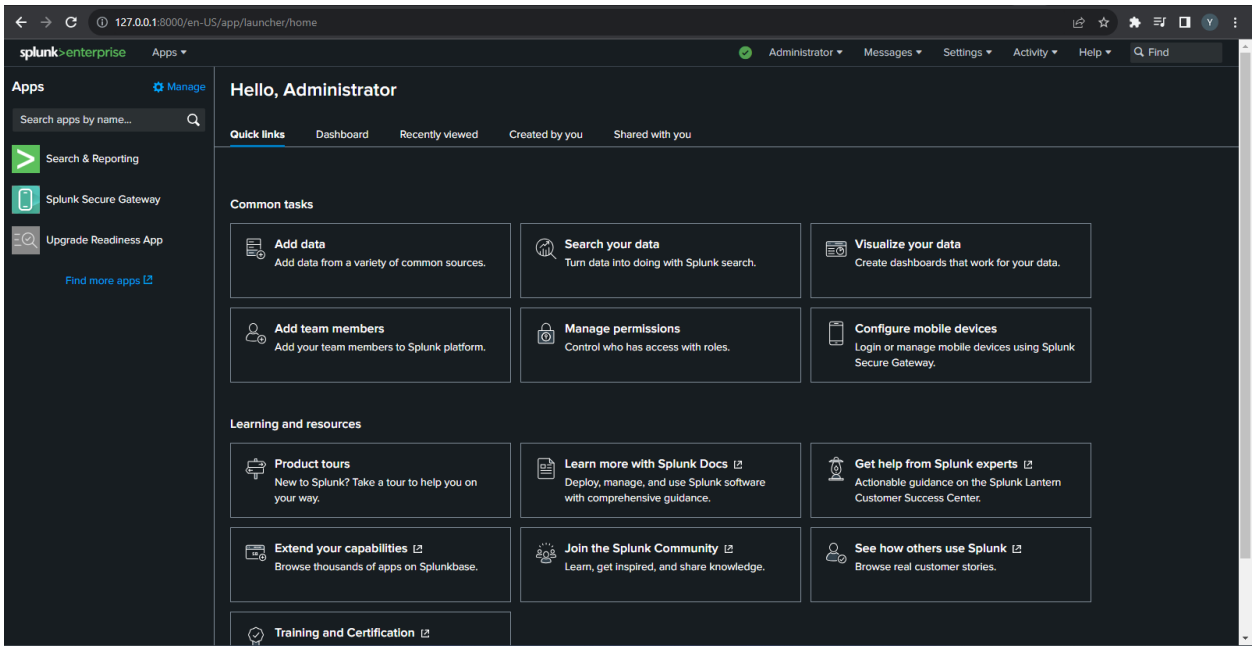
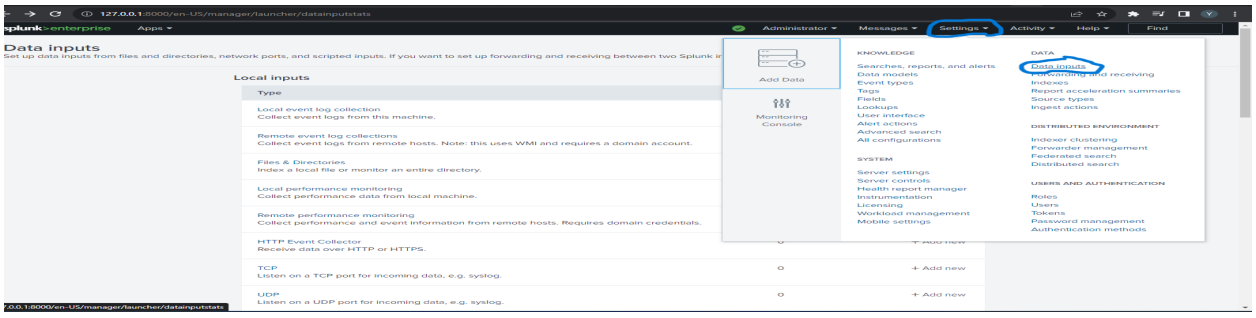
Splunk Configuration

In this lab I installed and configured Splunk on a local system account on windows endpoint. For lab purposes I cleared my event security event logs to create activity that shows what event code “1102” is in search,which is a clearing of audit logs.

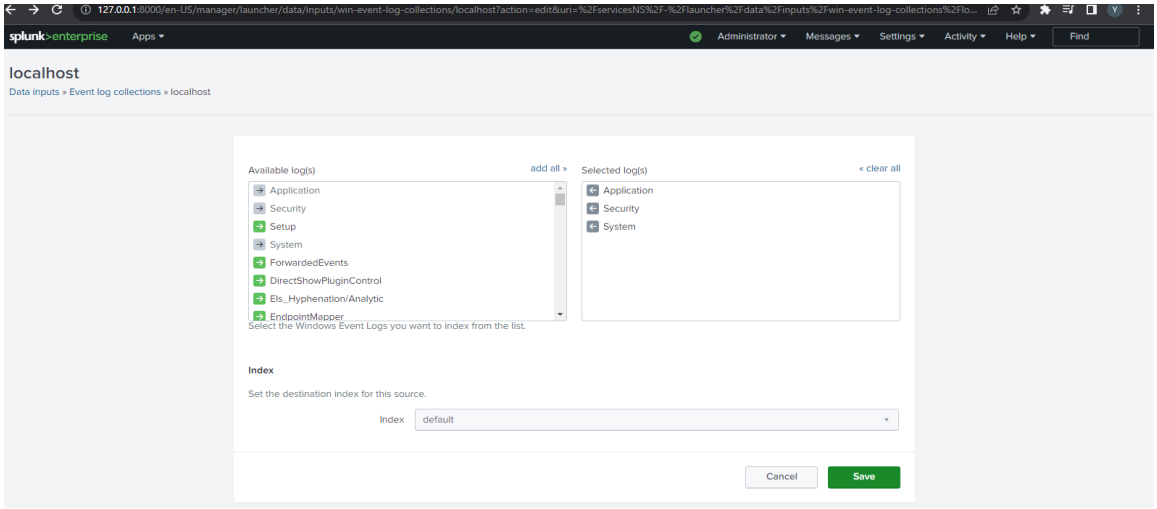
*Installed Splunk Enterprise Security on Windows Server



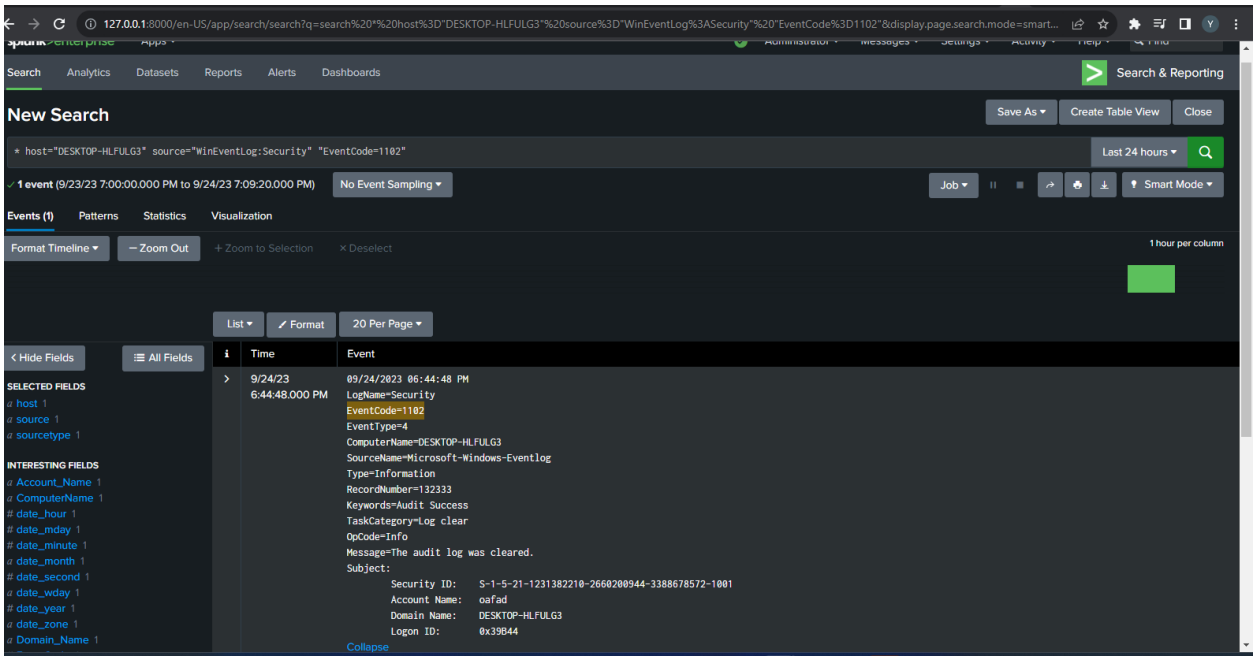
* Next tasks was to configure logs for ingestion in the settings and Data input options.



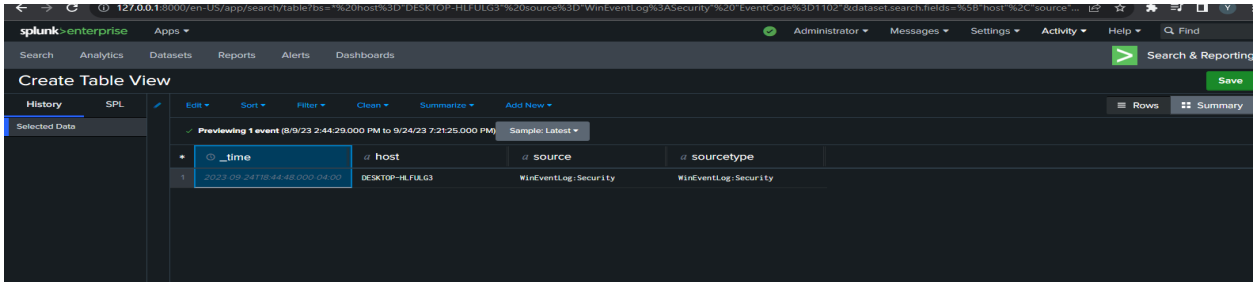
* Selected the Security, Application, and System logs for log collection



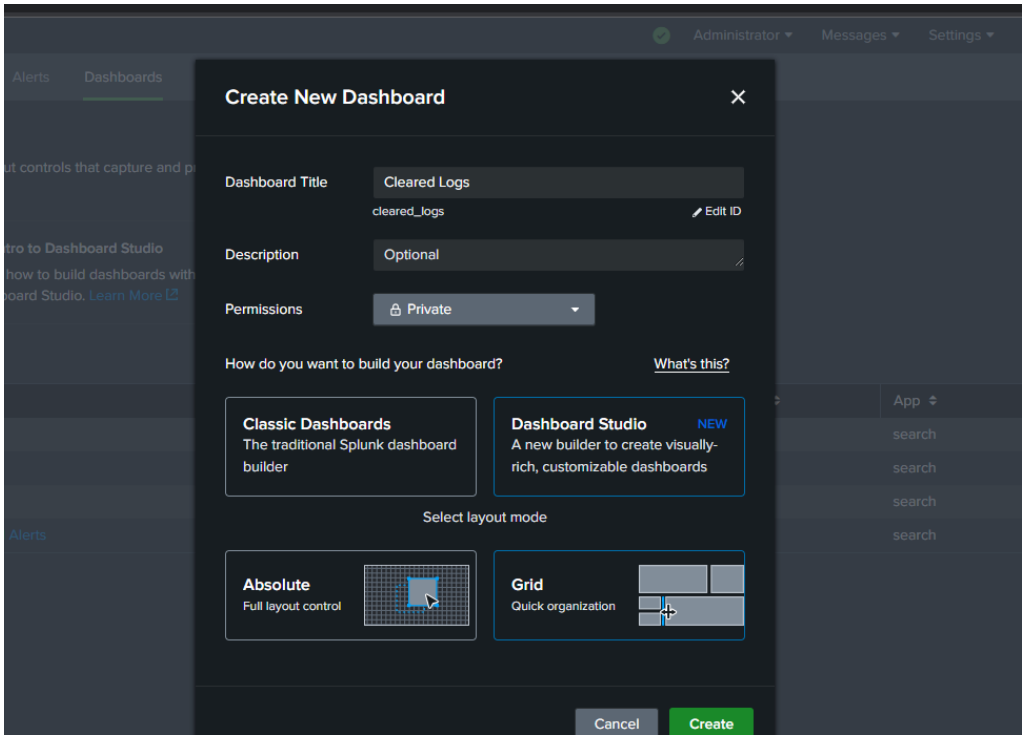
* Following the log collection, I refined my search by adding Host, Source, Event Code with this search Query I was able have Splunk show the clearing of logs in my Security events:



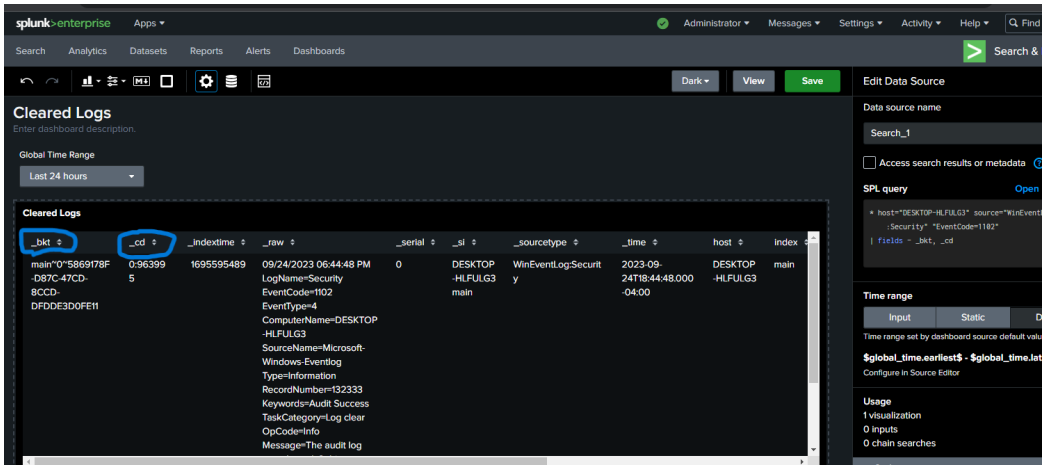
* Created table to explore the different options to view data that was collected from search



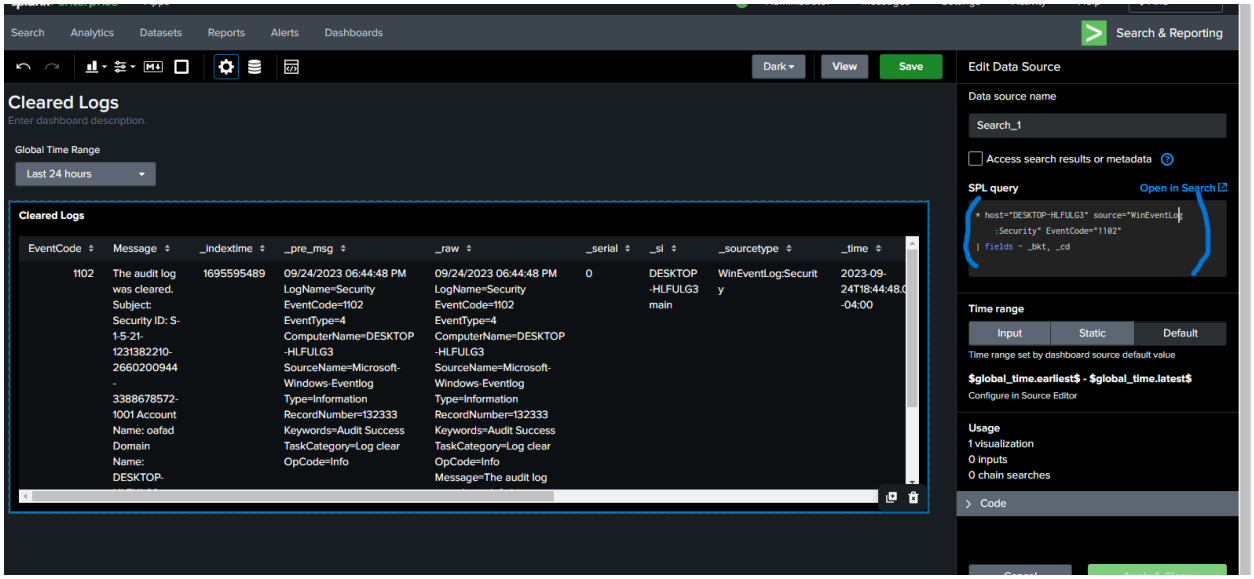
* Created dashboards with many options Splunk offers to display data



* With in the dashboard display shows fields “_bkt” and “ _cd”



* Next slide entered a query that removes “_bkt” and “_cd” fields in the display of the dashboard window.



This Lab was great to get hands-on experience with configuring logs and data in Splunk, which is a very versatile SIEM tool when collecting data to attempt to help keep networks as safe as possible.