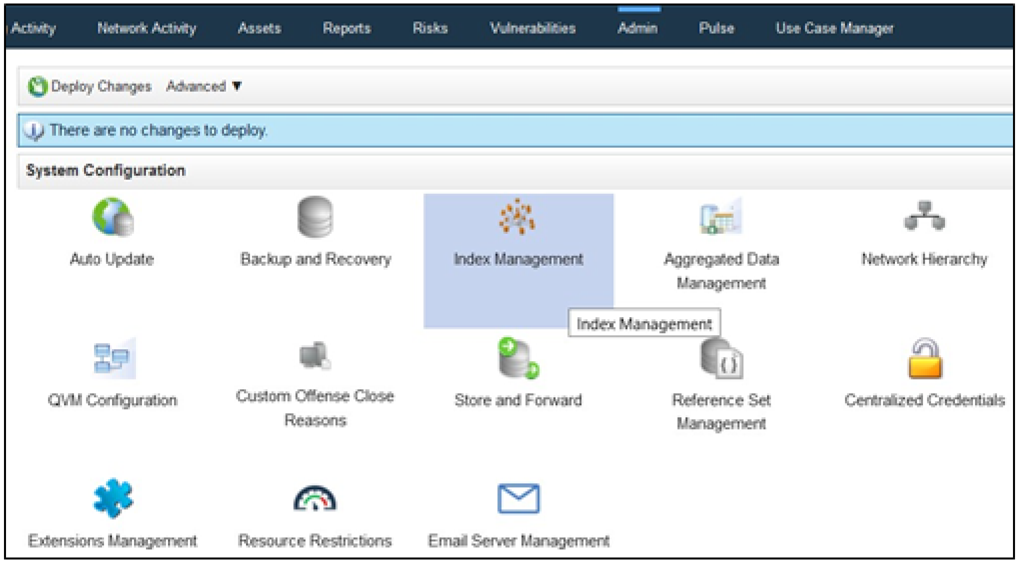
Index and Aggregated Data Management

Index and Aggregated Data Management

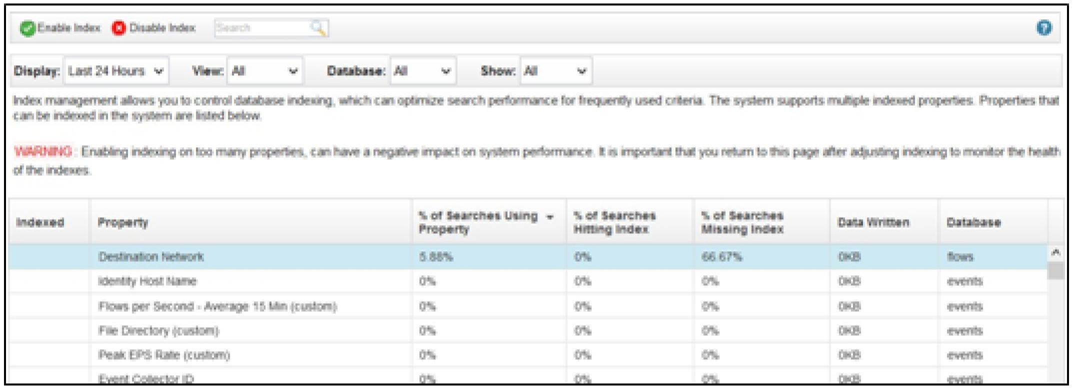
In this lab, we will explore and create indexes. We will also use the indexed properties in searches and observer how the statistics for the indexed properties are updated.

Enable an Index

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



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.

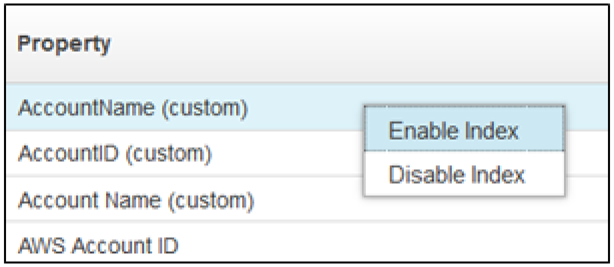
Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
	Destination Network	5.88%	0%	66.67%	0KB	flows
	Identity Host Name	0%	0%	0%	0KB	events
	Flows per Second - Average 15 Min (custom)	0%	0%	0%	0KB	events
	File Directory (custom)	0%	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 the Search Magnifier icon.

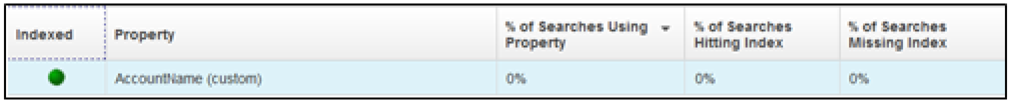
   a. Right click **AccountName (custom)** and click **Enable Index.**

   b. Click **Save.**

   c. Click **Ok.**



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



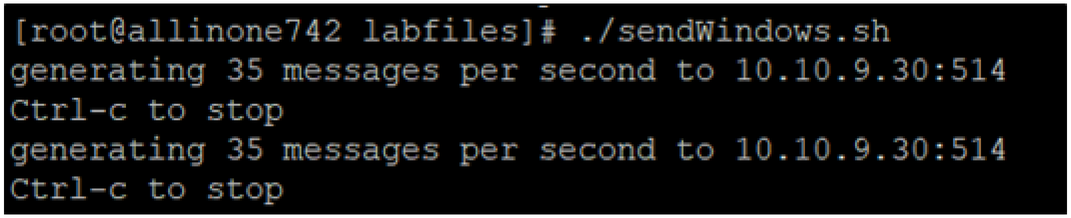
Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index
●	AccountName (custom)	0%	0%	0%

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.

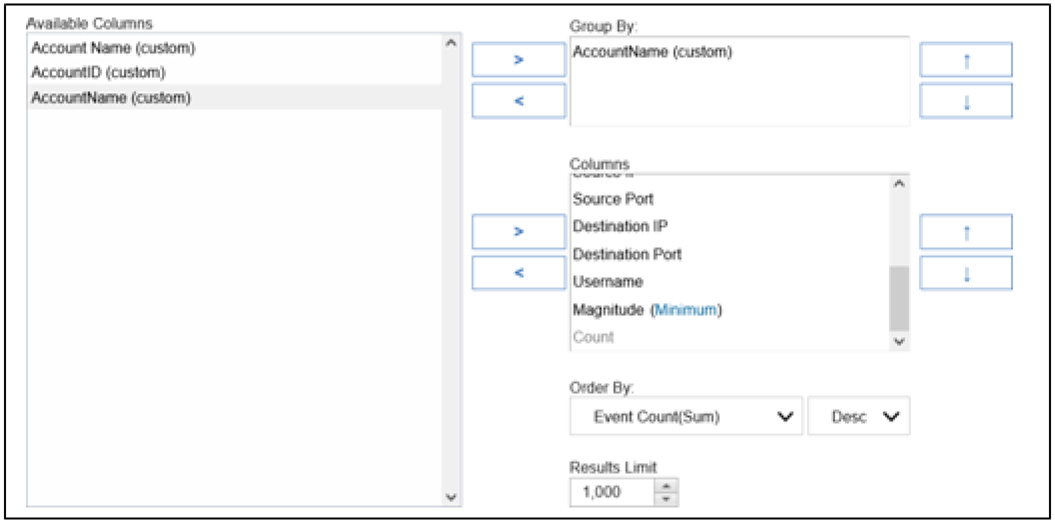
d. Edit the search.

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

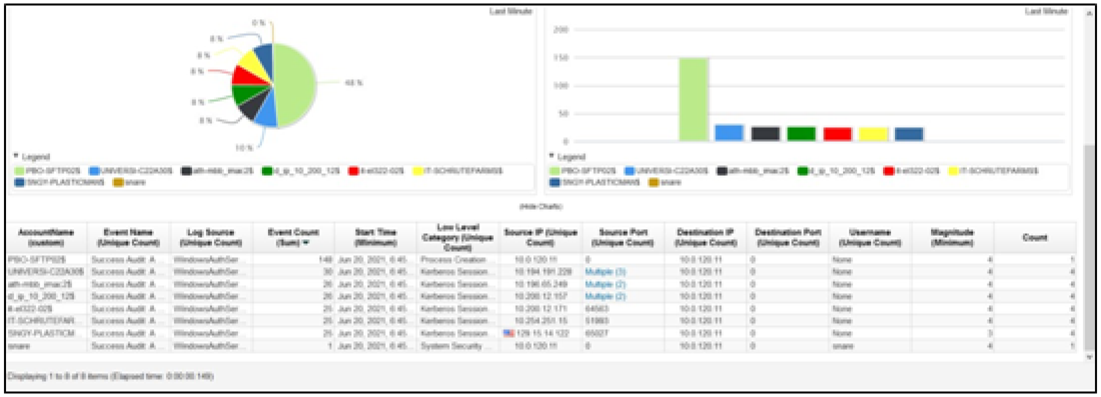
Order By:

Event Count(Sum) | Desc

Results Limit

1,000

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

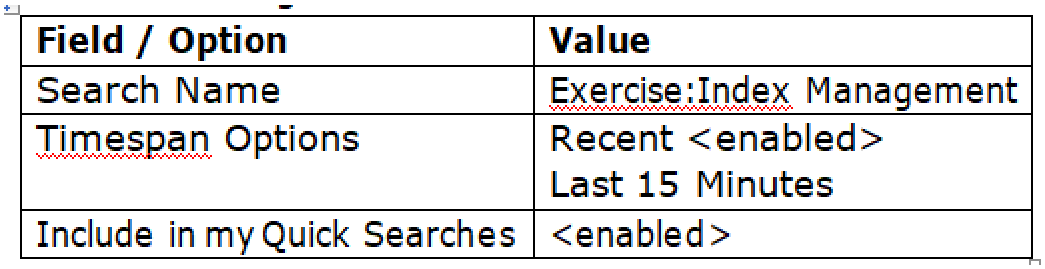


AccountName (custom)	Event Name (Unique Count)	Log Source (Unique Count)	Event Count (Sum) ▾	Start Time (Minimum)	Low Level Category (Unique Count)	Source IP (Unique Count)	Source Port (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Username (Unique Count)	Magnitude (Minimum)	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
SNOY-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.