**LAB-2 REPORT**

Course Code - Course Name: - COMP4040 – Introduction to SOC

Program: T433 - Cybersecurity

Term: - Winter 2024

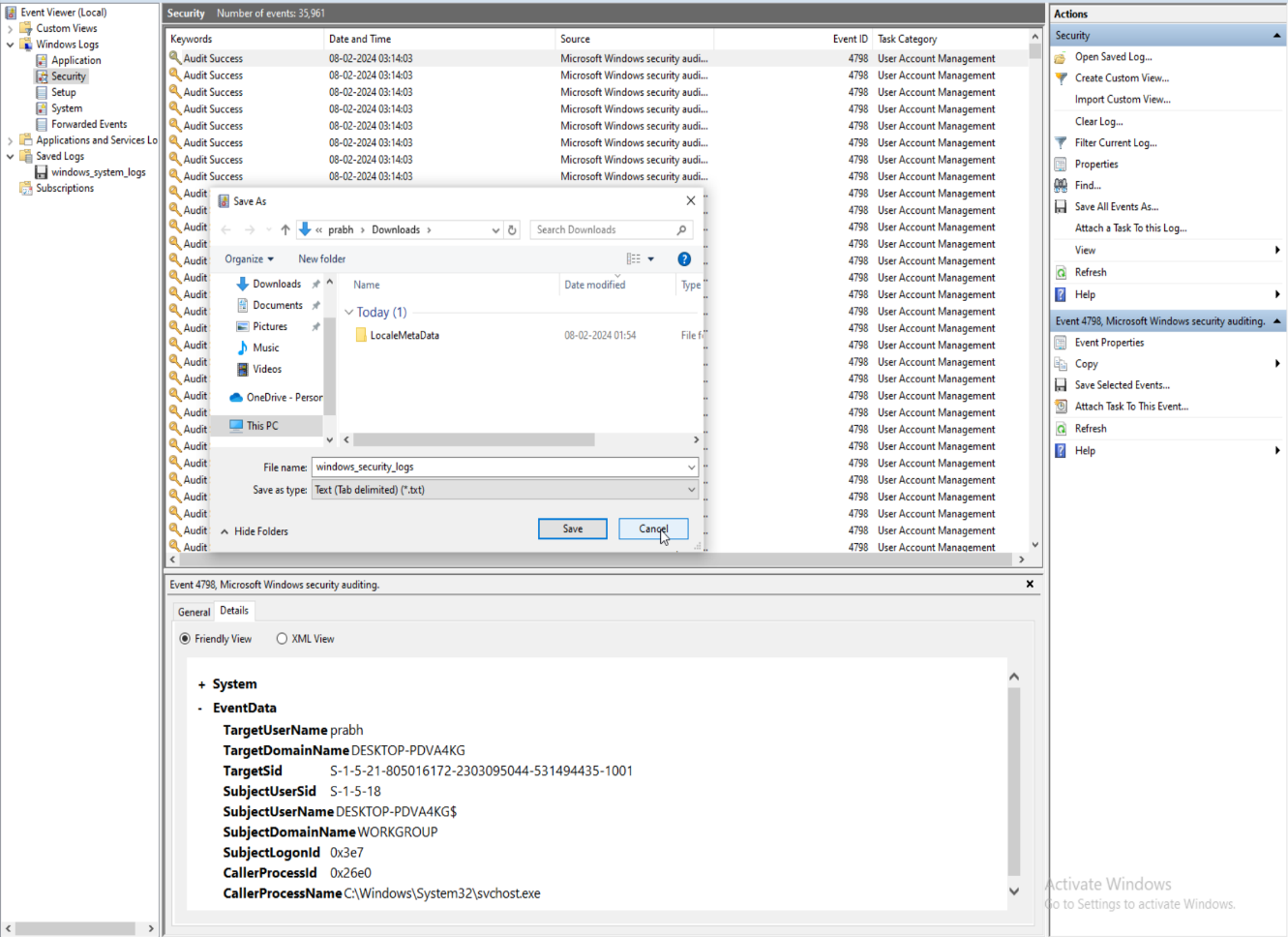
Group: SOC1-L2G- 11

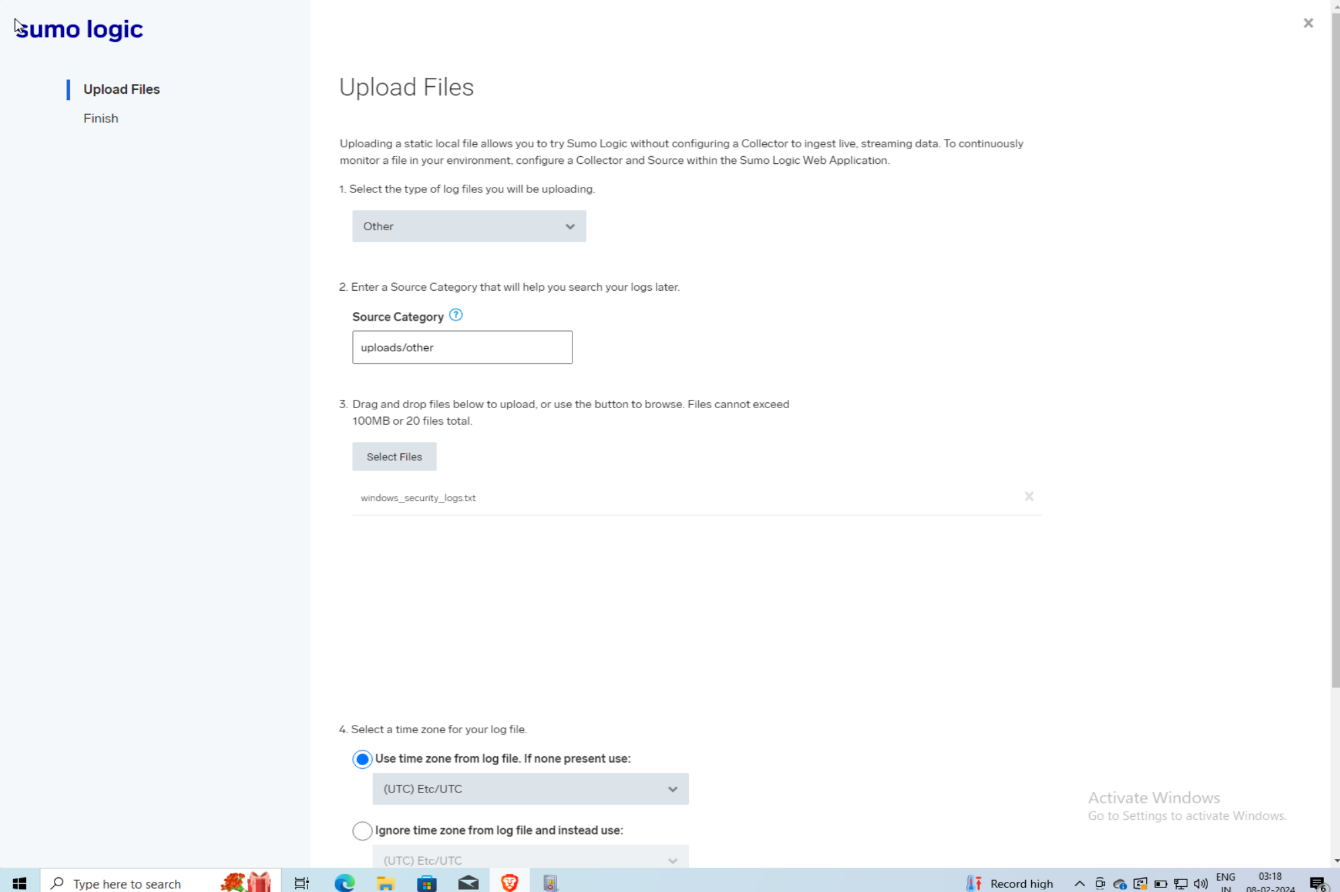
Student Names - ID:

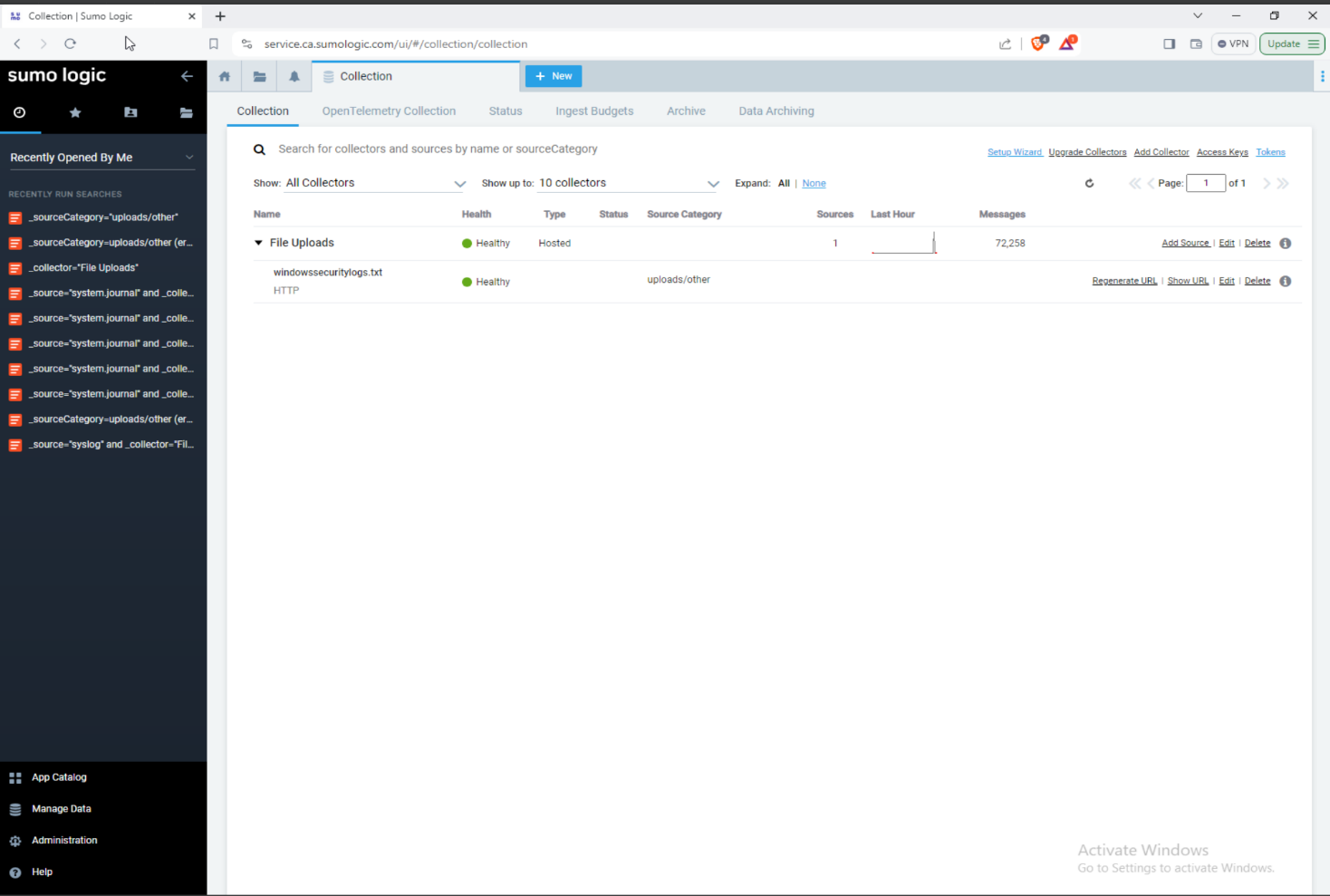
* Prabhjot Singh Sains – 101495218

1) Save Windows VM Security and system logs (separately) then upload In Sumologic - Saving, Uploading, and Sumologic collection page.

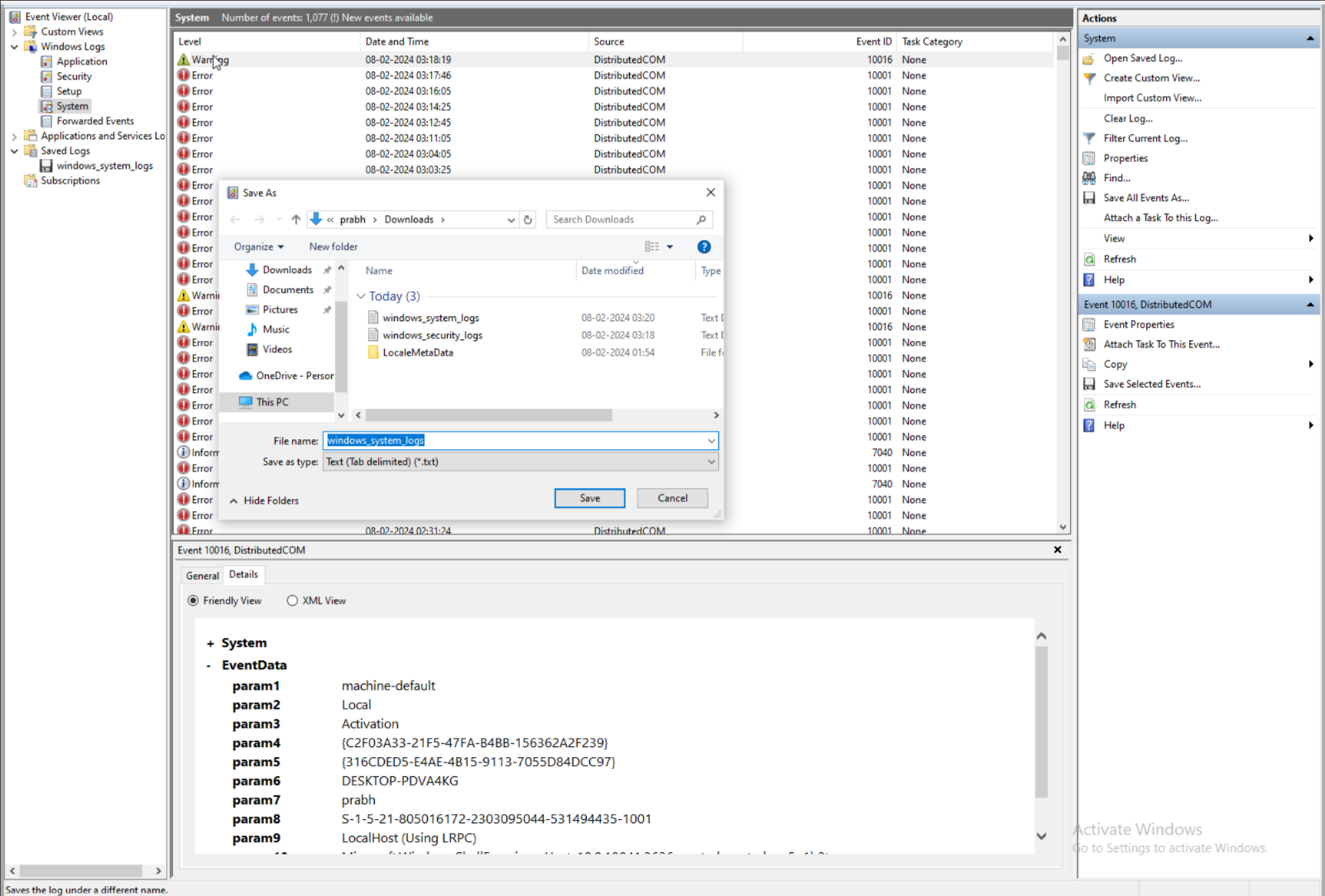
**Security logs:**

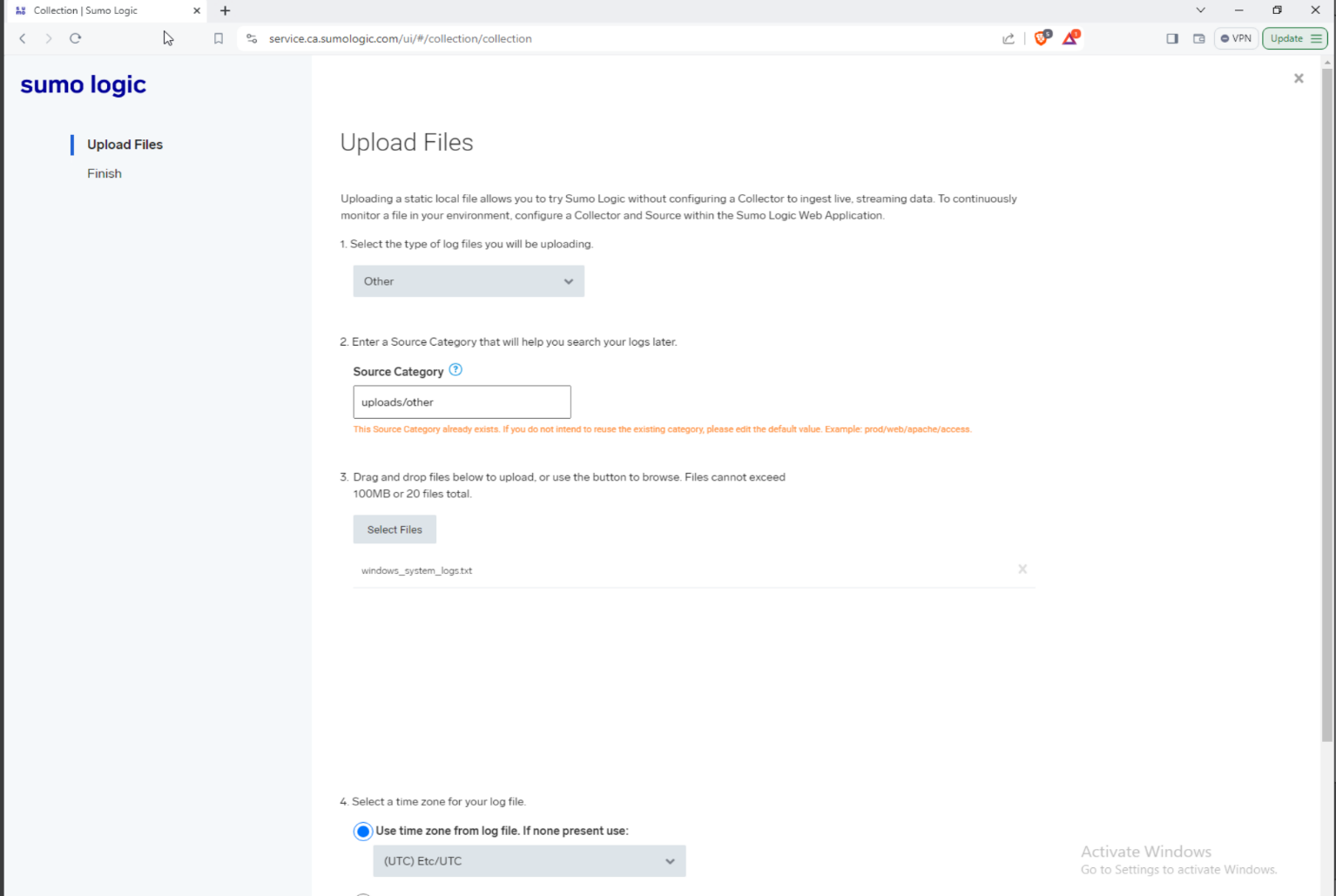


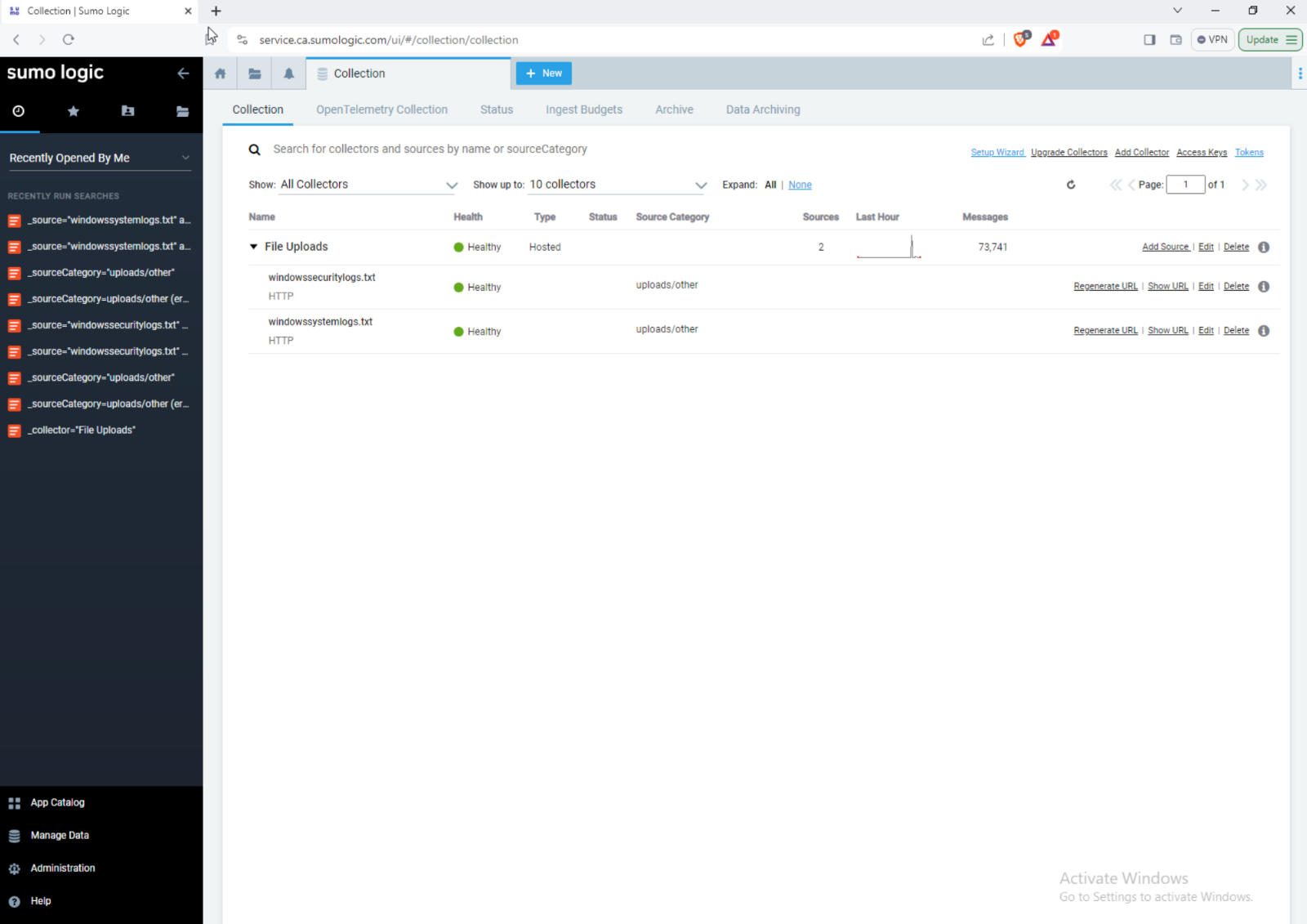




**System Log:**

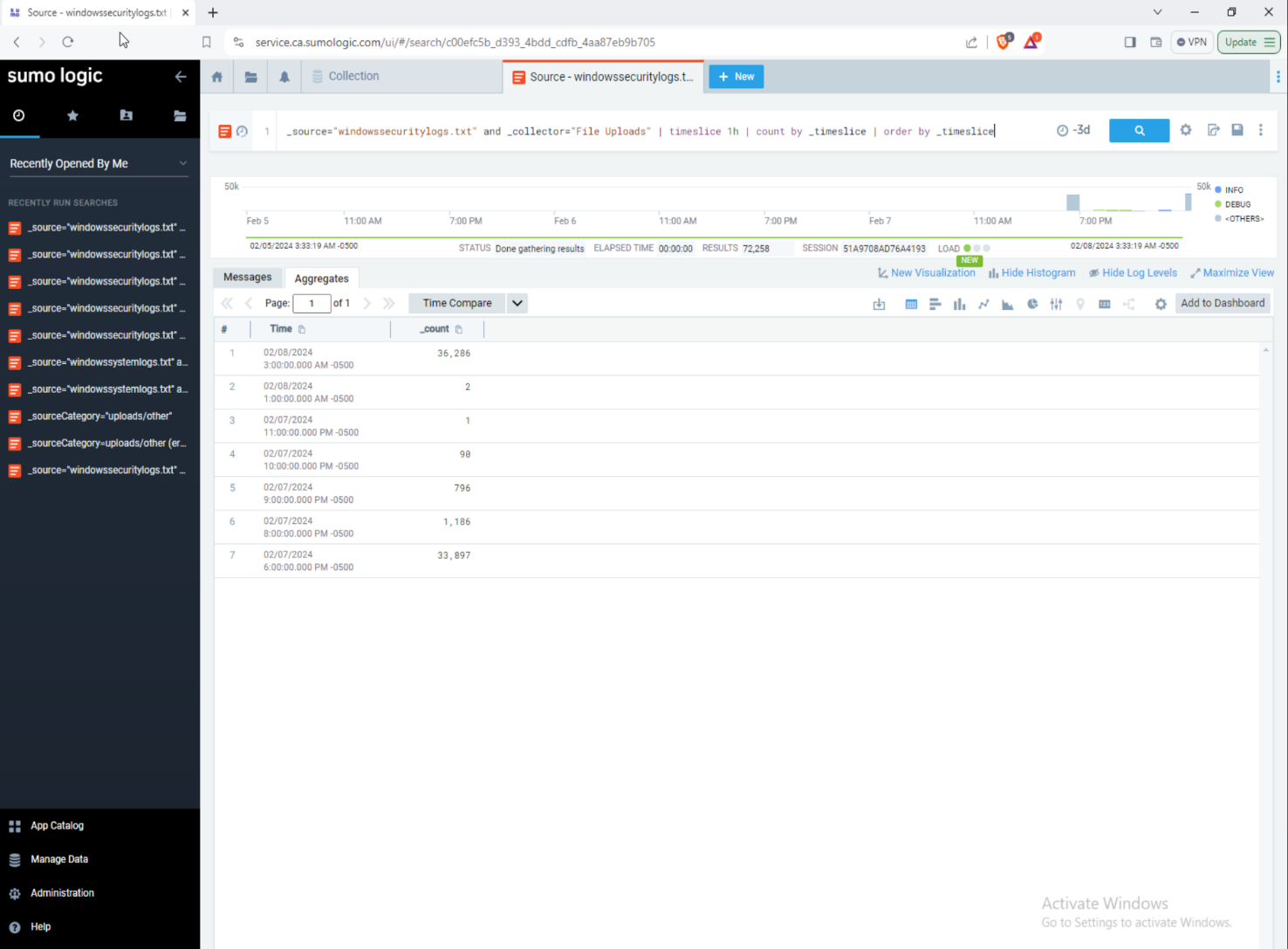


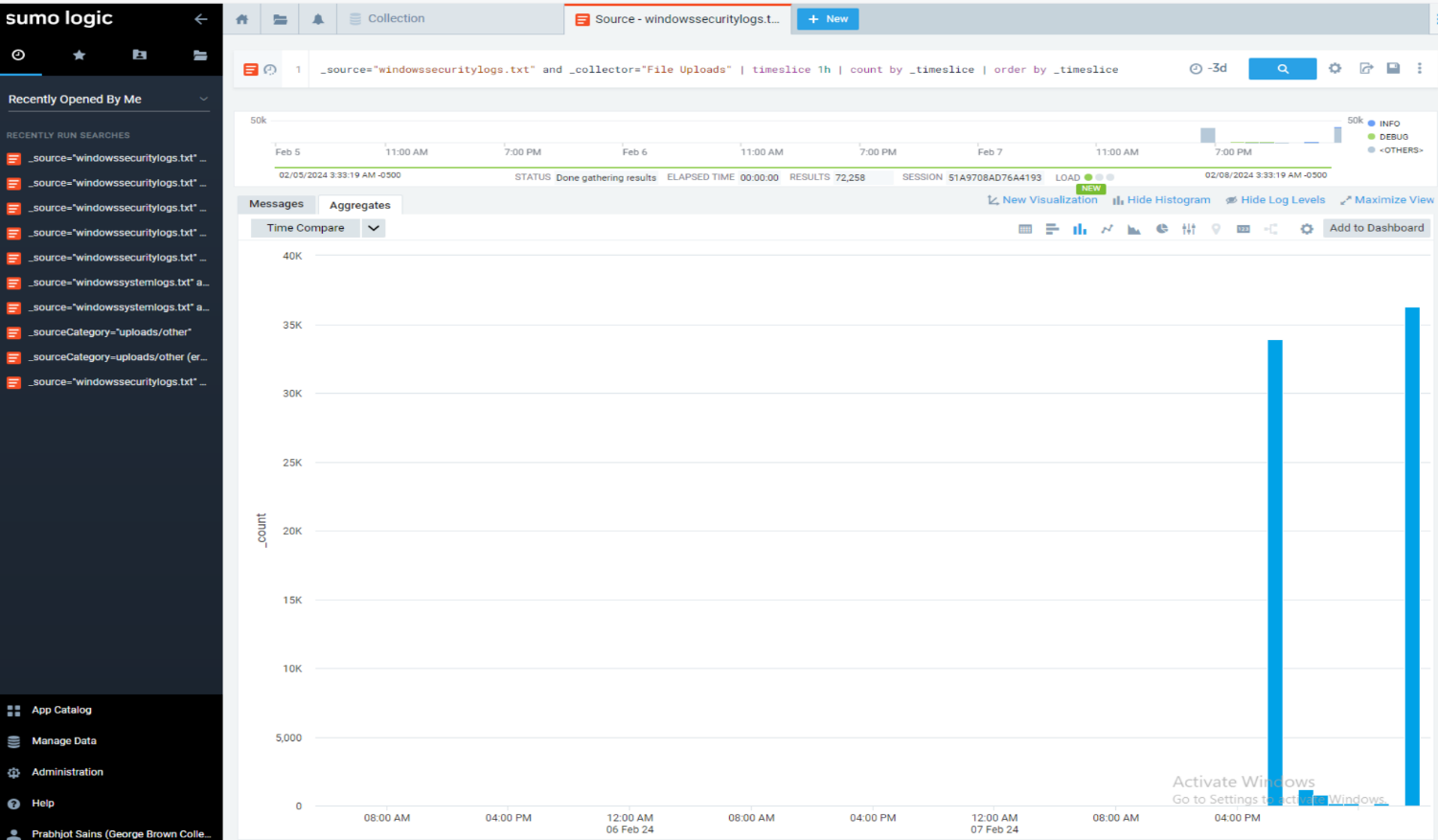




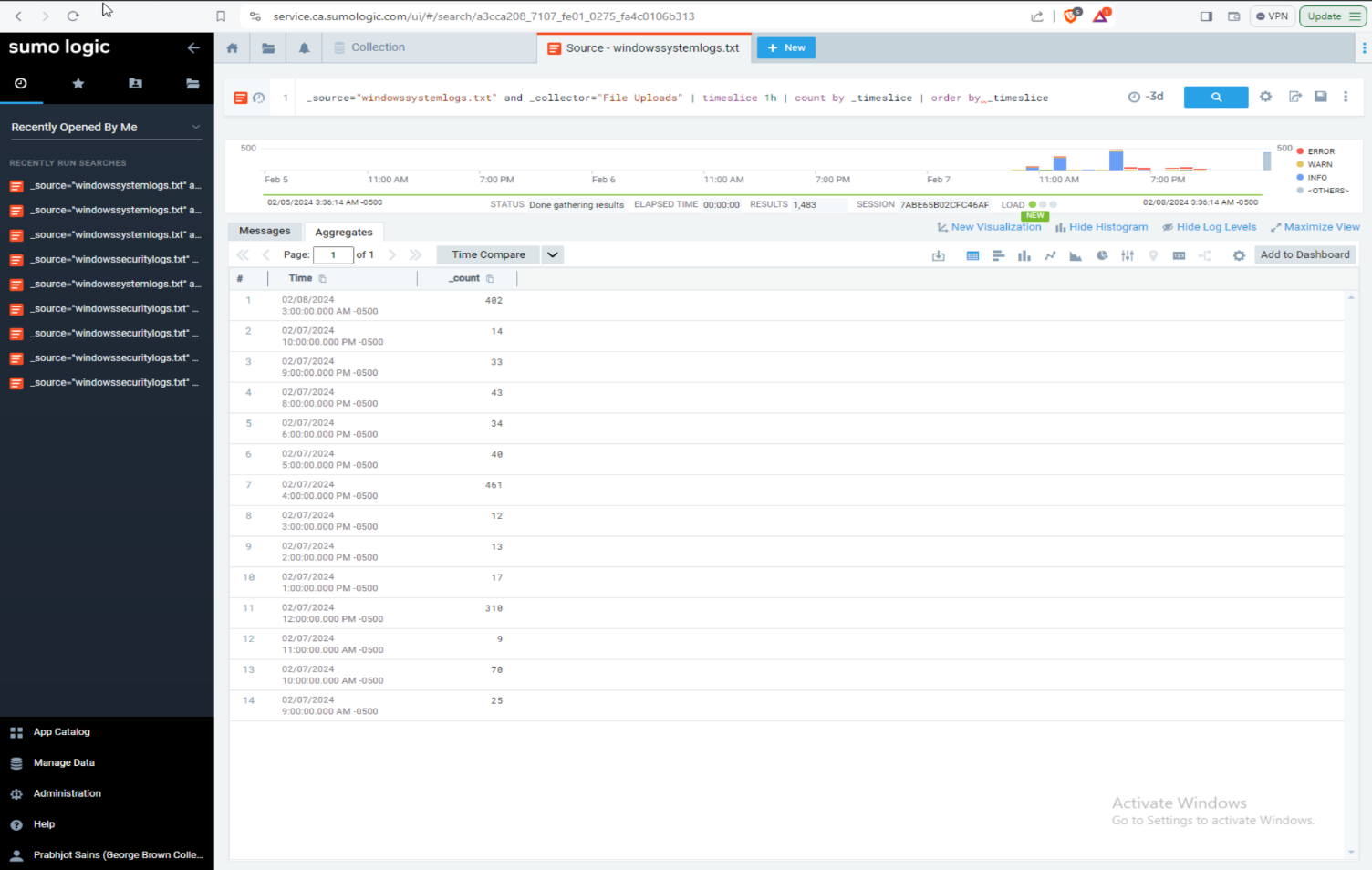
2) For the last 3 days order each 1-hour time window with the number of Security logs and system logs then create a graph for each.

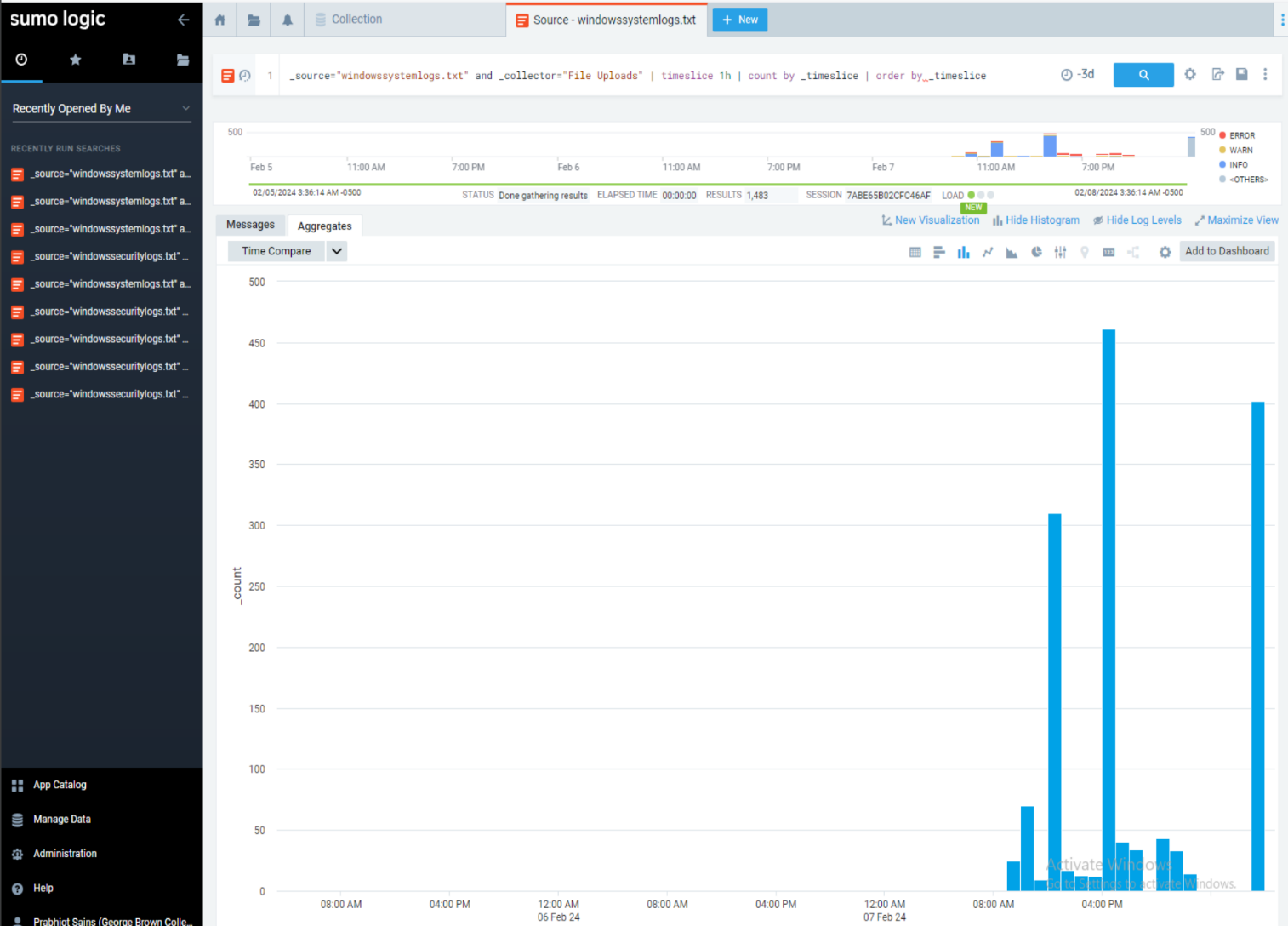
**Security Log:**





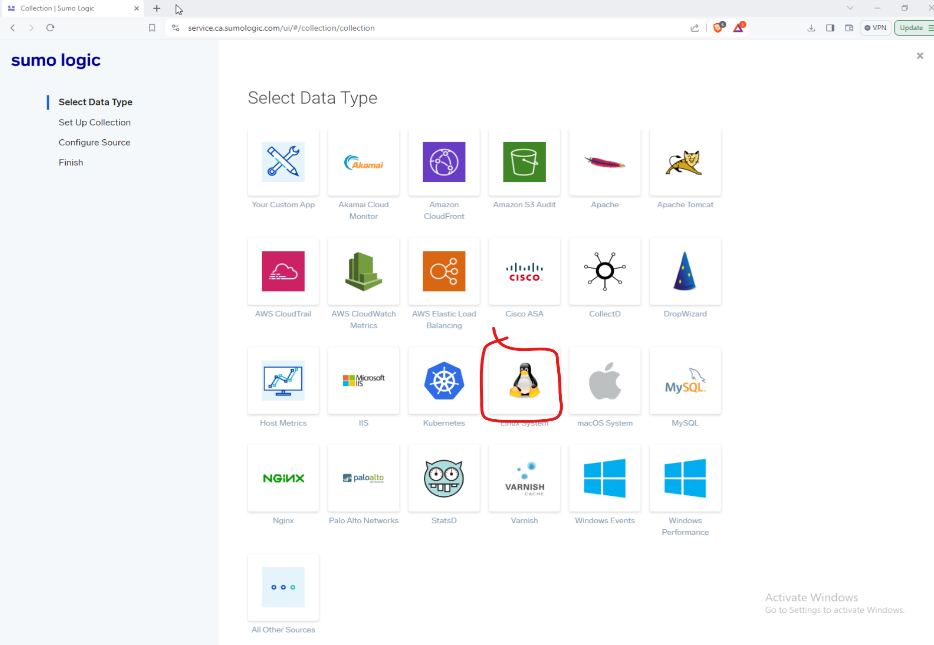
**System Log:**

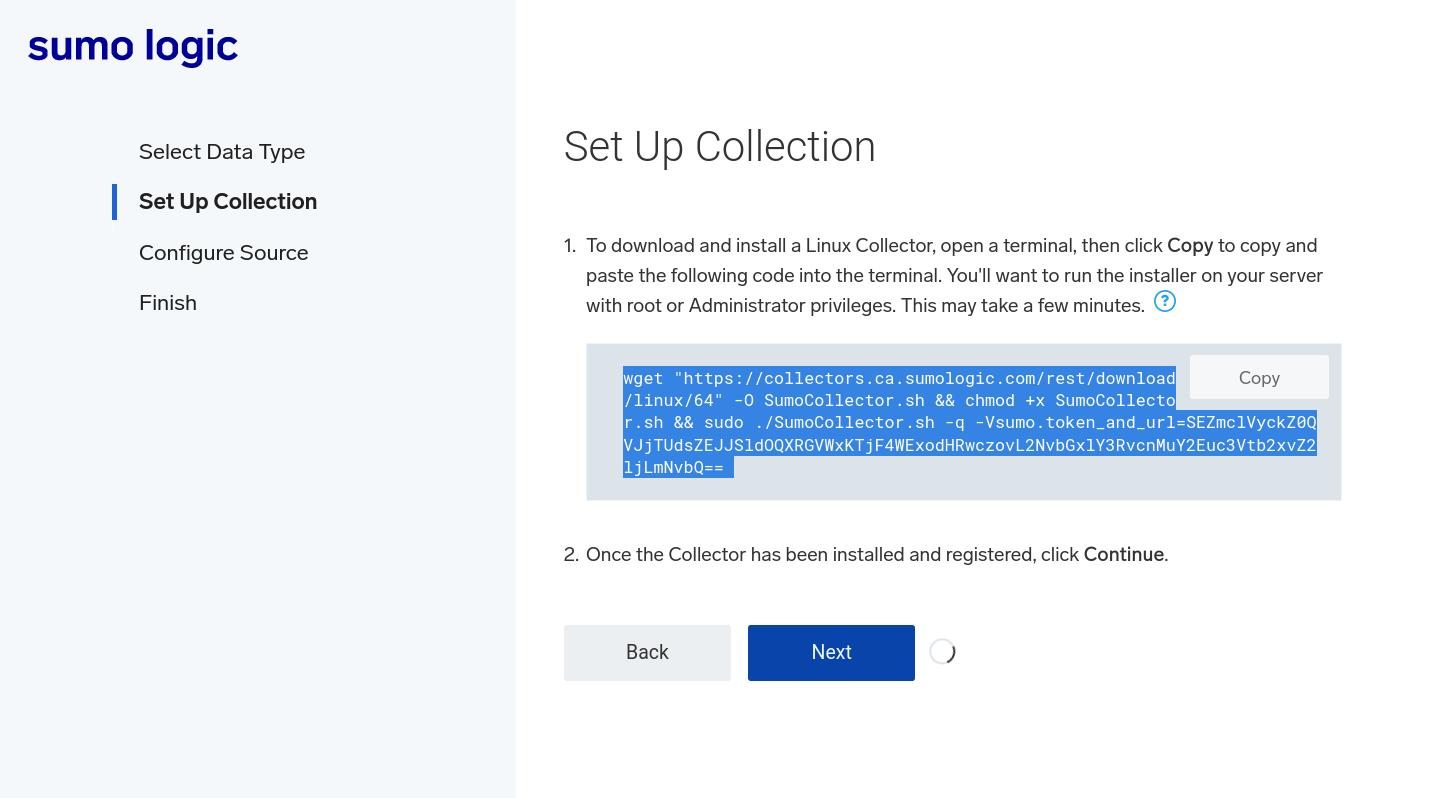


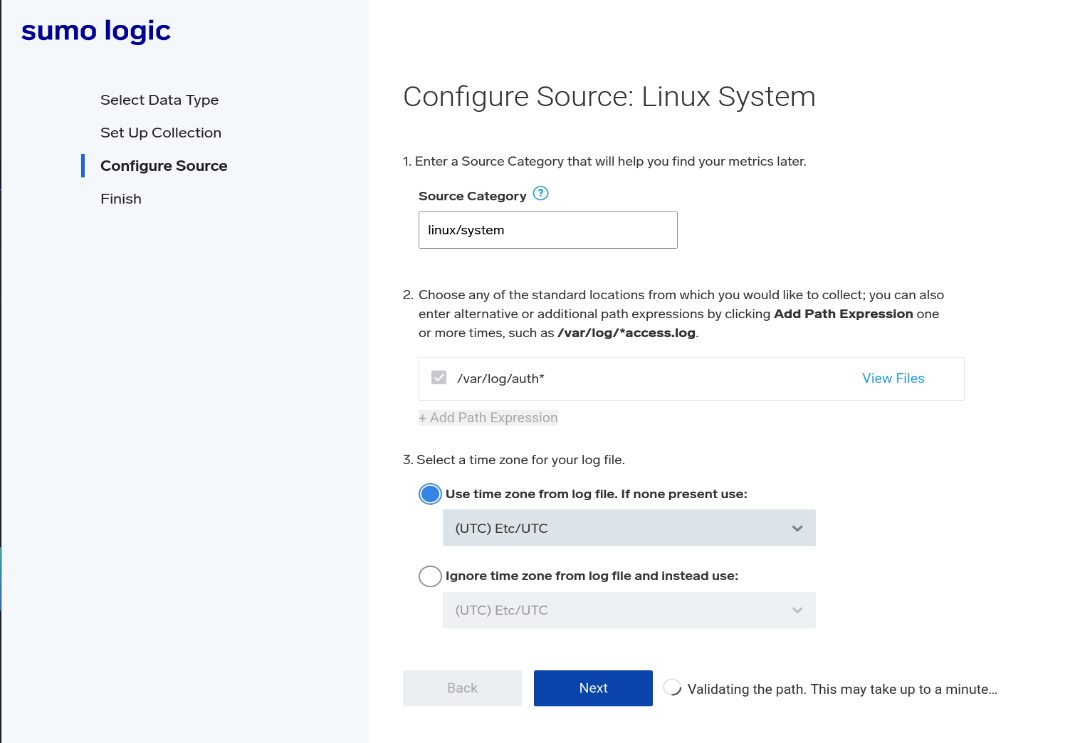


3) In Sumologic Using Manage Data\Collection\Setup Wizard

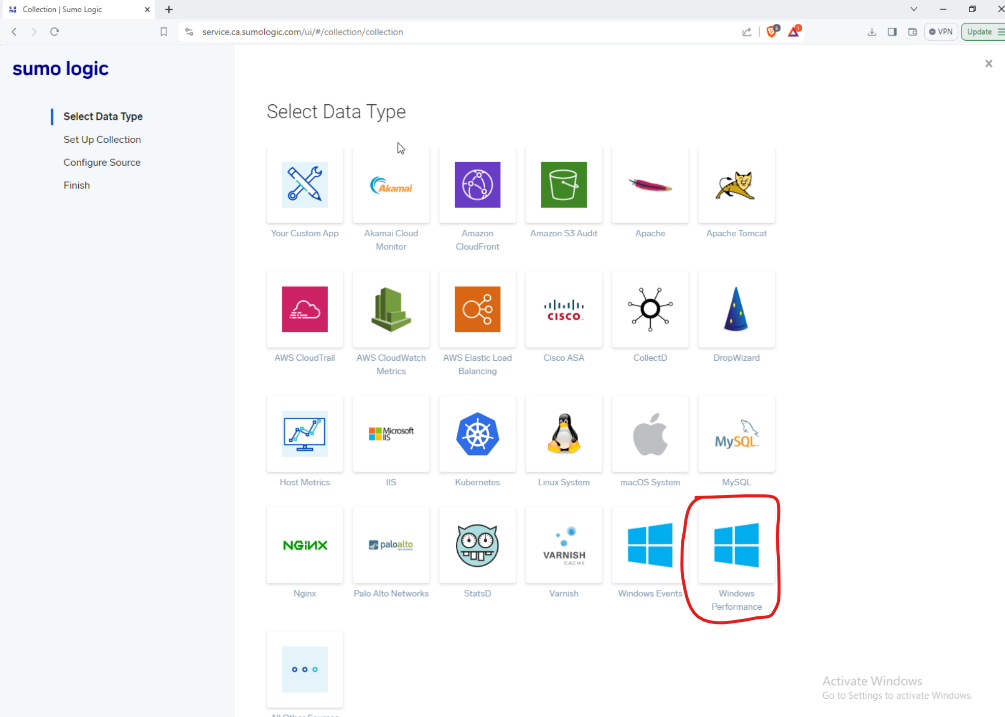
- Install Sumologic collector in Linux VM

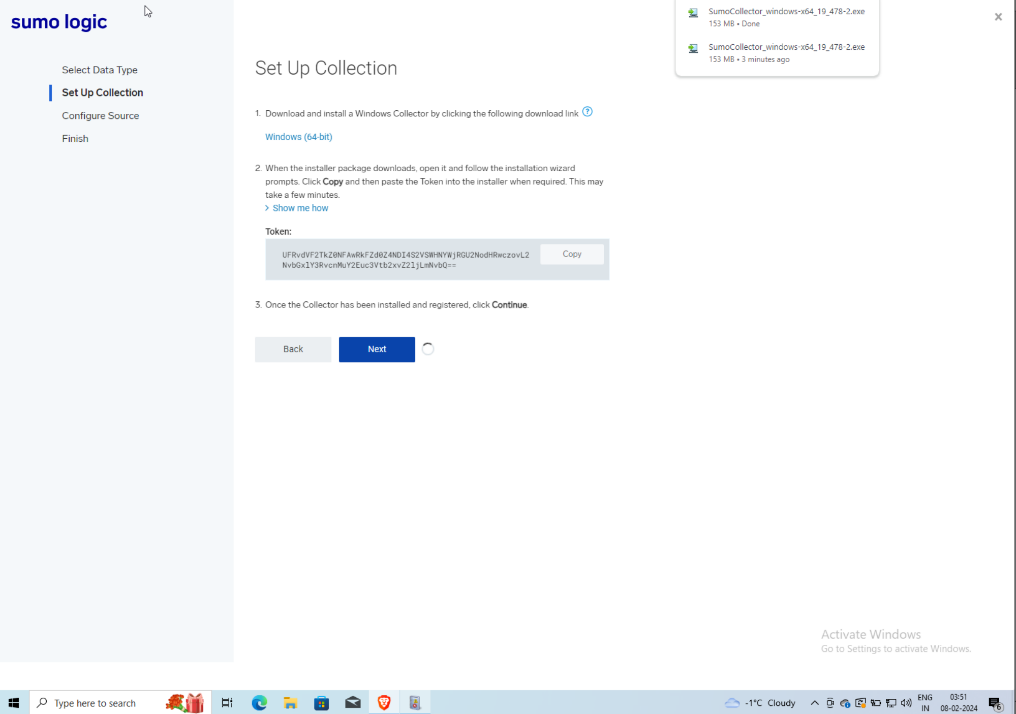


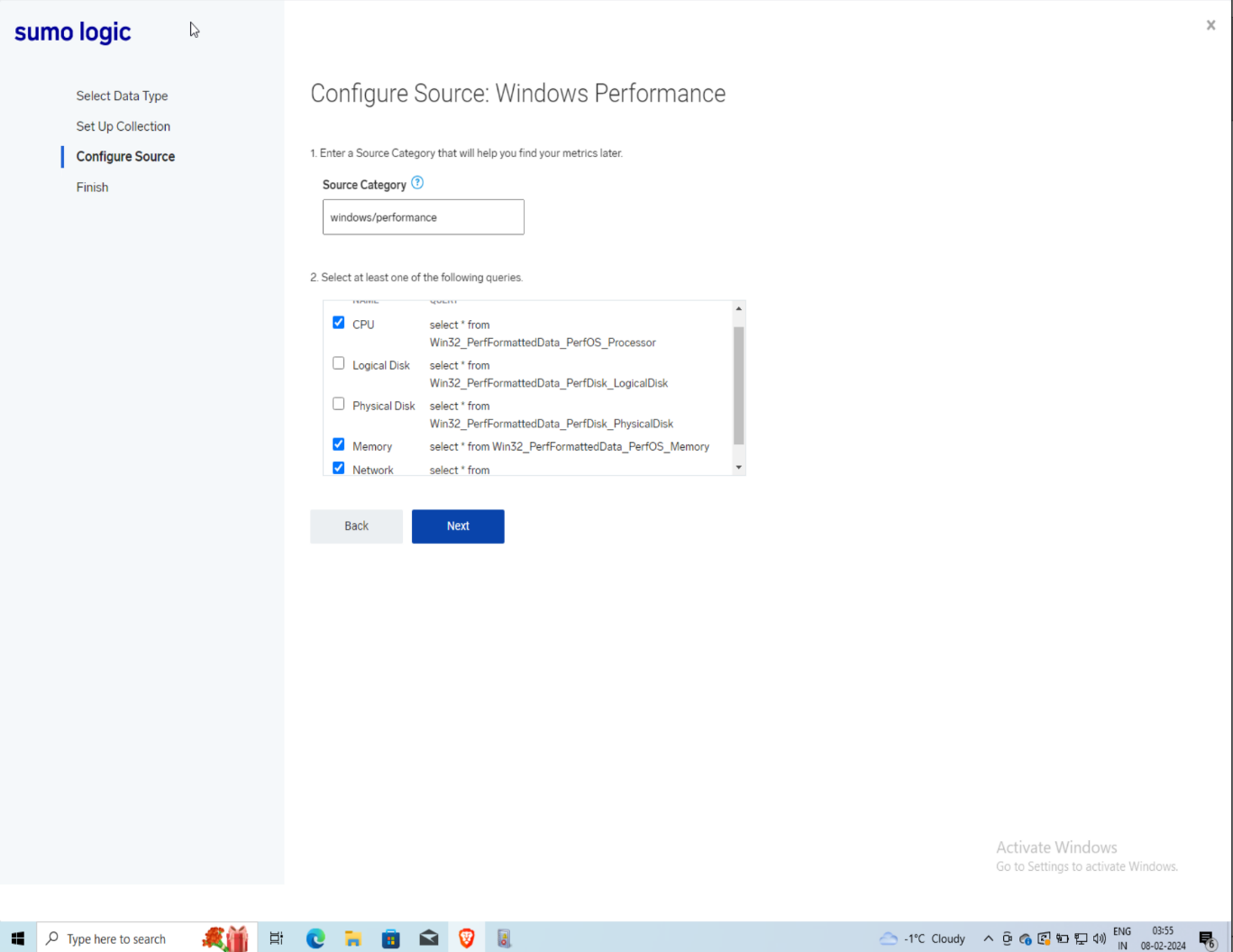




- Install Sumologic Collector in Windows 10 VM

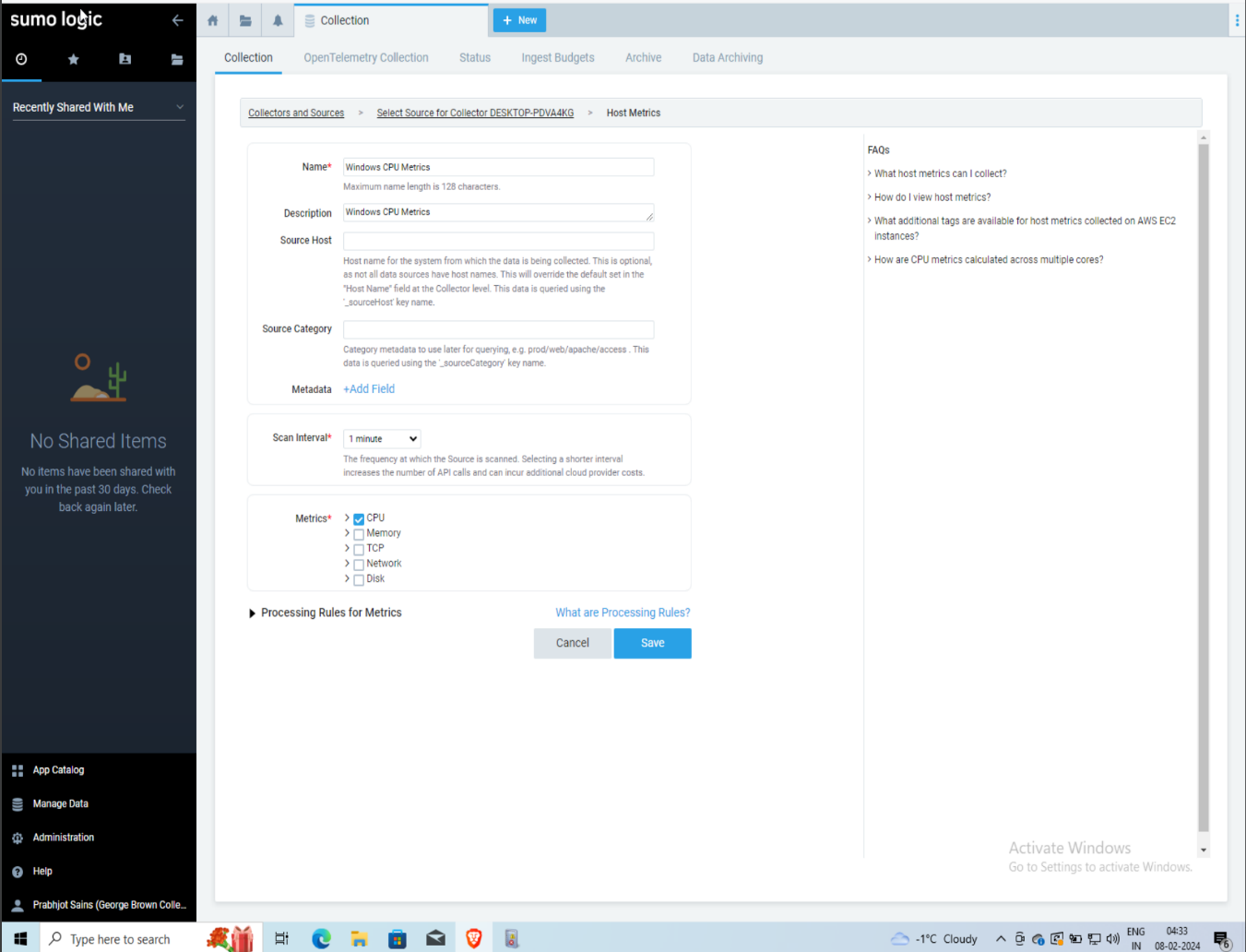




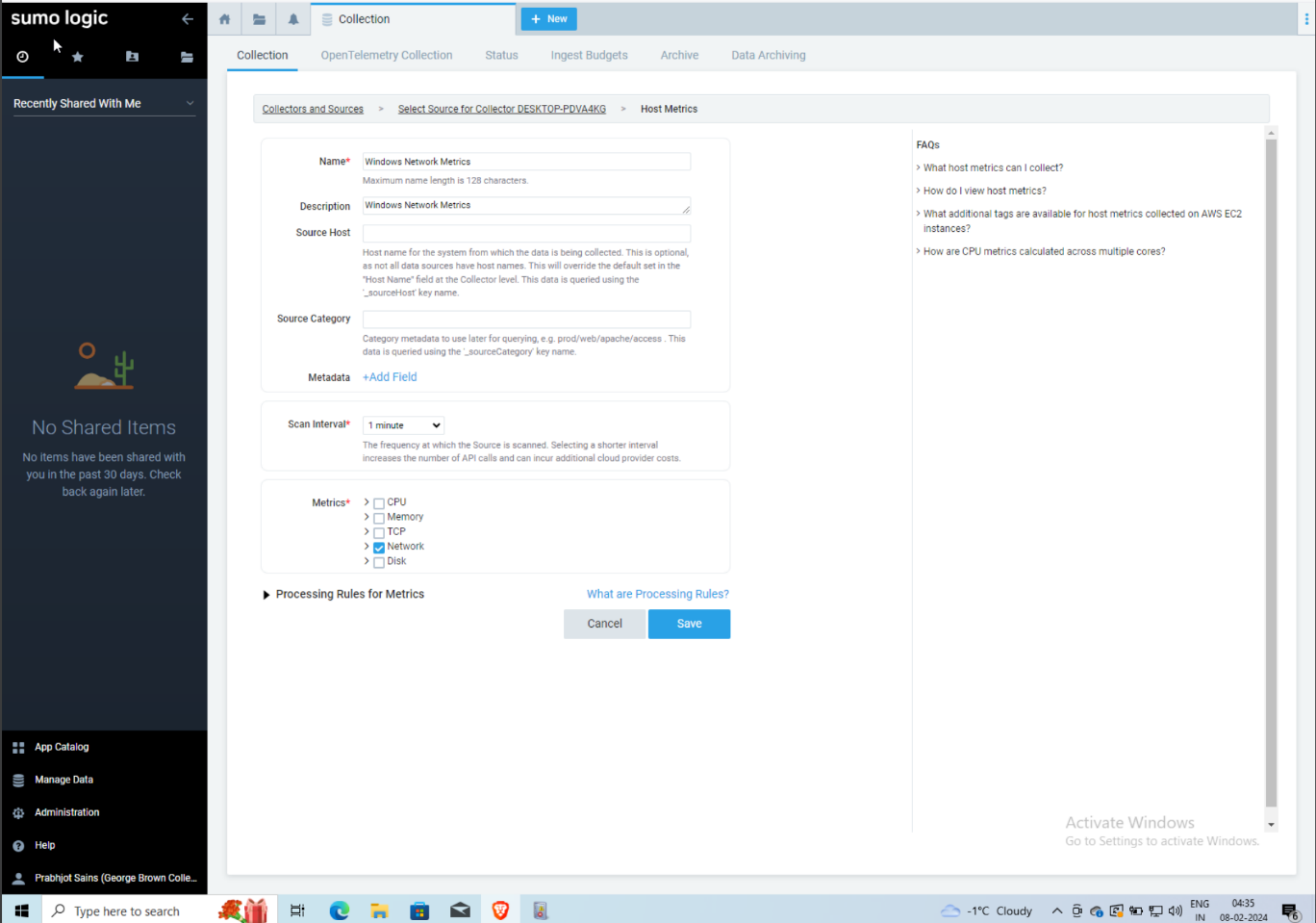


4) Add Windows and Linux VMs CPU and Network metrics.

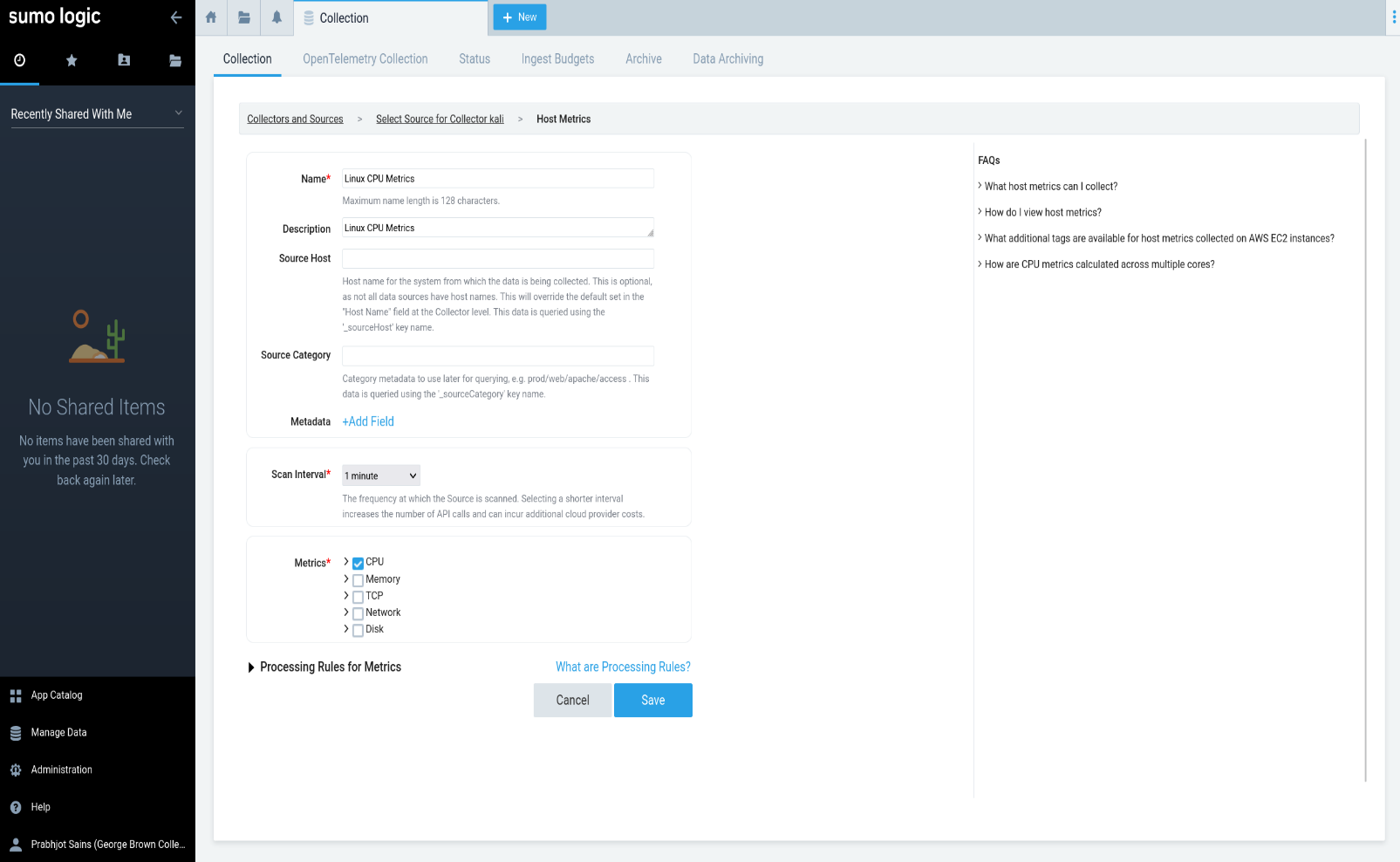
**Windows CPU metrics:**



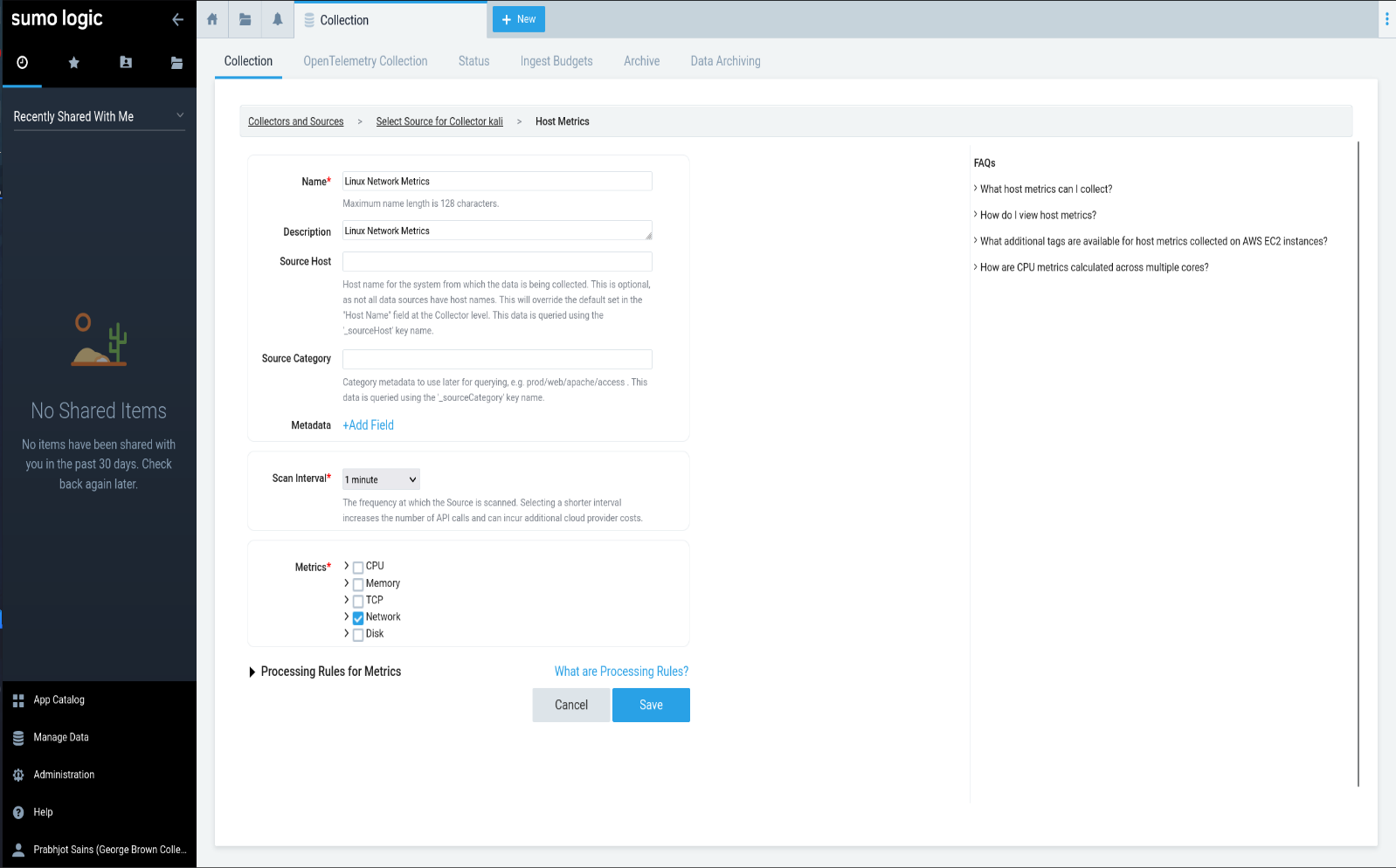
**Windows Network metrics:**



**Linux CPU Metrics:**

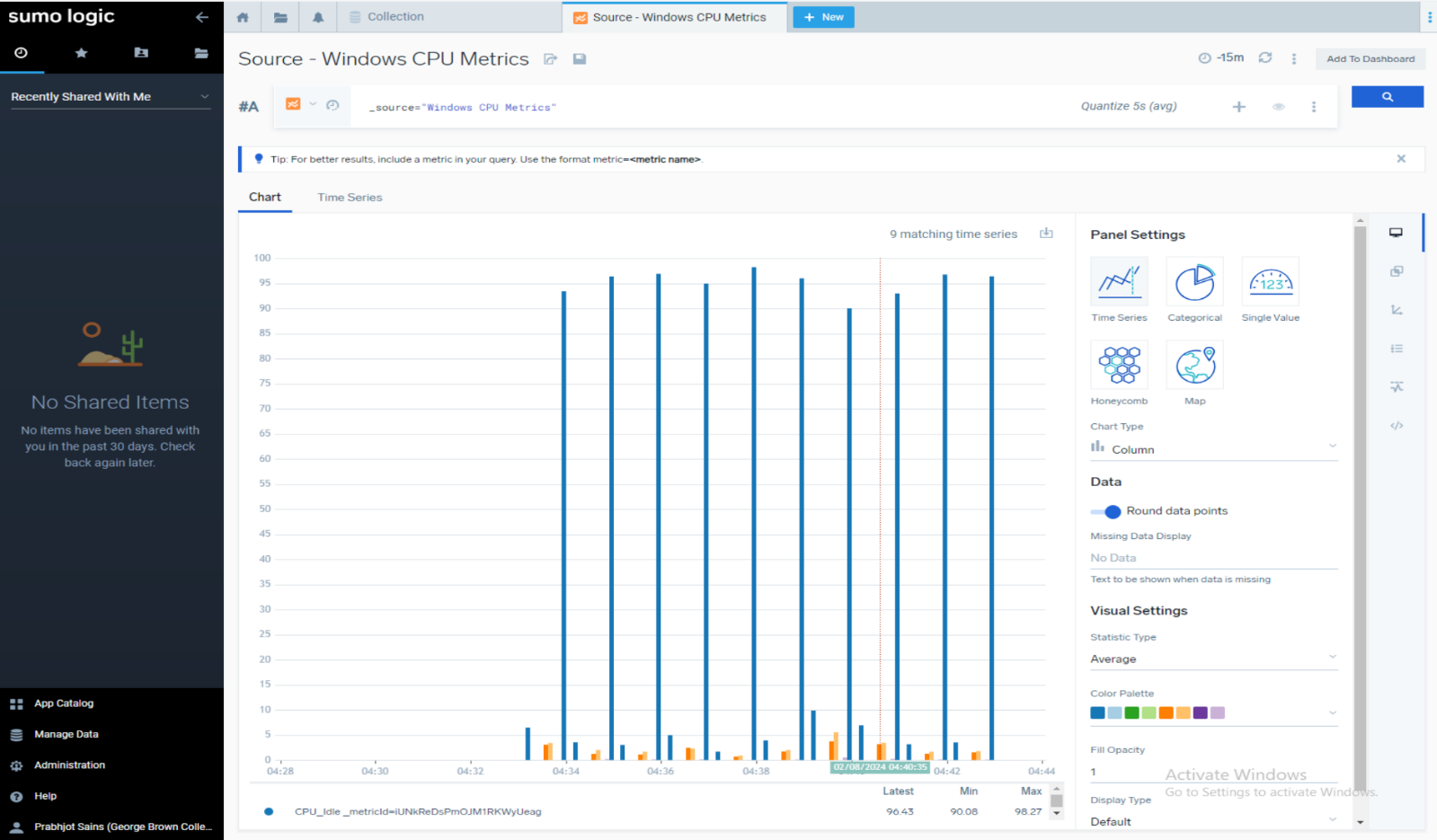
****

**Linux Network Metrics:**

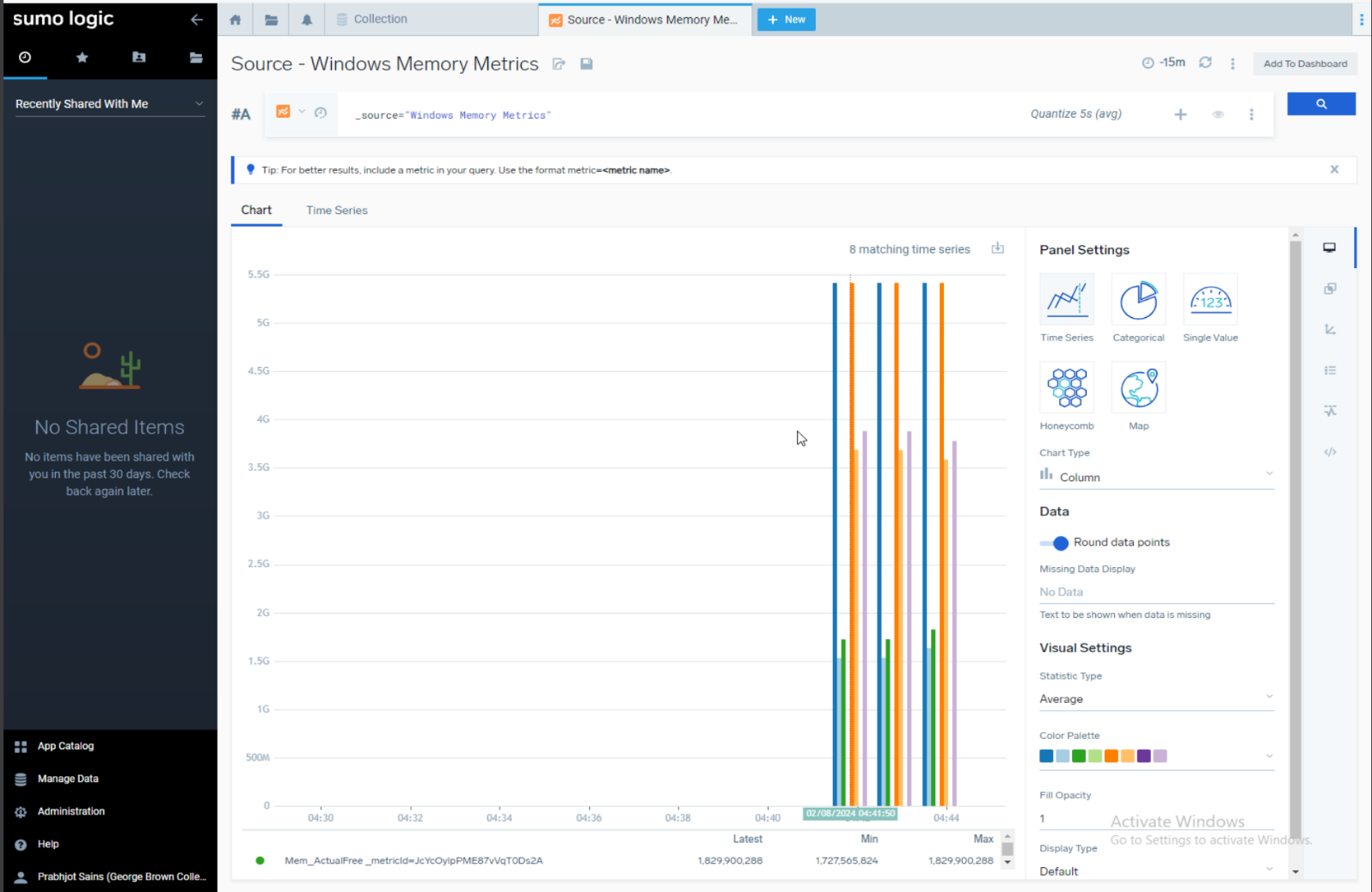
****

5) Create a graph of CPU and Memory utilization.

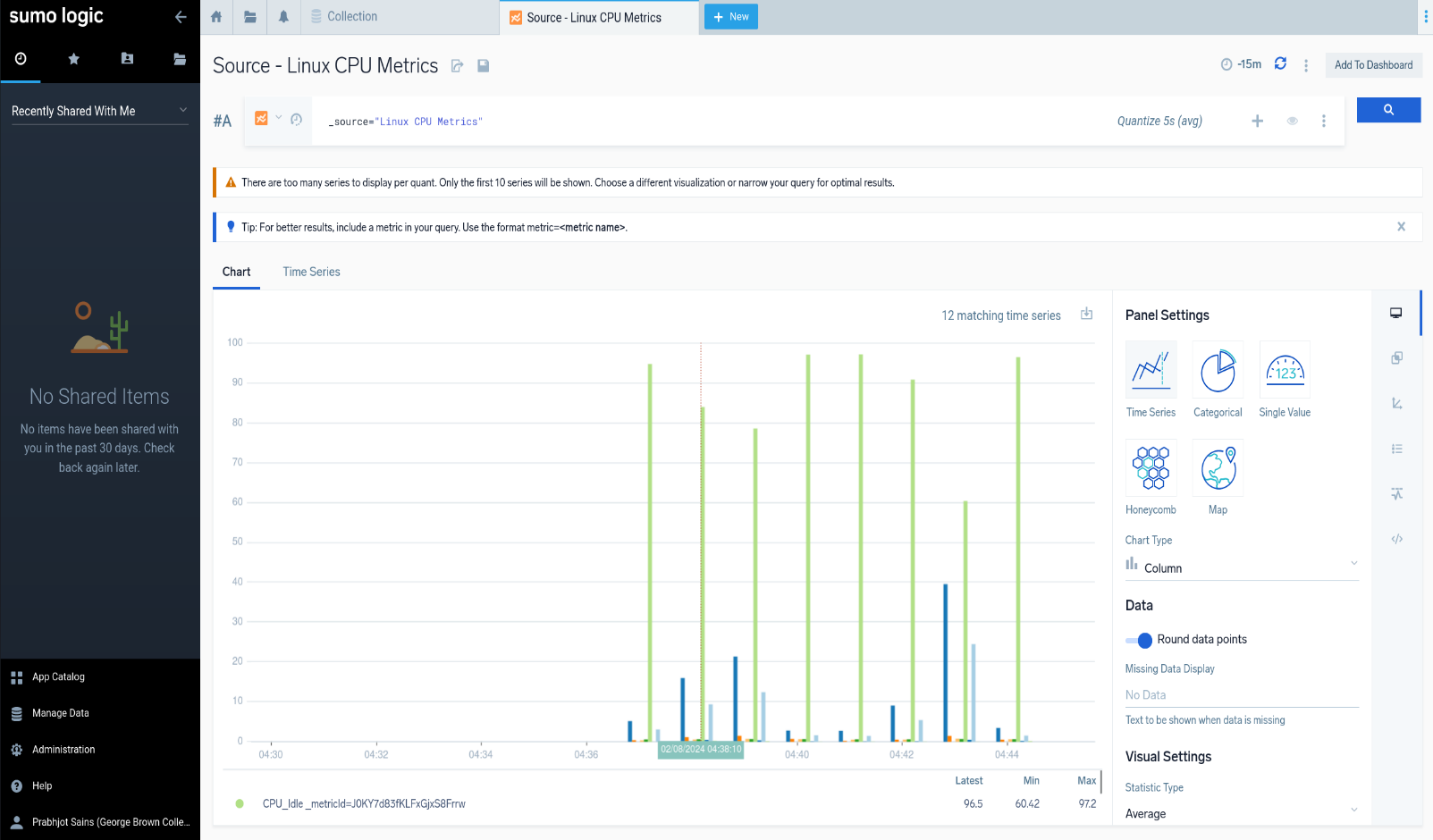
**Windows CPU metrics:**



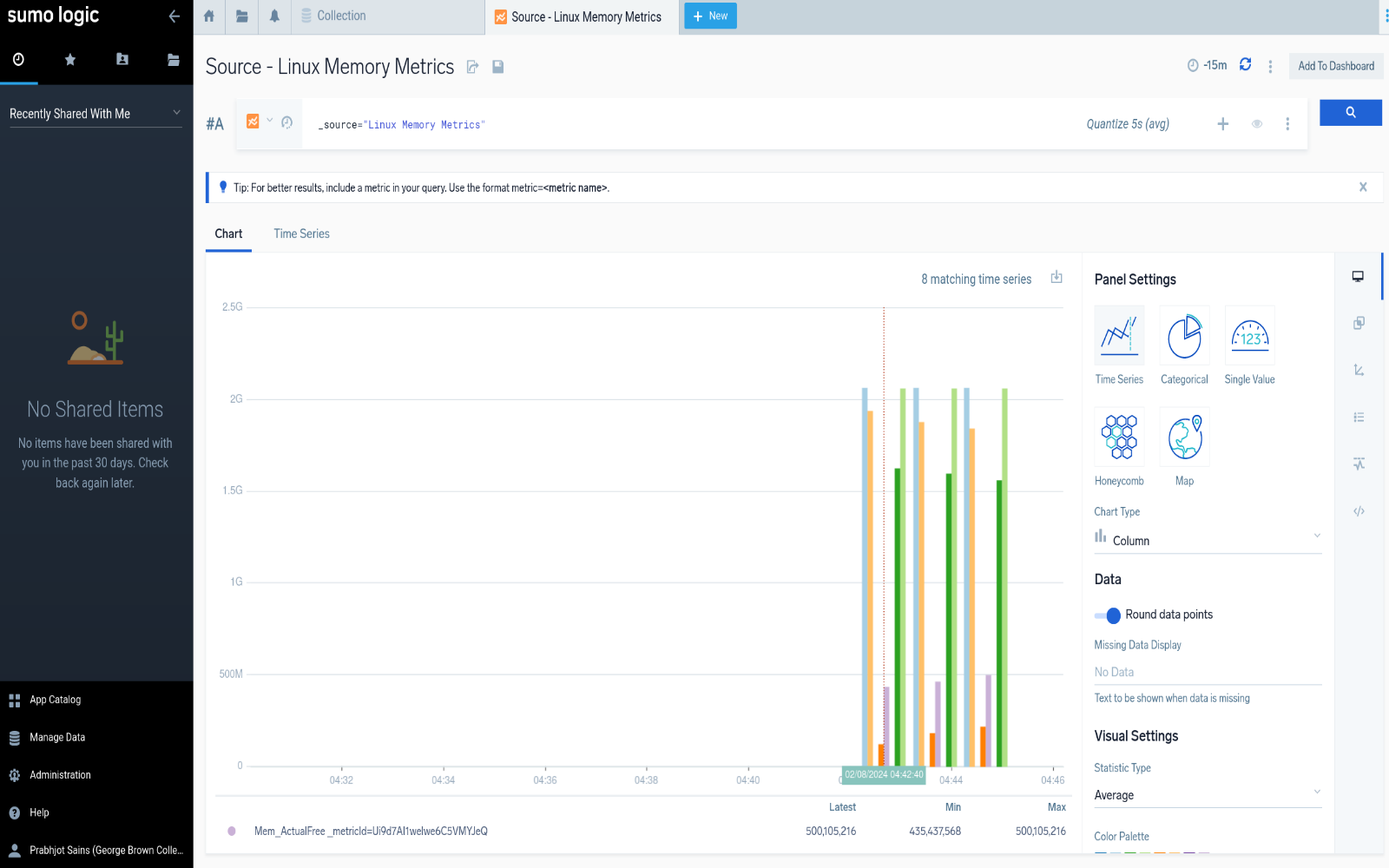
**Windows Memory metrics:**



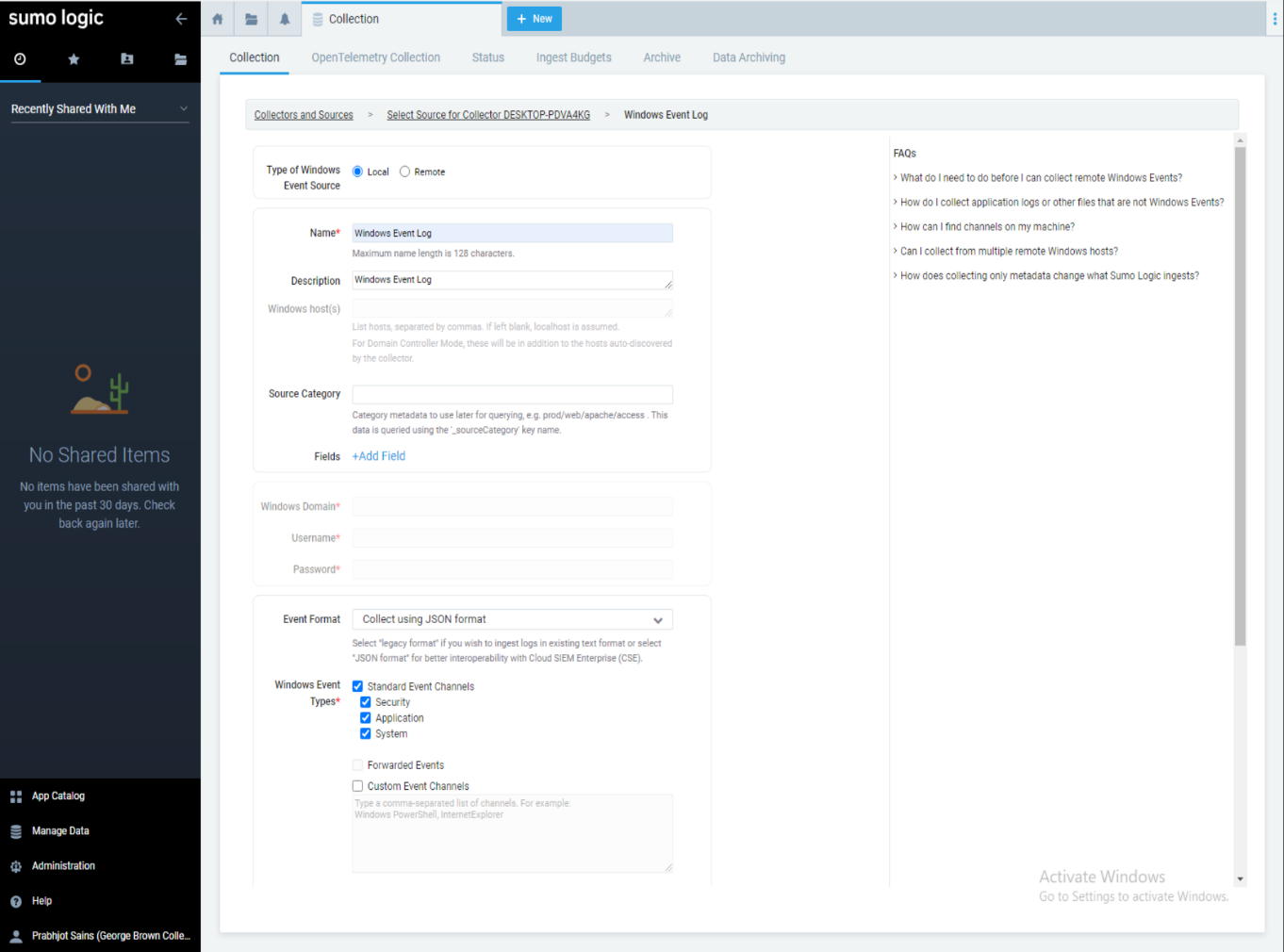
**Linux CPU metrics:**

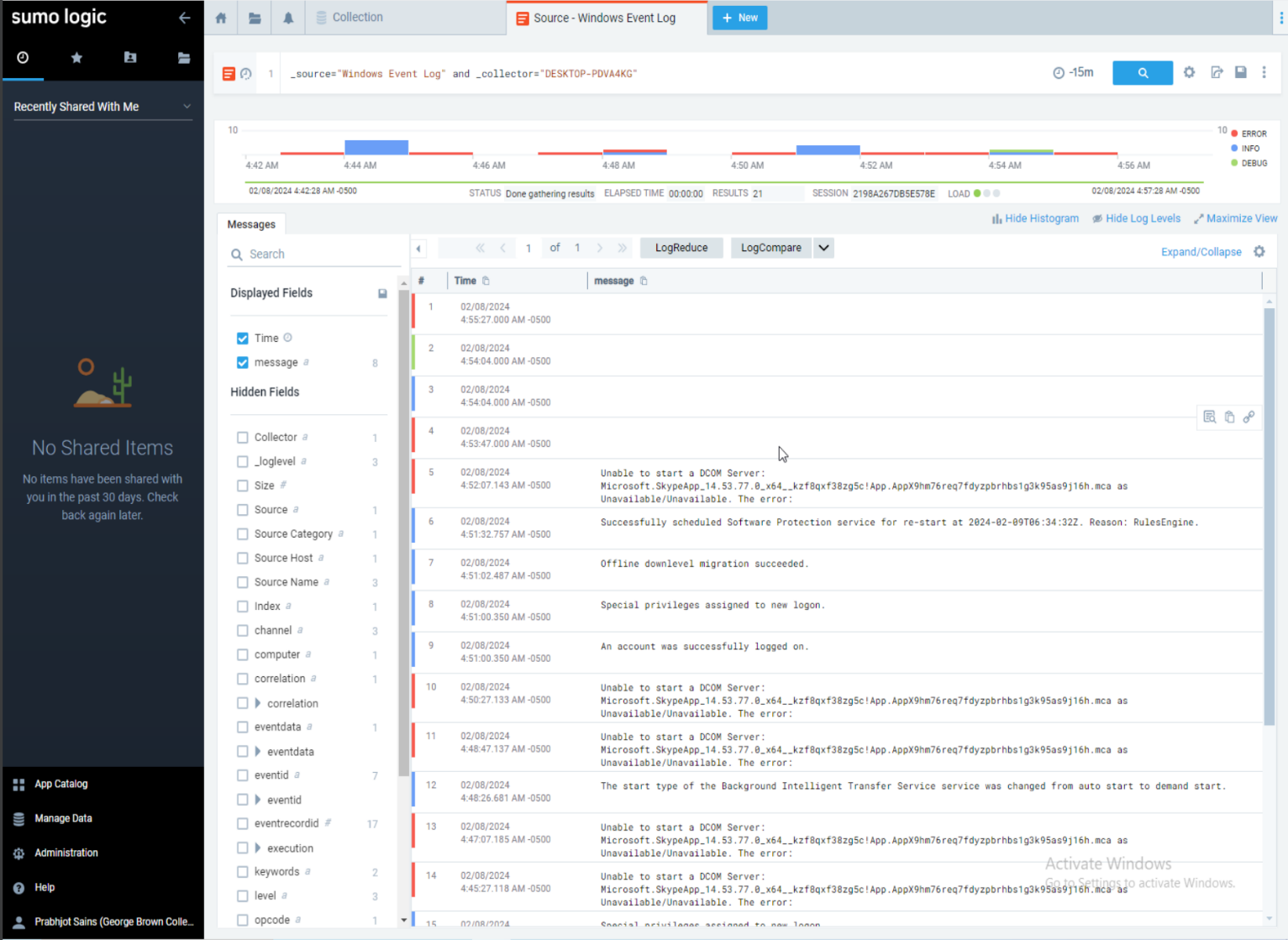


**Linux Memory metrics:**

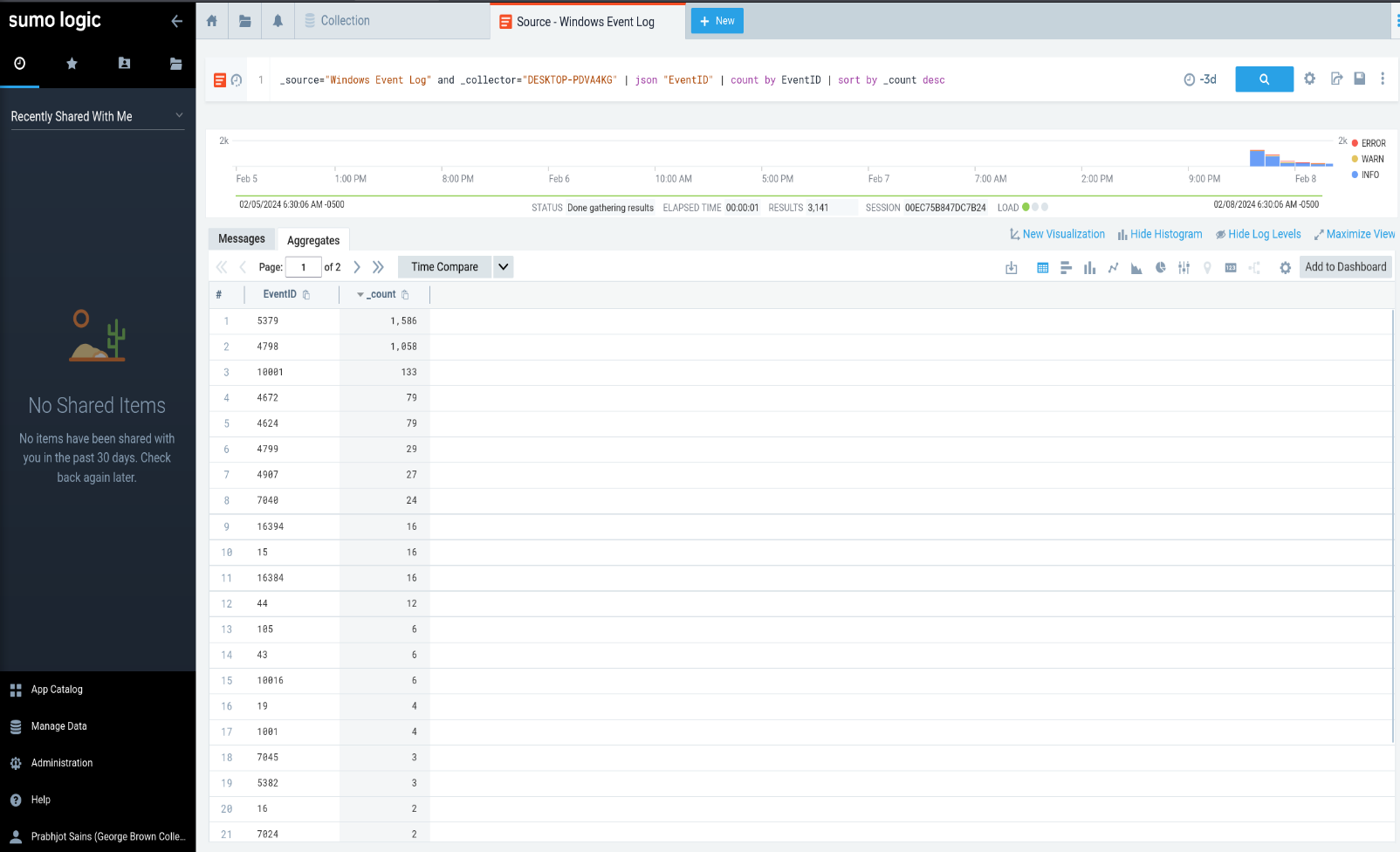


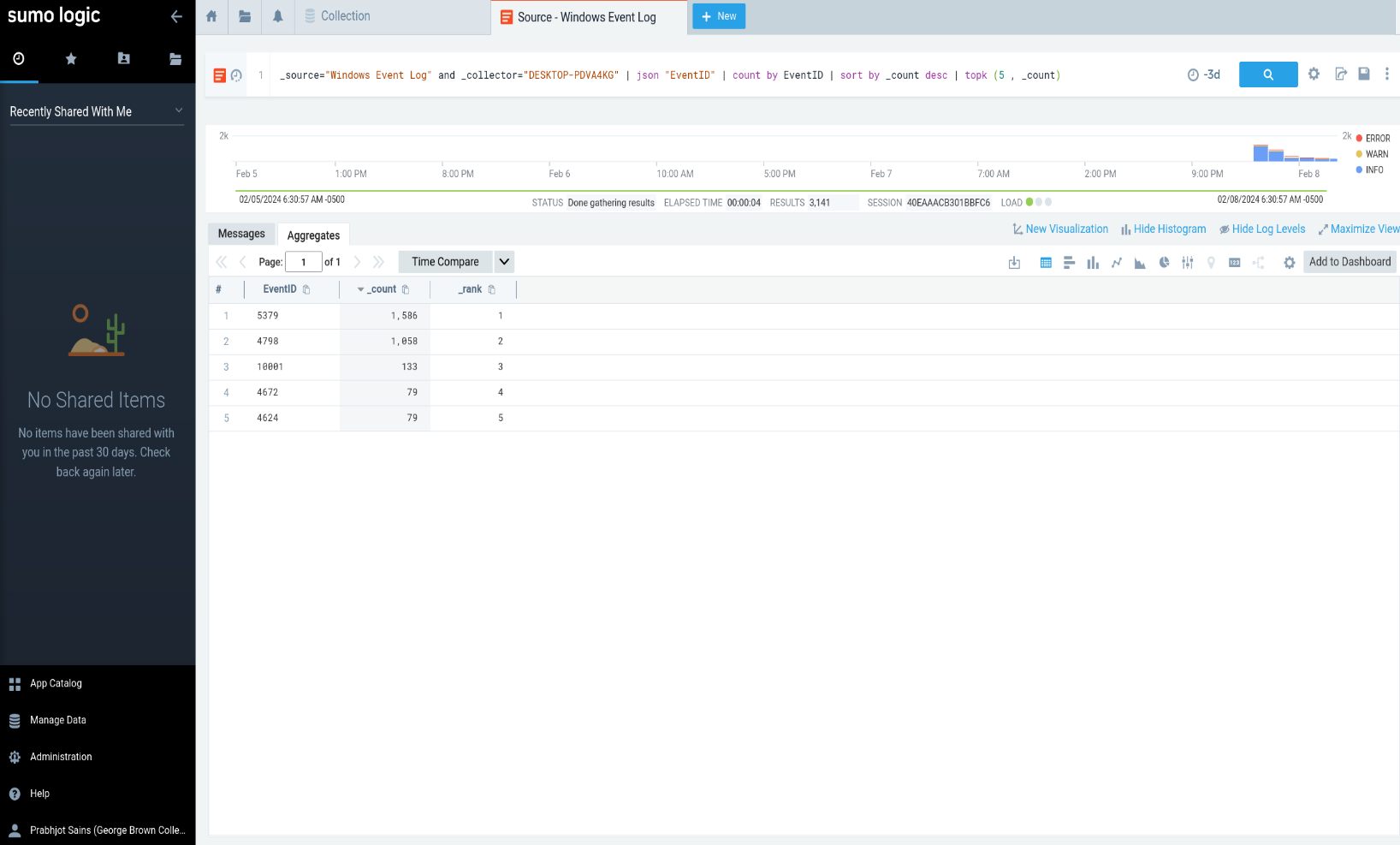
6) Collect Windows VM event logs (Security, Application, and system).



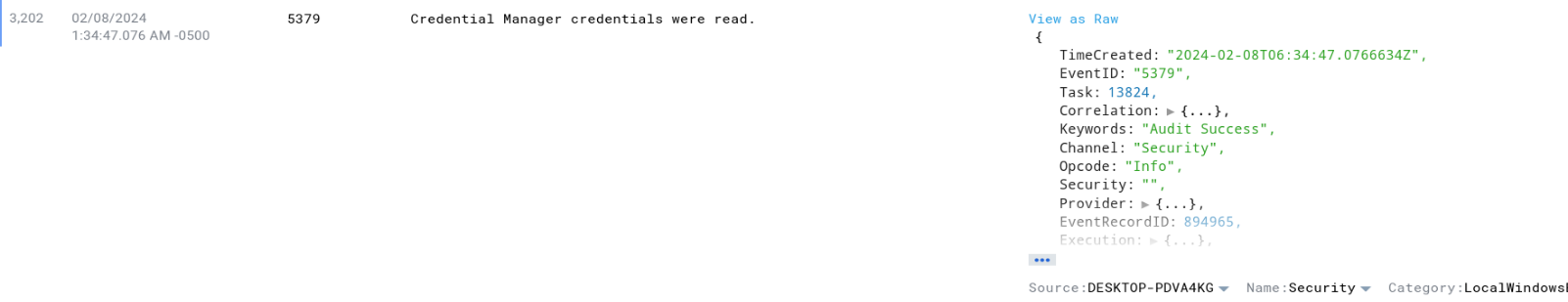


7) Count the number of each event ID and order by counts then explain the top 5 events.

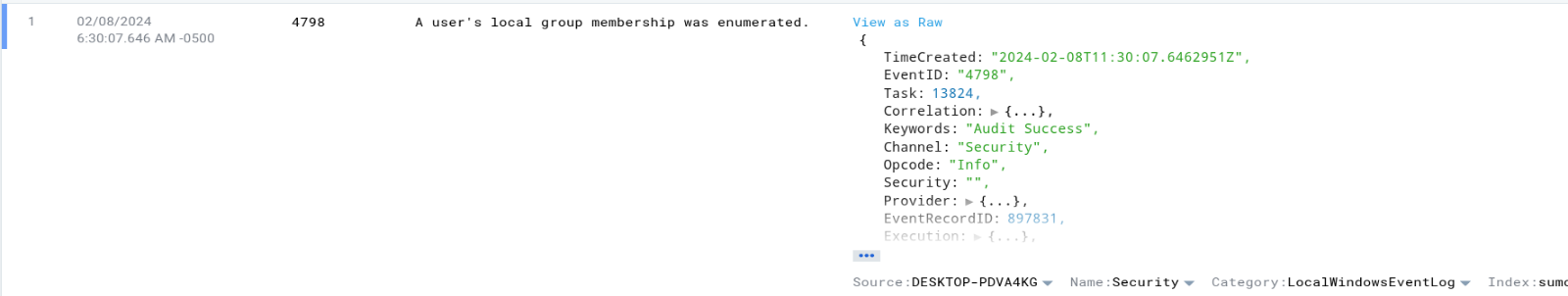




1. **5379:** This is a message that indicates that a user or a program accessed the stored credentials in the Credential Manager in Linux. The Credential Manager is a feature that allows users to store and manage their passwords, and other credentials in a secure way.



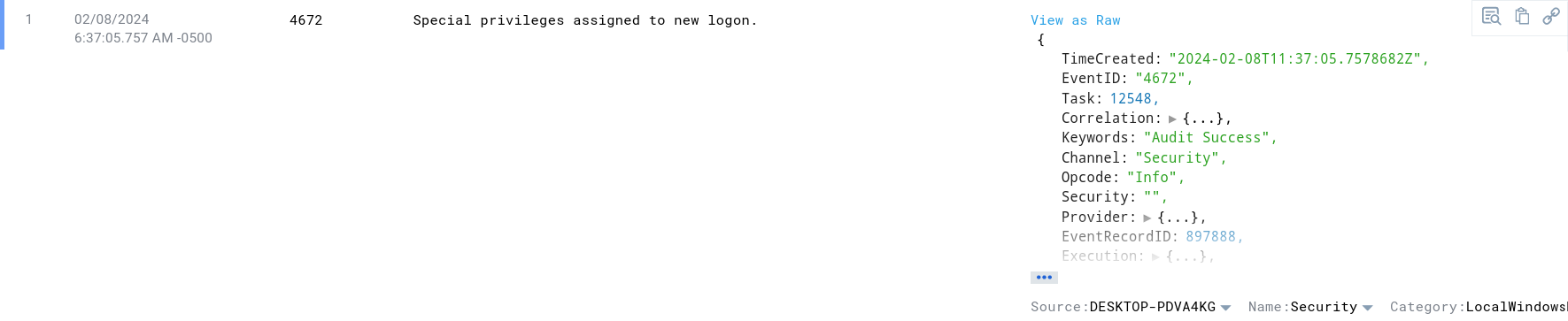
1. **4798:** This is a message that indicates that a process or a program listed the local groups that a user belongs to on a Linux system.



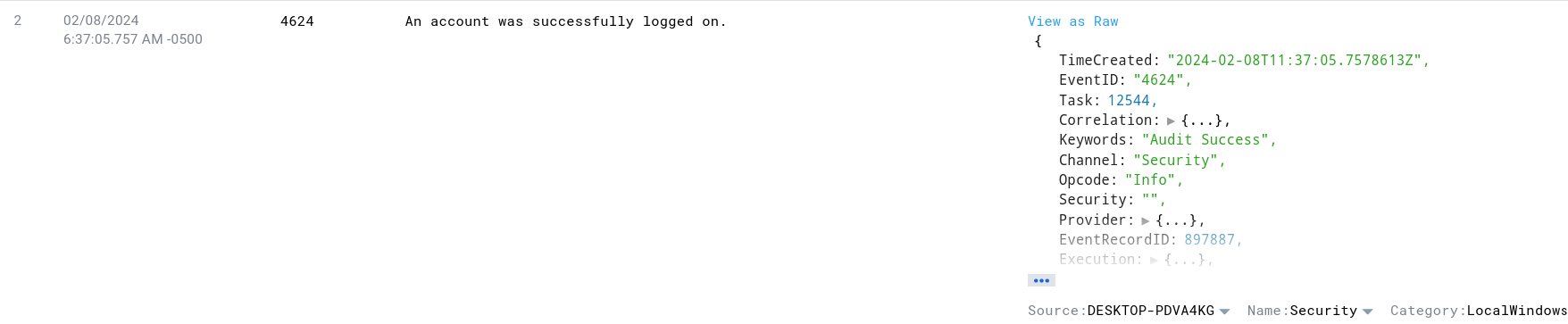
1. **1001:** Distributed Component Object Model (DCOM) is a proprietary Microsoft technology for communication between software components on networked computers. This is a message that indicates that there was an error in launching the Skype app on a Linux system.



1. **4672:** This is a message that indicates that a new logon session was created with some sensitive privileges like the root user logged in.

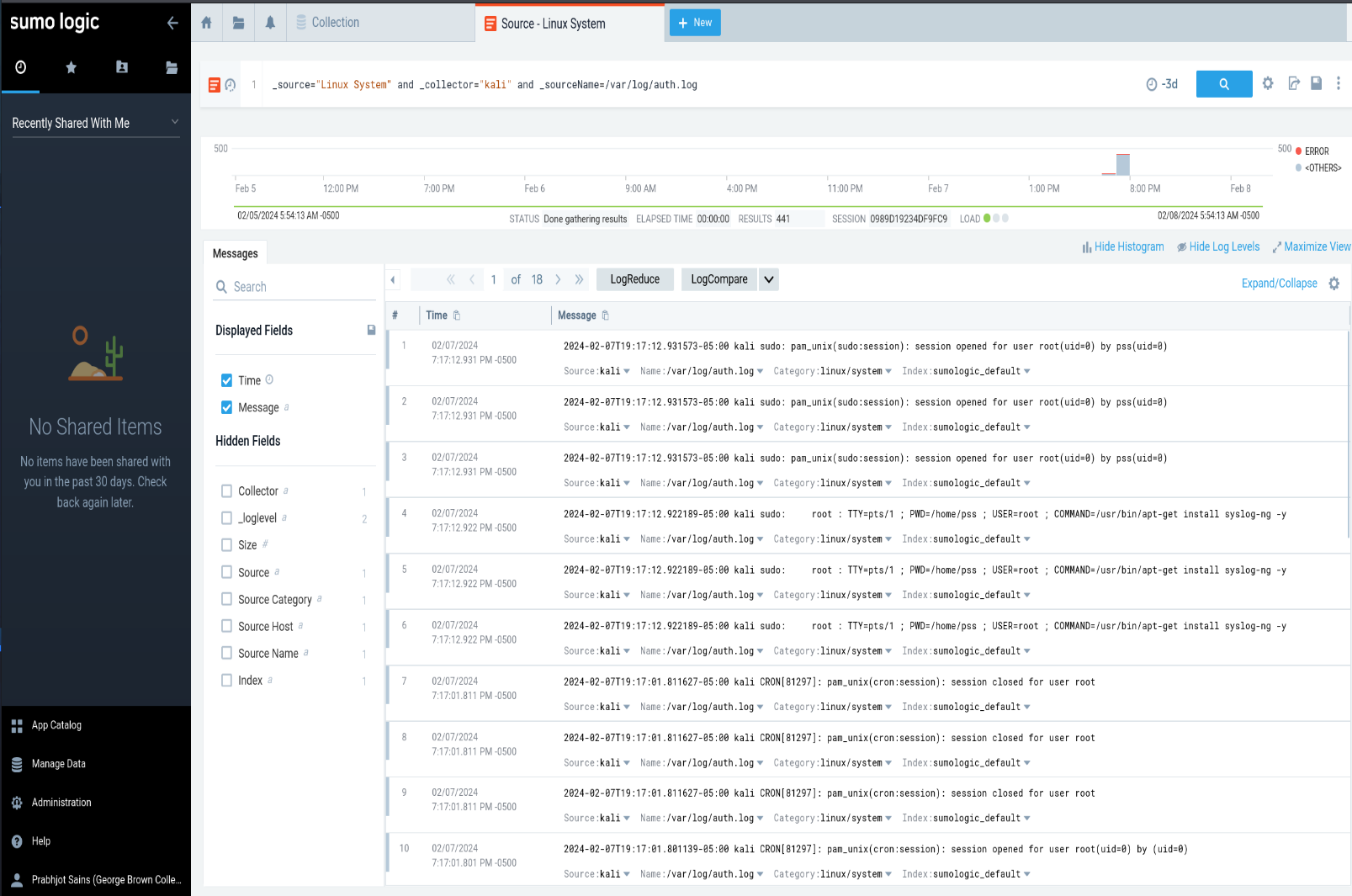


1. **4624:** This is a message that indicates that a user or a program logged on to a Linux system using a valid username and password.

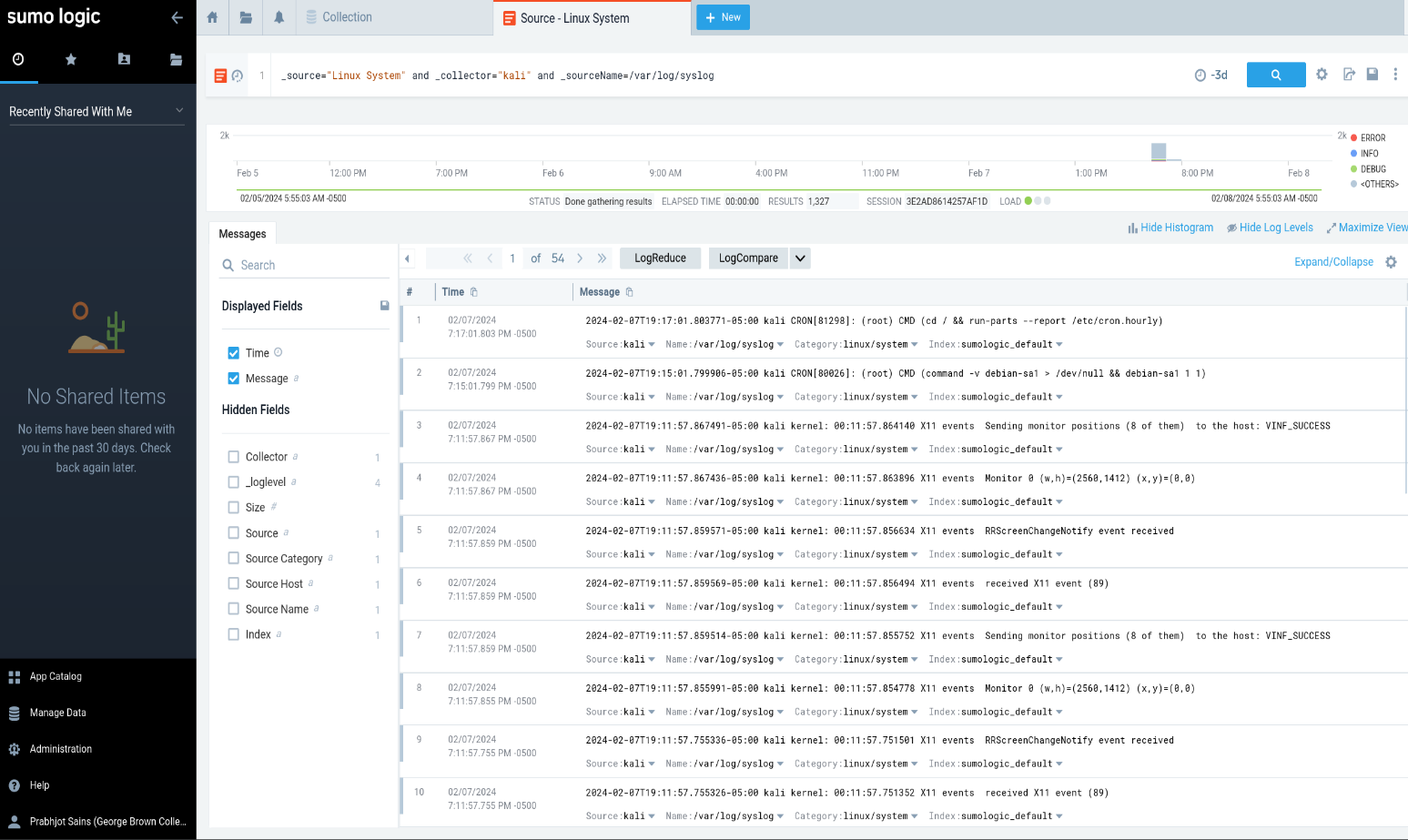


8) Collect Linux VM Auth and Syslog.

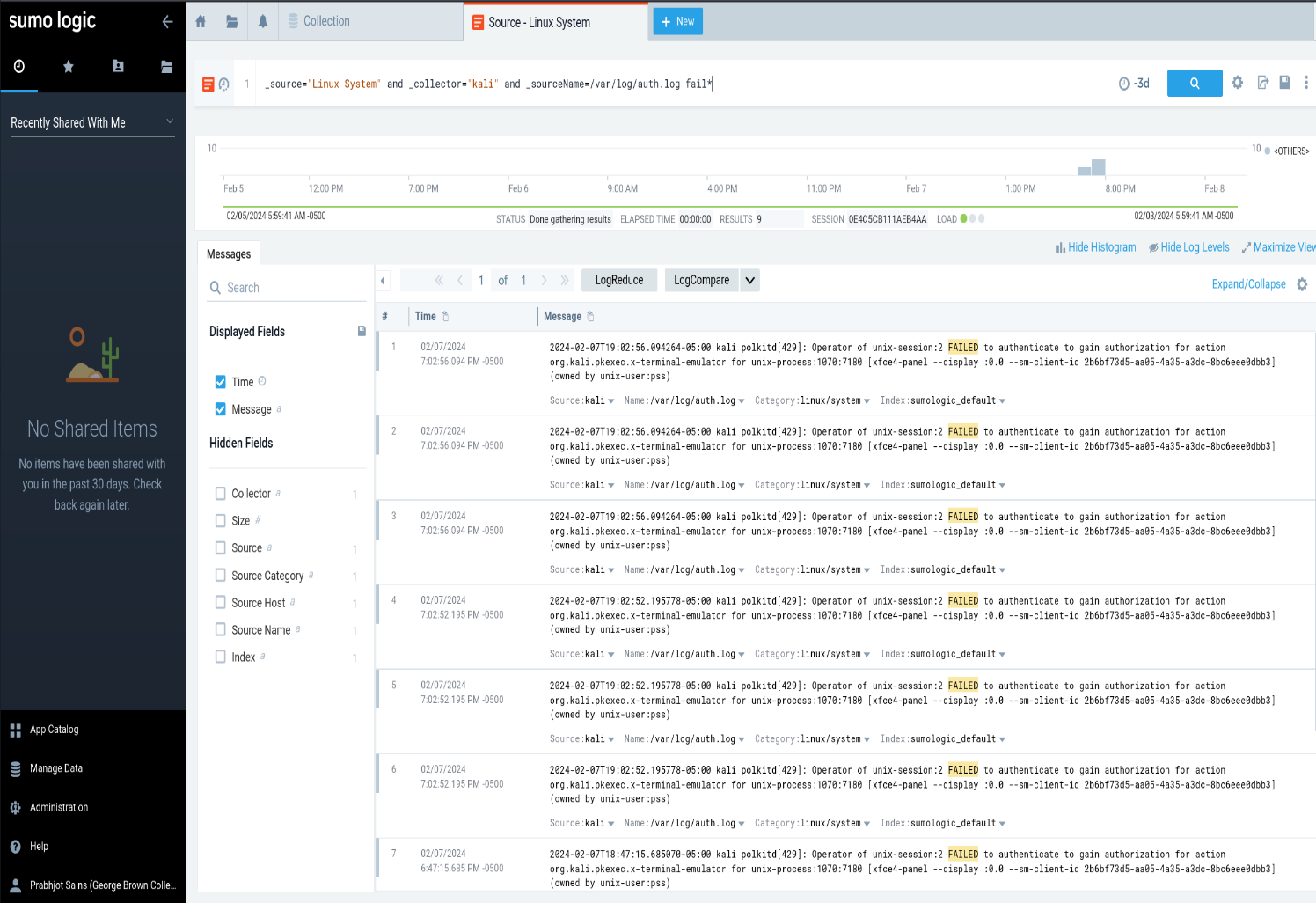
**Linux VM Auth:**



**Linux Syslog:**



9) Search for failures in Linux VM auth logs.



10) Create a panel to visualize the number of Linux VM Syslog events/ each 30m.

