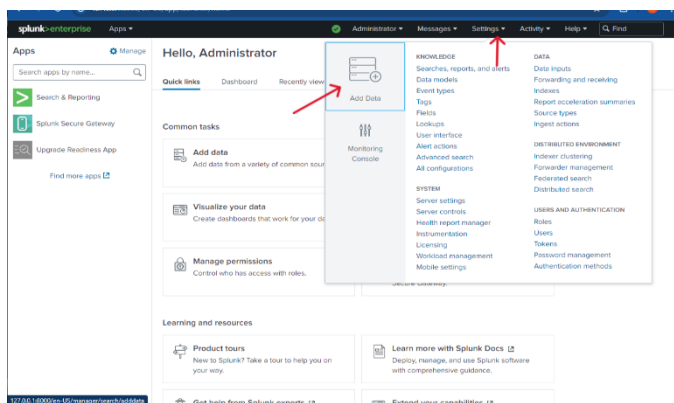


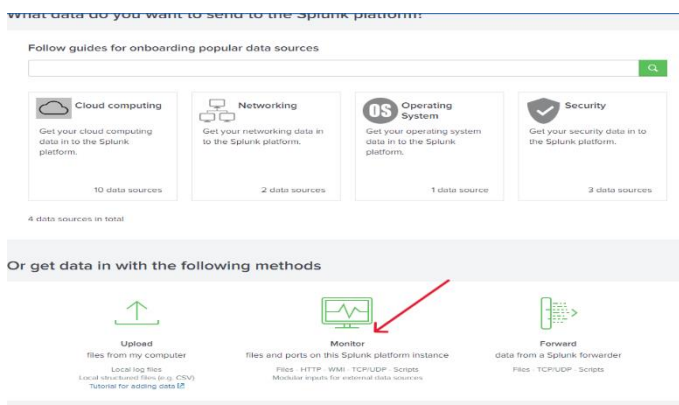
Instructions on log collection and basic searches:

To start monitoring local event logs in Splunk and utilize these search queries, follow these steps:

1. Go to the Settings tab and click "Add Data."



2. Select the monitor icon.



3. Choose to monitor local events logs and add security and system logs, then click "Next."

6. The results will be generated as per below. On the search bar you can generate more searches per the information you need.

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query `source=WinEventLog:* host=PC22`. The results show 113,182 events. The table below displays the first few results.

Time	Event
5/9/24 4:35:45.000 PM	05/09/2024 04:35:45 PM LogName=Security EventCode=4672 EventType=0 ComputerName=PC22 Show all 31 lines host = PC22 source = WinEventLog:Security sourcetype = WinEventLog:Security
5/9/24 4:35:45.000 PM	05/09/2024 04:35:45 PM LogName=Security EventCode=4624 EventType=0 ComputerName=PC22 Show all 70 lines host = PC22 source = WinEventLog:Security sourcetype = WinEventLog:Security
5/9/24 8:23:28 PM	05/09/2024 04:23:28 PM

7. 1. Search for Specific Event IDs :

This search will retrieve all security events with Event IDs 4624 (successful logins) and 4625 (failed logins).

`index=main sourcetype="WinEventLog:Security" EventCode=4624 OR EventCode=4625`

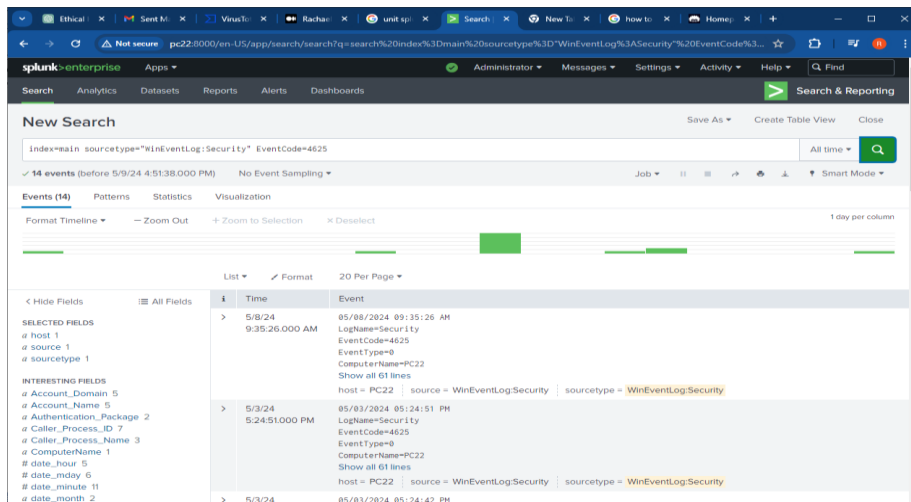
The screenshot shows the Splunk Enterprise search interface. The search bar contains the query `index=main sourcetype="WinEventLog:Security" EventCode=4624 OR EventCode=4625`. The results show 2,899 events. The table below displays the first few results.

Time	Event
5/9/24 4:43:02.000 PM	05/09/2024 04:43:02 PM LogName=Security EventCode=4624 EventType=0 ComputerName=PC22 Show all 70 lines host = PC22 source = WinEventLog:Security sourcetype = WinEventLog:Security
5/9/24 4:35:45.000 PM	05/09/2024 04:35:45 PM LogName=Security EventCode=4624 EventType=0 ComputerName=PC22 Show all 70 lines host = PC22 source = WinEventLog:Security sourcetype = WinEventLog:Security
5/9/24 8:23:28 PM	05/09/2024 04:23:28 PM

8. Search for Failed Logins:

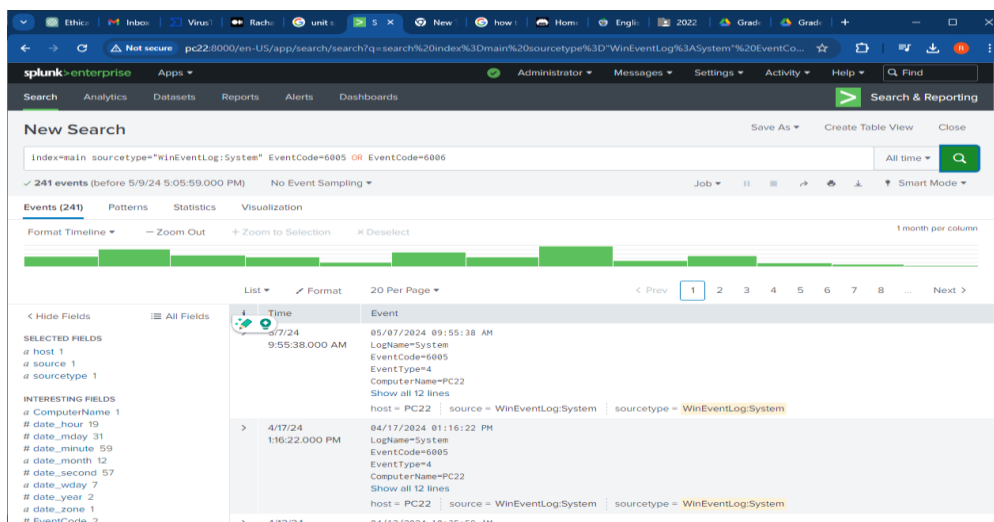
This search will retrieve all security events indicating failed login attempts.

`index=main sourcetype="WinEventLog:Security" EventCode=4625`



9. Search for System Startup and Shutdown Events:

`index=main sourcetype="WinEventLog:System" EventCode=6005 OR EventCode=6006`



10. Search for Logins by a Specific User. Replace "username" with the username you want to search for. This search will retrieve successful login events for the specified user.

`index=main sourcetype="WinEventLog:Security" EventCode=4624 Account_Name="username"`

11. 4. Search for Logins from Specific IP Addresses:

Replace "192.168.1.100" with the IP address you want to search for. This search will retrieve successful login events from the specified IP address.

index=main sourcetype="WinEventLog:Security" EventCode=4624
Source_Network_Address="192.168.1.100"

12. Search for Account Lockouts

index=main sourcetype="WinEventLog:Security" EventCode=4740

13. Search for Specific Error Codes

index=main sourcetype="WinEventLog:System" EventCode=100