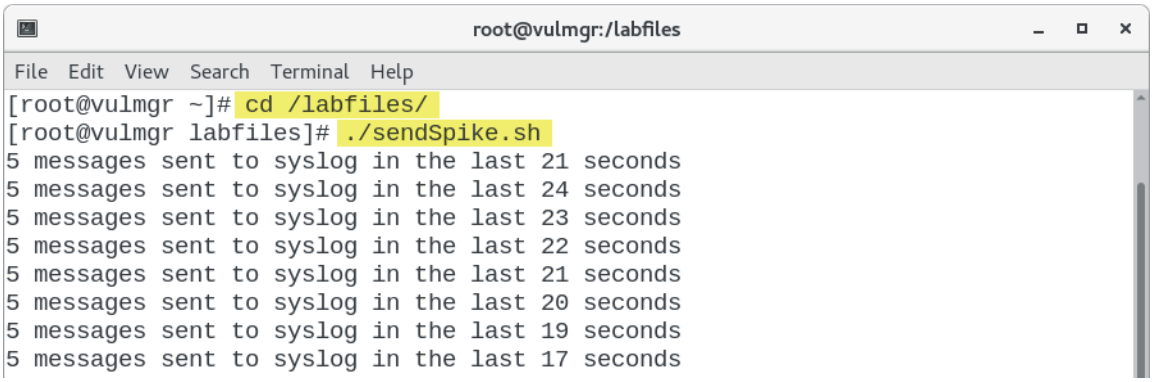
Task 1 Feeding sample data to QRadar SIEM

QRadar SIEM needs to process sample data to create the example used in this lab guide. Perform the following steps to start the applicable script:

1. To open a remote shell to the QRadar VM, use the procedure as outlined in Running commands on the QRadar VM.

2. To feed repeatedly the prepared syslog message to QRadar, run the following commands:

```
cd /labfiles
./sendSpike.sh
```



The script runs for about 10 minutes. Do not close the terminal window.

Even after you can log in to the user interface, a newly started QRadar VM still needs to run for a few minutes before the syslog server can ingest messages. Wait a few minutes and start again if the script terminates with the following error message:

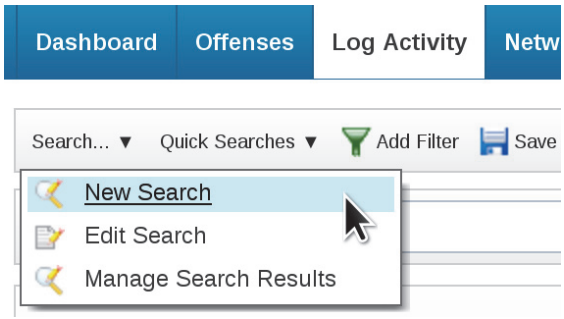
```
Ncat: Connection refused.
```

If feeding sample data runs successfully, QRadar discovers after around 25 syslog messages that they originate from a system running Linux. QRadar automatically creates a log source of the *Linux OS* log source type while you perform the next task.

Task 2 Creating a grouped search

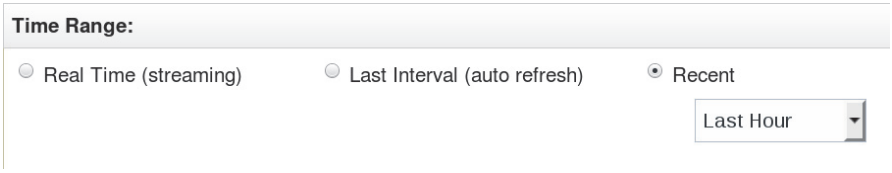
Anomaly detection rules test the results of a grouped event or flow search. To create this search, perform the following steps:

1. To log in to the QRadar user interface, use the procedure as outlined in Logging in to the QRadar user interface.
2. Navigate to the **Log Activity** tab.
3. Locate the **Search** drop-down list on the left in the toolbar.
4. From the **Search** drop-down list, select **New Search**.



As a result, the Log Activity tab displays the form to create a new search.

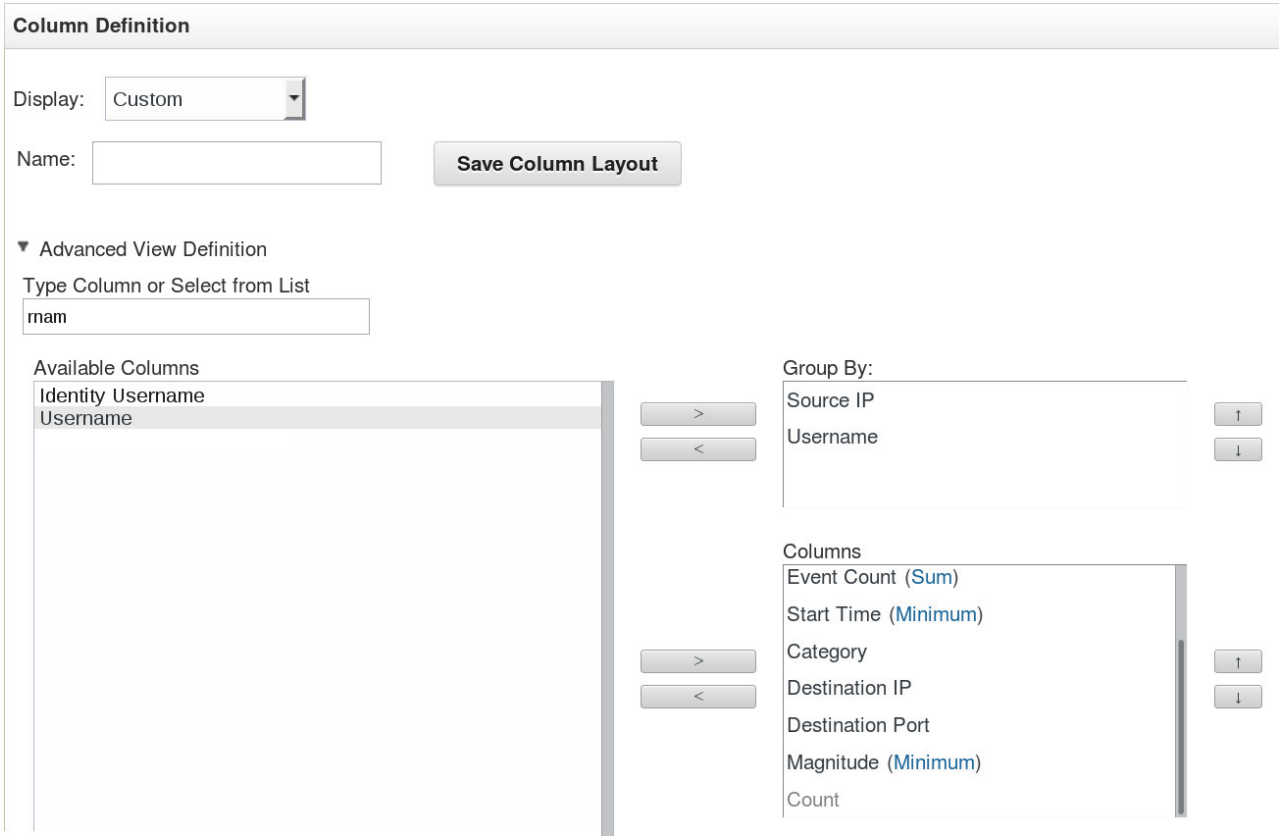
5. Scroll down to the **Time Range** section and perform the following steps:
   a. In the Time Range section, select **Recent** and **Last Hour**.



This time frame is not relevant for the anomaly rule. However, if you select a very short time frame for **Recent** or select **Last Interval (auto refresh)**, you might miss the visual confirmation that your search works as intended because the search result is empty if the script feeding sample data has already terminated a while ago.

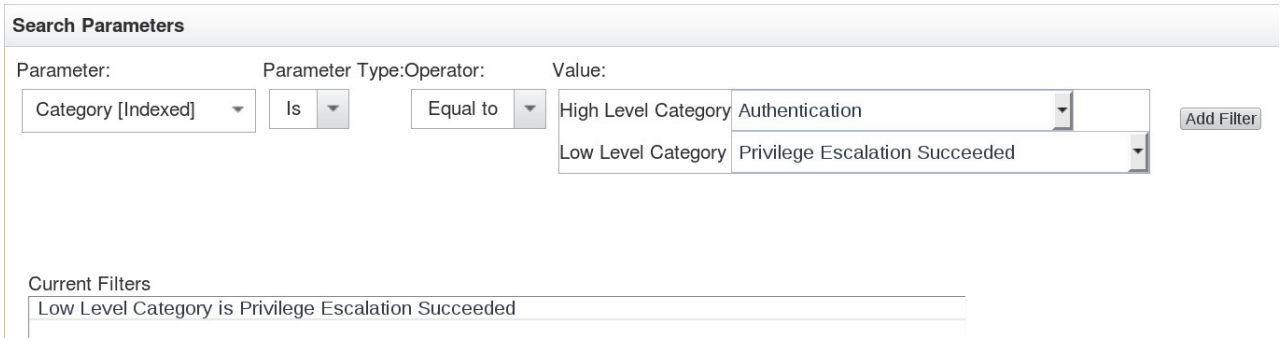
Do not select **Real Time (streaming)** because it does not allow grouping.

6. Scroll down to the **Column Definition** section and perform the following steps:
   a. From the **Columns** list, remove the following two properties:
      - Source IP
      - Username
   b. From the **Available Columns** list, add the same properties to the **Group By** list.
   c. Move the **Source IP** property to the top of the **Group By** list.



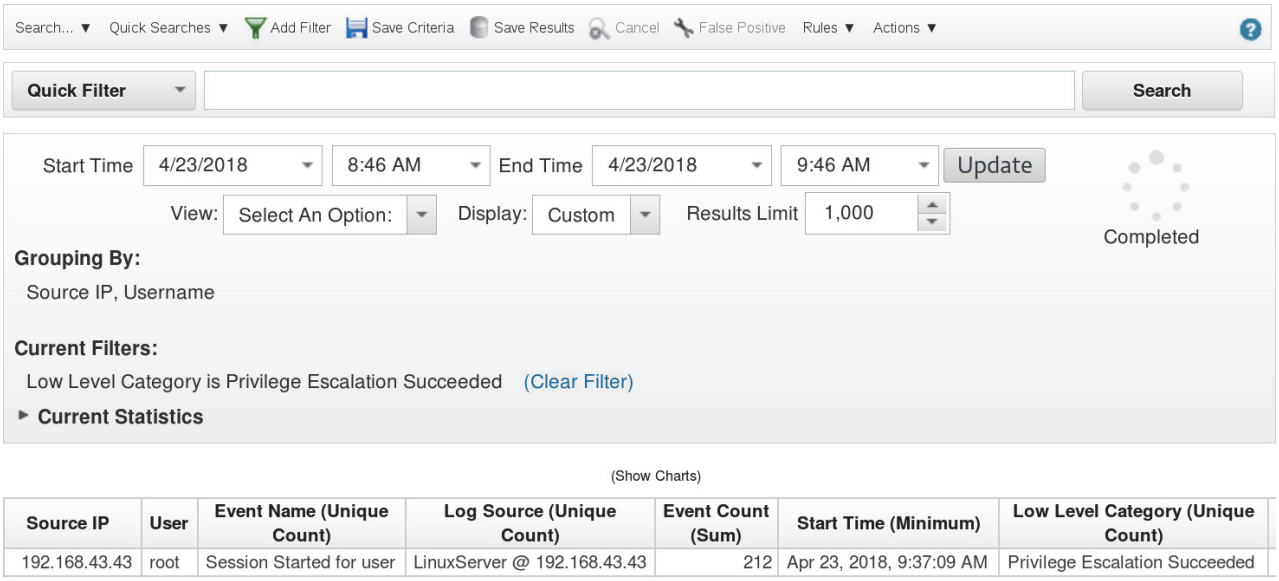
7. Scroll down to the **Search Parameters** section and perform the following steps:
   a. For **Parameter**, select **Category [Indexed]**.
   b. For **Parameter Type**, select **Is**.
   c. For **Operator**, select **Equal to**.
   d. For **High Level Category**, select **Authentication**.
   e. For **Low Level Category**, select **Privilege Escalation Succeeded**.

f. Click **Add Filter**.



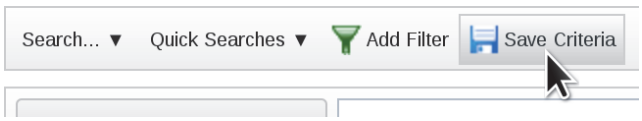
8. To run the new search, click one of the **Search** buttons.

   As a result, the Log Activity tab displays the search result.



Source IP	User	Event Name (Unique Count)	Log Source (Unique Count)	Event Count (Sum)	Start Time (Minimum)	Low Level Category (Unique Count)
192.168.43.43	root	Session Started for user	LinuxServer @ 192.168.43.43	212	Apr 23, 2018, 9:37:09 AM	Privilege Escalation Succeeded

9. To save the new search, click **Save Criteria** in the toolbar.



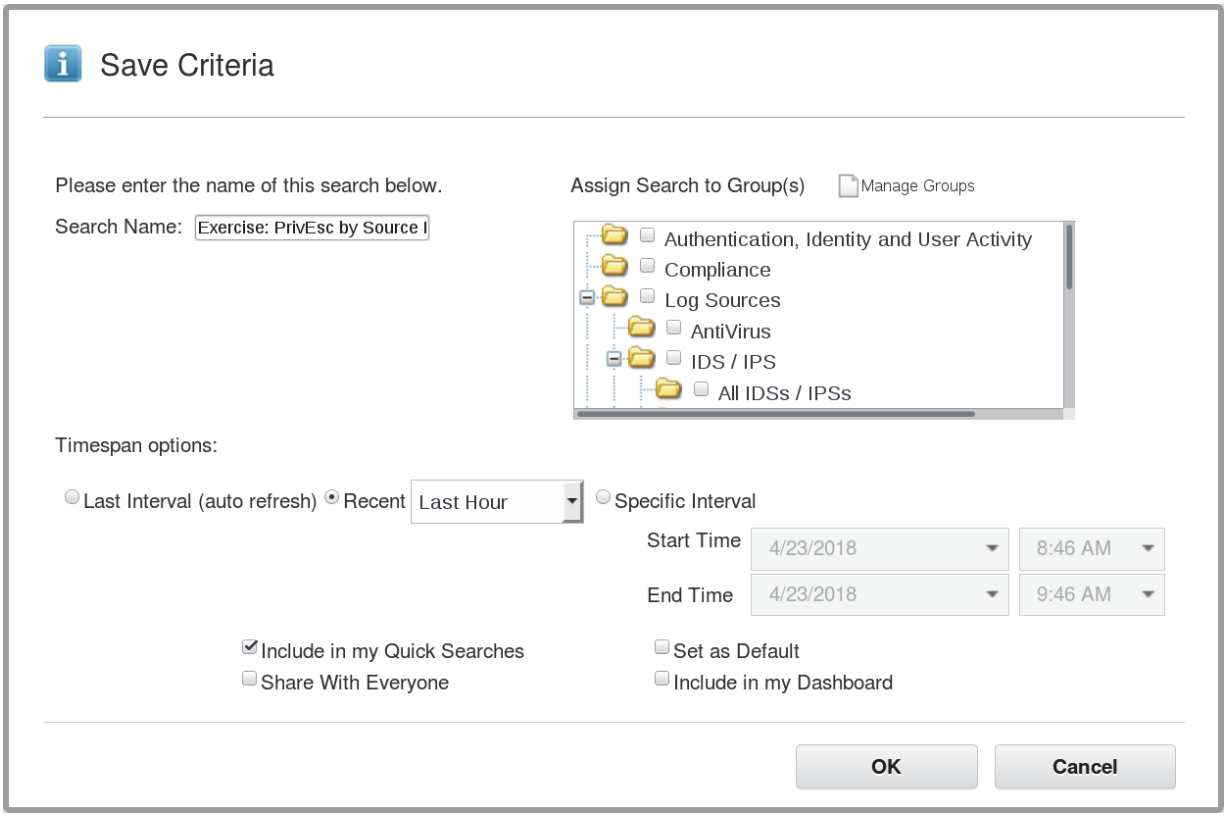
   As a result, the Save Criteria window opens.

10. In the Save Criteria window, perform the following steps:

    a. For **Search Name**, enter **Exercise: PrivEsc by Source IP and Username**

       Best practice is to enter names that describe what a search does. However, for this lab, you can enter a shorter search name because the name is not used anywhere.

b. Not required for this exercise but useful in case you need to locate your search easily, select **Include in my Quick Searches**.



c. To save the search criteria, click **OK**.

As a result, the Save Criteria window closes, and the Search Saved window opens.

d. Click **OK**.

As a result, the Search Saved window closes.

Exercise 2 Creating an anomaly rule

In this exercise, you create the anomaly rule and configure its tests and rule response.

Task 1 Stopping to feed sample data

After creating an anomaly rule in this exercise, you will verify it in the next exercise. The verification needs to start from a clean slate. Therefore, stop feeding sample data to QRadar SIEM because the tests of the new anomaly rule immediately match sample data once the rule is created. To terminate the script, that feeds sample data, perform the following steps:

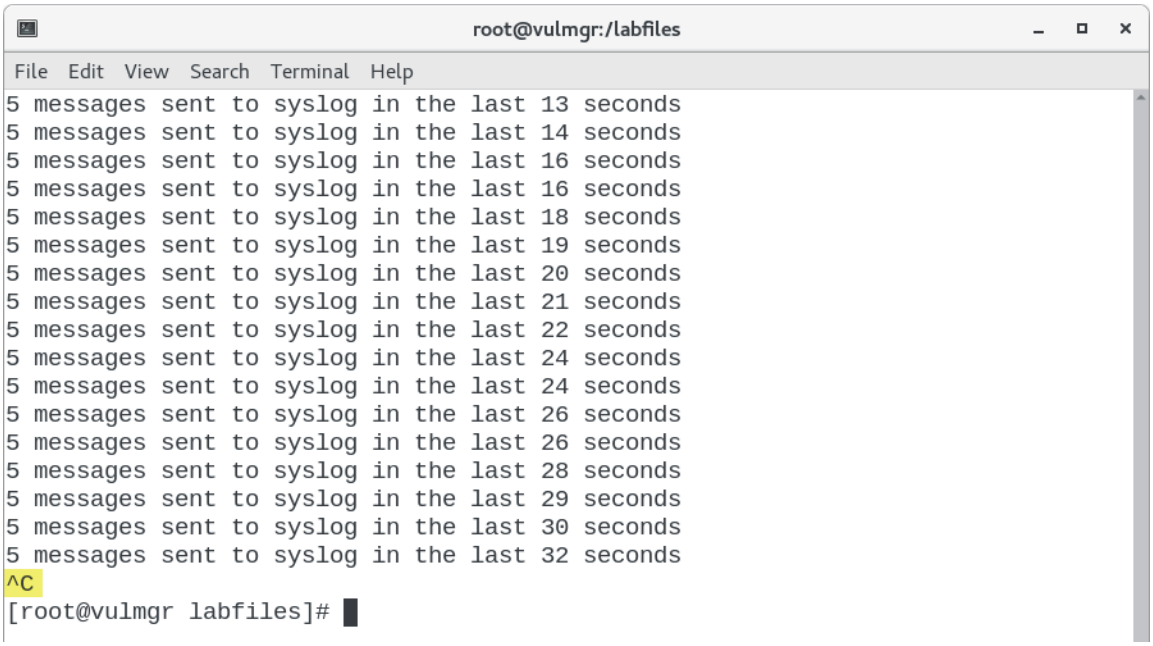
1. Bring the terminal window to the front.

   The terminal window displays the output of script that feeds sample data to QRadar SIEM.

2. If the script has finished, move on to the next task.

3. If the script is still running, press **Ctrl+C** repeatedly in the terminal window, to stop feeding sample data to QRadar SIEM.

   The terminal window displays **^C** when Ctrl+C terminates the script.



   Do not close the terminal window.

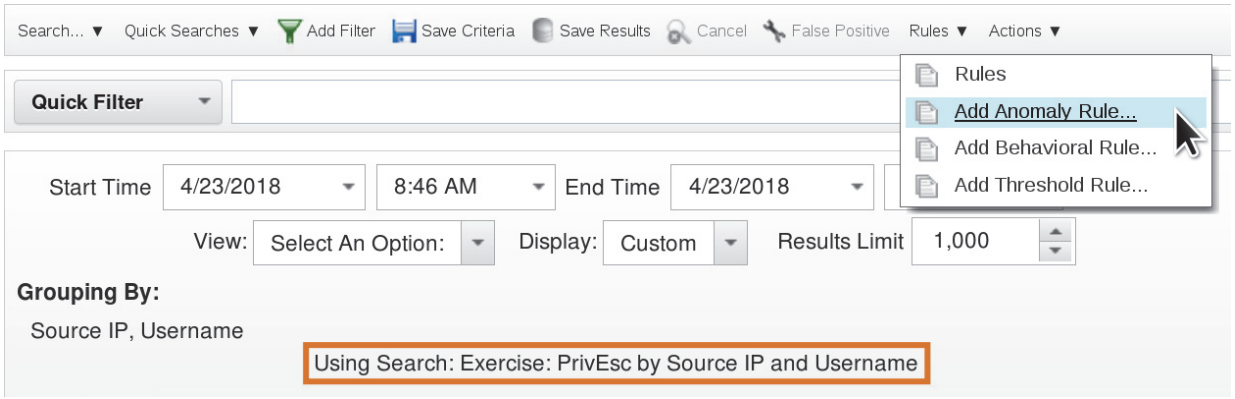
Task 2 Starting the Rule Wizard

To start creating an anomaly rules, that uses the grouped search from the previous exercise, perform the following steps:

1. Bring the browser to the front.

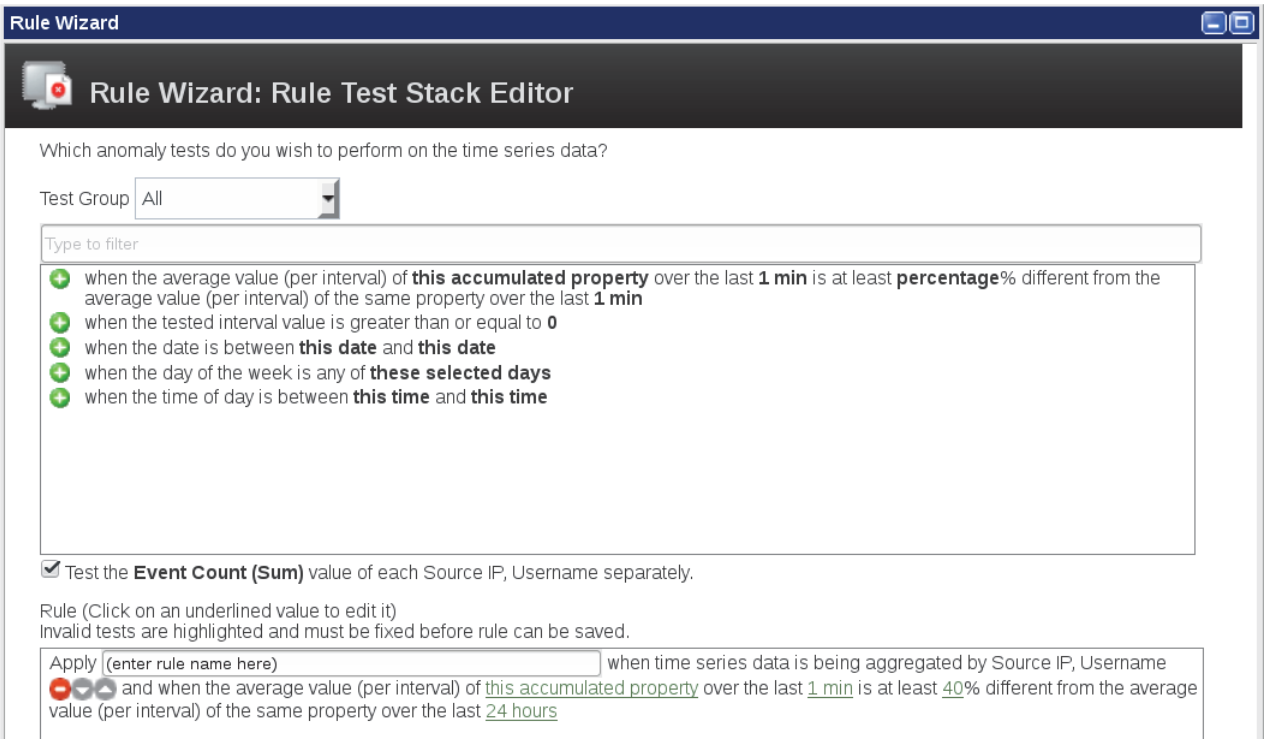
2. Verify that the **Log Activity** tab still displays the search that you saved in the previous exercise. If it does not, select the **Exercise: PrivEsc by Source IP and Username** search from the **Quick Searches** drop-down list in the toolbar.

3. From the **Rules** drop-down list on the toolbar, select **Add Anomaly Rule...**



As a result, QRadar opens the Rule Wizard while staying on the Log Activity tab.

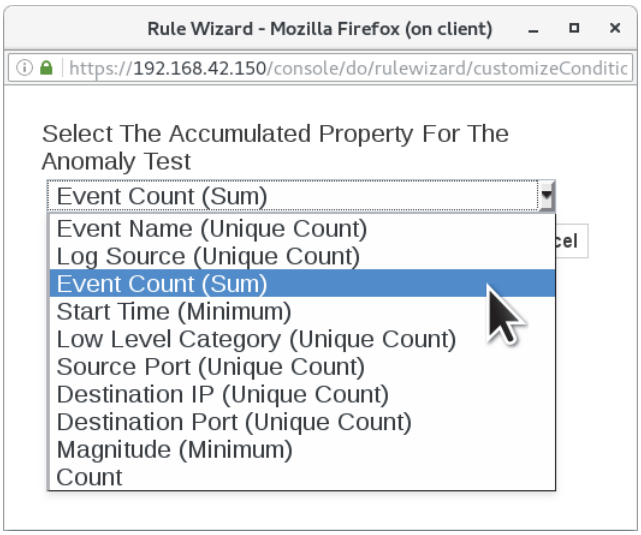
4. If the Rule Wizard starts with its welcome page, read the introductory text and select **Skip this page when running this rules wizard**. To navigate to the Rule Test Stack Editor, click **Next** twice.



Task 3 Configuring test parameters

The Rule Test Stack Editor has already automatically added the test that is essential for an anomaly rule. To configure the test parameters, perform the following steps:

1. To open a window to select the property for which you want to compute interval averages, click the this accumulated property parameter.
2. In the window, select the **Event Count (Sum)** accumulated property.

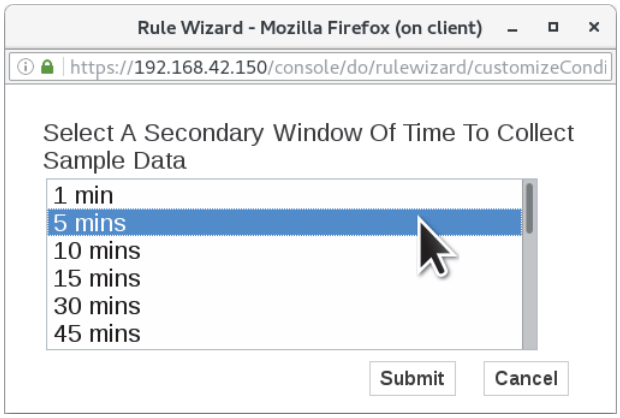


3. To add the accumulated property to the test, click **Submit**.

   The window closes.
4. The second parameter 1 min configures the interval length. Leave the parameter unchanged.
5. The third parameter 40% configures above which deviation of the current interval from the weighted moving average of the previous intervals the test evaluates to true. Leave the parameter unchanged.
6. The last parameter of the test configures, for which time range the Anomaly Detection Engine computes the weighted moving average in intervals.

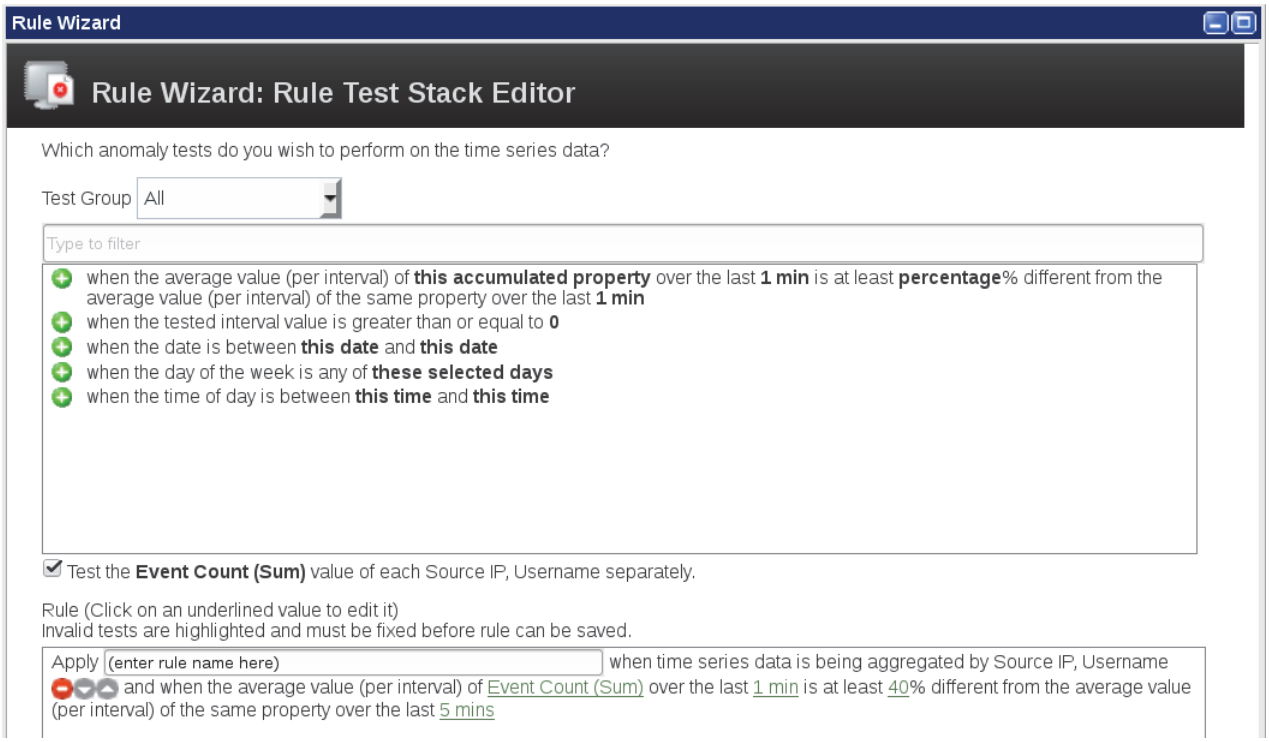
   The Rule Test Stack Editor has automatically selected 24 hours for the last parameter. To open a window to select another time frame, click the parameter.

7. In the window, select the **5 mins** time frame.



8. To update the parameter, click **Submit**.
   The window closes.

9. Verify that your Rule Test Stack Editor looks like the following screen capture.



Hint: In real-world IT environments, probably unusual number of privilege escalations occur at certain times legitimately, for example when automated operational processes run. Therefore, add time tests to only run an anomaly detection rule at times when a deviation from a weighted moving average indicates a concern.

Task 4 Providing a minimum value for each interval

Typically statistical tests lead only to helpful results when a minimum of relevant events or flows arrives per interval. For anomaly detection rules in your environment, the minimums are probably in the hundreds or thousands. This example needs to work with a relatively small number of sample events. Therefore, perform the following steps to require a minimum of 8 events per interval:

1. Click the green **plus (+)** icon next to the following test:

   when the tested interval value is greater than or equal 0

2. To open a window to enter a number as the minimum, click the 0 parameter.

3. In the window, for **Provide A Minimum Value For Each Interval**, replace the **0** by **8**

4. To configure the minimum test, click **Submit**.

   The window closes.

Task 5 Configuring the anomaly rule

Typically statistical tests lead only to helpful results when a minimum of relevant events or flows arrives per interval. For anomaly detection rules in your environment, the minimums are probably in the hundreds or thousands. This example needs to work with a relatively small number of sample events. Therefore, perform the following steps to require a minimum of 8 events per interval:

1. For the rule name in the **Apply** field, enter the following name:

   `Exercise-Authentication: Unusual Privilege Escalations`

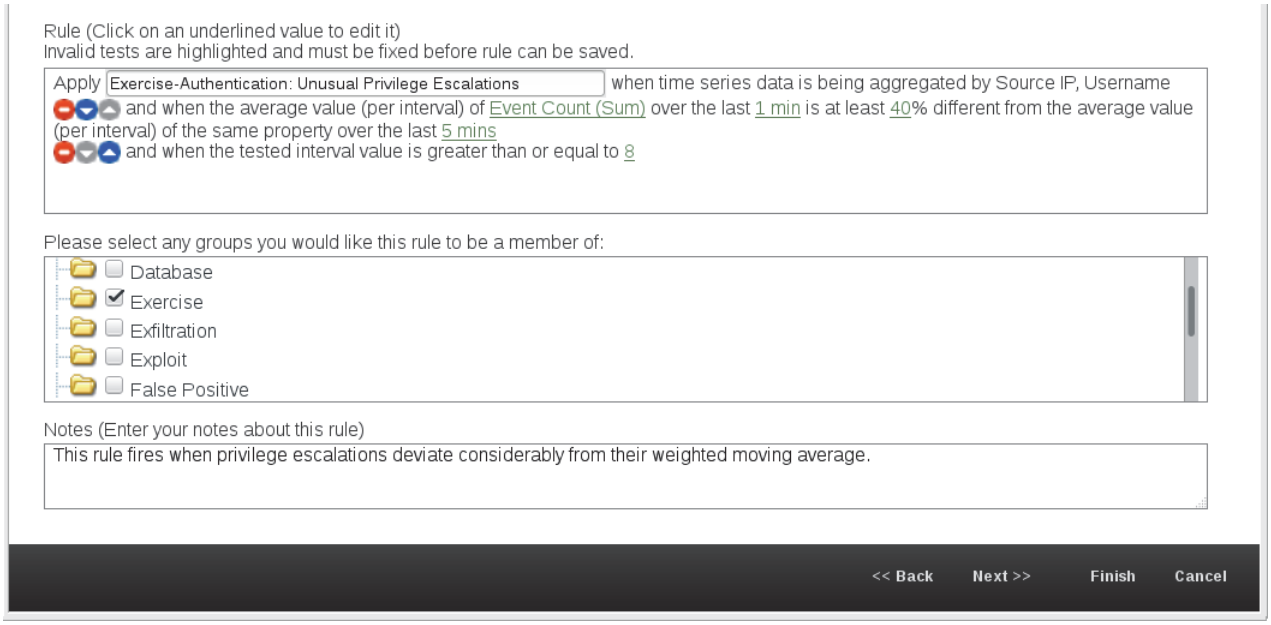
Note: This exercise uses the prefix `Exercise-` to distinguish the predefined rules from your own development.

2. To assign the custom rule to the **Exercise** group, scroll down in the list of groups and select **Exercise**.

3. To document the custom rule in the **Notes** field, enter the following text:

   `This rule fires when privilege escalations deviate considerably from their weighted moving average.`

4. Verify that your Rule Wizard looks like the following screen capture.



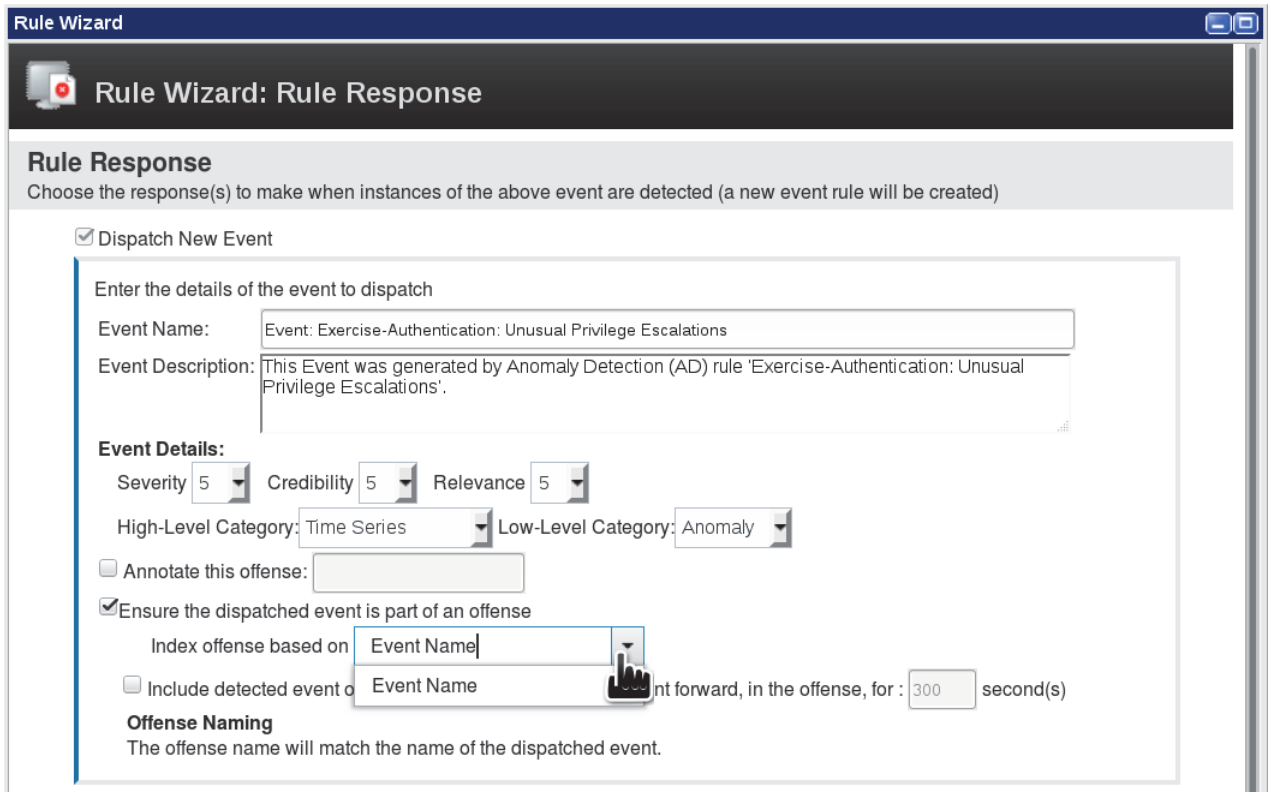
Note: When you need to locate all anomaly detection rules and custom rules that you have developed, navigate to **Rules** on the **Offenses** tab, select **Rules** in the **Display** drop-down list, and then select **Exercise** in the **Group** drop-down list.

Task 6 Observing rule responses

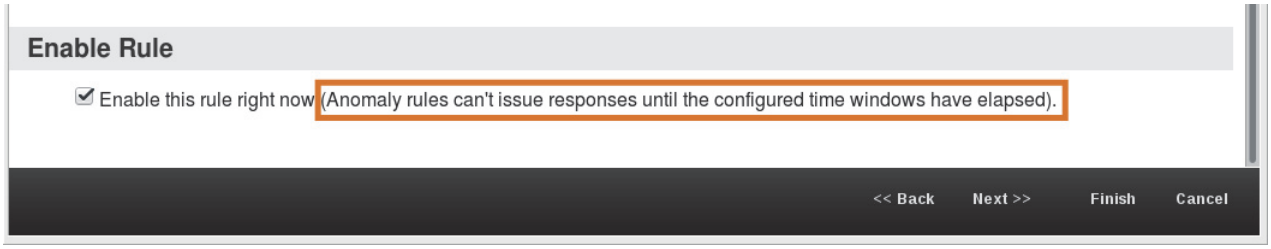
To have an offense created for the unusual privilege escalations that the anomaly detection rule tests for, perform the following steps:

1. To navigate to the Rule Response, click **Next**.
2. The Rule Wizard has already prepared the Rule Response. For this example, do not make any changes.

3. To observe, that the offense can only be indexed on Event Name, open the **Index offense based on** drop-down list.



4. Scroll down to the **Enable Rule** section. Do not change anything. Read the important hint next to the checkbox.



5. To navigate to the Rule Summary, click **Next**.

6. To create the rule, click **Finish**.

   The Rule Wizard closes.

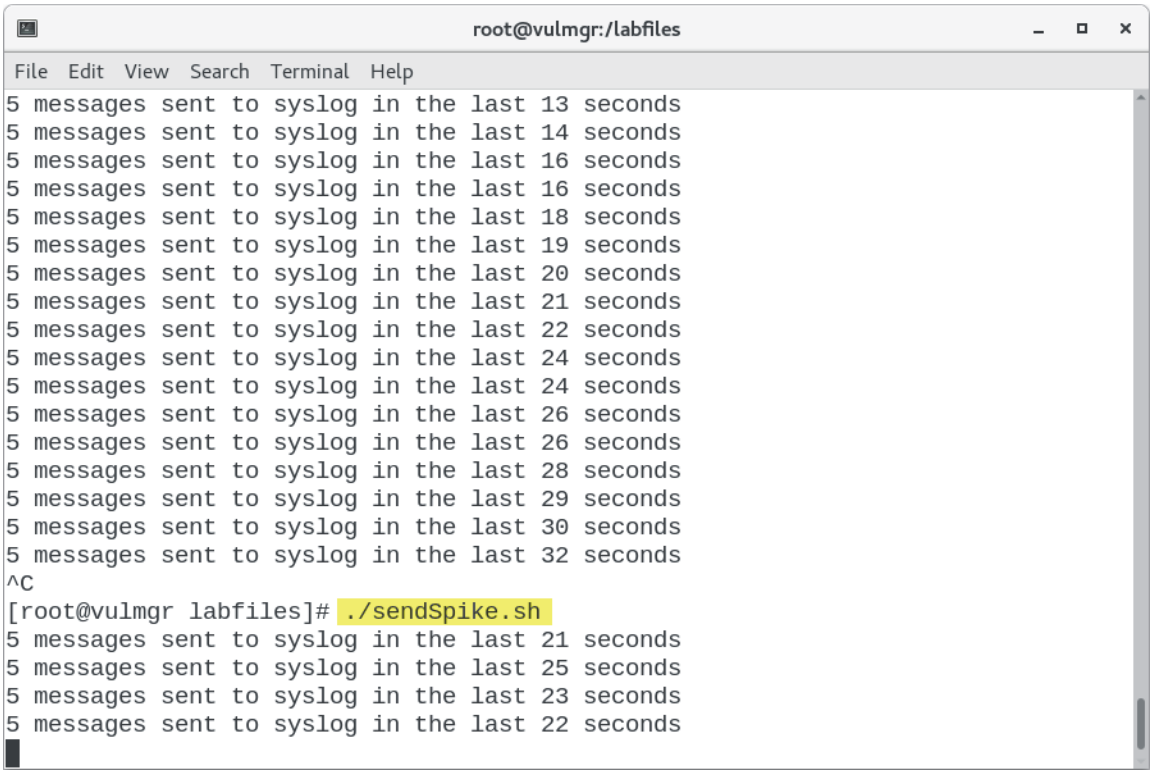
Exercise 3 Verifying the anomaly rule

In this exercise, you verify whether your development creates an offense.

Task 1 Feeding sample data to QRadar SIEM

To terminate the script, that feeds sample data, perform the following steps:

1. Bring the terminal window to the front.
   The terminal window still displays the output from running the script previously.
2. To feed repeatedly the prepared syslog message to QRadar, run the following command:
   `./sendSpike.sh`



The script runs for about 10 minutes. Do not close the terminal window.

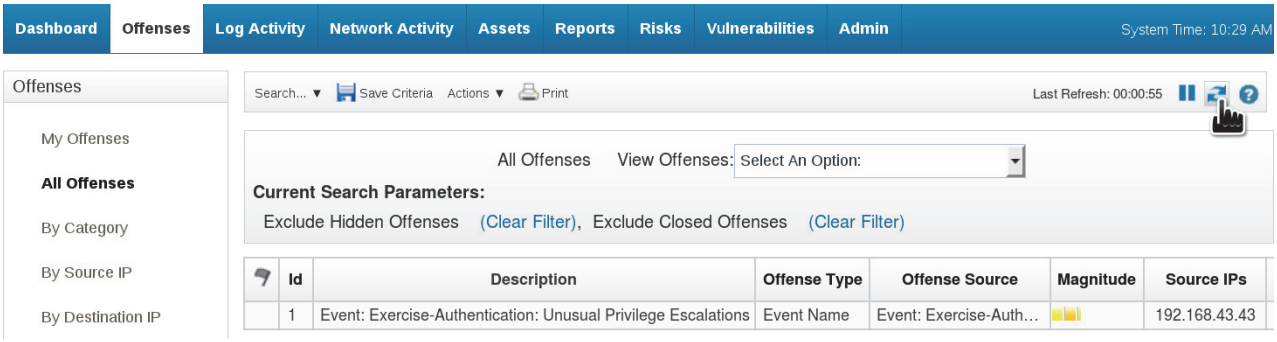
Task 2 Observing the offense

The script feeds events to QRadar SIEM, that match your anomaly rule. For the first five minutes, the rate of events increases to a spike. After the spike, the rate decreases mirroring the rate of the increase in the first five minutes.

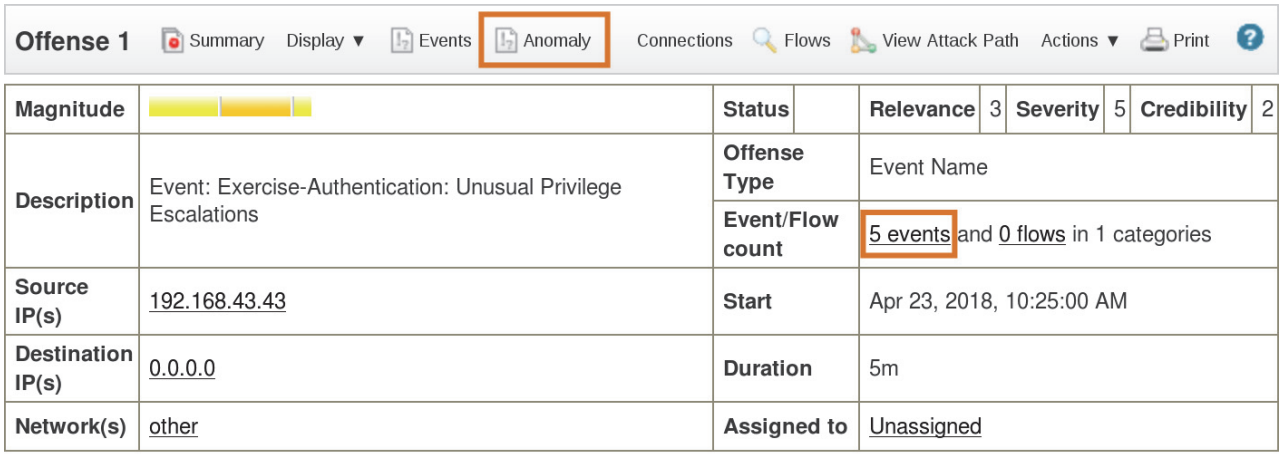
The average of the interval with the spike deviates by a higher percentage than configured in the anomaly rule from the weighted moving average. Therefore, QRadar SIEM creates an offense after the script has run for about six minutes. To observe the offense, perform the following steps:

1. Navigate to the **Offenses** tab.
2. To refresh the listed offenses, click the **double arrow** icon in the upper-right corner of the QRadar SIEM user interface, or double-click the **Offenses** tab. The double-click refreshes and resets the tab to its default settings.

3. When the new offense appears, double-click it.



The Offense Summary opens.

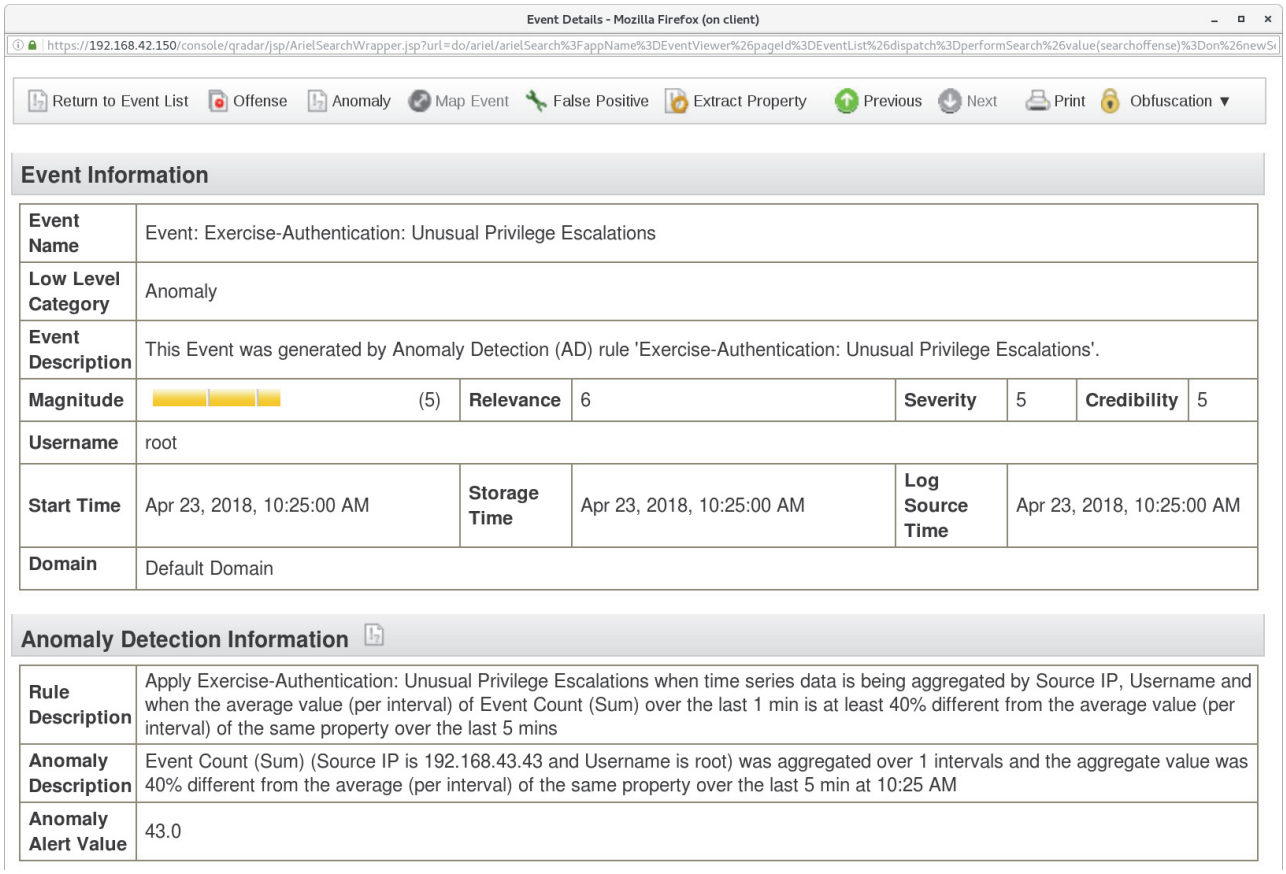


4. Optionally, click **Anomaly** in the toolbar.
   A separate window opens with the results of the search that your anomaly rule uses.

5. In the **Event/Flow count** field, click **5 events**. The number of events can differ.
   A separate window opens with the events that the anomaly rule dispatched as Rule Response.

6. To open the Event Details, double-click one of the events.

7. Observe the **Anomaly Detection Information** section. It only appears for events that anomaly detection rules dispatch as a Rule Response.



This concludes the exercises.

IBM Training