SIEM Courseware Beginner

LAB GUIDE

This material is meant for IBM Academic Initiative use only. NOT FOR RESALE.

Preface

June 2021

NOTICES

<Any necessary notices with regards to the course material.>

TRADEMARKS

IBM, the IBM logo, ibm.com and Python are trademarks or registered trademarks of the 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 in available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.html.

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

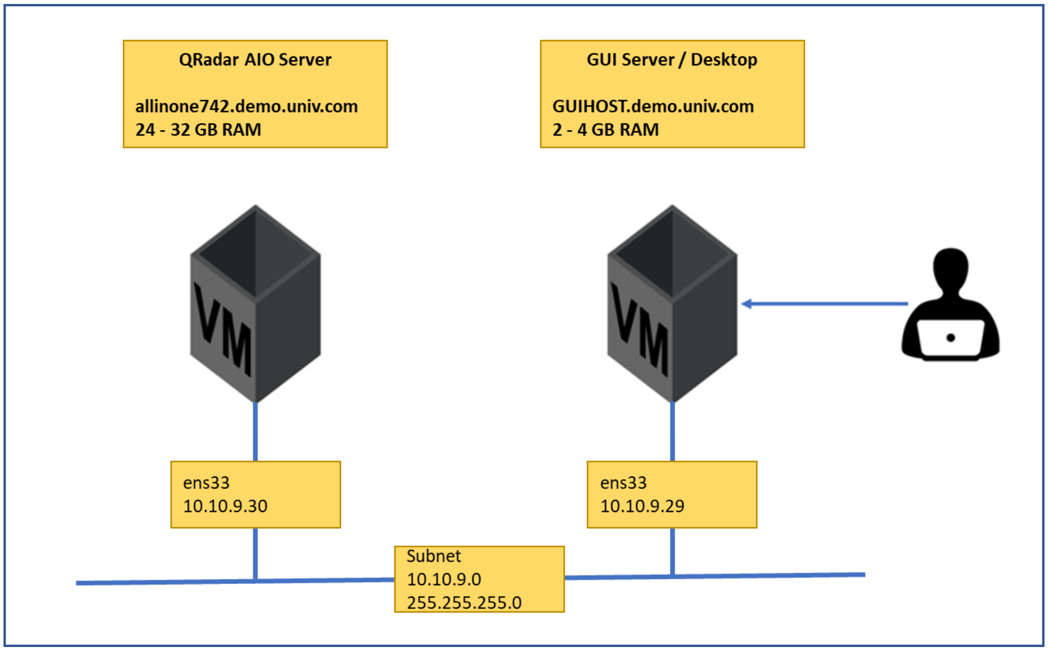
Microsoft, Windows and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries or both.

Table of Contents

Beginning

Virtual Machines

The following figure shows the setup of the virtual machines in the training lab.

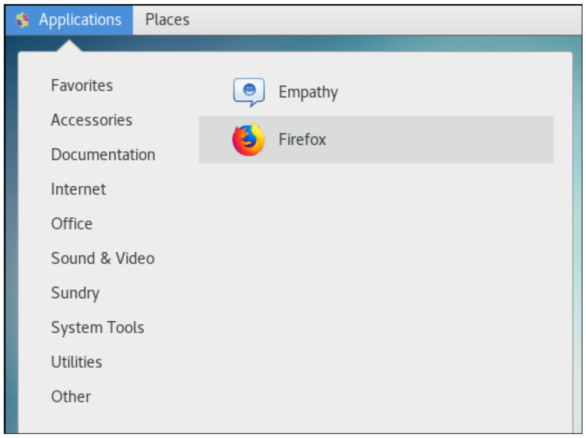


The lab environment uses the following two virtual machines (VMs):

- Qradar AIO Server - a virtual machine running IBM QRadar All-in-one setup on Red Hat Enterprise Linux.
  - Hostname - **allinone742.demo.univ.com**
  - IP Address - **10.10.9.30**
- GUI Server - a virtual machine providing a graphical user interface to access Qradar Application. It hosts the graphical desktop where you perform the course exercises.
  - Hostname - **GUIHOST.demo.univ.com**
  - IP Address - **10.10.9.29**

You log in to **guihost** as user **root** with password **p@ssw0rd**. You need two tools on the desktop to perform the exercises:

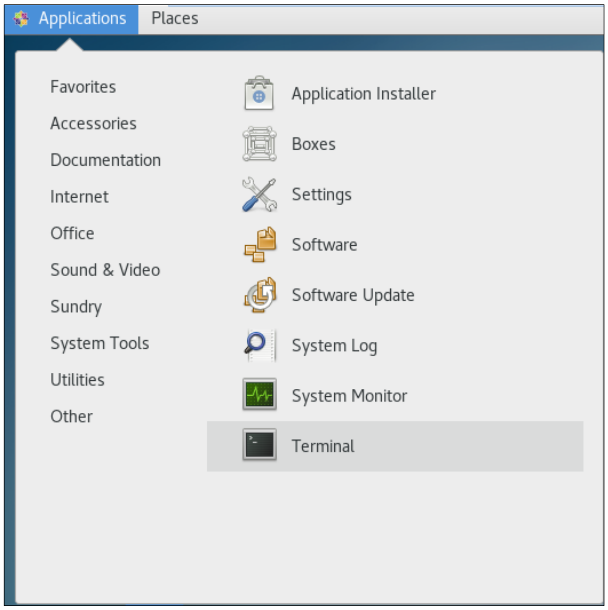
1. A web browser for accessing the Qradar interface, found at Applications > Internet > Firefox Web Browser



   Use the URL https://10.10.9.30/console to access Qradar Graphical Interface, 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.

2. A terminal window to run commands on osprey and G10, found on the desktop or through Application > System Tools > Terminal



You need the following accounts and passwords to complete the labs.

- GUIHOST
  - User root, password p@ssw0rd
  - User gui, password p@ssw0rd123
- ALLINONE742
  - User root, password p@ssw0rd
  - User admin, password p@ssw0rd

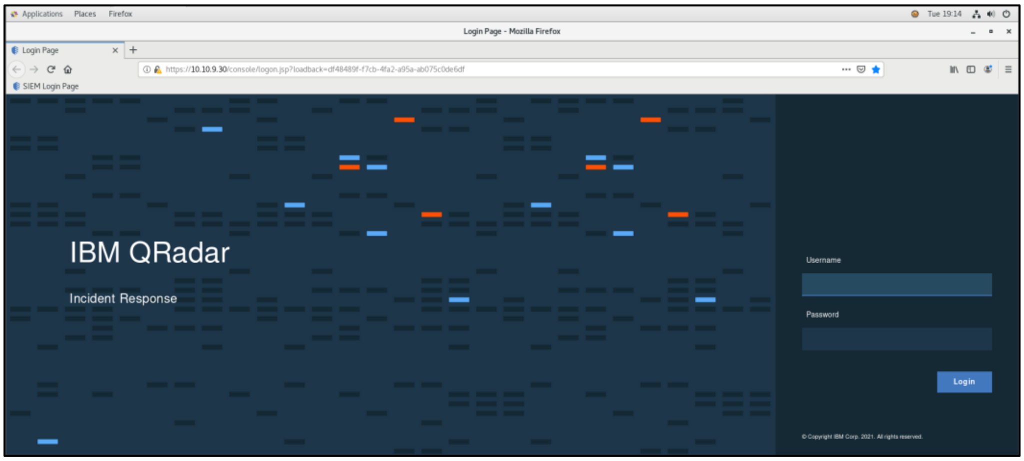
QRadar UI - Overview exercises

1. Where can you see an initial summary view of your QRadar Console?
2. How do you pin tabs to the Console?
3. Which two main functions that are included in your in QRadar installation require additional licensing?
4. What is the name of the default user that is used to establish SSH connections to the command-line interface?
5. In addition to the local system, name 3 other authentication methods that are supported by QRadar.
6. How can you access the system notification center?
7. How can you access the QRadar documentation from the Console
8. How often is data refreshed by default?
9. What range of intervals can you select to monitor network or log activity?
10. On which tab can you view QRadar rules and building blocks?

Login into the Qradar Interface

Follow these steps to prepare for the course exercises:

1. Start GUI Server **guihost** “**Centos-GUI**” and Qradar Server Allinone742 “**SIEM-All-in-One-742**” virtual machines.
2. Login to the **guihost** virtual machine as user *root* with password *p@ssw0rd*.
3. Ensure the GUI Server can connect to the QRadar Application and that Qradar is running.
   a. Start the Firefox web browser and navigate to the Qradar interface.



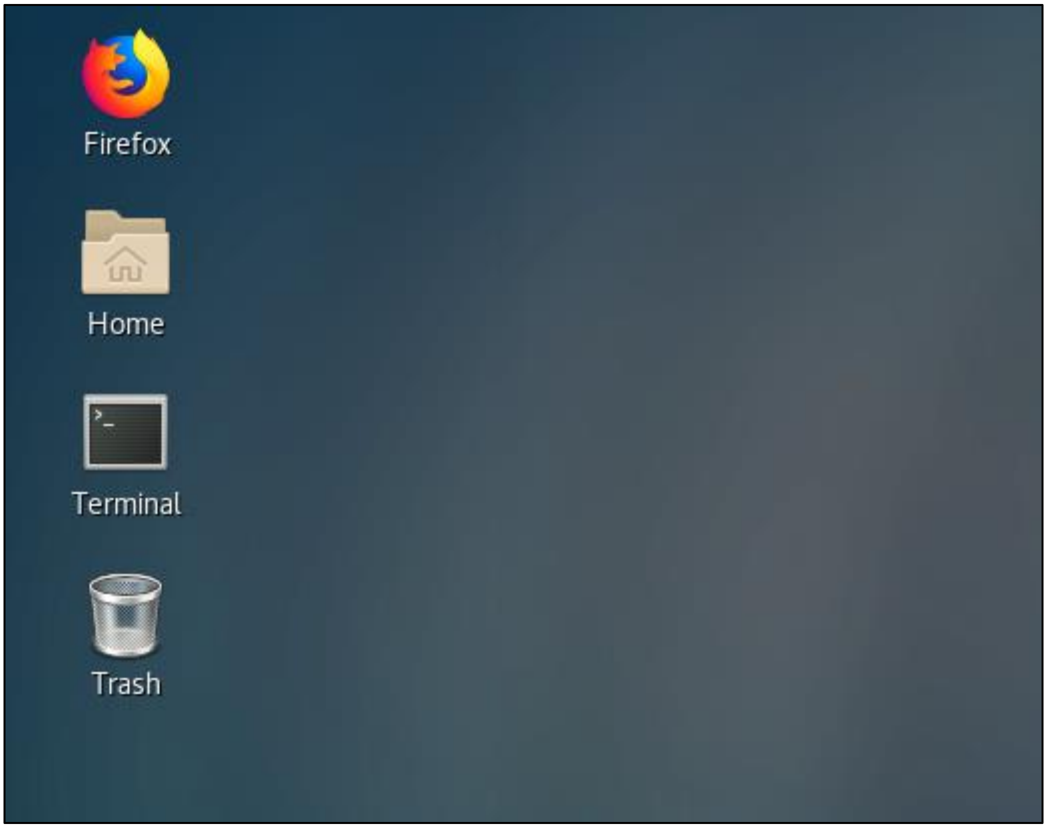
Login Page - Mozilla Firefox

https://10.10.9.30/console/logon.jsp?loadback=df48489f-f7cb-4fa2-a95a-ab075c0de6df

   b. If the Qradar interface does not appear, consult with the instructor to troubleshoot the issue.

Access Command Line Interface of Qradar Server

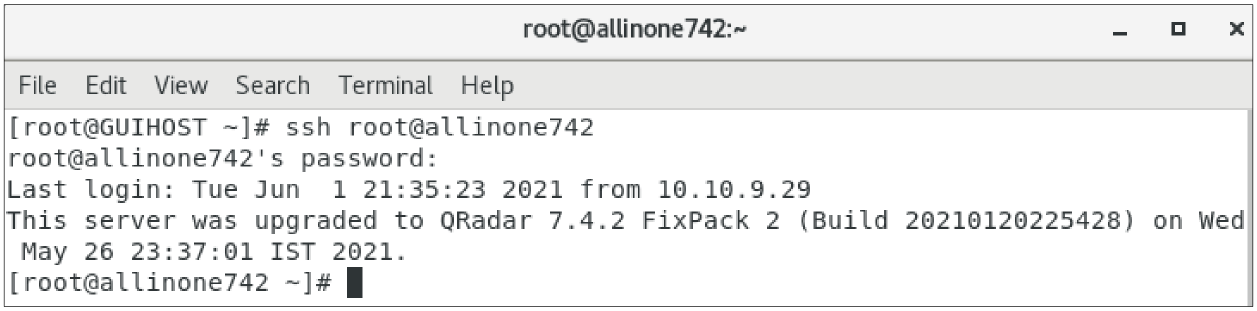
1. To open the SSH session to the Qradar VM, click the Terminal Icon on the Desktop window.



2. Run the following command on SSH Terminal –

   ssh root@allinone742

   Enter the password as ‘p@ssw0rd’



```
[root@GUIHOST ~]# ssh root@allinone742
root@allinone742's password:
Last login: Tue Jun  1 21:35:23 2021 from 10.10.9.29
This server was upgraded to QRadar 7.4.2 FixPack 2 (Build 20210120225428) on Wed
 May 26 23:37:01 IST 2021.
[root@allinone742 ~]#
```

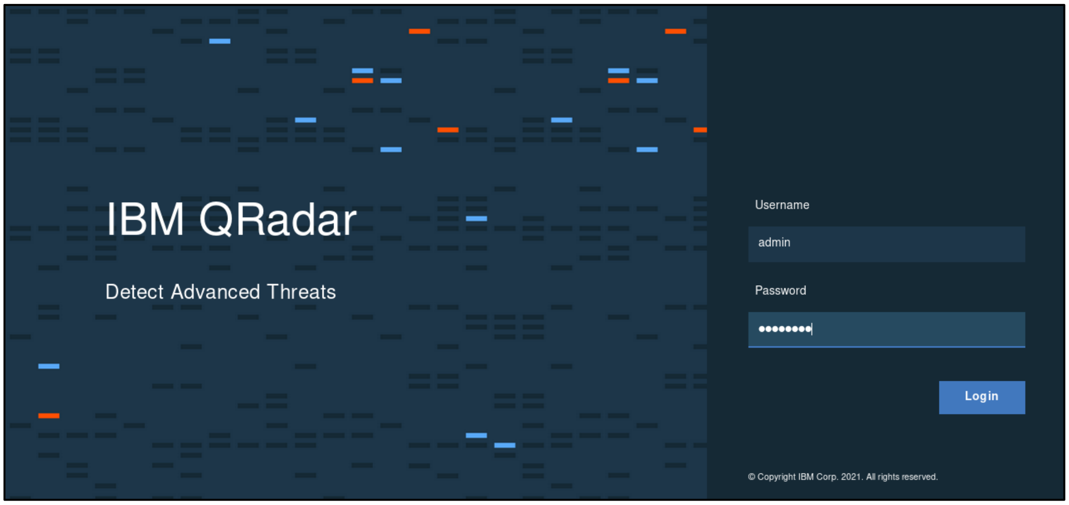
Lab 1 - Using the QRadar SIEM user interface

In these exercises, you become familiar with the web-based control center and sending sample data to Qradar.

Explore Qradar User Interface

In this exercise, you become familiar with the Qradar Web Based control center.

1. Use a web browser to go to URL https://10.10.9.30/console to access the web interface login page.
2. Log in to the web interface with the user admin and password p@ssw0rd to access the home page.



IBM QRadar

Detect Advanced Threats

Username

admin

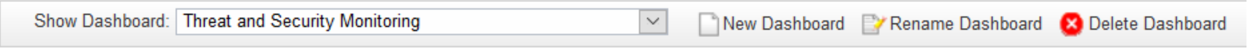
Password

••••••••

Login

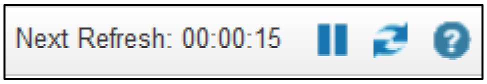
© Copyright IBM Corp. 2021. All rights reserved.

3. The Qradar Dashboard interface opens. Most of the sections in this dashboard may be empty. We will initiate a sample feed to see all these data.
4. You can navigate from one dashboard to another and create, rename or remove any existing dashboard from the panel as shown in the screenshot.



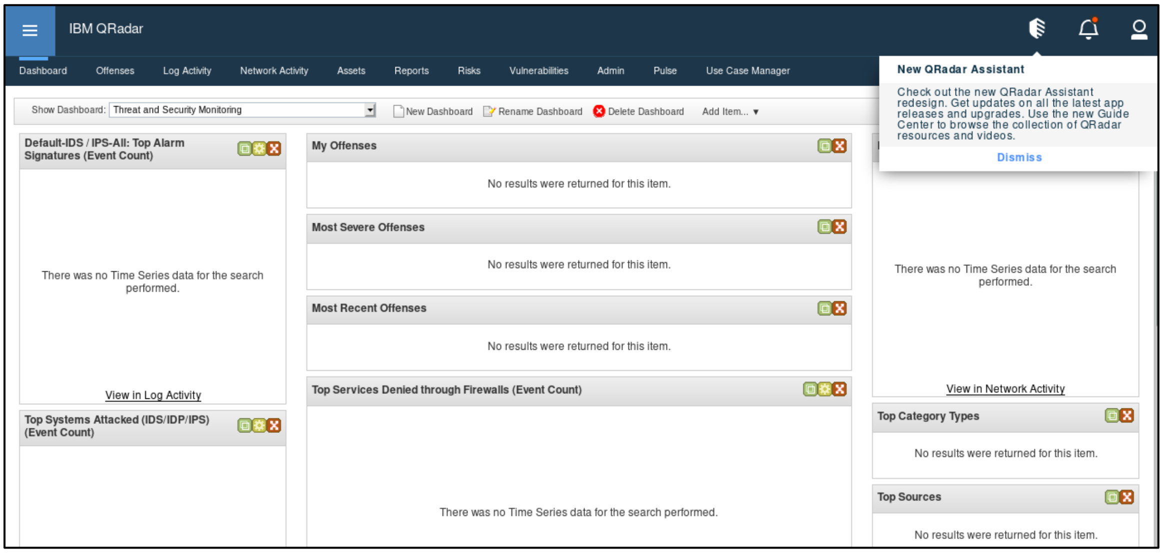
Show Dashboard: Threat and Security Monitoring

5. The Dashboard tab automatically refreshes every 60 seconds. The timer indicates the amount of time that remains until the tab is automatically refreshed.



Next Refresh: 00:00:15

6. Functionality is divided into tabs. The Dashboard tab is displayed when you log in. You can easily navigate the tabs to locate the data or functionality you require.



New QRadar Assistant

Check out the new QRadar Assistant redesign. Get updates on all the latest app releases and upgrades. Use the new Guide Center to browse the collection of QRadar resources and videos.

There was no Time Series data for the search performed.

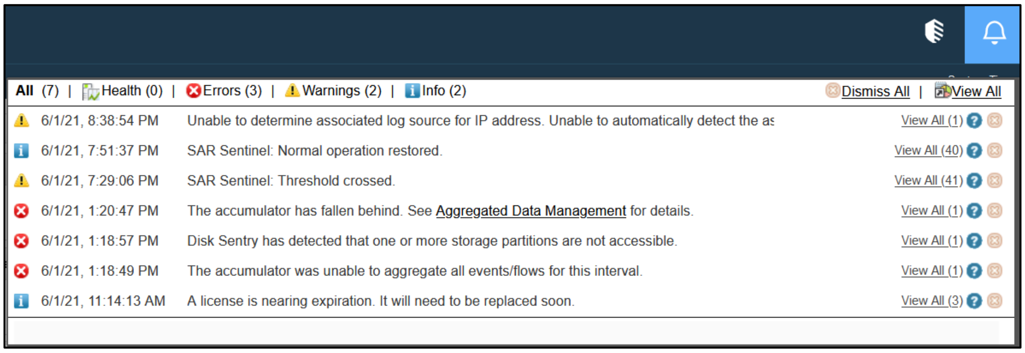
No results were returned for this item.

Click and Explore each tab in the user interface.

- **Dashboard tab** - The Dashboard tab is a workspace environment that provides summary and detailed information on events occurring in your network.
- **Offenses tab** - View offenses that occur on your network, which you can locate by using various navigation options or through powerful searches.
- **Log activity tab** - Investigate event logs that are sent to QRadar in real-time, perform powerful searches, and view log activity by using configurable time-series charts.
- **Network activity tab** - Use the Network Activity tab to investigate flows that are sent in real-time, perform powerful searches, and view network activity by using configurable time-series charts.
- **Assets tab** - QRadar automatically discovers assets, servers, and hosts that are operating on your network.
- **Reports tab** - Use the Reports tab to create, distribute, and manage reports for any data within QRadar.

- **IBM QRadar Risk Manager** - IBM QRadar Risk Manager is a separately installed appliance for monitoring device configurations, simulating changes to your network environment, and prioritizing risks and vulnerabilities in your network.
- **Admin tab**– In this tab, an Administrator can perform Admin related tasks.
  - Deploy and manage Qradar Hosts and licenses.
  - Configure user accounts and authentication.
  - Build a network hierarchy
  - Configure domains and set up a multi-tenant environment
  - Define and manage log and flow data sources etc.

7. Click Notifications 🔔.
   a. On the Messages window, view the system notification details.

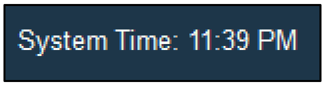


All (7) | Health (0) | Errors (3) | Warnings (2) | Info (2)		Dismiss All | View All
⚠ 6/1/21, 8:38:54 PM	Unable to determine associated log source for IP address. Unable to automatically detect the as	View All (1)
ℹ 6/1/21, 7:51:37 PM	SAR Sentinel: Normal operation restored.	View All (40)
⚠ 6/1/21, 7:29:06 PM	SAR Sentinel: Threshold crossed.	View All (41)
☒ 6/1/21, 1:20:47 PM	The accumulator has fallen behind. See Aggregated Data Management for details.	View All (1)
☒ 6/1/21, 1:18:57 PM	Disk Sentry has detected that one or more storage partitions are not accessible.	View All (1)
☒ 6/1/21, 1:18:49 PM	The accumulator was unable to aggregate all events/flows for this interval.	View All (1)
ℹ 6/1/21, 11:14:13 AM	A license is nearing expiration. It will need to be replaced soon.	View All (3)

   b. To refine the list of system notifications, click one of the following options:
      - Health
      - Errors
      - Warnings
      - Info

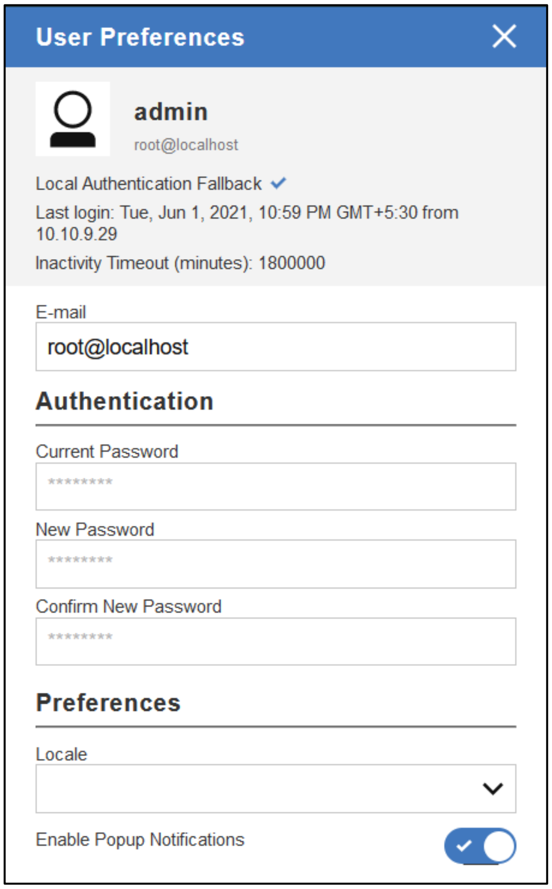
   c. Optional: To close system notifications, choose one of the following options:
      - Dismiss All Info
      - Dismiss

8. The upper right of the QRadar® console displays the system time, which is the local time on the console. The console time is used to determine what time events were received from other devices for correct time synchronization correlation.



System Time: 11:39 PM

9. Click the **user** icon, and then click **User Preferences** to access your user information.
   a. You can update your user preferences from this panel.



User Preferences

admin

root@localhost

Local Authentication Fallback ✓

Last login: Tue, Jun 1, 2021, 10:59 PM GMT+5:30 from 10.10.9.29

Inactivity Timeout (minutes): 1800000

E-mail: root@localhost

Authentication

Current Password: ********

New Password: ********

Confirm New Password: ********

Preferences

Locale:

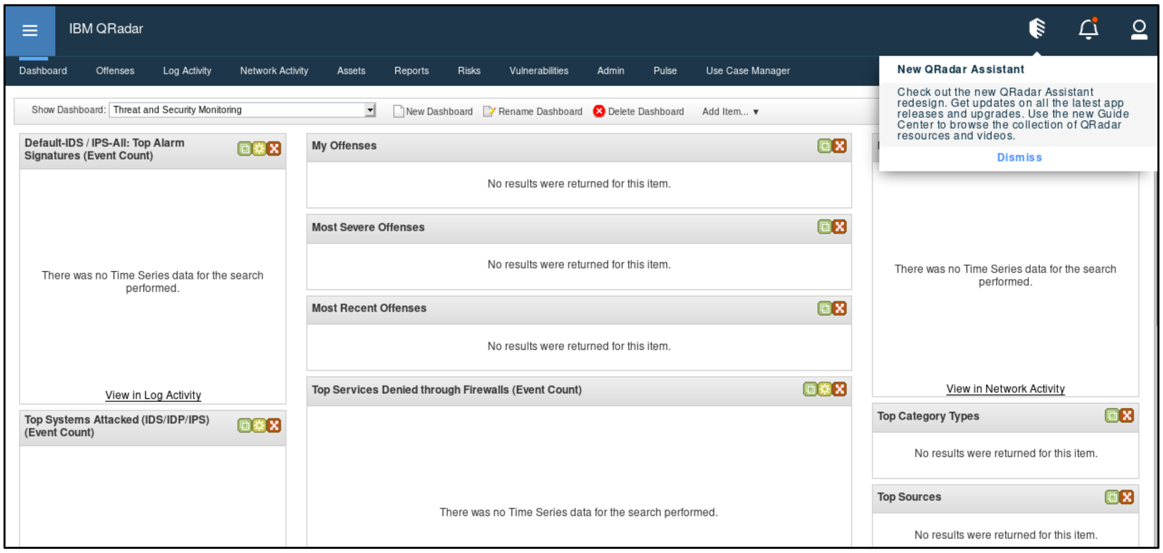
Enable Popup Notifications ✓

   b. Click **Save**.

Sending Sample Data to QRadar

In this exercise, you will become familiar with sending and process sample data in the Qradar. This Data will be useful for further exercises in this course.

1. Verify the Qradar VM is started and accessible from the GUI Virtual machine.
2. Log in the Qradar portal (https://10.10.9.30/console) use the procedure as outlined in the earlier section.
3. After logging in, you see a home dashboard screen like the below screenshot.



Check out the new QRadar Assistant redesign. Get updates on all the latest app releases and upgrades. Use the new Guide Center to browse the collection of QRadar resources and videos.

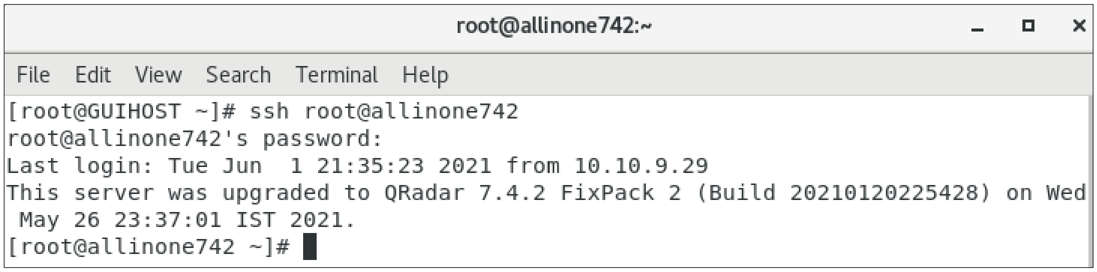
There was no Time Series data for the search performed.

No results were returned for this item.

4. Run the following command on SSH Terminal, to access the remote shell to the Qradar.

   ssh root@allinone742

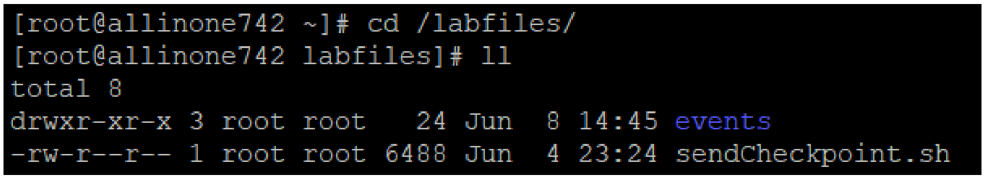
   Enter the password as ‘p@ssw0rd’



```
[root@GUIHOST ~]# ssh root@allinone742
root@allinone742's password:
Last login: Tue Jun  1 21:35:23 2021 from 10.10.9.29
This server was upgraded to QRadar 7.4.2 FixPack 2 (Build 20210120225428) on Wed
 May 26 23:37:01 IST 2021.
[root@allinone742 ~]# 
```

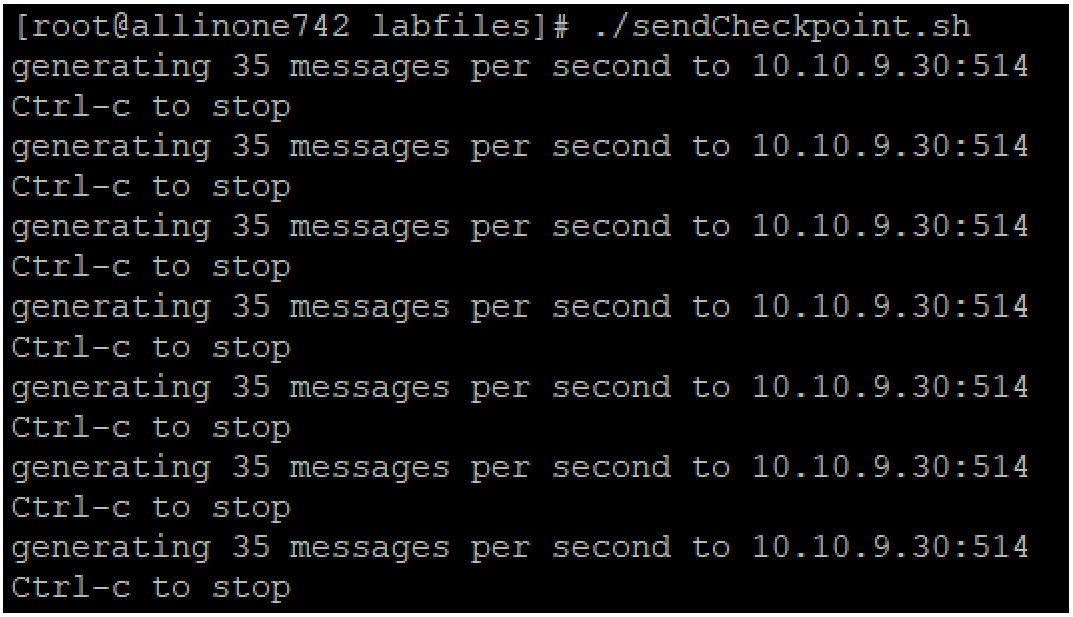
5. Run the following commands:

cd /labfiles



```
[root@allinone742 ~]# cd /labfiles/
[root@allinone742 labfiles]# ll
total 8
drwxr-xr-x 3 root root   24 Jun  8 14:45 events
-rw-r--r-- 1 root root 6488 Jun  4 23:24 sendCheckpoint.sh
```

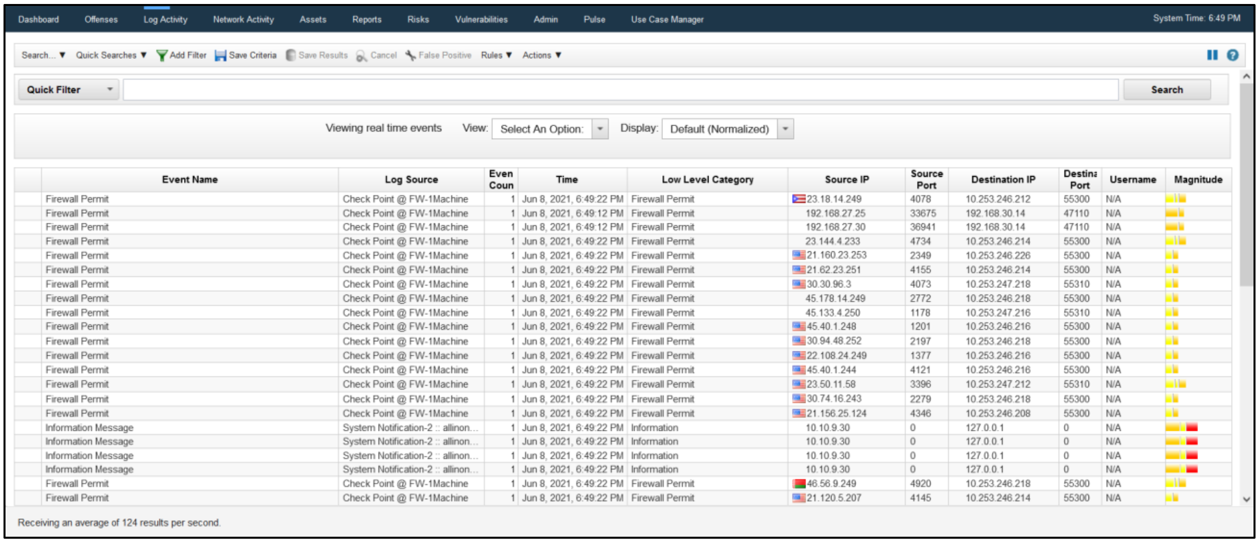
./sendCheckpoint.sh



```
[root@allinone742 labfiles]# ./sendCheckpoint.sh
generating 35 messages per second to 10.10.9.30:514
Ctrl-c to stop
generating 35 messages per second to 10.10.9.30:514
Ctrl-c to stop
generating 35 messages per second to 10.10.9.30:514
Ctrl-c to stop
generating 35 messages per second to 10.10.9.30:514
Ctrl-c to stop
generating 35 messages per second to 10.10.9.30:514
Ctrl-c to stop
generating 35 messages per second to 10.10.9.30:514
Ctrl-c to stop
generating 35 messages per second to 10.10.9.30:514
Ctrl-c to stop
```

This script runs for around 10 minutes. Do not close the terminal window.

6. Bring the browser to the front. One to two minutes after starting the script, dashboard items and the log activity tab start visualizing the sample data.



Viewing real time events View: Select An Option: Display: Default (Normalized)

	Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username	Magnitude
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	23.18.14.249	4078	10.253.246.212	55300	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:12 PM	Firewall Permit	192.168.27.25	33675	192.168.30.14	47110	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:12 PM	Firewall Permit	192.168.27.30	36941	192.168.30.14	47110	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	23.144.4.233	4734	10.253.246.214	55300	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	21.160.23.253	2349	10.253.246.226	55300	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	21.62.23.251	4155	10.253.246.214	55300	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	30.30.96.3	4073	10.253.247.218	55310	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	45.178.14.249	2772	10.253.246.218	55300	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	45.133.4.250	1178	10.253.247.216	55310	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	45.40.1.248	1201	10.253.246.216	55300	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	30.94.48.252	2197	10.253.246.218	55300	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	22.108.24.249	1377	10.253.246.216	55300	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	45.40.1.244	4121	10.253.246.216	55300	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	23.50.11.58	3396	10.253.247.212	55310	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	30.74.16.243	2279	10.253.246.218	55300	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	21.156.25.124	4346	10.253.246.208	55300	N/A	
	Information Message	System Notification-2 :: allinon...	1	Jun 8, 2021, 6:49:22 PM	Information	10.10.9.30	0	127.0.0.1	0	N/A	
	Information Message	System Notification-2 :: allinon...	1	Jun 8, 2021, 6:49:22 PM	Information	10.10.9.30	0	127.0.0.1	0	N/A	
	Information Message	System Notification-2 :: allinon...	1	Jun 8, 2021, 6:49:22 PM	Information	10.10.9.30	0	127.0.0.1	0	N/A	
	Information Message	System Notification-2 :: allinon...	1	Jun 8, 2021, 6:49:22 PM	Information	10.10.9.30	0	127.0.0.1	0	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	46.56.9.249	4920	10.253.246.218	55300	N/A	
	Firewall Permit	Check Point @ FW-1Machine	1	Jun 8, 2021, 6:49:22 PM	Firewall Permit	21.120.5.207	4145	10.253.246.214	55300	N/A	

Receiving an average of 124 results per second.

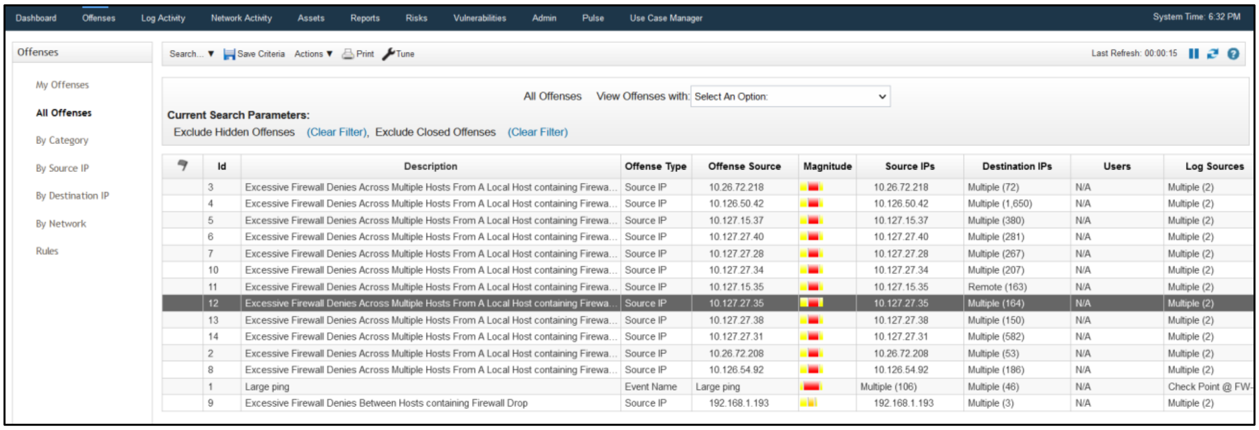
Lab 2 - Investigating the offense

In this Lab, We will try to investigate an offense triggered by events, we may have pushed in last lab.

We will look at the offense named “**Local DNS Scanner containing invalid DNS**” or “**Excessive Firewall Denies**”

Perform the below steps:

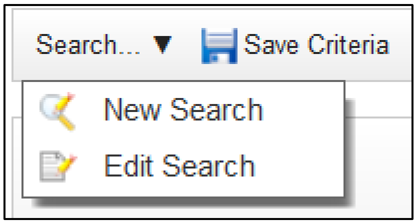
1. Login in the Qradar Interface, on Home page, Click the **Offenses** tab.



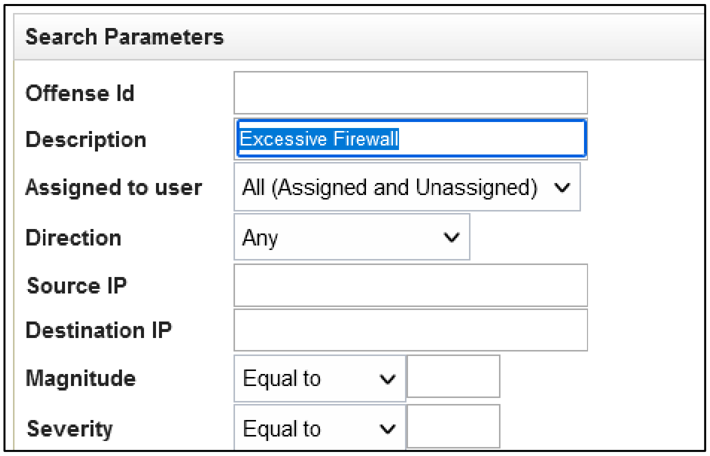
Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources
	3	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.26.72.218	▬	10.26.72.218	Multiple (72)	N/A	Multiple (2)
	4	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.126.50.42	▬	10.126.50.42	Multiple (1,650)	N/A	Multiple (2)
	5	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.15.37	▬	10.127.15.37	Multiple (380)	N/A	Multiple (2)
	6	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.40	▬	10.127.27.40	Multiple (281)	N/A	Multiple (2)
	7	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.28	▬	10.127.27.28	Multiple (267)	N/A	Multiple (2)
	10	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.34	▬	10.127.27.34	Multiple (207)	N/A	Multiple (2)
	11	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.15.35	▬	10.127.15.35	Remote (163)	N/A	Multiple (2)
	12	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.35	▬	10.127.27.35	Multiple (164)	N/A	Multiple (2)
	13	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.38	▬	10.127.27.38	Multiple (150)	N/A	Multiple (2)
	14	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.31	▬	10.127.27.31	Multiple (582)	N/A	Multiple (2)
	2	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.26.72.208	▬	10.26.72.208	Multiple (53)	N/A	Multiple (2)
	8	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.126.54.92	▬	10.126.54.92	Multiple (186)	N/A	Multiple (2)
	1	Large ping	Event Name	Large ping	▬	Multiple (106)	Multiple (46)	N/A	Check Point @ FW-
	9	Excessive Firewall Denies Between Hosts containing Firewall Drop	Source IP	192.168.1.193	▬	192.168.1.193	Multiple (3)	N/A	Multiple (2)

2. Select the Offense with the description **Local DNS Scanner containing Invalid DNS** or **Excessive Firewall Denies**
    a. If you are not able to the see the offense with this name, you may search of the offense.
    b. From the **Search** list, click **New Search**.



    c. In the Search parameters pane, define **Description** as any Keyword.



Search Parameters

Offense Id	
Description	Excessive Firewall
Assigned to user	All (Assigned and Unassigned)
Direction	Any
Source IP	
Destination IP	
Magnitude	Equal to
Severity	Equal to

d. Click **Search**.

The All Offenses page will the show the offenses that meets the search criteria.

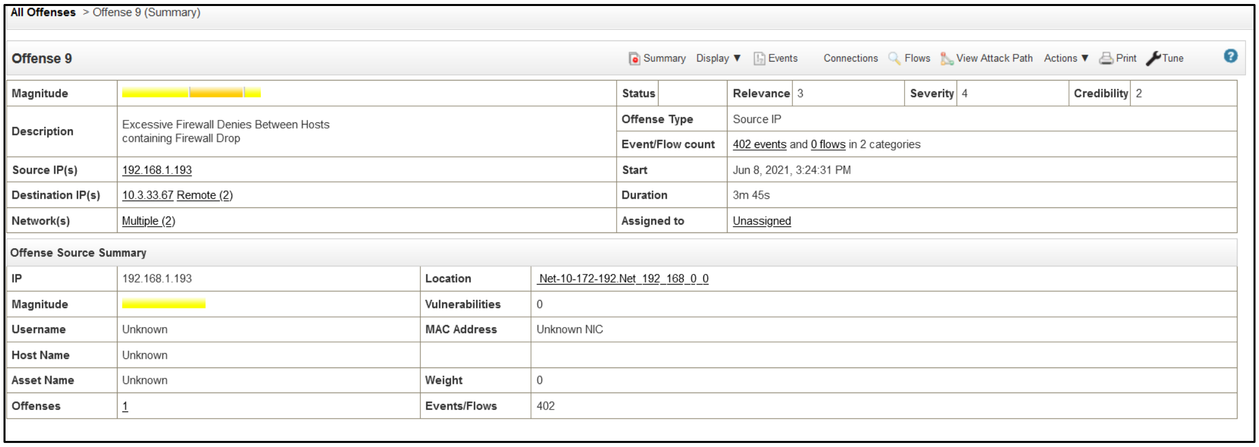
3. Answer the following questions for the selected offense.
   a. What is the offense type and offense source and magnitude?

   ____

   b. What Network does the offense source IP belong to?

   ____

4. Double click the offense to view the offense Summary page. This summary page provides detailed information about the offense.



Offense 9

Magnitude	🟨	Status		Relevance	3	Severity	4	Credibility	2
Description	Excessive Firewall Denies Between Hosts containing Firewall Drop	Offense Type	Source IP						
		Event/Flow count	402 events and 0 flows in 2 categories						
Source IP(s)	192.168.1.193	Start	Jun 8, 2021, 3:24:31 PM						
Destination IP(s)	10.3.33.67 Remote (2)	Duration	3m 45s						
Network(s)	Multiple (2)	Assigned to	Unassigned						

Offense Source Summary

IP	192.168.1.193	Location	Net-10-172-192.Net_192_168_0_0
Magnitude	🟨	Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	1	Events/Flows	402

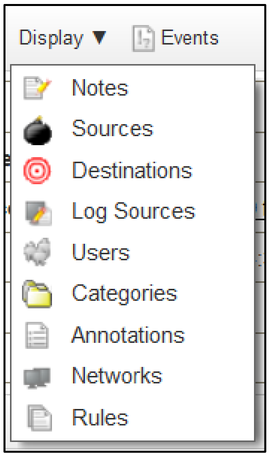
5. Answer the following questions for this offense.
    a. How many events or flows have been added to this offense?

    b. What time did this offense begin?

    c. Is the Source IP involved in any other offenses?

    d. How many destination IPS are targets o the offense? Are the destination Ips local or remote?

    e. List the categories of the events that contributed to this offense. From the **Display** drop-down list on the toolbar, select **Categories** to display the event categories.



---

f. What do you learn about this offense based on the annotation? From the **Display** drop-down list on the toolbar, select **Annotations**.

---

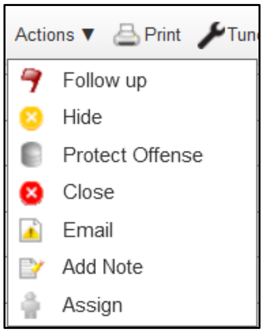
g. What is the event name, event category, and destination port for the events listed in the **Last 10 Events list**? Click Summary on the toolbar and scroll down to the Last 10 Events list.

---

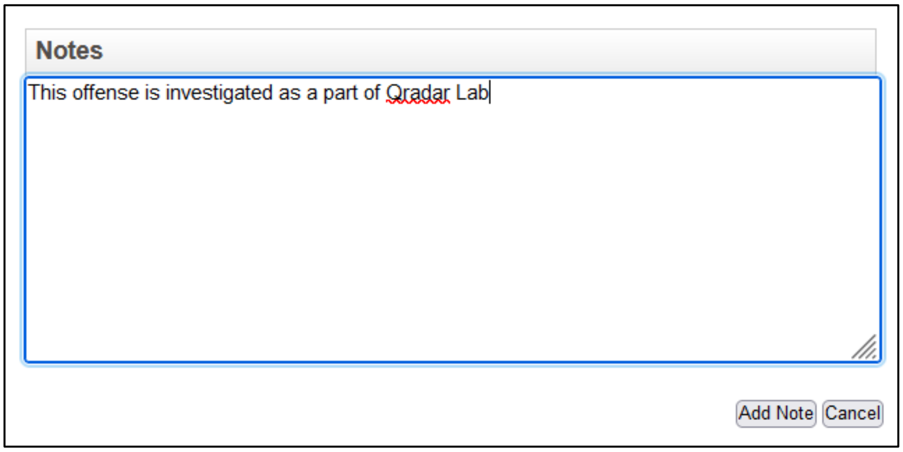
h. For which service is the destination port well known?

---

6. Perform the following actions on this offense.
   a. Add a note:
      i. From the **Actions** drop-down list, select **Add Note**.



ii. Enter “This offense is investigated as a part of Qradar Lab”

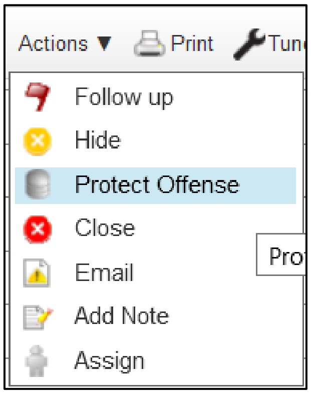


Notes

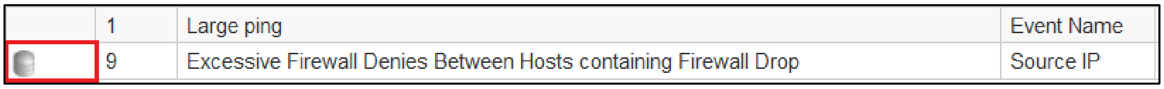
This offense is investigated as a part of Qradar Lab

iii. Click **Add Note**.

b. Protect the offense. From the **Actions** drop-down list on the Offense Summary page, select **Protect Offense**.



c. As a result, the **Protected** icon is displayed in the **Status** field on the Offense Summary page and in the flag column for the offense on the All Offenses page.



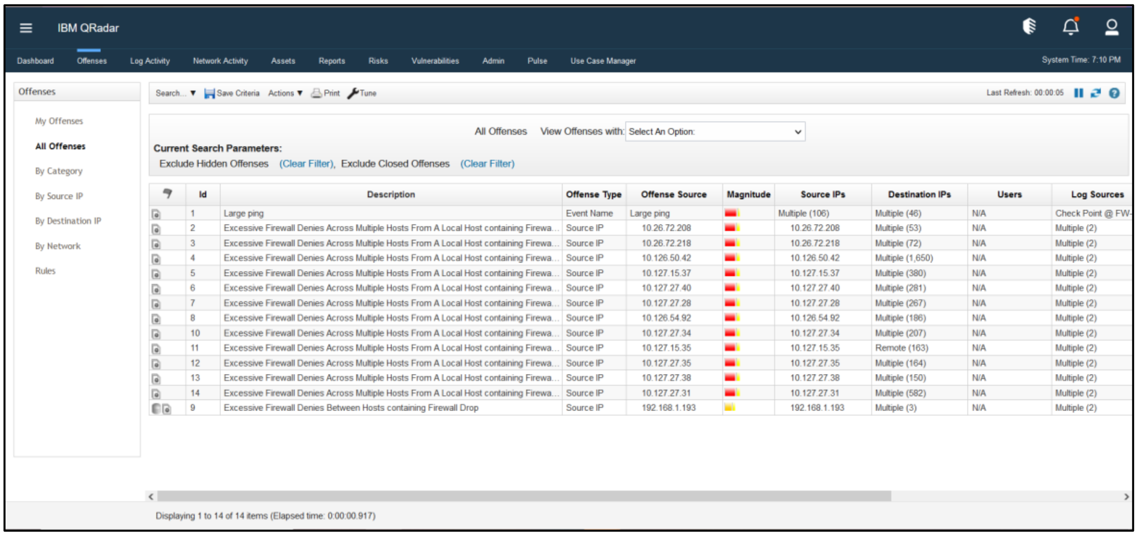
	1	Large ping	Event Name
	9	Excessive Firewall Denies Between Hosts containing Firewall Drop	Source IP

Lab 3 - Looking for events that contribute to an offense

In the previous lab exercise, we learnt about Investigating an offense. In this exercise, we will further analyze and explore the events that are contributed to any offense.

Perform the below steps:

1. Login in the Qradar Interface, on Home page, Click the **Offenses** tab. The All Offenses page opens.



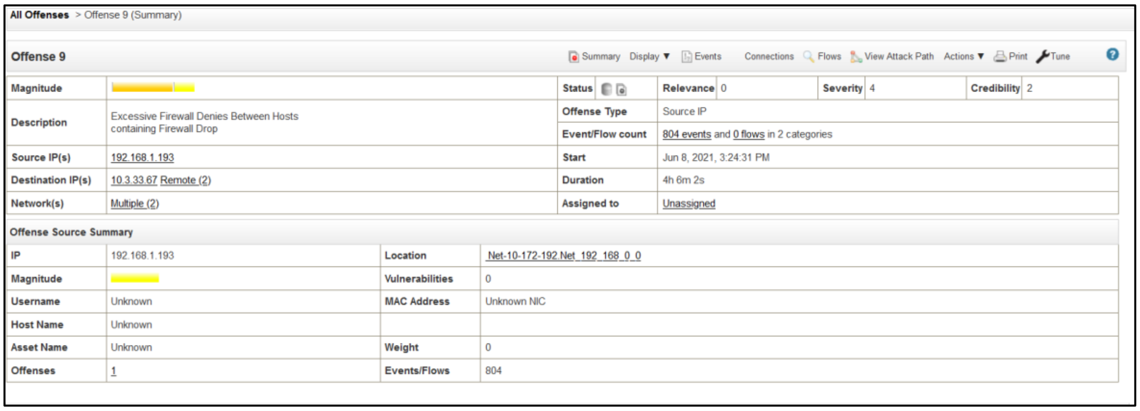
All Offenses View Offenses with: Select An Option:

Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources
1	Large ping	Event Name	Large ping	🟥	Multiple (106)	Multiple (46)	N/A	Check Point @ FW-
2	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.26.72.208	🟥	10.26.72.208	Multiple (53)	N/A	Multiple (2)
3	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.26.72.218	🟥	10.26.72.218	Multiple (72)	N/A	Multiple (2)
4	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.126.50.42	🟥	10.126.50.42	Multiple (1,650)	N/A	Multiple (2)
5	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.15.37	🟥	10.127.15.37	Multiple (380)	N/A	Multiple (2)
6	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.40	🟥	10.127.27.40	Multiple (281)	N/A	Multiple (2)
7	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.28	🟥	10.127.27.28	Multiple (267)	N/A	Multiple (2)
8	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.126.54.92	🟥	10.126.54.92	Multiple (186)	N/A	Multiple (2)
10	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.34	🟥	10.127.27.34	Multiple (207)	N/A	Multiple (2)
11	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.15.35	🟥	10.127.15.35	Remote (163)	N/A	Multiple (2)
12	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.35	🟥	10.127.27.35	Multiple (164)	N/A	Multiple (2)
13	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.38	🟥	10.127.27.38	Multiple (150)	N/A	Multiple (2)
14	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.31	🟥	10.127.27.31	Multiple (582)	N/A	Multiple (2)
9	Excessive Firewall Denies Between Hosts containing Firewall Drop	Source IP	192.168.1.193	🟨	192.168.1.193	Multiple (3)	N/A	Multiple (2)

Displaying 1 to 14 of 14 items (Elapsed time: 0:00:00.917)

2. Find and double-click the “**Excessive Firewall Denies between Hosts containing Firewall Drop**”.



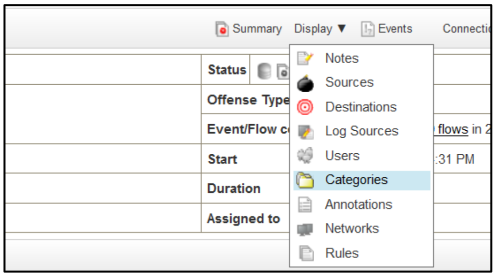
Offense 9

Magnitude	🟨	**Status**		**Relevance** 0	**Severity** 4	**Credibility** 2	
Description	Excessive Firewall Denies Between Hosts containing Firewall Drop	**Offense Type**	Source IP				
		Event/Flow count	804 events and 0 flows in 2 categories				
Source IP(s)	192.168.1.193	**Start**	Jun 8, 2021, 3:24:31 PM				
Destination IP(s)	10.3.33.67 Remote (2)	**Duration**	4h 6m 2s				
Network(s)	Multiple (2)	**Assigned to**	Unassigned				

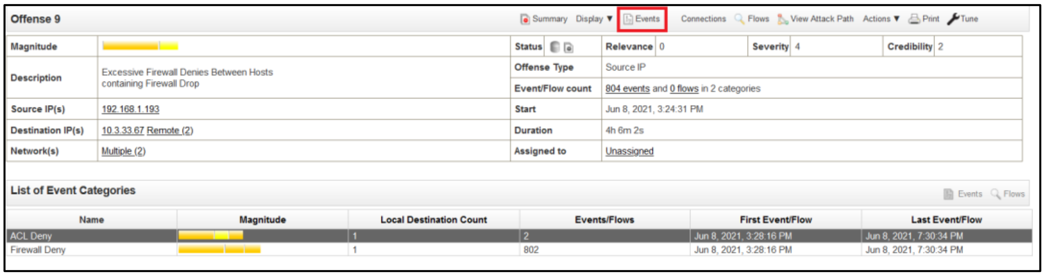
Offense Source Summary

IP	192.168.1.193	**Location**	Net-10-172-192.Net_192_168_0_0
Magnitude	🟨	**Vulnerabilities**	0
Username	Unknown	**MAC Address**	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	**Weight**	0
Offenses	1	**Events/Flows**	804

3. Show the low-level categories of the offense's events by selecting **Display > Categories** on the toolbar



4. To investigate the events that are associated with this offense in the low-level category, Right click the table row that shows the Event category and click **Events**.



Offense 9

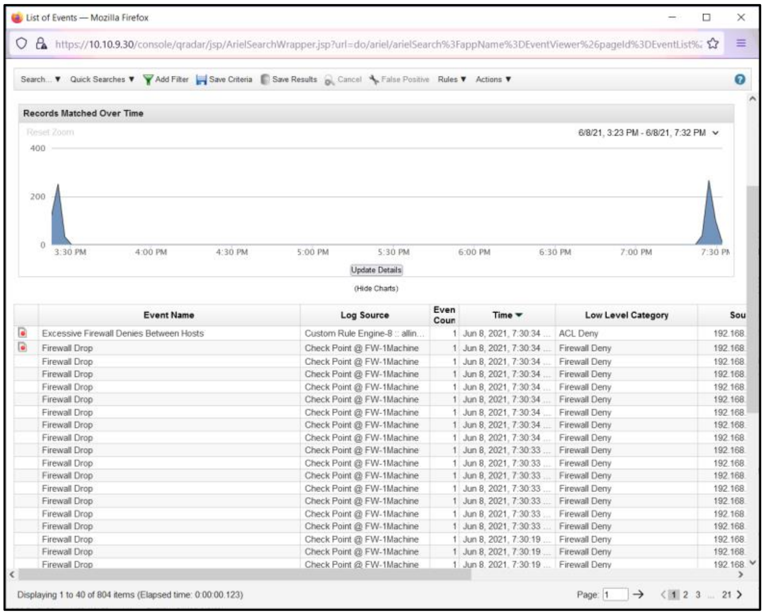
Magnitude		Status		Relevance	0	Severity 4	Credibility 2
Description	Excessive Firewall Denies Between Hosts containing Firewall Drop	Offense Type	Source IP				
		Event/Flow count	804 events and 0 flows in 2 categories				
Source IP(s)	192.168.1.193	Start	Jun 8, 2021, 3:24:31 PM				
Destination IP(s)	10.3.33.67 Remote (2)	Duration	4h 6m 2s				
Network(s)	Multiple (2)	Assigned to	Unassigned				

List of Event Categories

Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow	Last Event/Flow
ACL Deny		1	2	Jun 8, 2021, 3:28:16 PM	Jun 8, 2021, 7:30:34 PM
Firewall Deny		1	802	Jun 8, 2021, 3:28:16 PM	Jun 8, 2021, 7:30:34 PM

Note: You can select any of the event and category from the "**List of Event categories**" table.

The List of the events page opens.

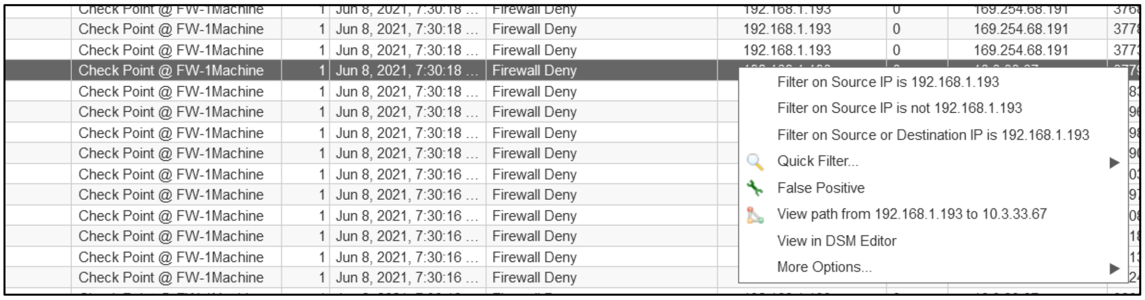

List of Events — Mozilla Firefox
https://10.10.9.30/console/qradar/jsp/ArielSearchWrapper.jsp?url=do/ariel/arielSearch%3FappName%3DEventViewer%26pageId%3DEventList%
Search... ▼
Quick Searches ▼
Add Filter
Save Criteria
Save Results
Cancel
False Positive
Rules ▼
Actions ▼
Records Matched Over Time
Reset Zoom
6/8/21, 3:23 PM - 6/8/21, 7:32 PM
400
200
0
3:30 PM
4:00 PM
4:30 PM
5:00 PM
5:30 PM
6:00 PM
6:30 PM
7:00 PM
7:30 PM
Update Details
(Hide Charts)

Event Name	Log Source	Even Coun	Time ▼	Low Level Category	Sou
Excessive Firewall Denies Between Hosts	Custom Rule Engine-8 :: allin...	1	Jun 8, 2021, 7:30:34 ...	ACL Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:19 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:19 ...	Firewall Deny	192.168.
Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:19 ...	Firewall Deny	192.168.

Displaying 1 to 40 of 804 items (Elapsed time: 0:00:00.123)

Page: 1 → ‹ 1 2 3 ... 21 ›

5. Create a filter to exclude the source IP that contributed to the offense.
    - Select an event, Right click on **<IP Address>** and select **Filter on Source IP is not <IP Address>**.



Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny	192.168.1.193	0	169.254.68.191	376
Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny	192.168.1.193	0	169.254.68.191	377
Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny	192.168.1.193	0	169.254.68.191	377
Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny				
Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny				83
Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny				96
Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny				98
Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny				90
Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:16 ...	Firewall Deny				03
Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:16 ...	Firewall Deny				97
Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:16 ...	Firewall Deny				08
Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:16 ...	Firewall Deny				18
Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:16 ...	Firewall Deny				13
Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:16 ...	Firewall Deny				24

Filter on Source IP is 192.168.1.193
Filter on Source IP is not 192.168.1.193
Filter on Source or Destination IP is 192.168.1.193
Quick Filter... ▶
False Positive
View path from 192.168.1.193 to 10.3.33.67
View in DSM Editor
More Options... ▶

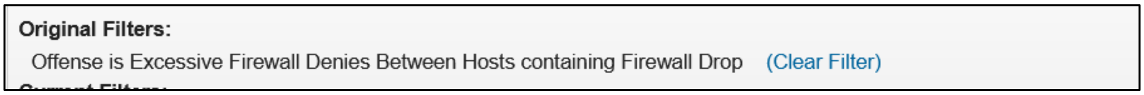
6. What results are returned?

____

7. What do the results of this search indicate?

____

8. To look for similar other events unrelated to the particular offense, click Clear Filter for the Offense is "**Excessive Firewall Denies between Hosts containing Firewall Drop**".



Original Filters:
Offense is Excessive Firewall Denies Between Hosts containing Firewall Drop (Clear Filter)

What results are returned? Why?

____

9. Select **Last 24 Hours** to view events from the last 24 hours, in the View drop-down list.

Explore other search filters and options. You can also save the filter criteria by following the below steps.

1. Save the current search criteria
    a. On the Toolbar, click **Save Criteria.**
    b. Configure the Save Criteria window as shown below

➢ Search Name	Firewall Deny events
➢ Assign Search to group(s)	Disable
➢ Timespan options	Recent last 24 hours
➢ Include in my Quick Searches	Enable
➢ Set as Default	Disable
➢ Share with Everyone	Disable

   c. Review the Save Criteria and Click **OK**.

2. Save the current search results.
   a. On the toolbar, click **Save Results**.
   b. Enter the name in the name field.
   c. Click **Ok**.
3. Revisit or delete your saved search results.
   a. On the list of events page’s toolbar, click **Search > Manage Search Results**.
   b. In the Search Results management page, select your search results and click Delete.
   c. Close the Search Results Management page

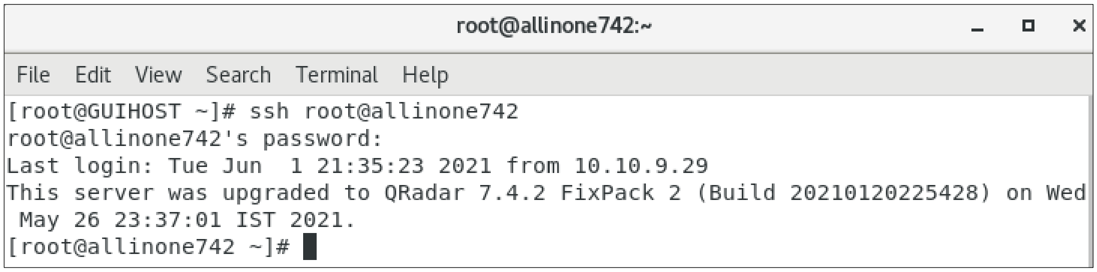
Lab 4 - Investigating an offense that is triggered by flows

Follow the below steps to investigate an offense that is triggered by flows.

1. Run the following command on SSH Terminal, to access the remote shell to the Qradar.

   ssh root@allinone742

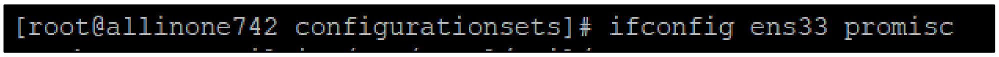
   Enter the password as ‘p@ssw0rd’



```
[root@GUIHOST ~]# ssh root@allinone742
root@allinone742's password:
Last login: Tue Jun  1 21:35:23 2021 from 10.10.9.29
This server was upgraded to QRadar 7.4.2 FixPack 2 (Build 20210120225428) on Wed
 May 26 23:37:01 IST 2021.
[root@allinone742 ~]#
```

2. Run the following commands:

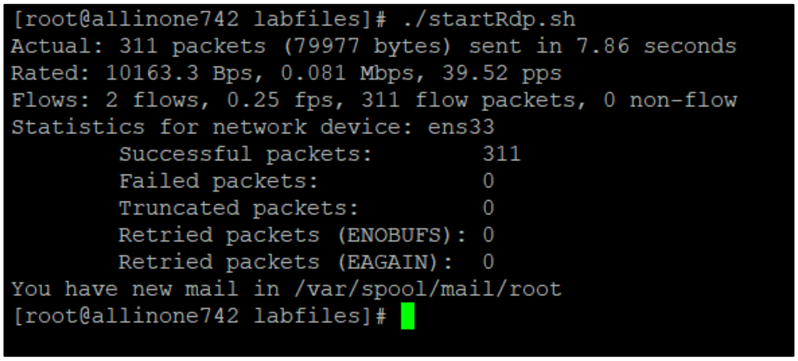
   inconfig ens33 promisc



```
[root@allinone742 configurationsets]# ifconfig ens33 promisc
```

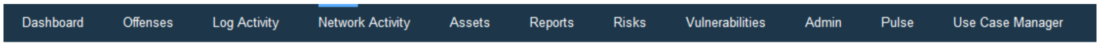
   cd /labfiles

   ./startRdp.sh

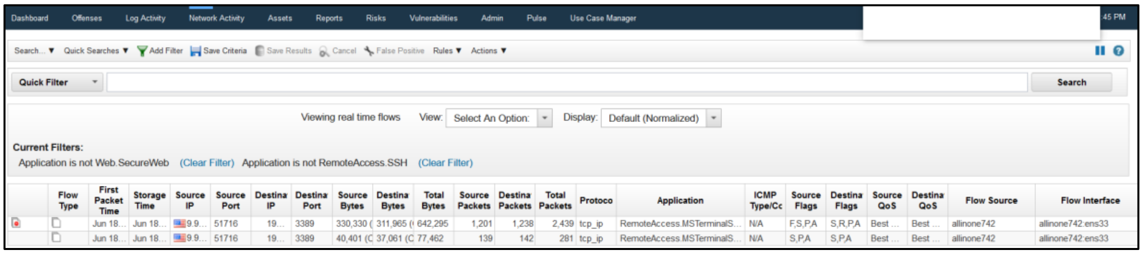


```
[root@allinone742 labfiles]# ./startRdp.sh
Actual: 311 packets (79977 bytes) sent in 7.86 seconds
Rated: 10163.3 Bps, 0.081 Mbps, 39.52 pps
Flows: 2 flows, 0.25 fps, 311 flow packets, 0 non-flow
Statistics for network device: ens33
        Successful packets:        311
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
You have new mail in /var/spool/mail/root
[root@allinone742 labfiles]#
```

3. In the Qradar user interface, navigate to the Network Activity tab.



4. Observe the network activity and verify that a network activity triggers and offense.



Viewing real time flows View: Select An Option: Display: Default (Normalized)

Current Filters:
Application is not Web.SecureWeb (Clear Filter) Application is not RemoteAccess.SSH (Clear Filter)

	Flow Type	First Packet Time	Storage Time	Source IP	Source Port	Destina IP	Destina Port	Source Bytes	Destina Bytes	Total Bytes	Source Packets	Destina Packets	Total Packets	Protoco	Application	ICMP Type/Cc	Source Flags	Destina Flags	Source QoS	Destina QoS	Flow Source	Flow Interface
●	□	Jun 18...	Jun 18...	9.9...	51716	19...	3389	330,330 (	311,965 ((	642,295	1,201	1,238	2,439	tcp_ip	RemoteAccess.MSTerminalS...	N/A	F,S,P,A	S,R,P,A	Best ...	Best ...	allinone742	allinone742:ens33
	□	Jun 18...	Jun 18...	9.9...	51716	19...	3389	40,401 (C	37,061 (C	77,462	139	142	281	tcp_ip	RemoteAccess.MSTerminalS...	N/A	S,P,A	S,P,A	Best ...	Best ...	allinone742	allinone742:ens33

5. To investigate the offense, click the red icon in the left-most column. Red Icon in the left most column signifies the flows that contribute to an offense.
6. The Offense Summary page opens.
7. What is the name of the offense, Offense Type, Offense Source and Destination IP?

8. How many events or Flows are associated with this offense?

9. Which Rule added events or flows to this offense?

To investigate the flows that contributed to the offense. Follow the below steps.

1. Click **Flows** on the Offense Summary page toolbar
   The Flow List page opens.
2. Examine the Flow associated with this offense. Double-Click on the flow listed.
3. Answer the flowing questions:
   a. What is the flow direction?

____

b. What is the Application name?

____

c. Which Activity triggered this offense?

____

4. Tune the flow as a false positive.
    a. On the Flow details page’s toolbar, click **False Positive**.
    b. Click **Tune**.
    c. Click **Close**.
5. Close the offense.
    a. On the **Offense** tab navigation menu, select **All Offenses**.
    b. From the **Actions** drop-down list on the toolbar, select **Close**.
    c. From the **Reason for Closing** list, select **False-Positive, Tuned**.
    d. Click **OK**.

Lab 5 - Using rules

In this lab, we will create Rules to monitor the Login Activity. Below is the use case.

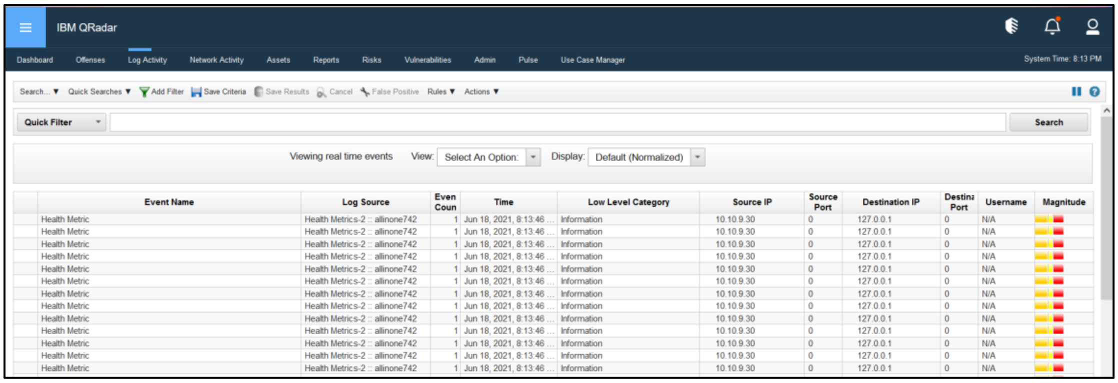
An Organization wants to monitor the user accounts of terminated employees.

a. Create a rule to generate offenses for invalid login activities.
b. Reference set should be used to store and look up for the usernames of terminated employees.

Create an Event Rule

Perform the below steps in this lab.

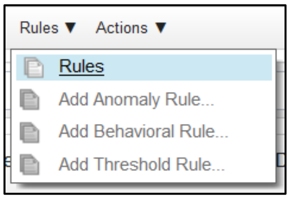
1. Login in the Qradar Interface, on Home page, Click the **Log Activity** tab.



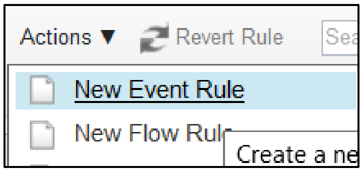
Viewing real time events View: Select An Option: Display: Default (Normalized)

	Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username	Magnitude
	Health Metric	Health Metrics-2 :: allinone742	1	Jun 18, 2021, 8:13:46 ...	Information	10.10.9.30	0	127.0.0.1	0	N/A	🟨🟥
	Health Metric	Health Metrics-2 :: allinone742	1	Jun 18, 2021, 8:13:46 ...	Information	10.10.9.30	0	127.0.0.1	0	N/A	🟨🟥
	Health Metric	Health Metrics-2 :: allinone742	1	Jun 18, 2021, 8:13:46 ...	Information	10.10.9.30	0	127.0.0.1	0	N/A	🟨🟥
	Health Metric	Health Metrics-2 :: allinone742	1	Jun 18, 2021, 8:13:46 ...	Information	10.10.9.30	0	127.0.0.1	0	N/A	🟨🟥
	Health Metric	Health Metrics-2 :: allinone742	1	Jun 18, 2021, 8:13:46 ...	Information	10.10.9.30	0	127.0.0.1	0	N/A	🟨🟥
	Health Metric	Health Metrics-2 :: allinone742	1	Jun 18, 2021, 8:13:46 ...	Information	10.10.9.30	0	127.0.0.1	0	N/A	🟨🟥
	Health Metric	Health Metrics-2 :: allinone742	1	Jun 18, 2021, 8:13:46 ...	Information	10.10.9.30	0	127.0.0.1	0	N/A	🟨🟥
	Health Metric	Health Metrics-2 :: allinone742	1	Jun 18, 2021, 8:13:46 ...	Information	10.10.9.30	0	127.0.0.1	0	N/A	🟨🟥
	Health Metric	Health Metrics-2 :: allinone742	1	Jun 18, 2021, 8:13:46 ...	Information	10.10.9.30	0	127.0.0.1	0	N/A	🟨🟥
	Health Metric	Health Metrics-2 :: allinone742	1	Jun 18, 2021, 8:13:46 ...	Information	10.10.9.30	0	127.0.0.1	0	N/A	🟨🟥
	Health Metric	Health Metrics-2 :: allinone742	1	Jun 18, 2021, 8:13:46 ...	Information	10.10.9.30	0	127.0.0.1	0	N/A	🟨🟥
	Health Metric	Health Metrics-2 :: allinone742	1	Jun 18, 2021, 8:13:46 ...	Information	10.10.9.30	0	127.0.0.1	0	N/A	🟨🟥
	Health Metric	Health Metrics-2 :: allinone742	1	Jun 18, 2021, 8:13:46 ...	Information	10.10.9.30	0	127.0.0.1	0	N/A	🟨🟥

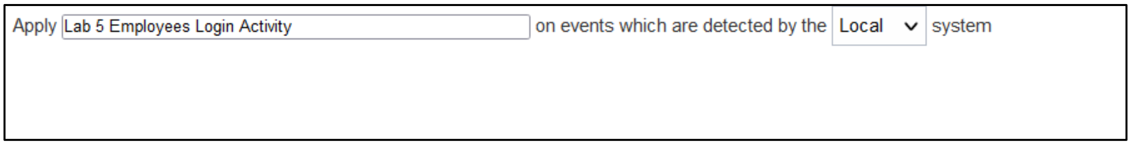
2. From the **Rules** drop-down menu, select **Rules.**



3. From the **Actions** Drop-down menu, select **New Event Rule**.

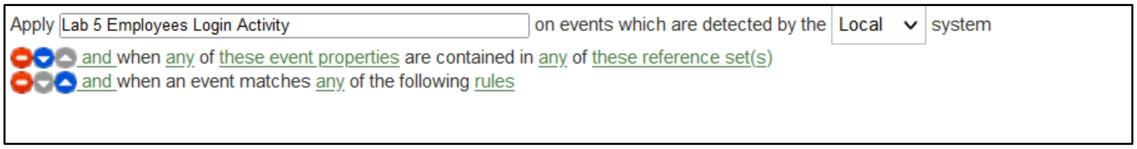


4. In the Rules Wizard window, click **Next** twice.
5. In the Rule Test Stack Editor Window, Enter the following name in the rule name field.
   Lab 5 Employees Login Activity



Apply Lab 5 Employees Login Activity on events which are detected by the Local system

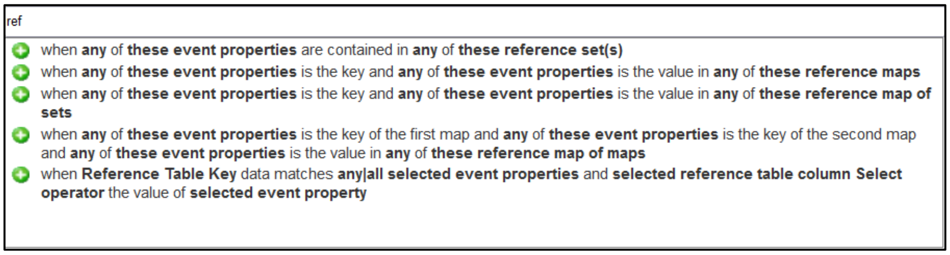
6. Add the following tests by clicking ⊕ to the rule under these conditions:
   - when any of these event properties are contained in any of these reference set(s)
   - when an event matches any|all of the following rules



Apply Lab 5 Employees Login Activity on events which are detected by the Local system
and when any of these event properties are contained in any of these reference set(s)
and when an event matches any of the following rules

To add the first rule test, when any of these event properties are contained in any of these reference set(s), perform the following steps:

i. Filter the options in the **Test Group** list. For **Type to filter**, enter *ref*



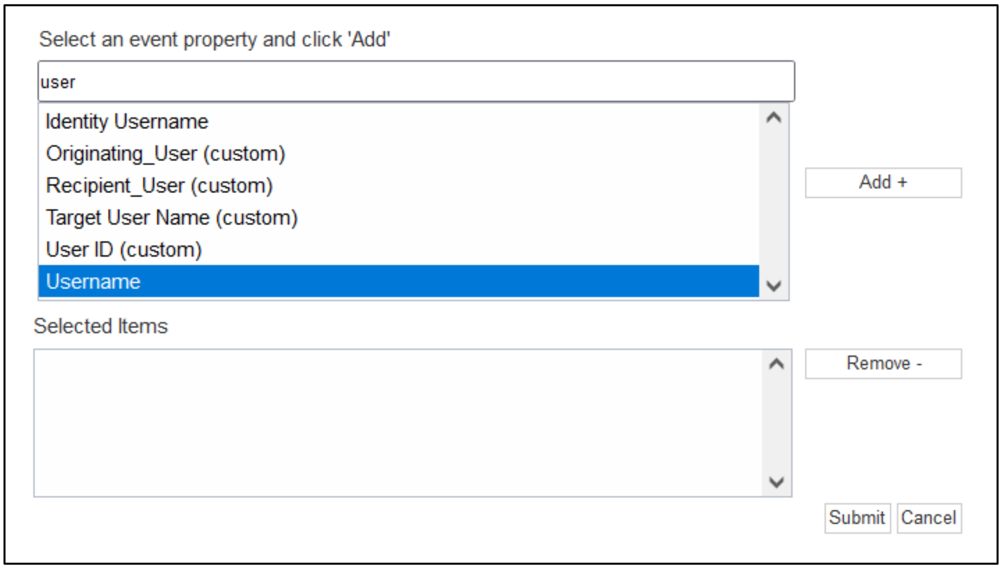
ref

⊕ when **any** of **these event properties** are contained in **any** of **these reference set(s)**
⊕ when **any** of **these event properties** is the key and **any** of **these event properties** is the value in **any** of **these reference maps**
⊕ 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**
⊕ when **any** of **these event properties** is the key of the first map and **any** of **these event properties** is the key of the second map and **any** of **these event properties** is the value in **any** of **these reference map of maps**
⊕ when **Reference Table Key** data matches **any|all selected event properties** and **selected reference table column Select operator** the value of **selected event property**

ii. Click the green **plus (+)** ⊕ icon next to the when any of these event properties are contained in any of these reference set(s) test.

iii. Click the parameter **these event properties**.

iv. Filter the fields in the event property list. In the **Type to filter** field, enter user.



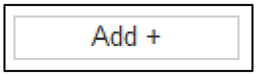
Select an event property and click 'Add'

user

Identity Username
Originating_User (custom)
Recipient_User (custom)
Target User Name (custom)
User ID (custom)
Username

Selected Items

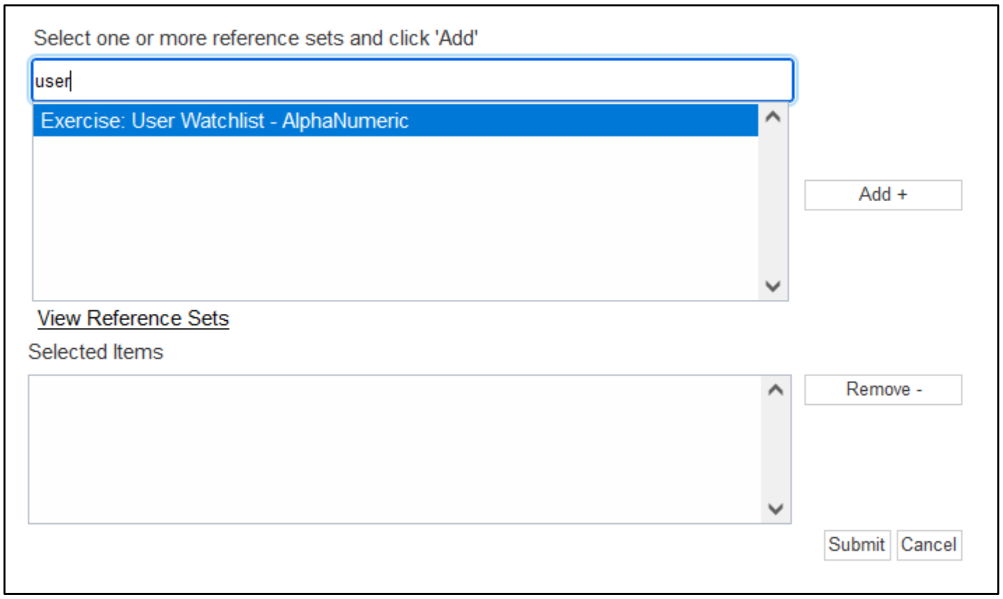
v. Select **Username** and click **Add**.



vi. Click **Submit**.

vii. Click the parameter **these reference set(s)**.

viii. Select the reference set **Exercise: User Watchlist** and click **Add** and Click **Submit**.



Select one or more reference sets and click 'Add'

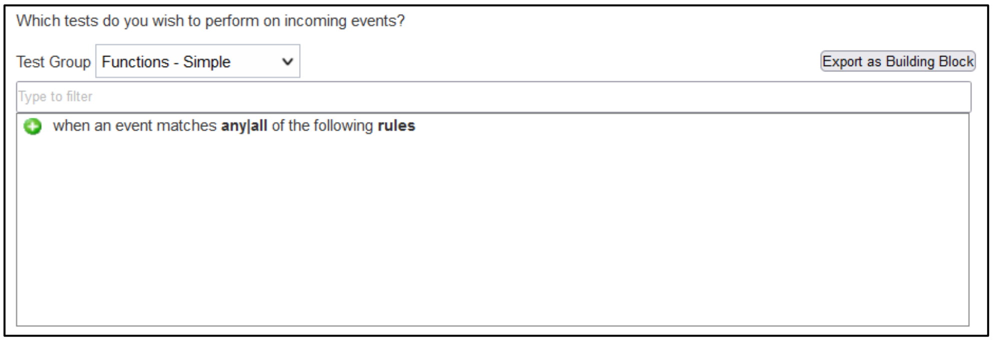
user

Exercise: User Watchlist - AlphaNumeric

View Reference Sets

Selected Items

7. To add the second rule test, when an event matches any | all of the following rules, perform the following steps:
   i. In the **Test Group** drop-down list, select **Functions - Simple**.
   ii. Click the **green plus (+)** icon next to the only test listed.

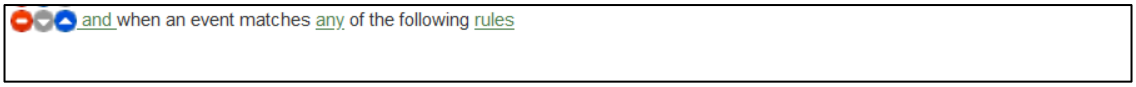


Which tests do you wish to perform on incoming events?

Test Group: Functions - Simple

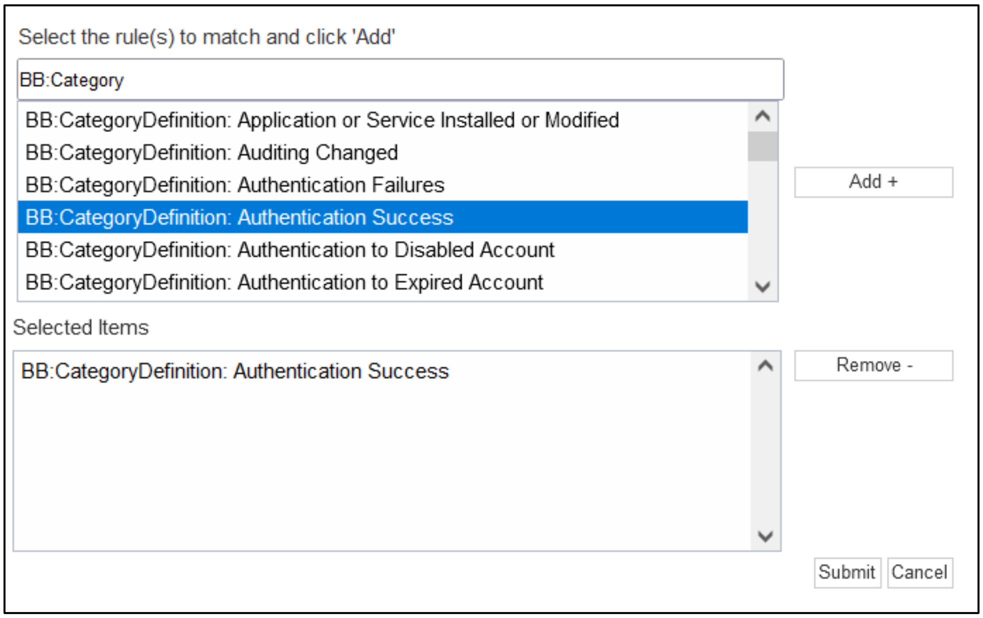
when an event matches **any|all** of the following **rules**

   iii. Click the parameter **rules**.



and when an event matches any of the following rules

   iv. Filter the options in the rules list. In the **Type to filter** field, enter the following text:
   BB: Category
   v. Select **BB: Category Definition: Authentication Success** and click **Add**, and Click Submit.



Select the rule(s) to match and click 'Add'

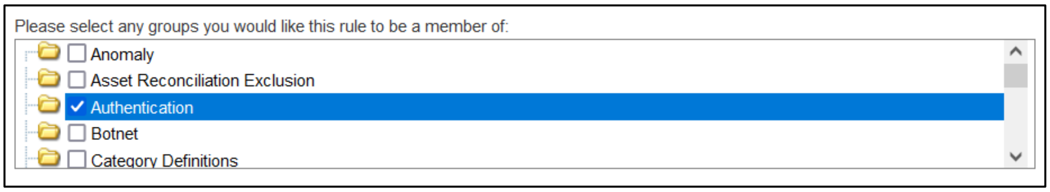
BB:Category

BB:CategoryDefinition: Application or Service Installed or Modified
BB:CategoryDefinition: Auditing Changed
BB:CategoryDefinition: Authentication Failures
BB:CategoryDefinition: Authentication Success
BB:CategoryDefinition: Authentication to Disabled Account
BB:CategoryDefinition: Authentication to Expired Account

Selected Items

BB:CategoryDefinition: Authentication Success

8. Assign the rule to the group **Authentication**.

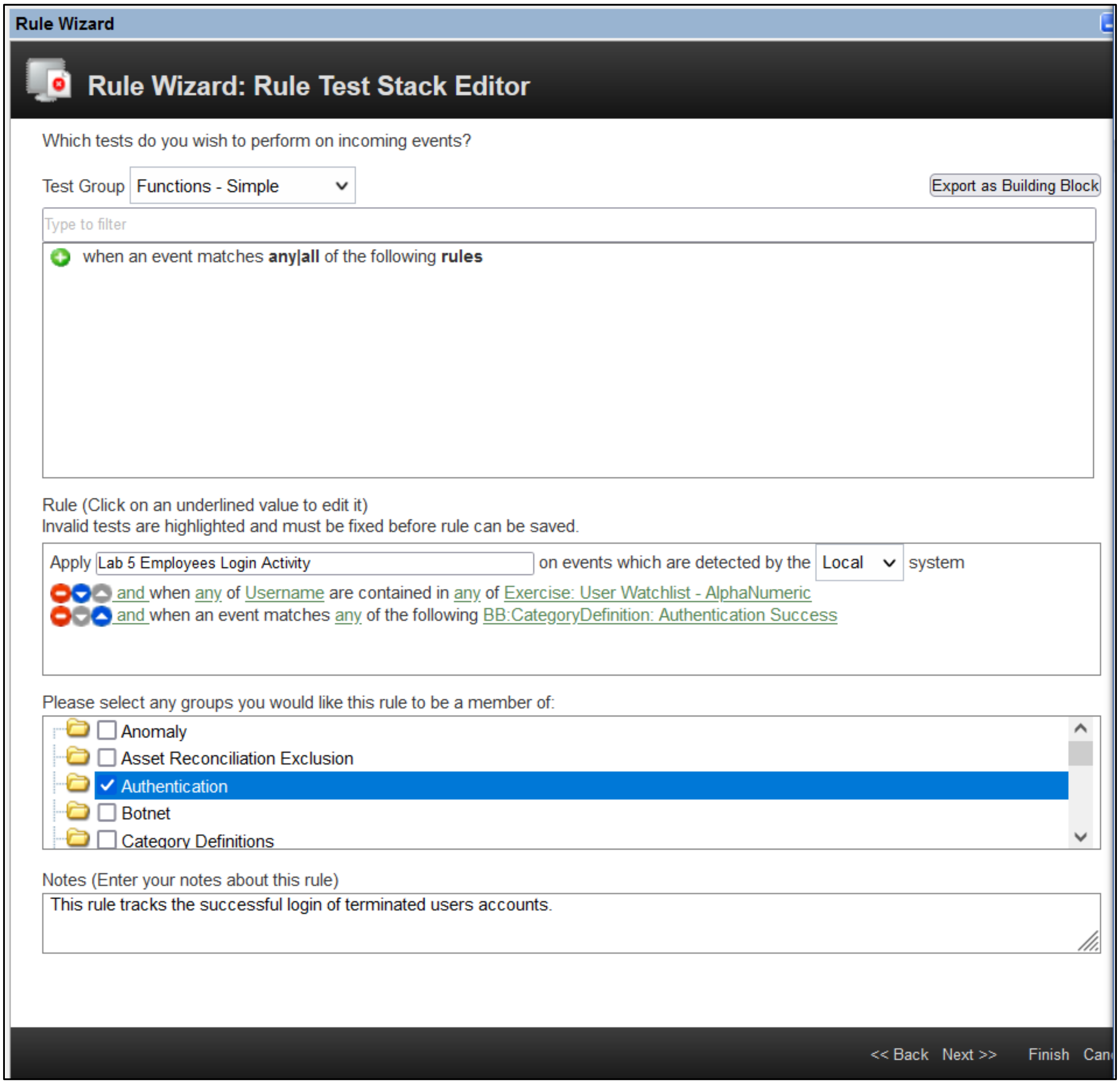


Please select any groups you would like this rule to be a member of:

- ☐ Anomaly
- ☐ Asset Reconciliation Exclusion
- ☑ Authentication
- ☐ Botnet
- ☐ Category Definitions

9. To document the rule in the **Notes** field, enter the following text. *This rule tracks the successful login of terminated users accounts.*

10. Click **Next**.



Rule Wizard

Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group: Functions - Simple

when an event matches **any|all** of the following **rules**

Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply Lab 5 Employees Login Activity on events which are detected by the Local system
and when any of Username are contained in any of Exercise: User Watchlist - AlphaNumeric
and when an event matches any of the following BB:CategoryDefinition: Authentication Success

Please select any groups you would like this rule to be a member of:

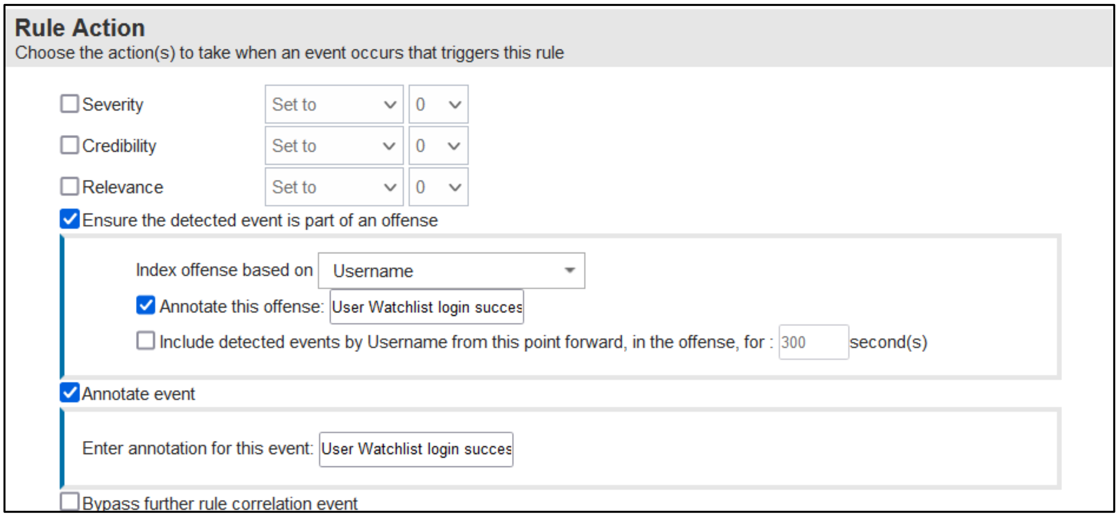
- ☐ Anomaly
- ☐ Asset Reconciliation Exclusion
- ☑ Authentication
- ☐ Botnet
- ☐ Category Definitions

Notes (Enter your notes about this rule)
This rule tracks the successful login of terminated users accounts.

11. Configure the rule action and response as shown below

Rule Action

- Ensure the detected event is part of an offense: **enable**
- Index offense based on list: **Username**
- Annotate this offense: **enable, User Watchlist login success**
- Annotate event: **enable, User Watchlist login success**



Rule Action

Choose the action(s) to take when an event occurs that triggers this rule

□ Severity Set to 0

□ Credibility Set to 0

□ Relevance Set to 0

☑ Ensure the detected event is part of an offense

Index offense based on Username

☑ Annotate this offense: User Watchlist login succes

□ Include detected events by Username from this point forward, in the offense, for : 300 second(s)

☑ Annotate event

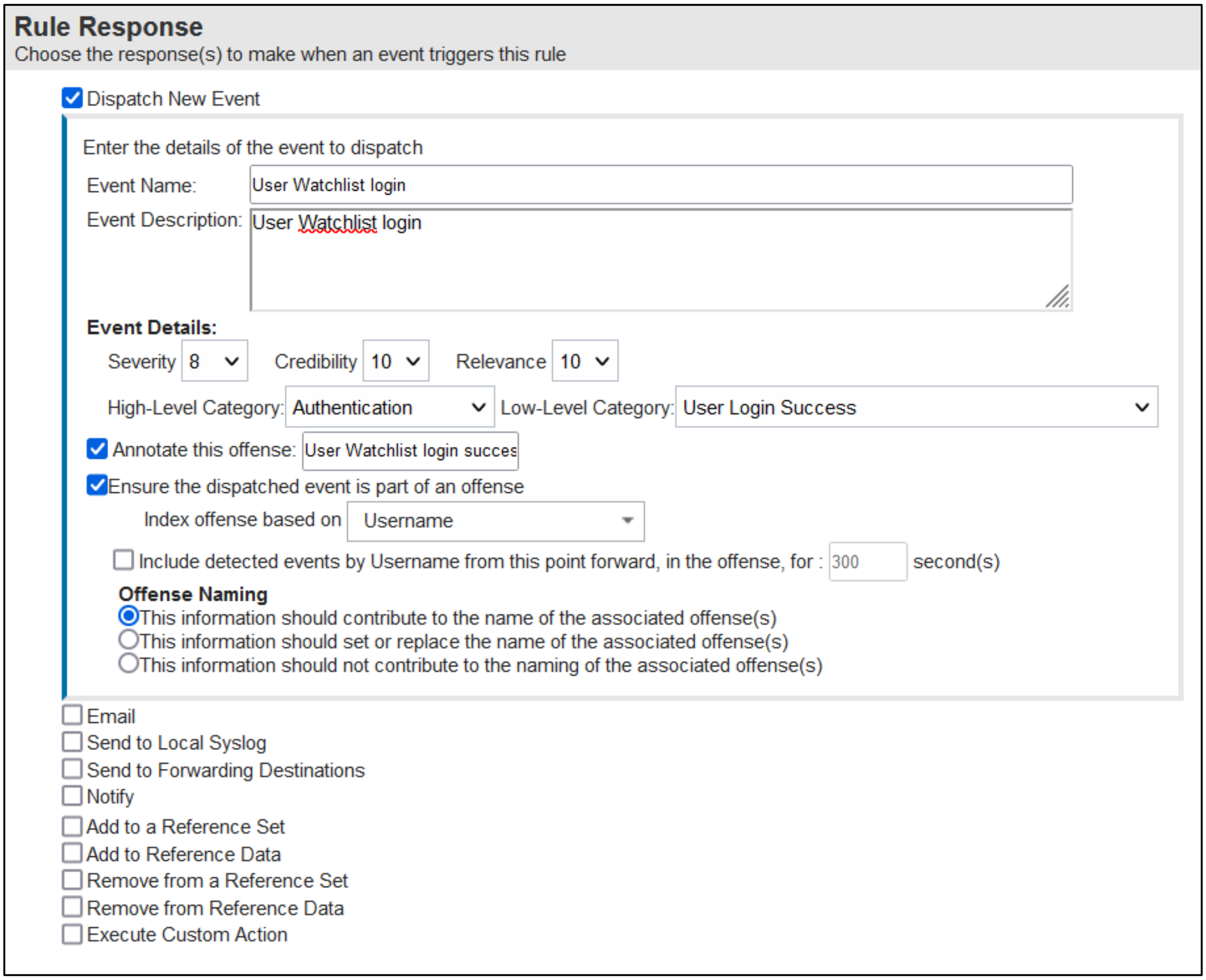
Enter annotation for this event: User Watchlist login succes

□ Bypass further rule correlation event

Rule Response

- Dispatch New Event: **enable**
- Type Event Name: **User Watchlist login**
- Type Event Description: **User Watchlist login**
- Severity: **8**
- Credibility: **10**
- Relevance: **10**
- High Level Category: **Authentication**
- Low Level Category: **User Login Success**
- Annotate this offense: **enable, User Watchlist login success**
- Ensure the dispatched event is part of an offense: **enable**
- Index offense based on: **Username**

- This information should contribute to the naming of the associated offense(s): **enable**



Rule Response

Choose the response(s) to make when an event triggers this rule

☑ Dispatch New Event

Enter the details of the event to dispatch

Event Name: User Watchlist login

Event Description: User Watchlist login

Event Details:

Severity 8 · Credibility 10 · Relevance 10

High-Level Category: Authentication · Low-Level Category: User Login Success

☑ Annotate this offense: User Watchlist login succes

☑ Ensure the dispatched event is part of an offense

Index offense based on Username

□ Include detected events by Username from this point forward, in the offense, for : 300 second(s)

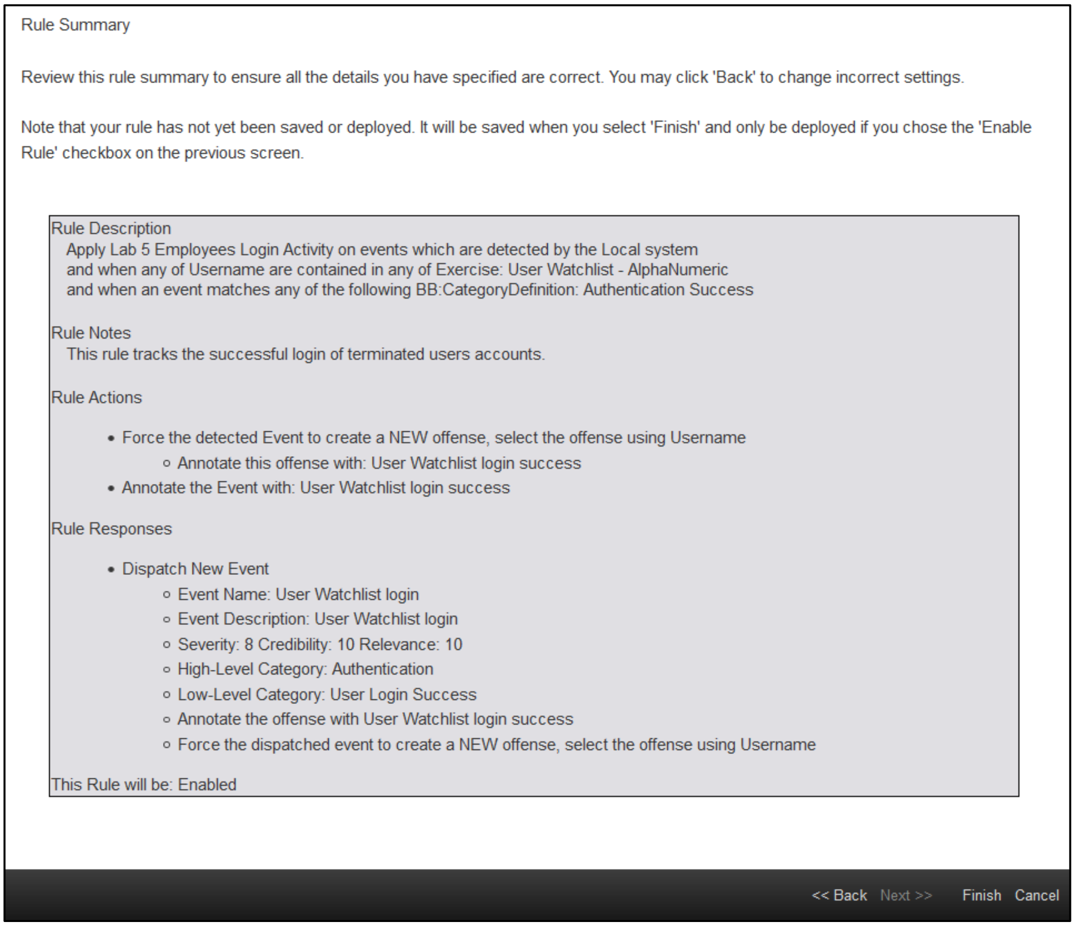
Offense Naming

● This information should contribute to the name of the associated offense(s)
○ This information should set or replace the name of the associated offense(s)
○ This information should not contribute to the naming of the associated offense(s)

□ Email
□ Send to Local Syslog
□ Send to Forwarding Destinations
□ Notify
□ Add to a Reference Set
□ Add to Reference Data
□ Remove from a Reference Set
□ Remove from Reference Data
□ Execute Custom Action

12. Click Next.

13. Verify that your rule summary looks similar to the one in the screen capture and click Finish


Rule Summary

Review this rule summary to ensure all the details you have specified are correct. You may click 'Back' to change incorrect settings.

Note that your rule has not yet been saved or deployed. It will be saved when you select 'Finish' and only be deployed if you chose the 'Enable Rule' checkbox on the previous screen.

Rule Description
Apply Lab 5 Employees Login Activity on events which are detected by the Local system
and when any of Username are contained in any of Exercise: User Watchlist - AlphaNumeric
and when an event matches any of the following BB:CategoryDefinition: Authentication Success

Rule Notes
This rule tracks the successful login of terminated users accounts.

Rule Actions

- Force the detected Event to create a NEW offense, select the offense using Username
  - Annotate this offense with: User Watchlist login success
- Annotate the Event with: User Watchlist login success

Rule Responses

- Dispatch New Event
  - Event Name: User Watchlist login
  - Event Description: User Watchlist login
  - Severity: 8 Credibility: 10 Relevance: 10
  - High-Level Category: Authentication
  - Low-Level Category: User Login Success
  - Annotate the offense with User Watchlist login success
  - Force the dispatched event to create a NEW offense, select the offense using Username

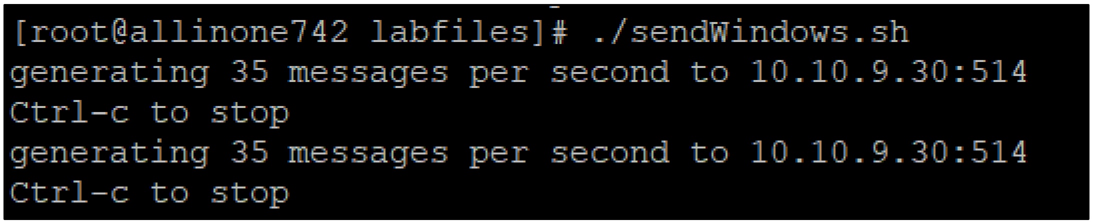
This Rule will be: Enabled

14. Open a remote shell to the QRadar VM. Use the procedure as outlined in Running commands on the QRadar VM.

15. To feed prepared syslog messages to QRadar, run the following commands:

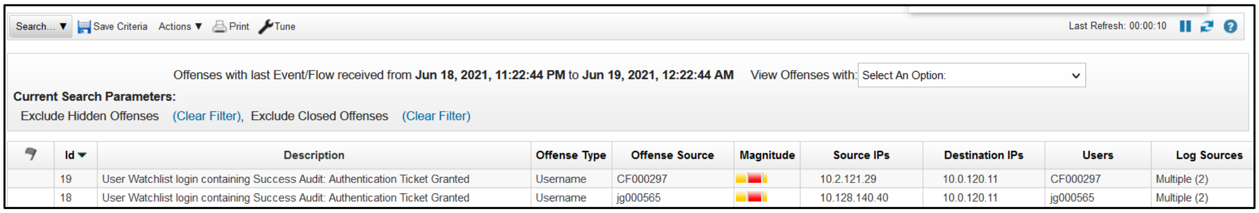
cd /labfiles

./sendWindows.sh



```
[root@allinone742 labfiles]# ./sendWindows.sh
generating 35 messages per second to 10.10.9.30:514
Ctrl-c to stop
generating 35 messages per second to 10.10.9.30:514
Ctrl-c to stop
```

Wait for five minutes and return to the Offenses tab in browser



Offenses with last Event/Flow received from **Jun 18, 2021, 11:22:44 PM** to **Jun 19, 2021, 12:22:44 AM** View Offenses with: Select An Option:

Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id ▼	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources
	19	User Watchlist login containing Success Audit: Authentication Ticket Granted	Username	CF000297	🟨🟥	10.2.121.29	10.0.120.11	CF000297	Multiple (2)
	18	User Watchlist login containing Success Audit: Authentication Ticket Granted	Username	jg000565	🟨🟥	10.128.140.40	10.0.120.11	jg000565	Multiple (2)

Investigate the offenses created. Answer the following questions:

a. How many offenses did the BQX Watchlist User Activity rule create? On the Rule list page, select the rule and look for the offense count parameter.

____

b. List the user IDs that created offenses. In the QRadar user interface, double-click the Offenses tab and find offenses that have Watchlist in the description.

____

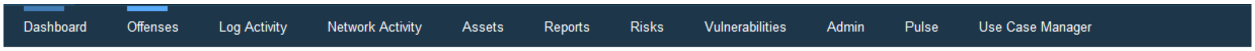
c. What is the source IP address of the offenses created?

____

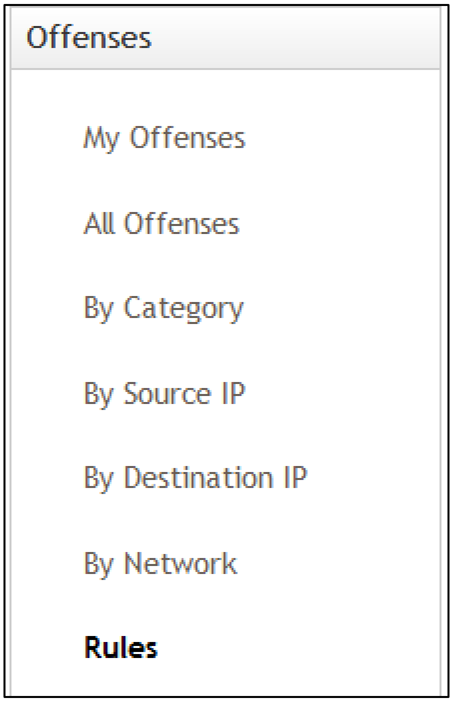
Working with rule parameters

To work with the parameters of a rule, perform the following steps:

1. In the QRadar user interface, navigate to the Offenses tab.



2. Click Rules in the left pane.



Offenses

My Offenses

All Offenses

By Category

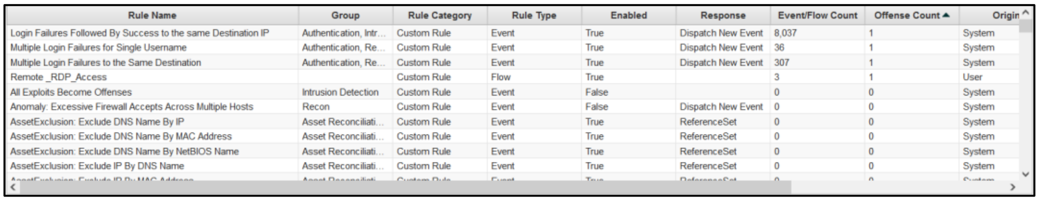
By Source IP

By Destination IP

By Network

Rules

3. Sort the Offense Count column in descending order, Click the header for the Offense Count column to sort in descending order.



Rule Name	Group	Rule Category	Rule Type	Enabled	Response	Event/Flow Count	Offense Count ▲	Origin
Login Failures Followed By Success to the same Destination IP	Authentication, Intr...	Custom Rule	Event	True	Dispatch New Event	8,037	1	System
Multiple Login Failures for Single Username	Authentication, Re...	Custom Rule	Event	True	Dispatch New Event	36	1	System
Multiple Login Failures to the Same Destination	Authentication, Re...	Custom Rule	Event	True	Dispatch New Event	307	1	System
Remote _RDP_Access		Custom Rule	Flow	True		3	1	User
All Exploits Become Offenses	Intrusion Detection	Custom Rule	Event	False		0	0	System
Anomaly: Excessive Firewall Accepts Across Multiple Hosts	Recon	Custom Rule	Event	False	Dispatch New Event	0	0	System
AssetExclusion: Exclude DNS Name By IP	Asset Reconciliati...	Custom Rule	Event	True	ReferenceSet	0	0	System
AssetExclusion: Exclude DNS Name By MAC Address	Asset Reconciliati...	Custom Rule	Event	True	ReferenceSet	0	0	System
AssetExclusion: Exclude DNS Name By NetBIOS Name	Asset Reconciliati...	Custom Rule	Event	True	ReferenceSet	0	0	System
AssetExclusion: Exclude IP By DNS Name	Asset Reconciliati...	Custom Rule	Event	True	ReferenceSet	0	0	System
AssetExclusion: Exclude IP By MAC Address	Asset Reconciliati...	Custom Rule	Event	True	ReferenceSet	0	0	System

   a. What rule created the most offenses?

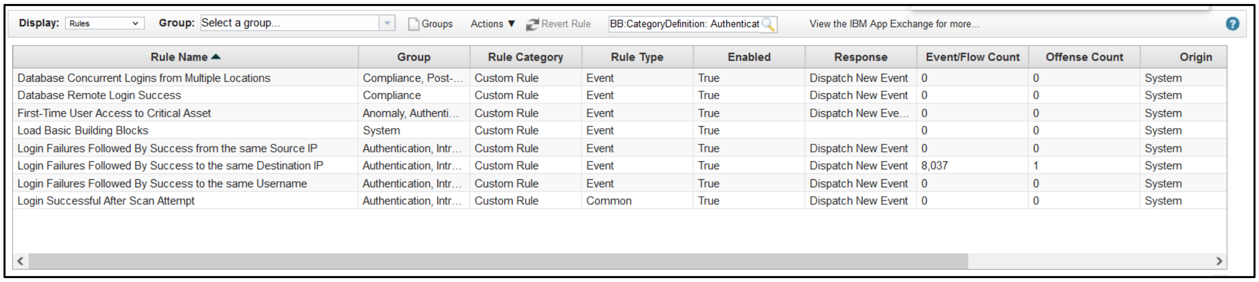
   ____

4. On the **Rules** page, from the **Display** drop-down list, select **Rules**.
5. From the **Group** drop-down list, do **not** select any group.
6. In the Search Rules field, enter the following name:

   BB:CategoryDefinition: Authentication Success

   The Rules display lists all the rules that meet the search criteria.
7. Select several of the rules and review the rule tests.

   Notice that the rules listed include the BB:CategoryDefinition: Authentication Success building block. Before editing a building block or rule, determine which other rules use it.



Display: Rules
Group: Select a group...
Groups
Actions ▼
Revert Rule
BB:CategoryDefinition: Authenticat
View the IBM App Exchange for more...

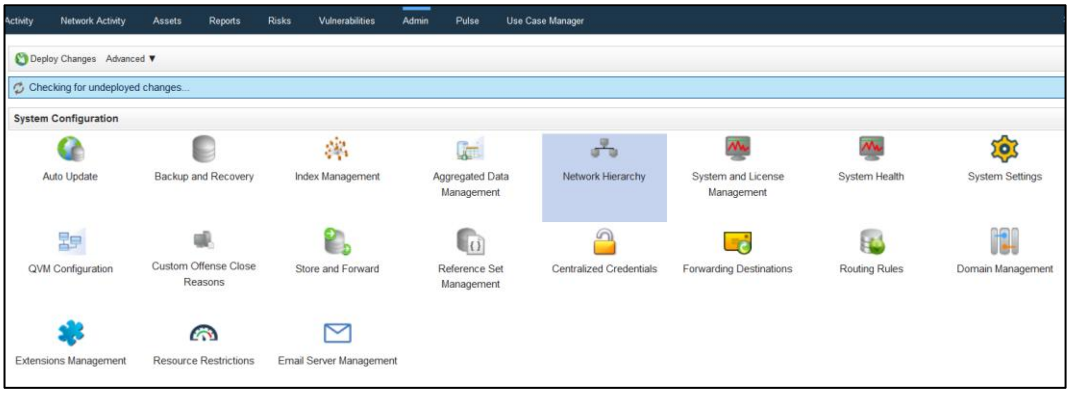
Rule Name ▲	Group	Rule Category	Rule Type	Enabled	Response	Event/Flow Count	Offense Count	Origin
Database Concurrent Logins from Multiple Locations	Compliance, Post-...	Custom Rule	Event	True	Dispatch New Event	0	0	System
Database Remote Login Success	Compliance	Custom Rule	Event	True	Dispatch New Event	0	0	System
First-Time User Access to Critical Asset	Anomaly, Authenti...	Custom Rule	Event	True	Dispatch New Eve...	0	0	System
Load Basic Building Blocks	System	Custom Rule	Event	True		0	0	System
Login Failures Followed By Success from the same Source IP	Authentication, Intr...	Custom Rule	Event	True	Dispatch New Event	0	0	System
Login Failures Followed By Success to the same Destination IP	Authentication, Intr...	Custom Rule	Event	True	Dispatch New Event	8,037	1	System
Login Failures Followed By Success to the same Username	Authentication, Intr...	Custom Rule	Event	True	Dispatch New Event	0	0	System
Login Successful After Scan Attempt	Authentication, Intr...	Custom Rule	Common	True	Dispatch New Event	0	0	System

Lab 6 - Using the Network Hierarchy

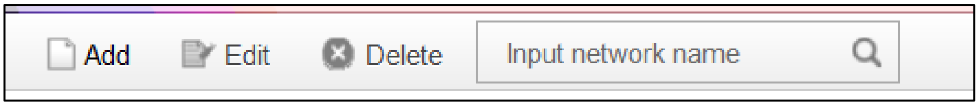
In this lab, we will explore the Network Hierarchy feature of Qradar. We will create and view a Network Hierarchy Object.

Create a Network Object

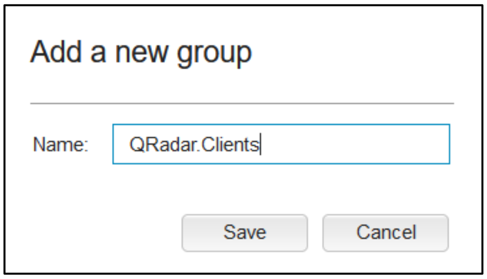
1. Navigate to the **Admin** tab and click the **Network Hierarchy** icon in the System configuration section.



2. Click **Add**.



3. In the Add network window, click the **Yellow gear wheel** icon.
4. For **Name** in the Add a new Group window, enter the following text. QR*adar.Clients* and Click **Save**.

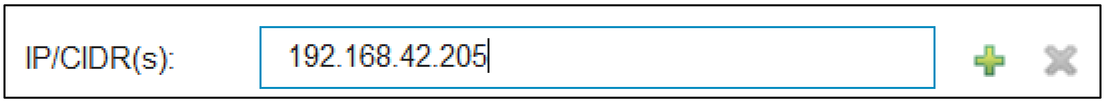


Name: QRadar.Clients

5. In the Add network Window, enter the values shown below.

Field	**Value**
Name	Student
Description	Exercise
IP/CIDR(s)	192.168.42.205

6. Make sure you click the plus icon to add the IP/CIDR(s) value to the object's list.

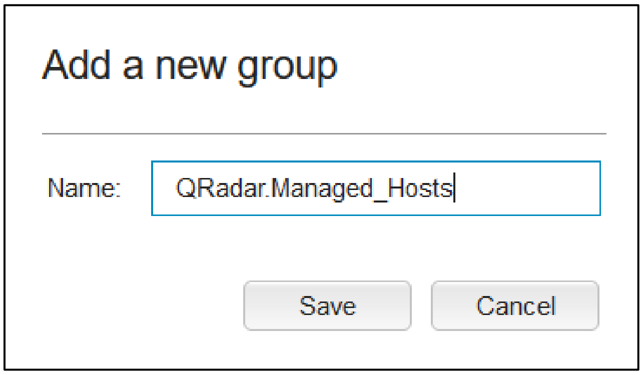


IP/CIDR(s): 192.168.42.205

7. Using the similar process from step 2 to 6, add a new network object as per below data.

   a. In the Add network window, click the ⚙ **Yellow gear wheel** icon.

   b. In the Name field, enter QRadar.Managed_Hosts. Click **Save**.



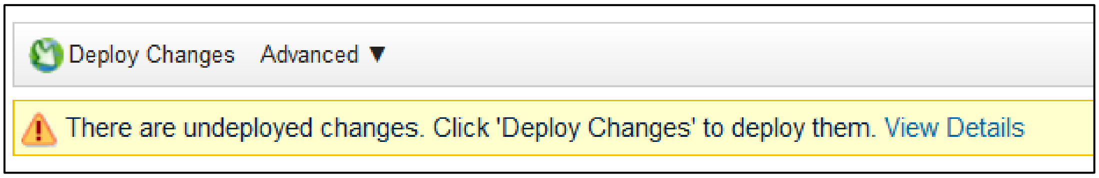
Add a new group

Name: QRadar.Managed_Hosts

   c. In the add network window, enter the values shown as below.

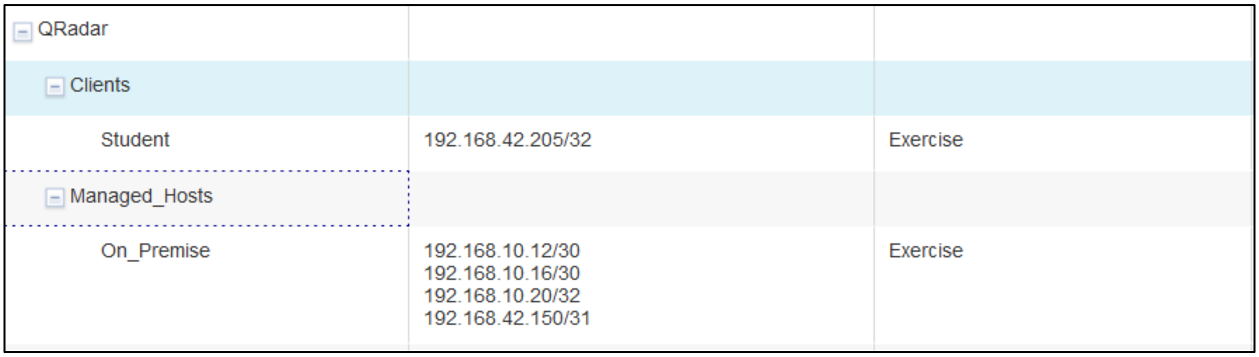
Field	**Value**
Name	On_Premise
Description	Exercise
IP/CIDR(s)	192.168.10.20/32 192.168.10.16/30 192.168.10.12/30 192.168.42.150/31

8. Close the Network Hierarchy Window and Click **Deploy Changes**.



There are undeployed changes. Click 'Deploy Changes' to deploy them. View Details

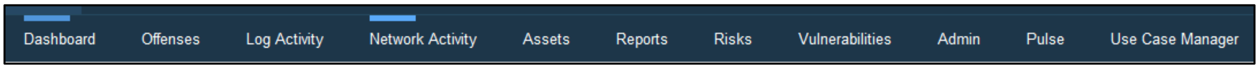
Open the Network hierarchy tab and verify that the **Student** and **On_Premise** network objects are listed.



⊟ QRadar		
⊟ Clients		
Student	192.168.42.205/32	Exercise
⊟ Managed_Hosts		
On_Premise	192.168.10.12/30 192.168.10.16/30 192.168.10.20/32 192.168.42.150/31	Exercise

View Network Objects in Flow

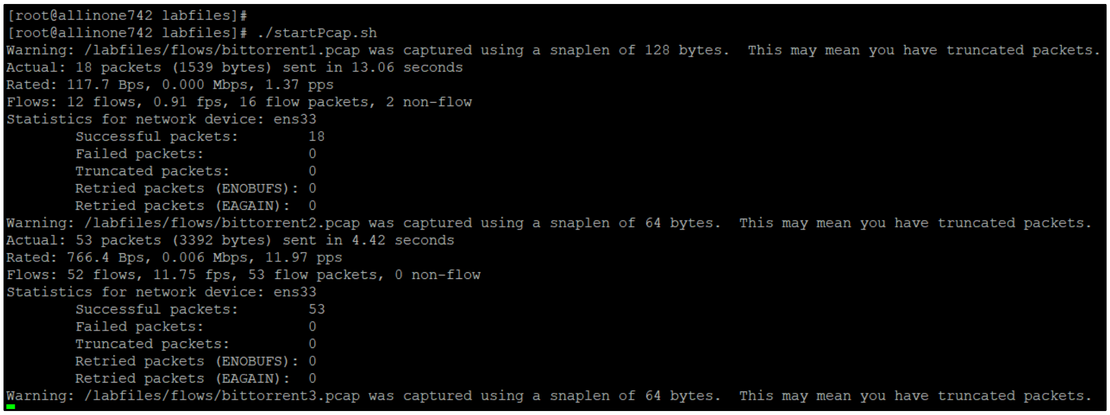
1. To view incoming flows, double-click the **Network Activity** tab.



   Note: The double-click resets the tab to its default settings.
2. Wait until you see flows with the IP addresses 192.168.42.150 and 192.168.42.205.
3. To pause the incoming events, click the **Pause** ❚❚ icon in the upper-right corner of the QRadar user interface.
4. Hover the mouse over either of the IP addresses and review the Network field information.
5. Open a remote shell to the QRadar VM. And run the following commands:

```
cd /labfiles

./startPcap.sh
```

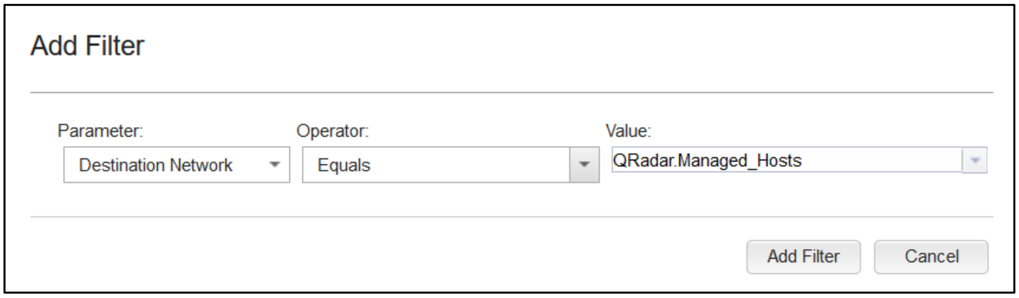


```
[root@allinone742 labfiles]#
[root@allinone742 labfiles]# ./startPcap.sh
Warning: /labfiles/flows/bittorrent1.pcap was captured using a snaplen of 128 bytes.  This may mean you have truncated packets.
Actual: 18 packets (1539 bytes) sent in 13.06 seconds
Rated: 117.7 Bps, 0.000 Mbps, 1.37 pps
Flows: 12 flows, 0.91 fps, 16 flow packets, 2 non-flow
Statistics for network device: ens33
        Successful packets:        18
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
Warning: /labfiles/flows/bittorrent2.pcap was captured using a snaplen of 64 bytes.  This may mean you have truncated packets.
Actual: 53 packets (3392 bytes) sent in 4.42 seconds
Rated: 766.4 Bps, 0.006 Mbps, 11.97 pps
Flows: 52 flows, 11.75 fps, 53 flow packets, 0 non-flow
Statistics for network device: ens33
        Successful packets:        53
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
Warning: /labfiles/flows/bittorrent3.pcap was captured using a snaplen of 64 bytes.  This may mean you have truncated packets.
```

6. In the browser return to the Network Activity Tab.
7. If refresh of the Network Activity tab is paused, press the **Play** button in the upper-right corner of the QRadar user interface. Wait for at least one minute.
8. To display only flows with destination IP addresses part of the network objects you created, click **Add Filter**. Add Filter
   a. In the Add Filter window, enter the values shown below.

Field	Value
Parameter	Destination Network
Operator	Equals
Value	Qradar.Managed_Hosts

   b. Click **Add Filter**.



Add Filter

Parameter: Destination Network

Operator: Equals

Value: QRadar.Managed_Hosts

9. If there are no rows with a Destination Network of **On_Premise** listed.
10. Change the View to show the **Last Hour**.
11. Change the Display to **Destination Network**.

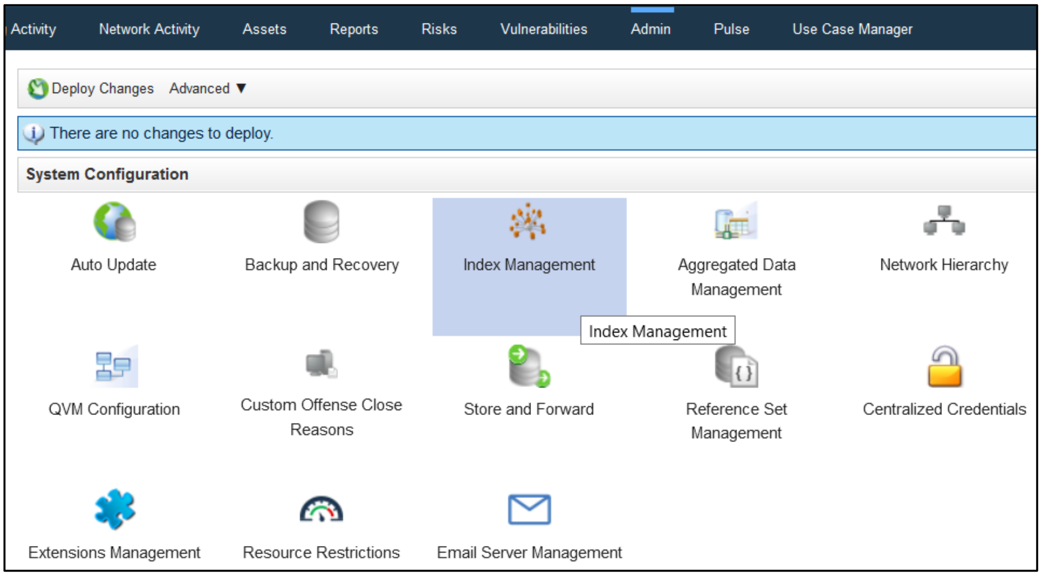
12. Use the right-click option menu on the Destination IP column to apply **Filter on Destination IP is not 192.168.42.150**.
13. Verify that you only see rows with Destination IP 192.168.10.12.
14. However the mouse over the Destination IP address and review the **Network** Field Information.
15. Navigate to the **Admin** tab, click the **Network Hierarchy** icon in the System Configuration section.
    a. Click the plus signs in front of Qradar and Managed_Hosts.
    b. Double click **On_Premise**.
    c. Select **192.168.10.12/30** from the IP/CIDR(s) list and click the red **X**.
    d. Click **Save**.
    e. Close the **Network Hierarchy** Window.
    f. Click **Deploy Changes**.
16. Return to the Network Activity page.
    a. Hover the mouse over the Destination IP address and review the **Network** field information to verify that it no longer displays **QRadar.Managed_Hosts.On_Premise**.
    b. Clear the **Destination Network is QRadar.Managed_Hosts** filter.
    c. Reapply the **Destination Network is QRadar.Managed_Hosts** filter.
    d. Verify that the result set is now empty.

Lab 7 - Index and Aggregated Data Management

In this lab, we will explore and create indexes. We will also use the indexed properties in searches and observer how the statistics for the indexed properties are updated.

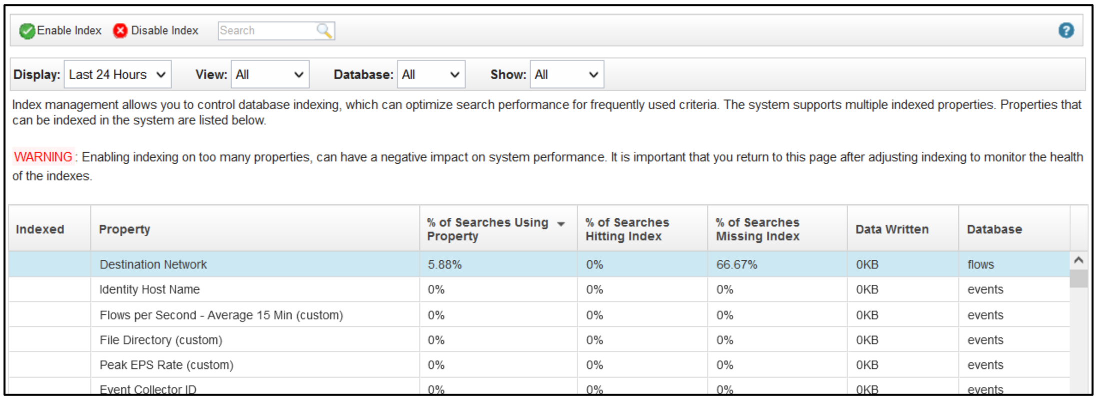
Enable an Index

1. In the QRadar user interface, click the **Index Management** icon under **Admin** tab.



There are no changes to deploy.

2. In the Index Management window opened, Verify that some indexed properties have data-written values by sorting the Data Written column in descending order.



Display: Last 24 Hours View: All Database: All Show: All

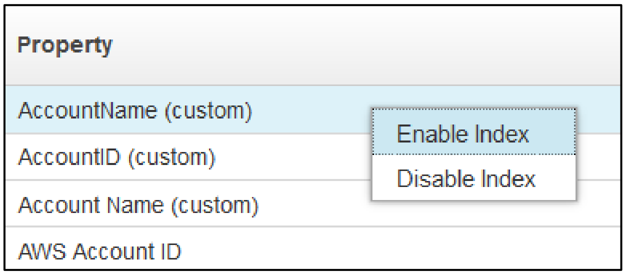
Index management allows you to control database indexing, which can optimize search performance for frequently used criteria. The system supports multiple indexed properties. Properties that can be indexed in the system are listed below.

WARNING : Enabling indexing on too many properties, can have a negative impact on system performance. It is important that you return to this page after adjusting indexing to monitor the health of the indexes.

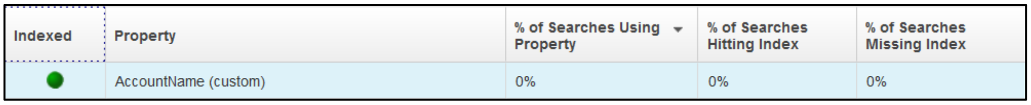
Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
	Destination Network	5.88%	0%	66.67%	0KB	flows
	Identity Host Name	0%	0%	0%	0KB	events
	Flows per Second - Average 15 Min (custom)	0%	0%	0%	0KB	events
	File Directory (custom)	0%	0%	0%	0KB	events
	Peak EPS Rate (custom)	0%	0%	0%	0KB	events
	Event Collector ID	0%	0%	0%	0KB	events

3. Enter *Account* in the search field on the top of the screen and click Search Magnifier icon.

a. Right click **AccountName (custom)** and click **Enable Index**.
b. Click **Save**.
c. Click **Ok**.



Property
AccountName (custom)
AccountID (custom)
Account Name (custom)
AWS Account ID



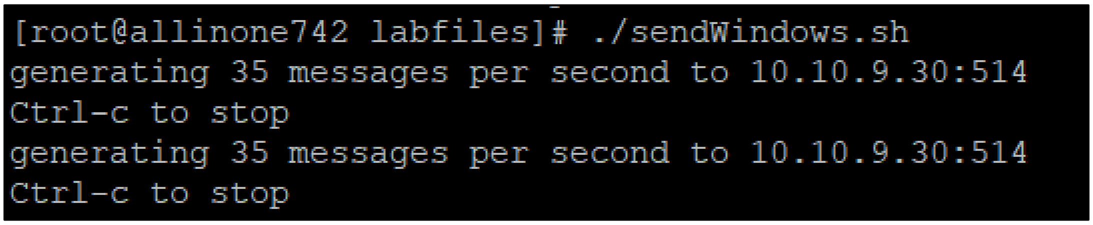
Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index
●	AccountName (custom)	0%	0%	0%

Use an Enabled Indexed property in a search

1. Open a remote shell to the QRadar VM and run the following commands.

   cd /labfiles

   ./sendWindows.sh



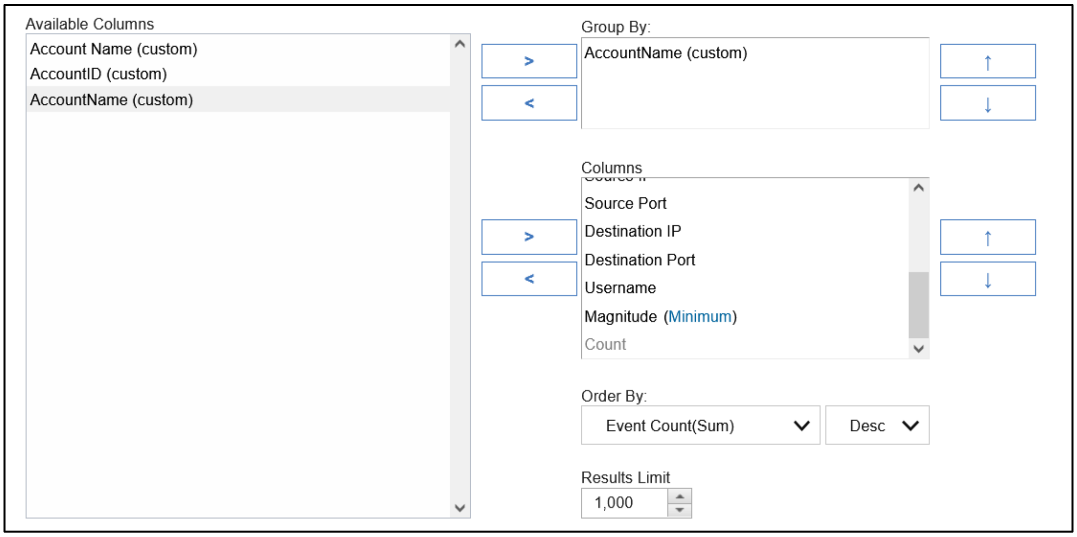
```
[root@allinone742 labfiles]# ./sendWindows.sh
generating 35 messages per second to 10.10.9.30:514
Ctrl-c to stop
generating 35 messages per second to 10.10.9.30:514
Ctrl-c to stop
```

2. In the QRadar user interface, double-click the Log Activity tab. Click on **Add Filter** and **View** using the following criteria.
   a. View the events from the last 30 minutes.
   b. Add the **AccountName (custom) [Indexed] is not N/A** filter.
   c. Add the **Log Source is WindowsAuthServer @ 10.0.120.11** filter.
   d. Edit the search.
      i. In the columns definition pane, group the search results by **AccountName (custom)**.

ii. For the Columns list, select only **Event Name** and **Event Count (Sum)**.

iii. From the Order By list, select **Event Count (Sum)**.

e. Click Search



Available Columns

Account Name (custom)
AccountID (custom)
AccountName (custom)

Group By:

AccountName (custom)

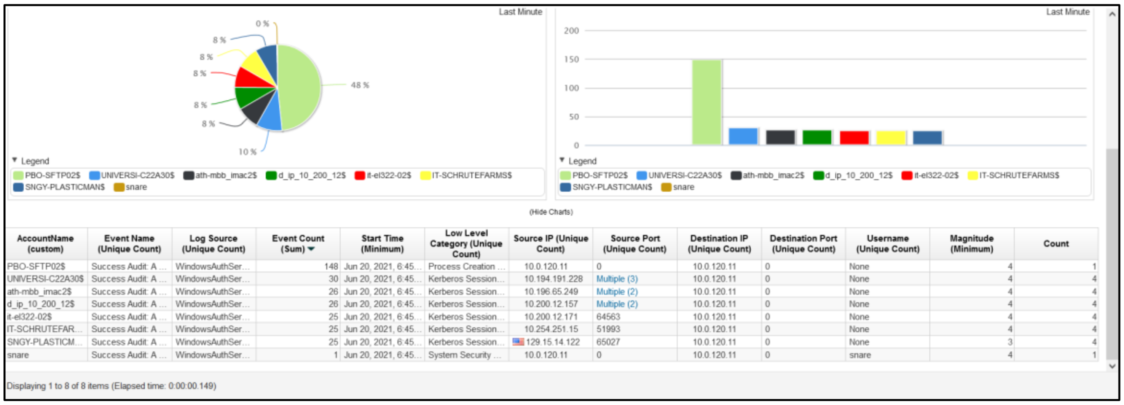
Columns

Source Port
Destination IP
Destination Port
Username
Magnitude (Minimum)
Count

Order By: Event Count(Sum) Desc

Results Limit: 1,000

3. Verify that search results look similar to the results in the following screen capture.



AccountName (custom)	Event Name (Unique Count)	Log Source (Unique Count)	Event Count (Sum) ▼	Start Time (Minimum)	Low Level Category (Unique Count)	Source IP (Unique Count)	Source Port (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Username (Unique Count)	Magnitude (Minimum)	Count
PBO-SFTP02$	Success Audit: A ...	WindowsAuthSer...	148	Jun 20, 2021, 6:45...	Process Creation ...	10.0.120.11	0	10.0.120.11	0	None	4	1
UNIVERSI-C22A30$	Success Audit: A ...	WindowsAuthSer...	30	Jun 20, 2021, 6:45...	Kerberos Session...	10.194.191.228	Multiple (3)	10.0.120.11	0	None	4	4
ath-mbb_imac2$	Success Audit: A ...	WindowsAuthSer...	26	Jun 20, 2021, 6:45...	Kerberos Session...	10.196.65.249	Multiple (2)	10.0.120.11	0	None	4	4
d_ip_10_200_12$	Success Audit: A ...	WindowsAuthSer...	26	Jun 20, 2021, 6:45...	Kerberos Session...	10.200.12.157	Multiple (2)	10.0.120.11	0	None	4	4
it-el322-02$	Success Audit: A ...	WindowsAuthSer...	25	Jun 20, 2021, 6:45...	Kerberos Session...	10.200.12.171	64563	10.0.120.11	0	None	4	4
IT-SCHRUTEFAR...	Success Audit: A ...	WindowsAuthSer...	25	Jun 20, 2021, 6:45...	Kerberos Session...	10.254.251.15	51993	10.0.120.11	0	None	4	4
SNGY-PLASTICM...	Success Audit: A ...	WindowsAuthSer...	25	Jun 20, 2021, 6:45...	Kerberos Session...	129.15.14.122	65027	10.0.120.11	0	None	3	4
snare	Success Audit: A ...	WindowsAuthSer...	1	Jun 20, 2021, 6:45...	System Security ...	10.0.120.11	0	10.0.120.11	0	snare	4	1

Displaying 1 to 8 of 8 items (Elapsed time: 0:00:00.149)

4. Click **Save Criteria** to save the search.

5. Save the search using the values shown below.

Field / Option	**Value**
Search Name	Exercise:Index Management
Timespan Options	Recent <enabled> Last 15 Minutes
Include in my Quick Searches	<enabled>

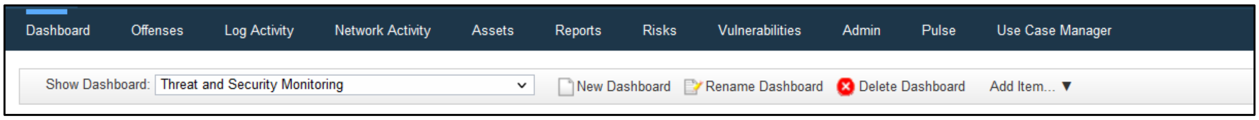
6. Wait for the sendWindows.sh script to finish.
7. Click **Index Management** Icon under **Admin** Tab.
8. Verify that the AccountName property now includes statistics for the indexed property.

Lab 8 - Using Dashboards

In this lab, we will learn about Creating a new dashboard and add items to the dashboard.

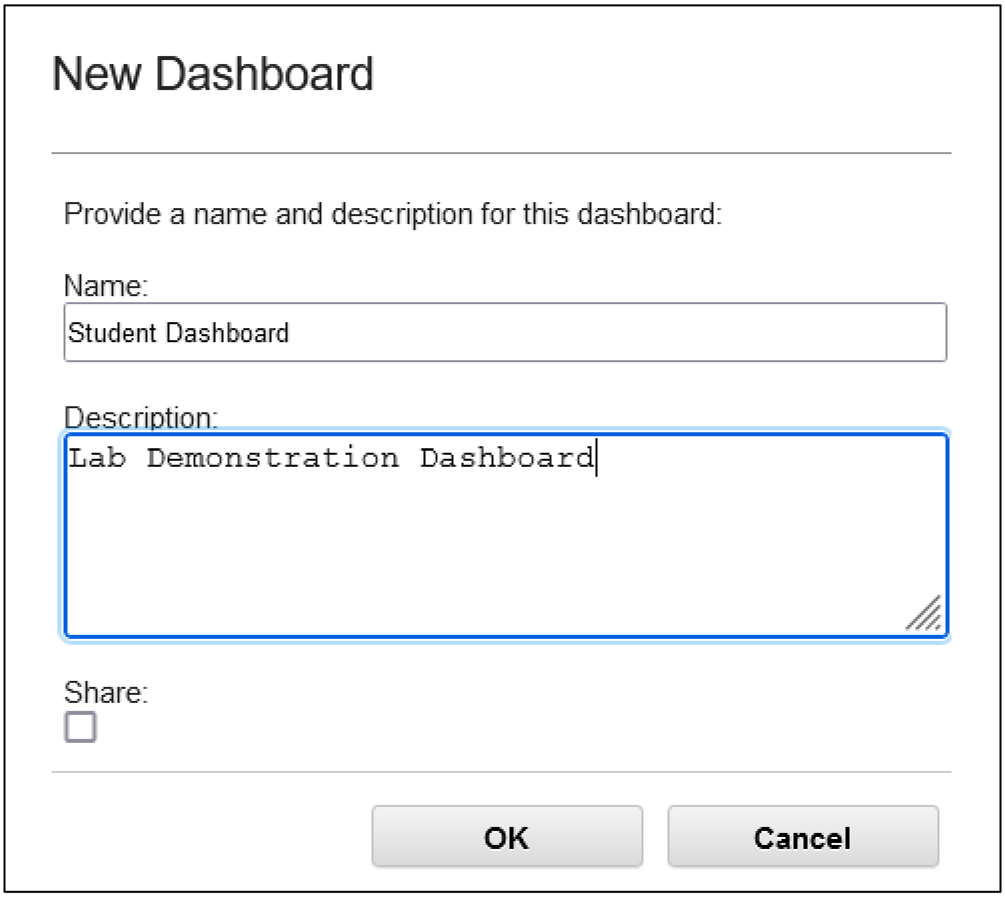
Follow the below steps to create a new dashboard.

1. Navigate to the **Dashboard** tab.
2. Click the **New Dashboard** button.



Show Dashboard: Threat and Security Monitoring

3. For **Name**, enter *Student Dashboard*.
4. For **Description**, enter *Lab Demonstration Dashboard.*
5. Click **Ok**.



New Dashboard

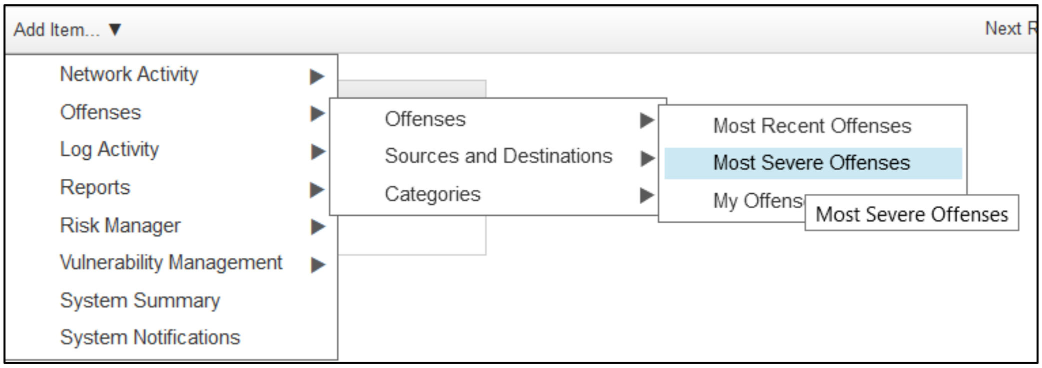
Provide a name and description for this dashboard:

Name: Student Dashboard

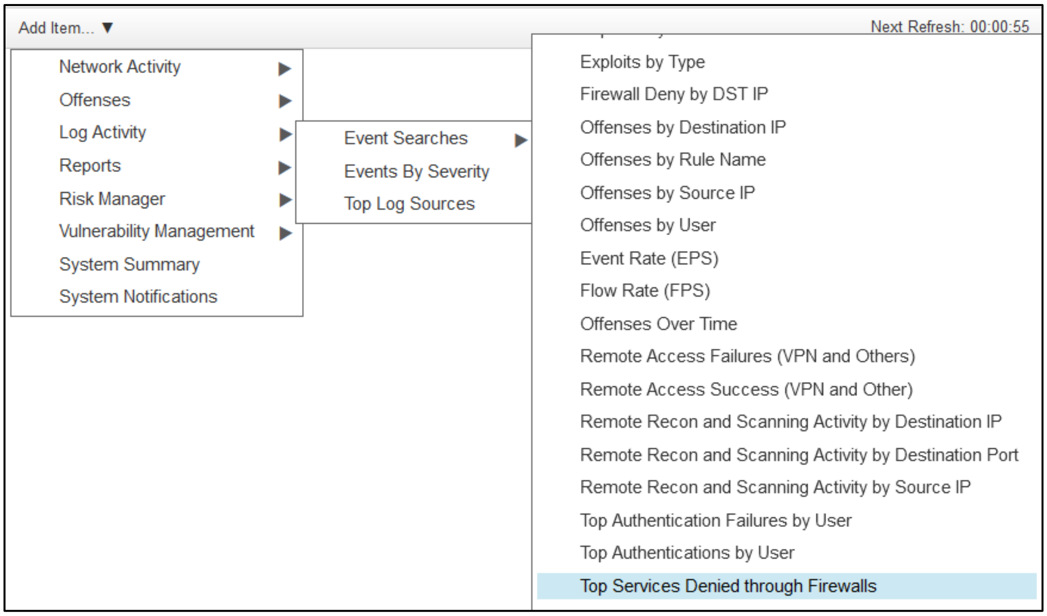
Description: Lab Demonstration Dashboard

Share: □

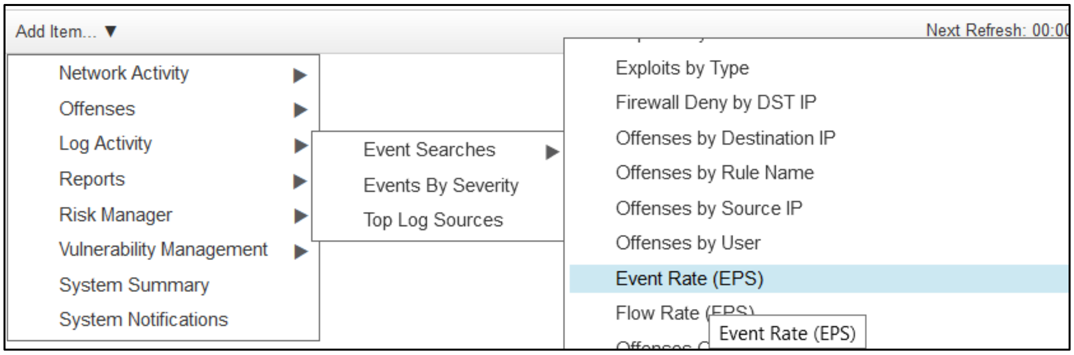
6. To add items to the new dashboard, from the **Add Item** list, select the following items:
    a. **Offenses > Offenses > Most Severe Offenses**



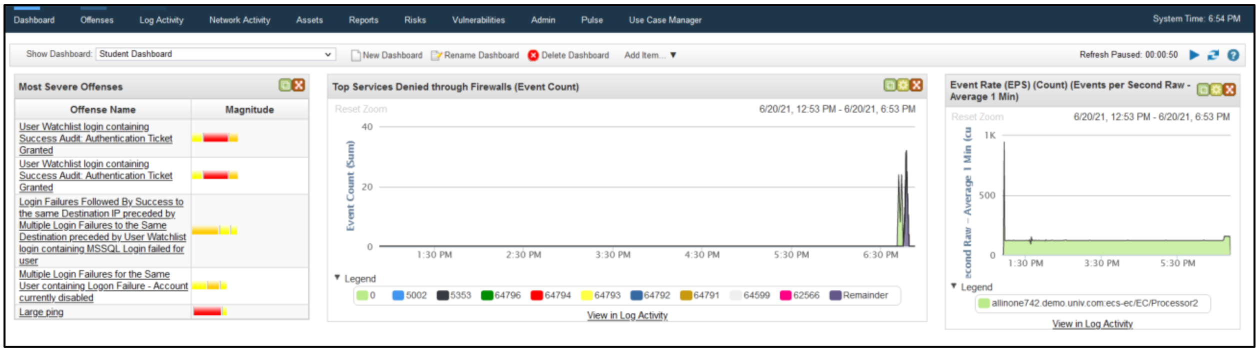
    b. **Log Activity > Event Searches > Top Services Denied through Firewalls**


Add Item... ▼
Next Refresh: 00:00:55
Network Activity ▶
Offenses ▶
Log Activity ▶
Reports ▶
Risk Manager ▶
Vulnerability Management ▶
System Summary
System Notifications
Event Searches ▶
Events By Severity
Top Log Sources
Exploits by Type
Firewall Deny by DST IP
Offenses by Destination IP
Offenses by Rule Name
Offenses by Source IP
Offenses by User
Event Rate (EPS)
Flow Rate (FPS)
Offenses Over Time
Remote Access Failures (VPN and Others)
Remote Access Success (VPN and Other)
Remote Recon and Scanning Activity by Destination IP
Remote Recon and Scanning Activity by Destination Port
Remote Recon and Scanning Activity by Source IP
Top Authentication Failures by User
Top Authentications by User
Top Services Denied through Firewalls

    c. **Log Activity > Event Searches > Event Rate (EPS)**



7. Drag the items to an empty spot on the dashboard.
8. Click the **Refresh** icon to update the window.
9. Verify that the dashboard includes an offense item and two log events items. Depending on where you positioned the items, your dashboard looks like below screenshot.



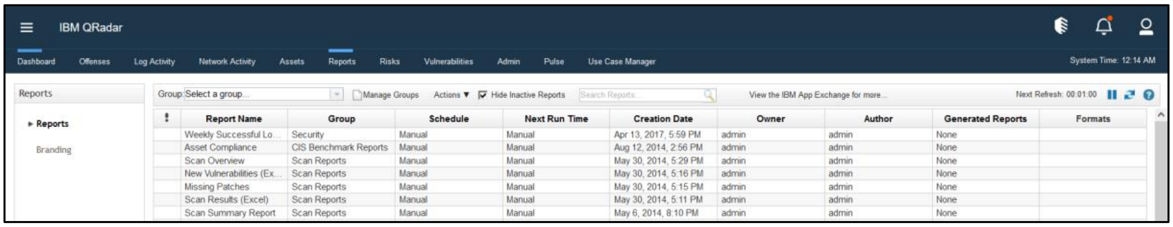
Offense Name	Magnitude
User Watchlist login containing Success Audit: Authentication Ticket Granted	
User Watchlist login containing Success Audit: Authentication Ticket Granted	
Login Failures Followed By Success to the same Destination IP preceded by Multiple Login Failures to the Same Destination preceded by User Watchlist login containing MSSQL Login failed for user	
Multiple Login Failures for the Same User containing Logon Failure - Account currently disabled	
Large ping	

Lab 9 - Creating reports

Viewing an existing Report

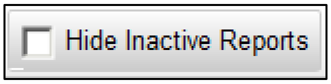
Qradar has over 100 ready to use reports. Perform the following steps to view the configuration and run a report provided by Qradar SIEM.

1. In the Qradar user interface, navigate to the **Reports** tab.

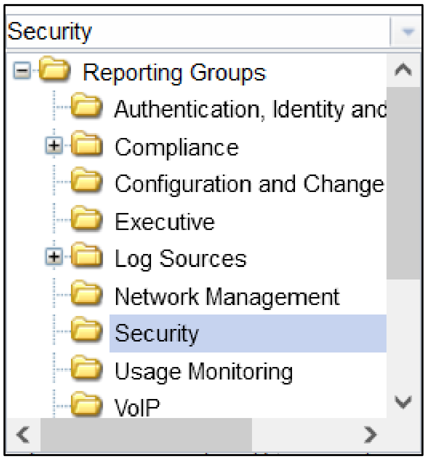


!	Report Name	Group	Schedule	Next Run Time	Creation Date	Owner	Author	Generated Reports	Formats
	Weekly Successful Lo...	Security	Manual	Manual	Apr 13, 2017, 5:59 PM	admin	admin	None	
	Asset Compliance	CIS Benchmark Reports	Manual	Manual	Aug 12, 2014, 2:56 PM	admin	admin	None	
	Scan Overview	Scan Reports	Manual	Manual	May 30, 2014, 5:29 PM	admin	admin	None	
	New Vulnerabilities (Ex...	Scan Reports	Manual	Manual	May 30, 2014, 5:16 PM	admin	admin	None	
	Missing Patches	Scan Reports	Manual	Manual	May 30, 2014, 5:15 PM	admin	admin	None	
	Scan Results (Excel)	Scan Reports	Manual	Manual	May 30, 2014, 5:11 PM	admin	admin	None	
	Scan Summary Report	Scan Reports	Manual	Manual	May 6, 2014, 8:10 PM	admin	admin	None	

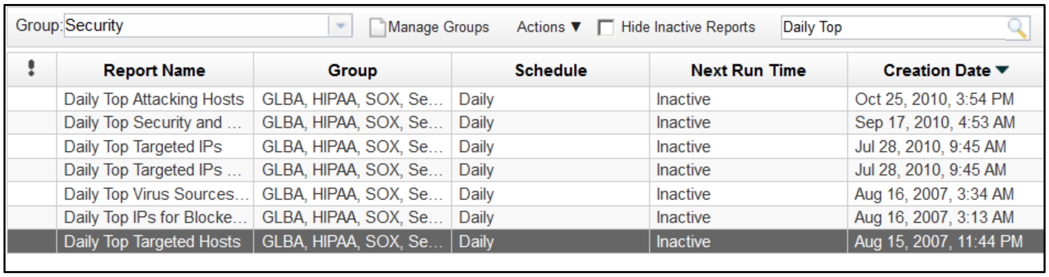
2. Disable the **Hide Inactive Reports** check box.



3. From the **Group** drop down list, scroll down and select the **Security** group.



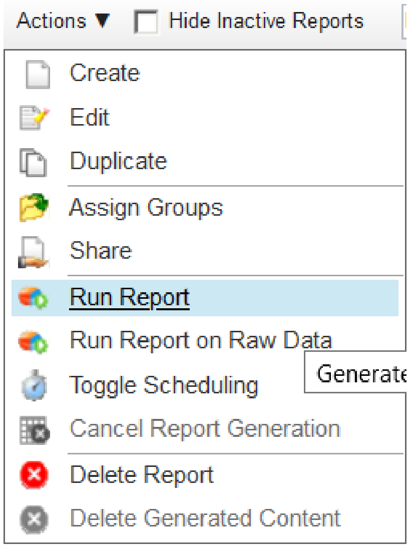
4. In the **Search Reports** field, type *Daily Top* and click the **Search Reports** icon to filter the report list.
5. Select **Daily Top Targeted Hosts**.



Group: Security | Manage Groups | Actions ▼ | □ Hide Inactive Reports | Daily Top

!	Report Name	Group	Schedule	Next Run Time	Creation Date ▼
	Daily Top Attacking Hosts	GLBA, HIPAA, SOX, Se...	Daily	Inactive	Oct 25, 2010, 3:54 PM
	Daily Top Security and ...	GLBA, HIPAA, SOX, Se...	Daily	Inactive	Sep 17, 2010, 4:53 AM
	Daily Top Targeted IPs	GLBA, HIPAA, SOX, Se...	Daily	Inactive	Jul 28, 2010, 9:45 AM
	Daily Top Targeted IPs ...	GLBA, HIPAA, SOX, Se...	Daily	Inactive	Jul 28, 2010, 9:45 AM
	Daily Top Virus Sources...	GLBA, HIPAA, SOX, Se...	Daily	Inactive	Aug 16, 2007, 3:34 AM
	Daily Top IPs for Blocke...	GLBA, HIPAA, SOX, Se...	Daily	Inactive	Aug 16, 2007, 3:13 AM
	Daily Top Targeted Hosts	GLBA, HIPAA, SOX, Se...	Daily	Inactive	Aug 15, 2007, 11:44 PM

6. From the **Actions** drop-down list on the **Reports** toolbar, select **Run Report.**



7. Explore the report and try to answer below query.
   a. What groups contain the **Daily Top Targeted Hosts** report?

   ____

8. Double click the **Daily Top Targeted Hosts**, click **Next** until you see the Specify Report Contents page.
9. Click **Define** in the top container.
   a. What is the name of the event search that generates the data in the top container?

   ____

   b. What is the graph type?

   ____

c. What parameters are graphed on the X and Y axes?

____

d. Click **Cancel** to exit the top container details page.

e. Click **Define** in the bottom container. The bottom container details page opens. What is the name of the event search that generates the data in the bottom container?

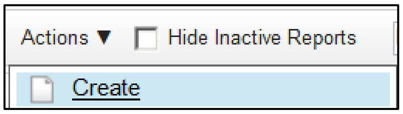
____

10. Click **Cancel** to exit the bottom container details page, click **Next** twice.
11. On the **Reports** tab, click the **Refresh** icon to update the status of the generation of the Daily Top Targeted Hosts Report.
    a. When the report generated content, click the **PDF** icon in the **Formats** column to view the report.
12. Clear the report filters.

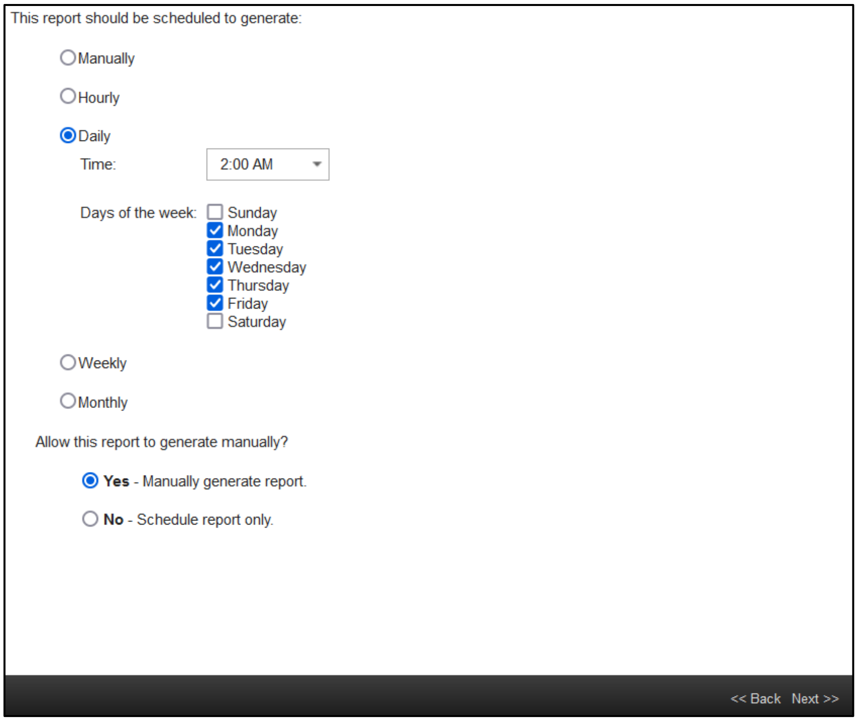
Creating a new event report

Saved Searches can be used to create reports. To use an existing search to create a report.

1. From the **Actions** drop-down list on the Reports toolbar, select Create. Click **Next**.



2. Select the **Daily** option and the check boxes for **Monday** through **Friday**.Click **Next**.



This report should be scheduled to generate:

○ Manually

○ Hourly

● Daily

Time: 2:00 AM

Days of the week:
☐ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☐ Saturday

○ Weekly

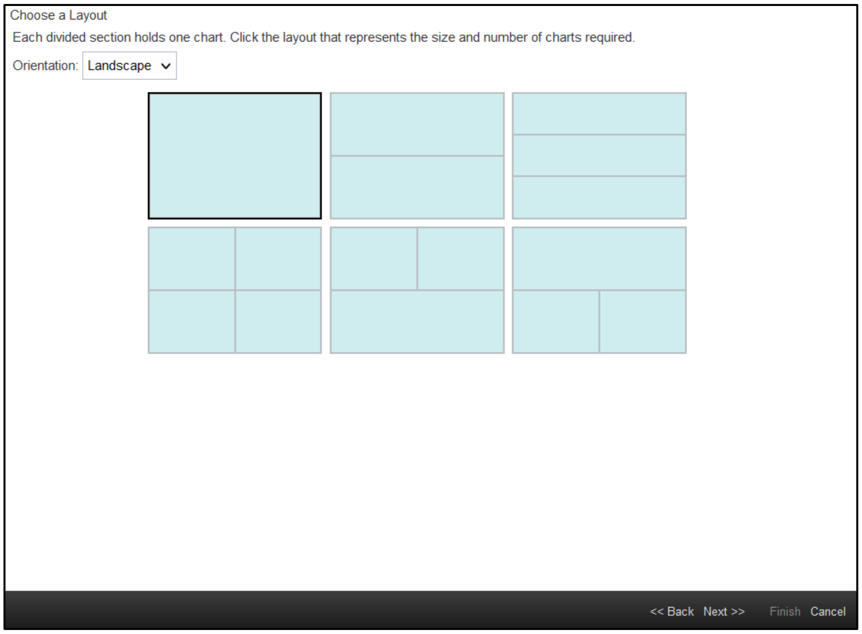
○ Monthly

Allow this report to generate manually?

● **Yes** - Manually generate report.

○ **No** - Schedule report only.

3. On the Choose a Layout page, from the **Orientation** drop-down list, select **Landscape**.
   a. Click the single-Container layout. Click **Next**.



Choose a Layout

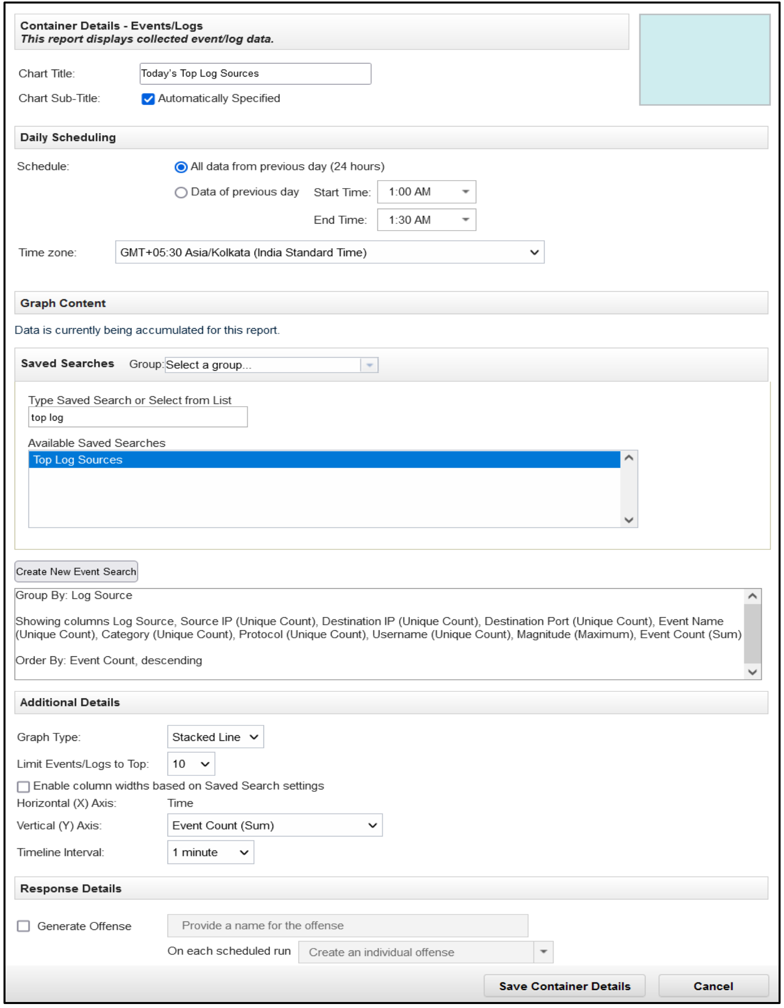
Each divided section holds one chart. Click the layout that represents the size and number of charts required.

Orientation: Landscape

4. On the Specify Report Contents page, in the **Reports Title** field, type *Top Log Sources*.

5. In the **Chart type** drop down list, select **Events/Logs**. Configure the **Container Details** as below data.

Field / Option	**Setting**
Type Chart Title	Today’s Top Log Sources
Limit the Events/Logs to Top	10
Graph type	Stacked Line
Saved Searches	Top Log Sources
Horizontal (X) Axis	Time
Vertical (Y) Axis	Event Count (Sum)
Timeline Interval	1 Minute



Container Details - Events/Logs
This report displays collected event/log data.

Chart Title: Today's Top Log Sources
Chart Sub-Title: ☑ Automatically Specified

Daily Scheduling

Schedule: ● All data from previous day (24 hours)
○ Data of previous day Start Time: 1:00 AM
End Time: 1:30 AM

Time zone: GMT+05:30 Asia/Kolkata (India Standard Time)

Graph Content

Data is currently being accumulated for this report.

Saved Searches Group: Select a group...

Type Saved Search or Select from List: top log

Available Saved Searches: Top Log Sources

Group By: Log Source

Showing columns Log Source, Source IP (Unique Count), Destination IP (Unique Count), Destination Port (Unique Count), Event Name (Unique Count), Category (Unique Count), Protocol (Unique Count), Username (Unique Count), Magnitude (Maximum), Event Count (Sum)

Order By: Event Count, descending

Additional Details

Graph Type: Stacked Line
Limit Events/Logs to Top: 10
□ Enable column widths based on Saved Search settings
Horizontal (X) Axis: Time
Vertical (Y) Axis: Event Count (Sum)
Timeline Interval: 1 minute

Response Details

□ Generate Offense Provide a name for the offense
On each scheduled run Create an individual offense

6. Verify the Container details and click Save Container Details.
7. Click **Next** Twice

8. On the reports format page, select **HTML** and **PDF**.
9. Click **Next** until the Finish page.
10. Type the below text in **Report Description** field.
    The Daily Top Log Sources report lists the top ten log sources by event count.
11. Verify that the **Yes – Run this report when the wizard is complete** check box is enabled.
12. Click **Next**.
13. Click **Finish**.
14. Click the **Refresh** icon to update the status of the generation of the **Top Log Sources** Report.
15. View the Next Run Time Column for the Top Log Sources Report.
16. Click PDF icon in the formats column to view the report.