Using the QRadar SIEM user interface

Using the QRadar SIEM user interface

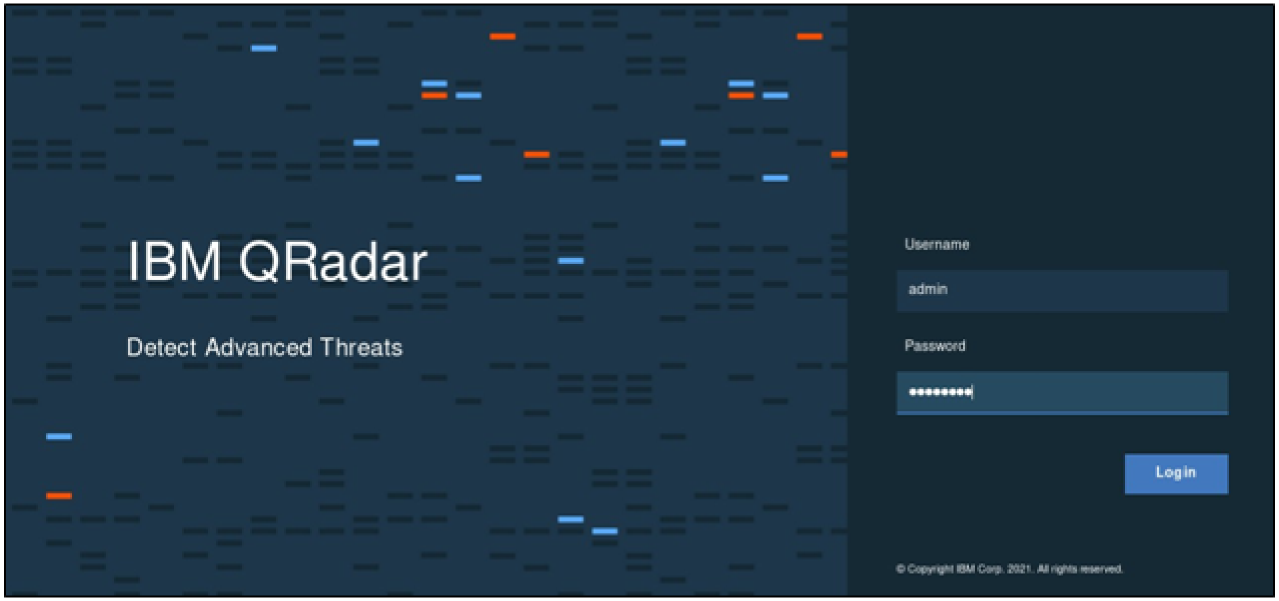
In these exercises, you become familiar with the web-based control center and sending sample data to Qradar.

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

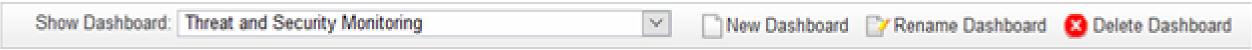
Username: admin

Password: •••••••••

© Copyright IBM Corp. 2021. All rights reserved.

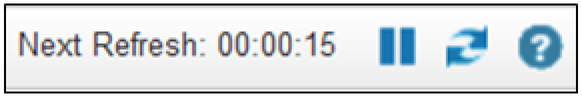
3. The Qradar Dashboard interface opens. Most of the sections in this dashboard may be empty. We will initiate a sample feed to see all these data.

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.



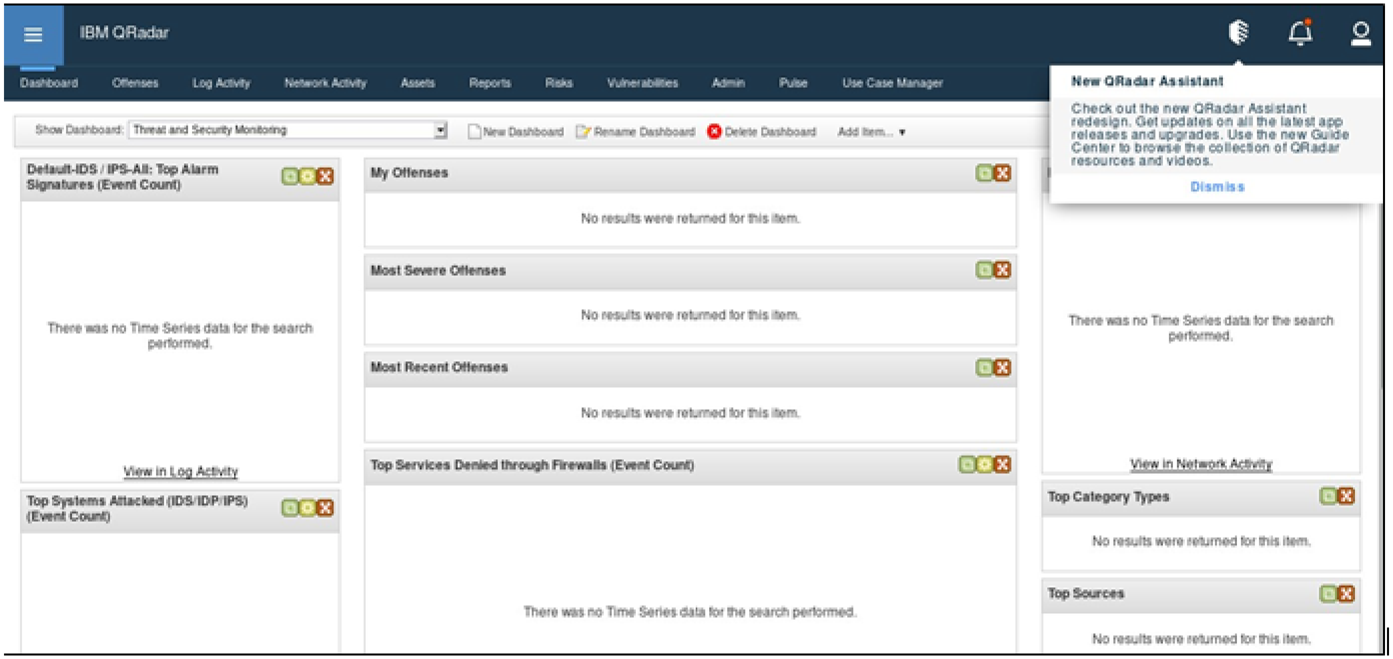
Show Dashboard: Threat and Security Monitoring

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.



Show Dashboard: Threat and Security Monitoring

Default-IDS / IPS-All: Top Alarm Signatures (Event Count)

There was no Time Series data for the search performed.

Top Systems Attacked (IDS/IDP/IPS) (Event Count)

My Offenses

No results were returned for this item.

Most Severe Offenses

No results were returned for this item.

Most Recent Offenses

No results were returned for this item.

Top Services Denied through Firewalls (Event Count)

There was no Time Series data for the search performed.

There was no Time Series data for the search performed.

Top Category Types

No results were returned for this item.

Top Sources

No results were returned for this item.

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.

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.

o Deploy and manage Qradar Hosts and licenses.

o Configure user accounts and authentication.

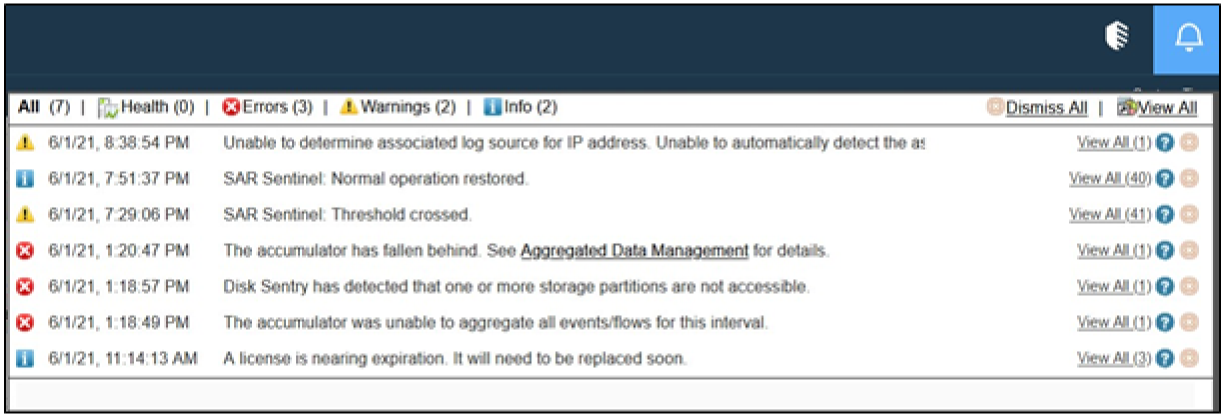
o Build a network hierarchy

o Configure domains and set up a multi-tenant environment

o Define and manage log and flow data sources etc.

7. Click Notifications 🔔 .

a. On the Messages window, view the system notification details.



⚠	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:

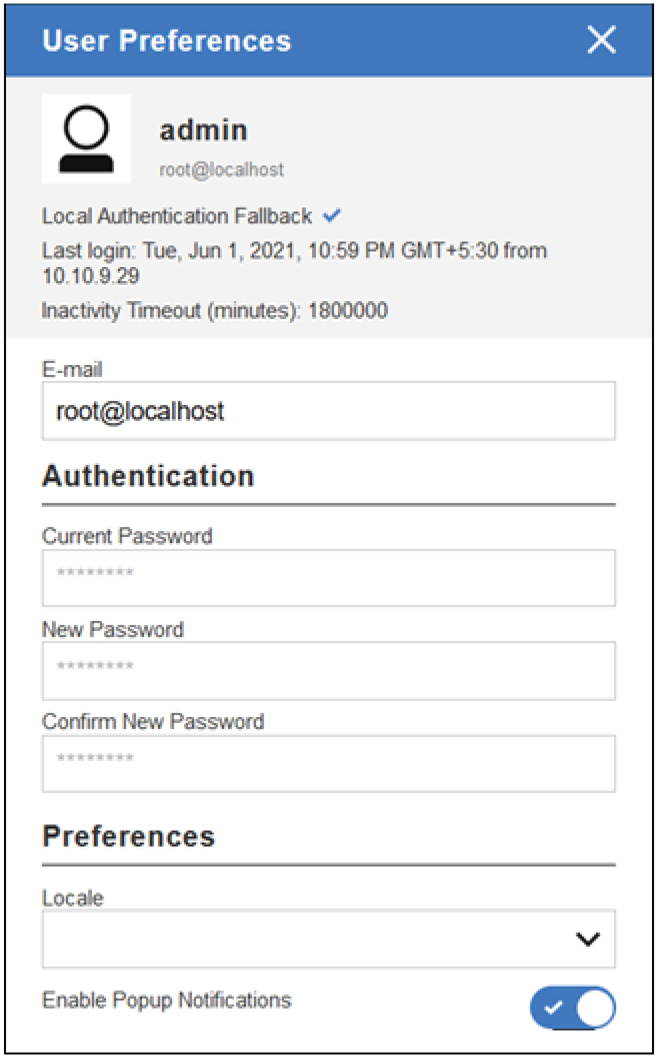
- Dismiss All Info
- Dismiss

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.**

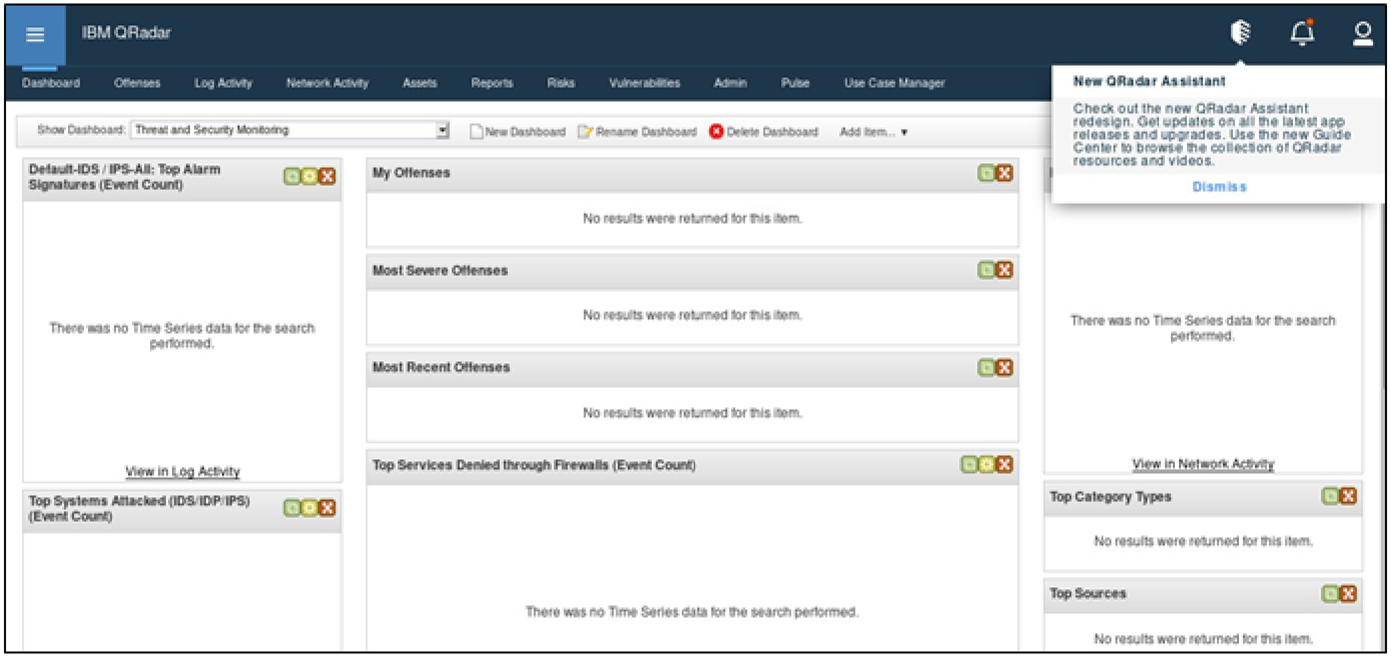
Sending Sample Data to QRadar

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.



Show Dashboard: Threat and Security Monitoring

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.

Default-IDS / IPS-All: Top Alarm Signatures (Event Count)

There was no Time Series data for the search performed.

Top Systems Attacked (IDS/IDP/IPS) (Event Count)

My Offenses

No results were returned for this item.

Most Severe Offenses

No results were returned for this item.

Most Recent Offenses

No results were returned for this item.

Top Services Denied through Firewalls (Event Count)

There was no Time Series data for the search performed.

There was no Time Series data for the search performed.

Top Category Types

No results were returned for this item.

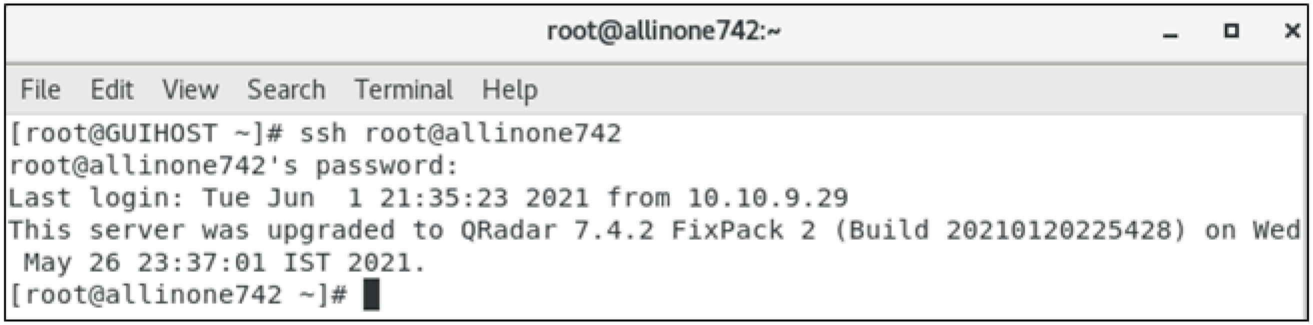
Top Sources

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
```

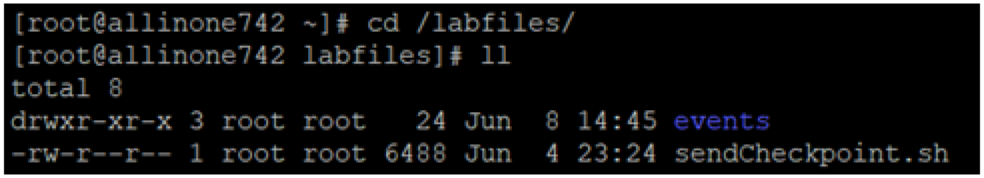
Enter the password as ‘p@ssw0rd’



```
[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 ~]# 
```

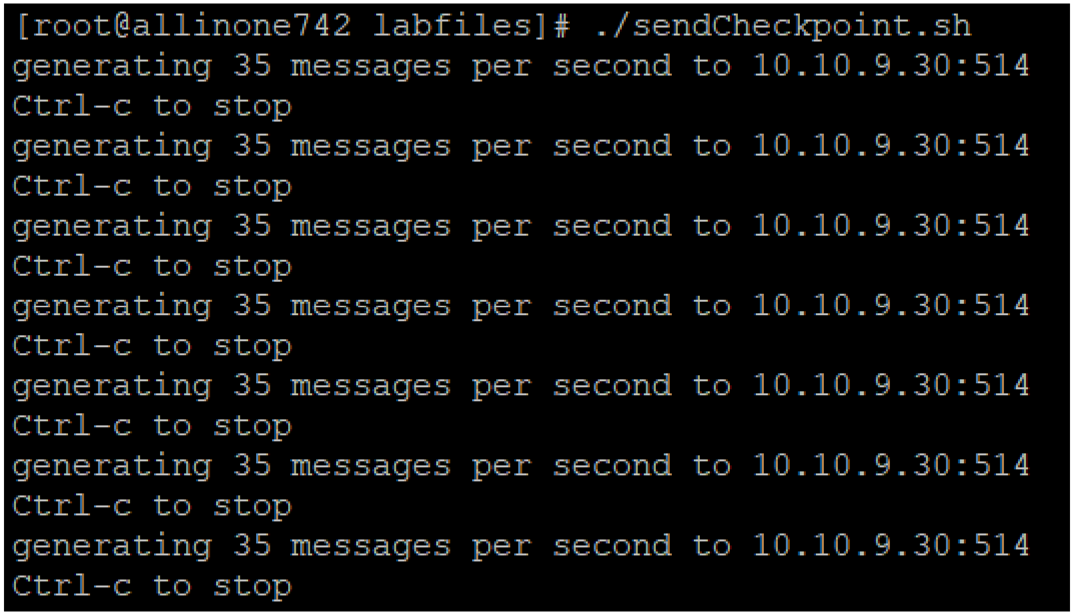
5. Run the following commands:

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
```

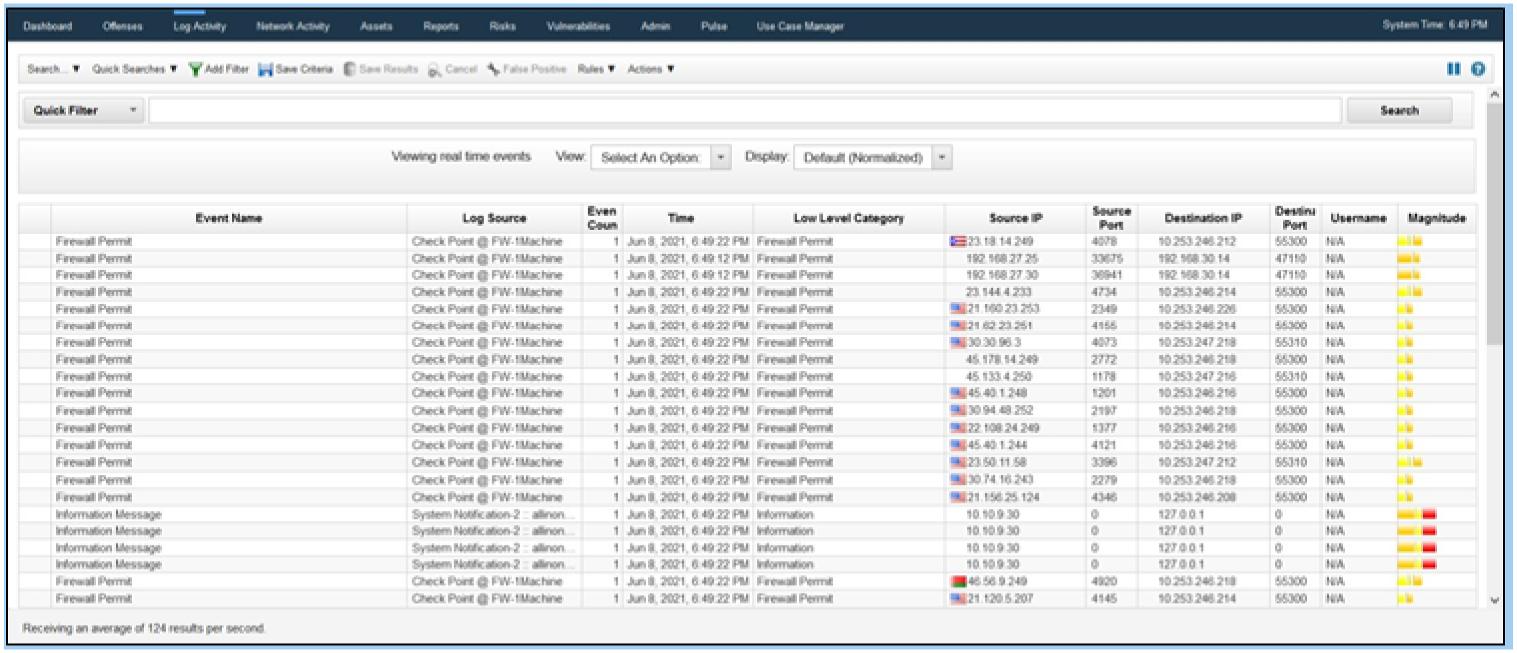
./sendCheckpoint.sh



```
[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	Destin 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.