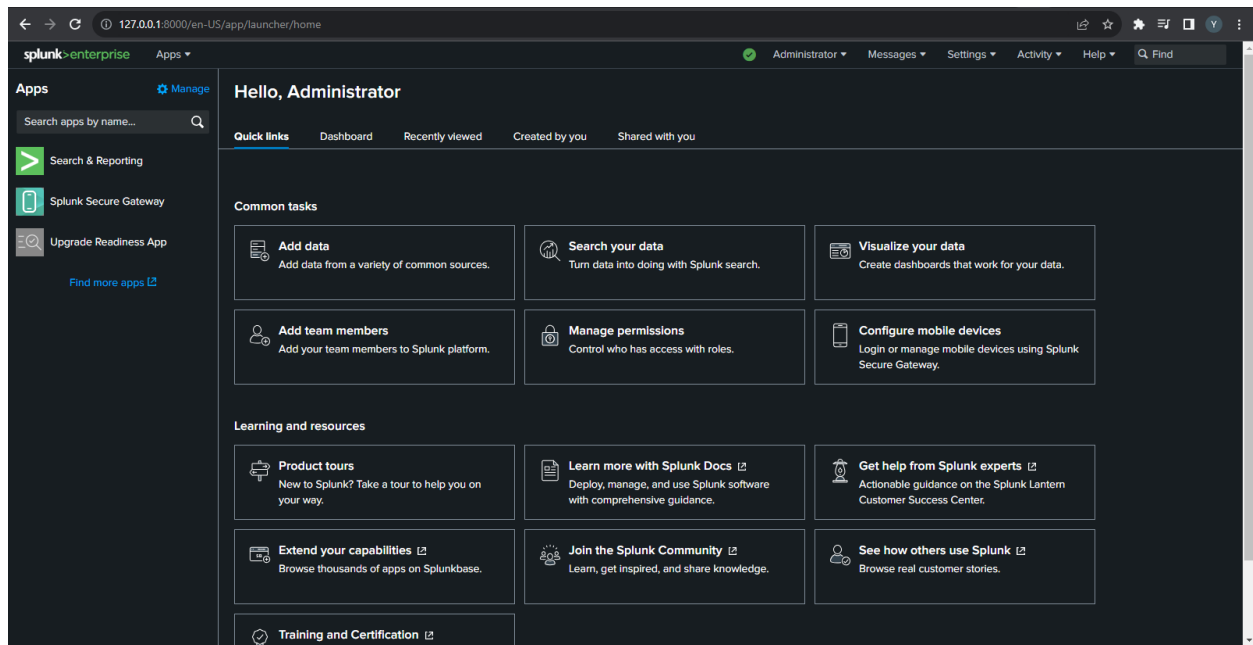


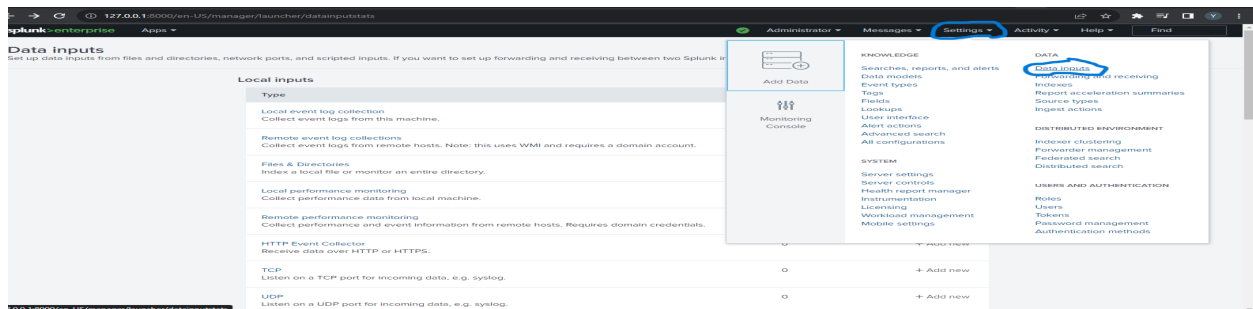
Splunk Configuration

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.

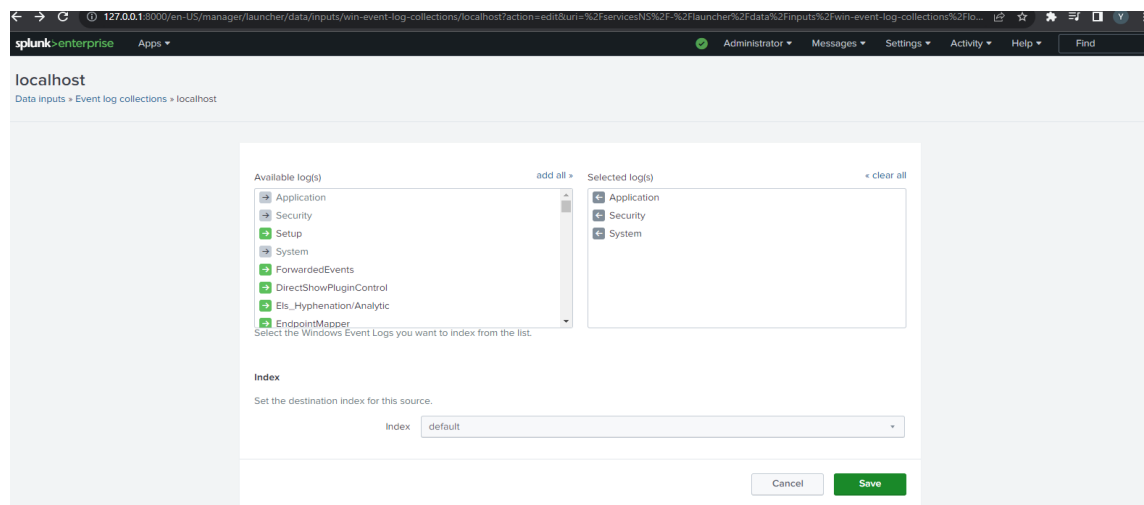
*Installed Splunk Enterprise Security on Windows Server



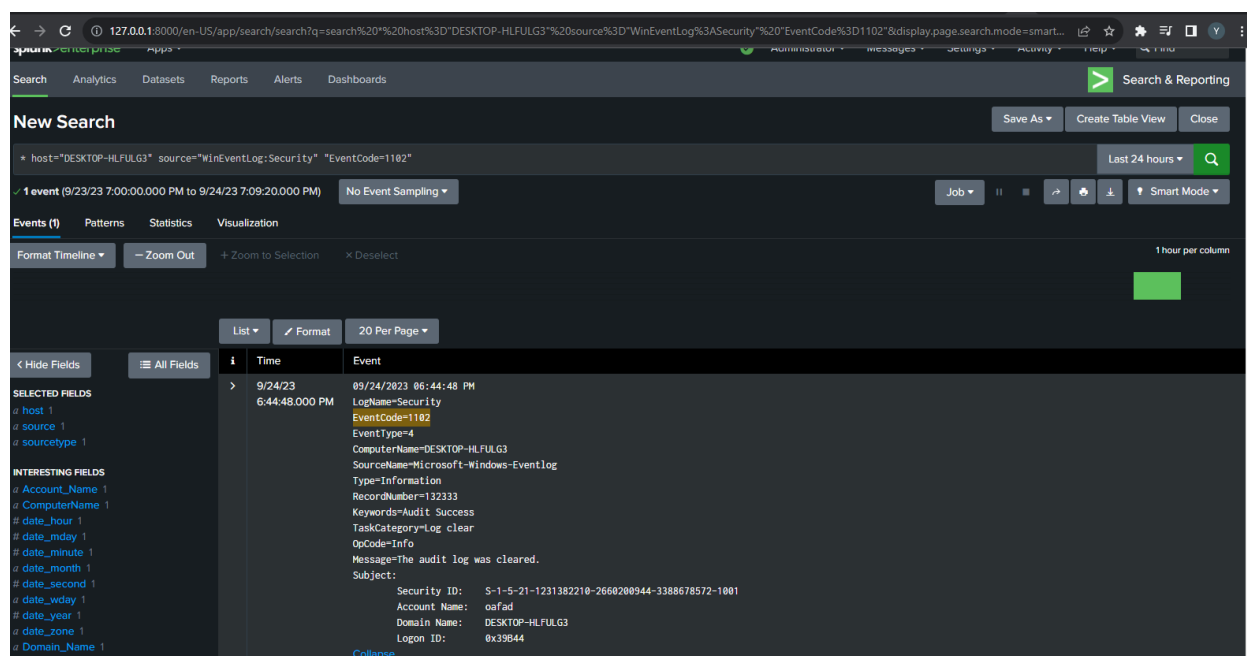
* Next tasks was to configure logs for ingestion in the settings and Data input options.



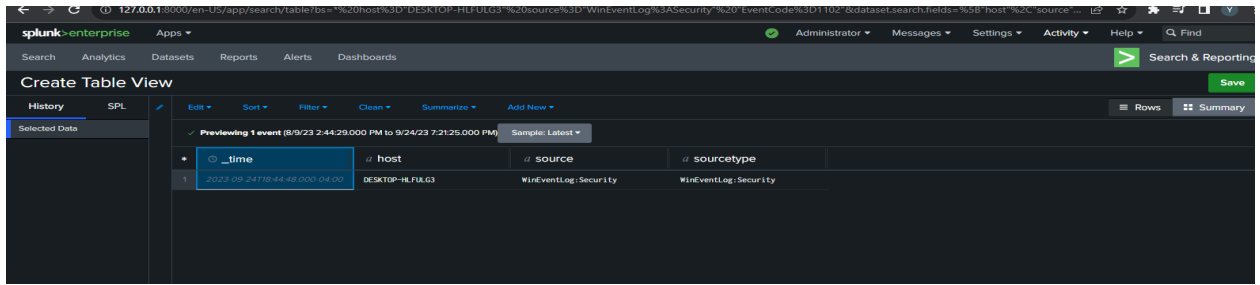
* Selected the Security, Application, and System logs for log collection



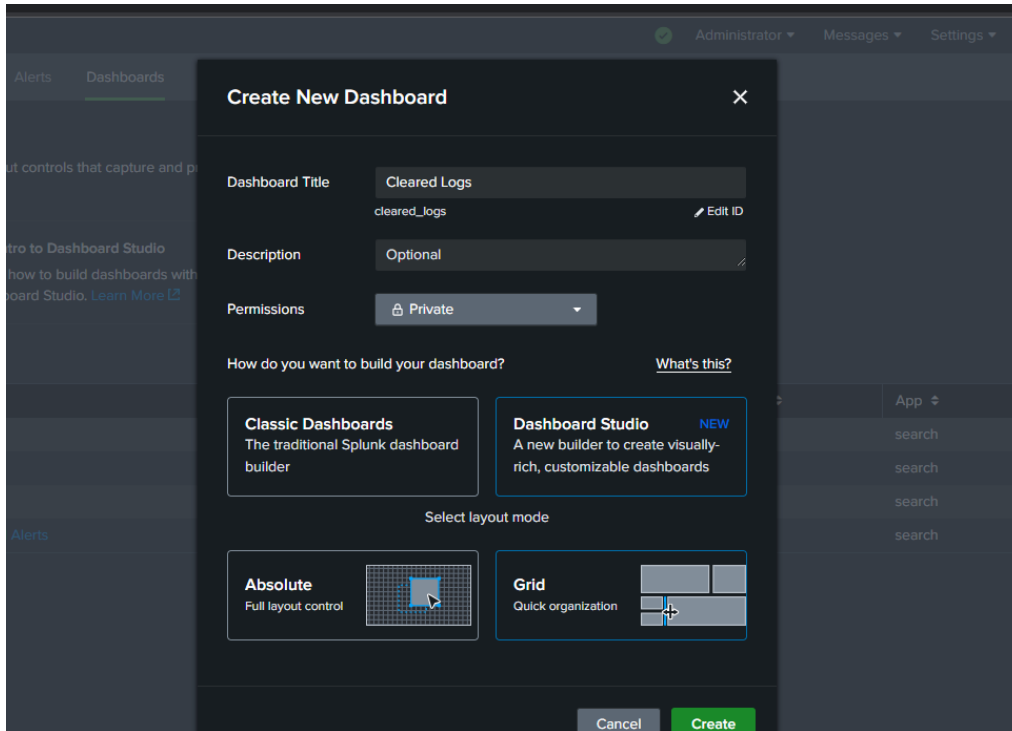
* Following the log collection, I refined my search by adding Host, Source, Event Code with this search Query I was able have Splunk show the clearing of logs in my Security events:



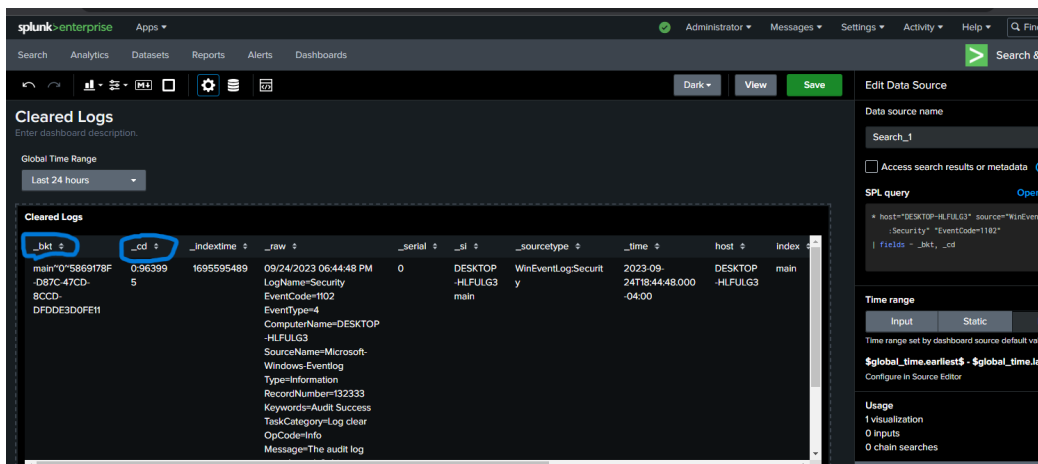
* Created table to explore the different options to view data that was collected from search



* 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.

The screenshot shows the Splunk interface with a dashboard titled "Cleared Logs". The main panel displays a table of log events. The table has columns: EventCode, Message, _Indextime, _pre_msg, _raw, _serial, _si, _sourcetype, and _time. The first row shows an event with EventCode 1102, Message "The audit log was cleared.", and various metadata fields.

EventCode	Message	_Indextime	_pre_msg	_raw	_serial	_si	_sourcetype	_time
1102	The audit log was cleared.	1695595489	09/24/2023 06:44:48 PM	09/24/2023 06:44:48 PM	0	DESKTOP-HLFULG3	WinEventLog:Security	2023-09-24T18:44:48.000-04:00

On the right side, the "Edit Data Source" panel is visible. It shows the "SPL query" field with the following query:

```
* host="DESKTOP-HLFULG3" source="WinEventLog:Security" EventCode="1102" | fields - _bkt, _cd
```

The query is highlighted with a blue bracket. Below the query, the "Time range" section shows the input field set to "Static" and the default value set to "\$global_time.earliest - \$global_time.latest\$".

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.