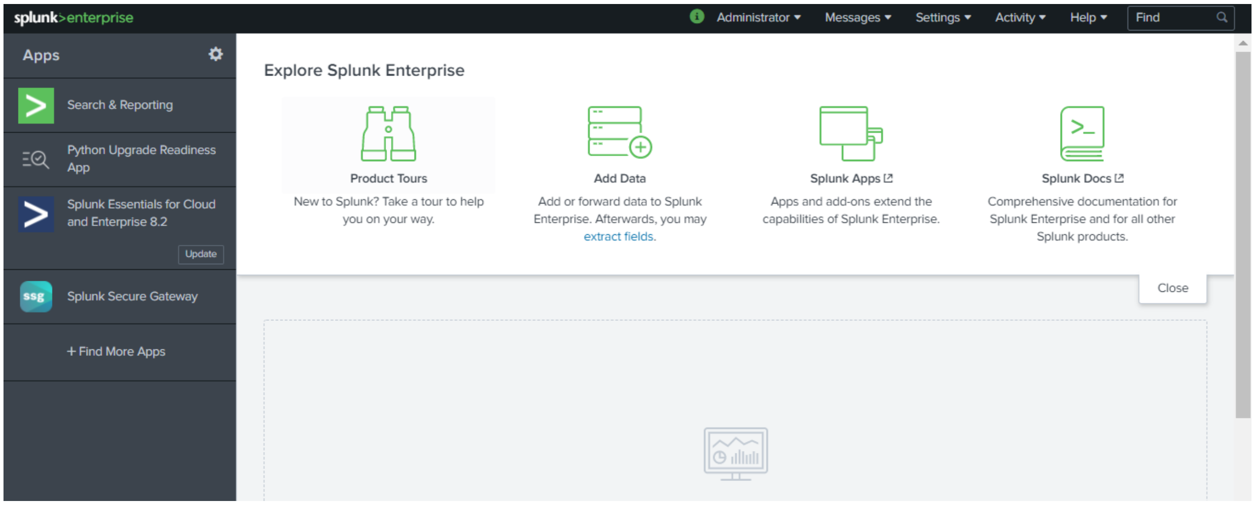
LAB ASSIGNMENT - 5

Name: Ashwin Balaji
Roll Number: 2020PMD4221
Course: M.Tech (Mobile Computing and Data Analytics)

Title: To perform the Log analysis using SPLUNK

Theory:

1. Download SPLUNK Enterprise
2. Login with username and password



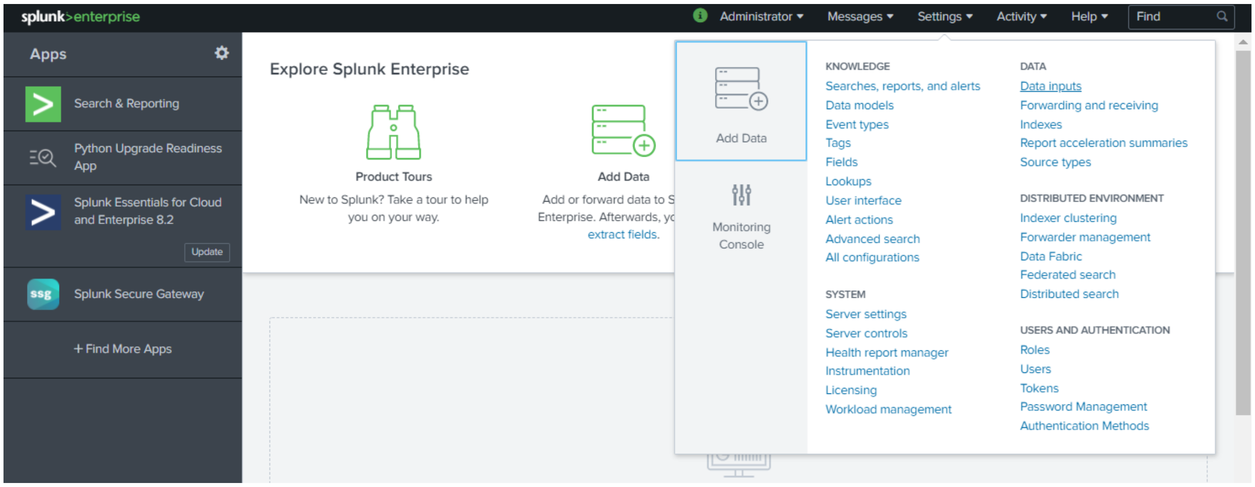
New to Splunk? Take a tour to help you on your way.

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

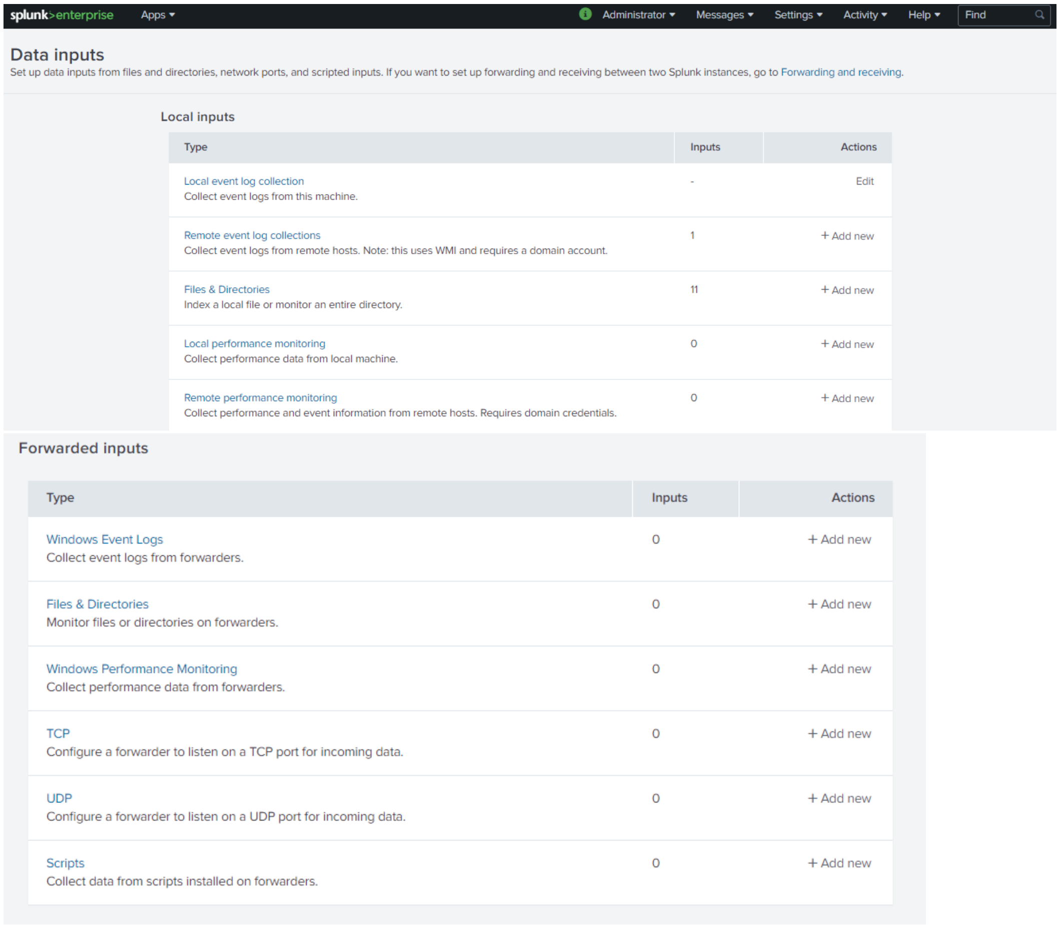
Apps and add-ons extend the capabilities of Splunk Enterprise.

Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

3. Go to **Settings -> Data Inputs**



4. Here we might encounter **Local Inputs and Forward Inputs**
   Set up data inputs from files and directories, network ports, and scripted inputs. If we want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.



Data inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.

Local inputs

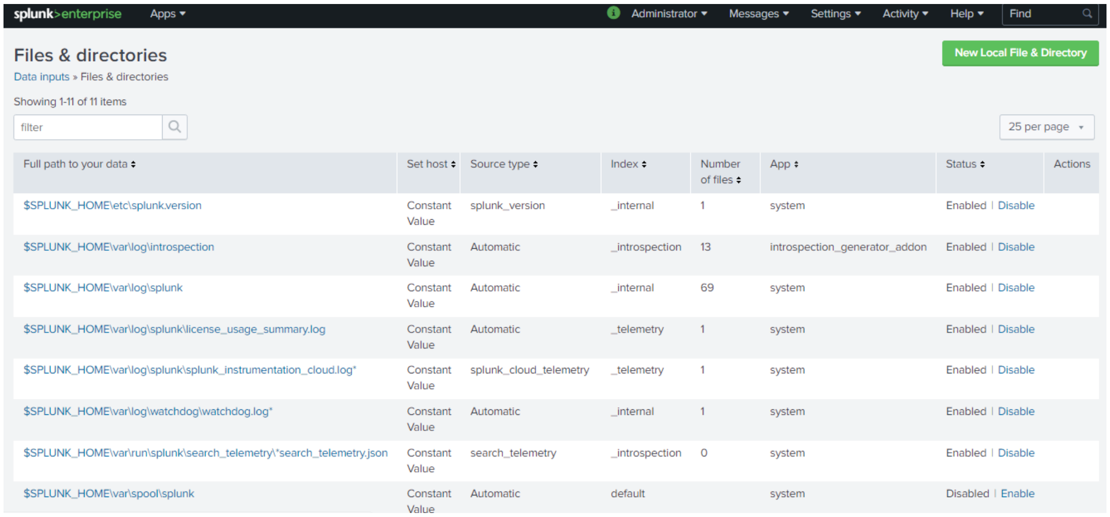
Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new
Files & Directories Index a local file or monitor an entire directory.	11	+ Add new
Local performance monitoring Collect performance data from local machine.	0	+ Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new

Forwarded inputs

Type	Inputs	Actions
Windows Event Logs Collect event logs from forwarders.	0	+ Add new
Files & Directories Monitor files or directories on forwarders.	0	+ Add new
Windows Performance Monitoring Collect performance data from forwarders.	0	+ Add new
TCP Configure a forwarder to listen on a TCP port for incoming data.	0	+ Add new
UDP Configure a forwarder to listen on a UDP port for incoming data.	0	+ Add new
Scripts Collect data from scripts installed on forwarders.	0	+ Add new

A) We will be starting with **Data Inputs -> Files & Directories**

   i) Like we can **Index a local file or monitor an entire directory**



Files & directories

Data inputs » Files & directories

Showing 1-11 of 11 items

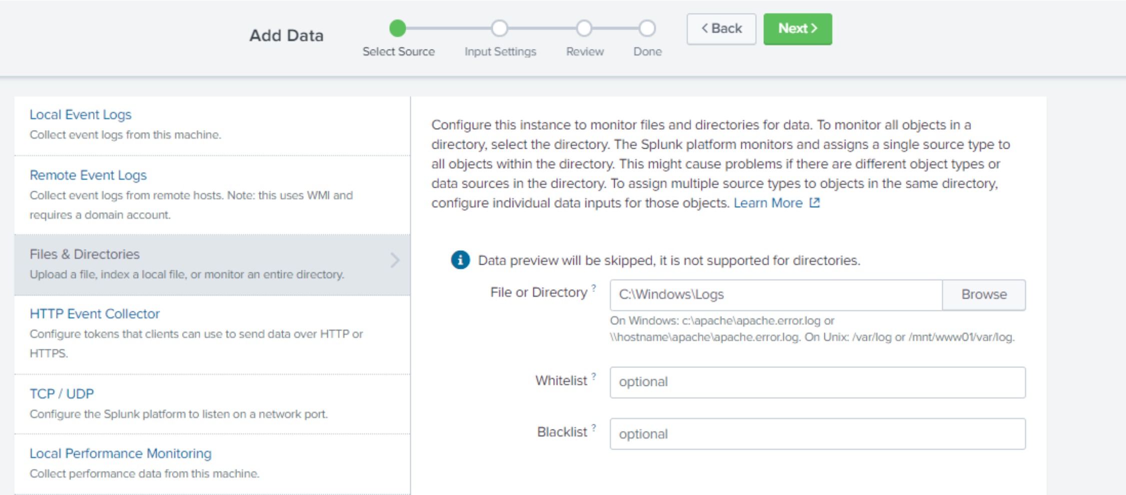
Full path to your data ⬍	Set host ⬍	Source type ⬍	Index ⬍	Number of files ⬍	App ⬍	Status ⬍	Actions
$SPLUNK_HOME\etc\splunk.version	Constant Value	splunk_version	_internal	1	system	Enabled | Disable	
$SPLUNK_HOME\var\log\introspection	Constant Value	Automatic	_introspection	13	introspection_generator_addon	Enabled | Disable	
$SPLUNK_HOME\var\log\splunk	Constant Value	Automatic	_internal	69	system	Enabled | Disable	
$SPLUNK_HOME\var\log\splunk\license_usage_summary.log	Constant Value	Automatic	_telemetry	1	system	Enabled | Disable	
$SPLUNK_HOME\var\log\splunk\splunk_instrumentation_cloud.log*	Constant Value	splunk_cloud_telemetry	_telemetry	1	system	Enabled | Disable	
$SPLUNK_HOME\var\log\watchdog\watchdog.log*	Constant Value	Automatic	_internal	1	system	Enabled | Disable	
$SPLUNK_HOME\var\run\splunk\search_telemetry\*search_telemetry.json	Constant Value	search_telemetry	_introspection	0	system	Enabled | Disable	
$SPLUNK_HOME\var\spool\splunk	Constant Value	Automatic	default		system	Disabled | Enable	

   ii) Click on **Files & Directories -> New Local File & Directory**

   iii) Setup the source where we want to perform analysis

Source -> C:\Windows\Logs

iv) Optionally we can add **blacklist and whitelist** for filtering purposes -> Click **Next**



Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More

Data preview will be skipped, it is not supported for directories.

File or Directory ? C:\Windows\Logs Browse

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Whitelist ? optional

Blacklist ? optional

v) **We can optionally specify input settings like source type, App context, Host type and Index**

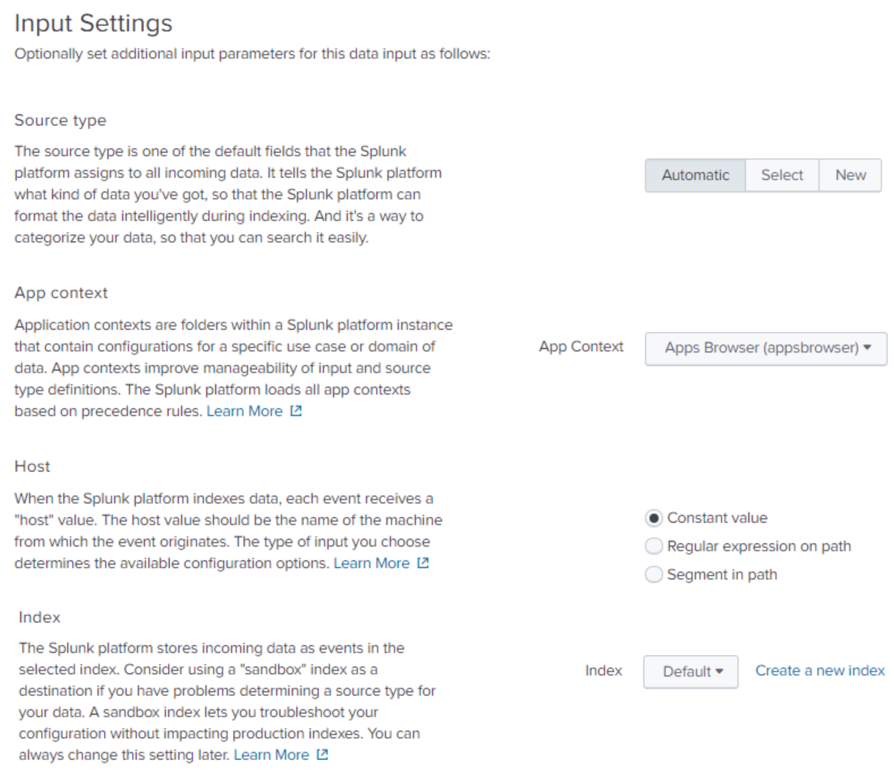
Source Type: The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

App Context: Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules

- ✓ **Here I have used Search & Reporting context**

Host: When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options

Index: The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes.



Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Automatic | Select | New

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

App Context: Apps Browser (appsbrowser) ▾

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

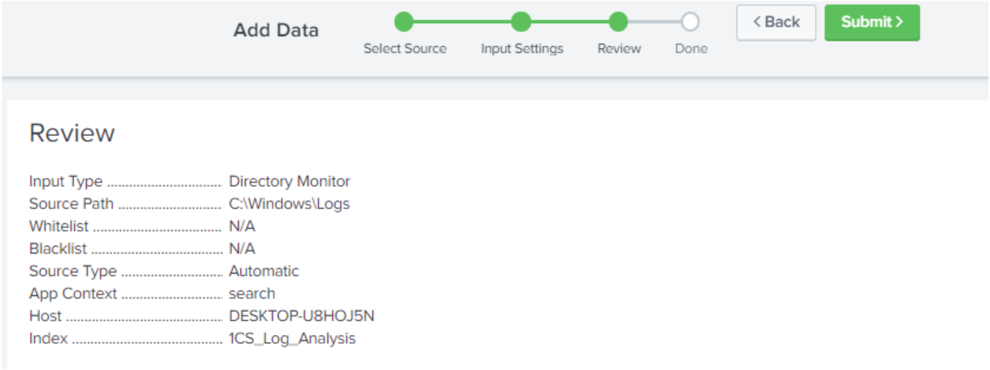
● Constant value
○ Regular expression on path
○ Segment in path

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: Default ▾ Create a new index

vi) **Review the settings/configuration ->** Click **Submit**



Add Data

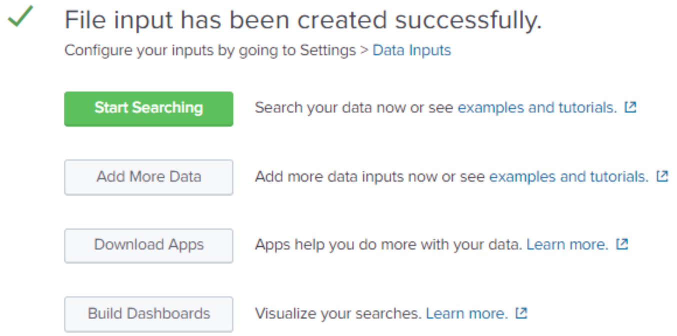
Select Source — Input Settings — Review — Done

‹ Back | Submit ›

Review

```
Input Type ........................ Directory Monitor
Source Path ....................... C:\Windows\Logs
Whitelist ......................... N/A
Blacklist ......................... N/A
Source Type ....................... Automatic
App Context ....................... search
Host .............................. DESKTOP-U8HOJ5N
Index ............................. 1CS_Log_Analysis
```

vii) After **finishing up the setup ->** Click on **Start Searching**



✓ File input has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Start Searching — Search your data now or see examples and tutorials.

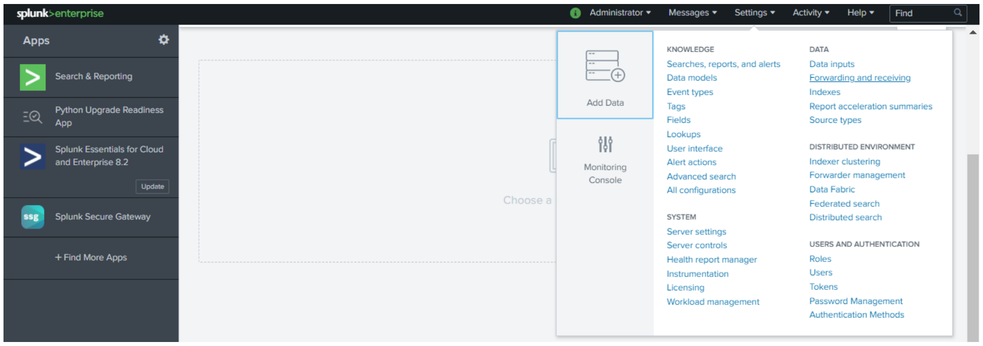
Add More Data — Add more data inputs now or see examples and tutorials.

Download Apps — Apps help you do more with your data. Learn more.

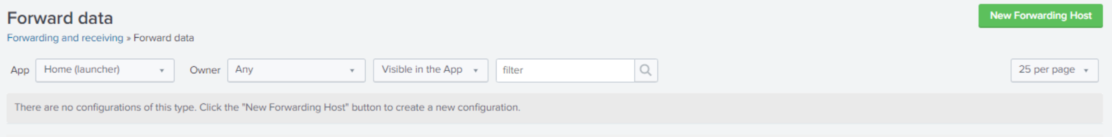
Build Dashboards — Visualize your searches. Learn more.

B) Next to setup **forwarding and receiving (For multiple machines in a network other than localhost)**

i) Settings -> Forwarding and Receiving



ii) Click on **Configure forwarding -> New Forwarding Host**

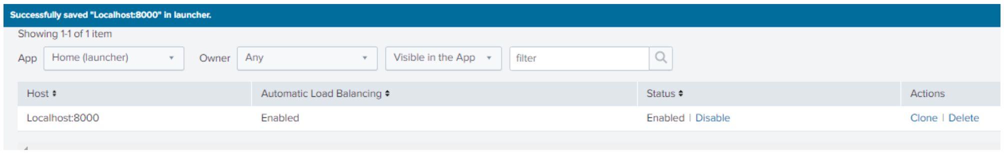


Forward data

Forwarding and receiving » Forward data

There are no configurations of this type. Click the "New Forwarding Host" button to create a new configuration.

iii) Define **Host port or IP port of other machine -> Save**

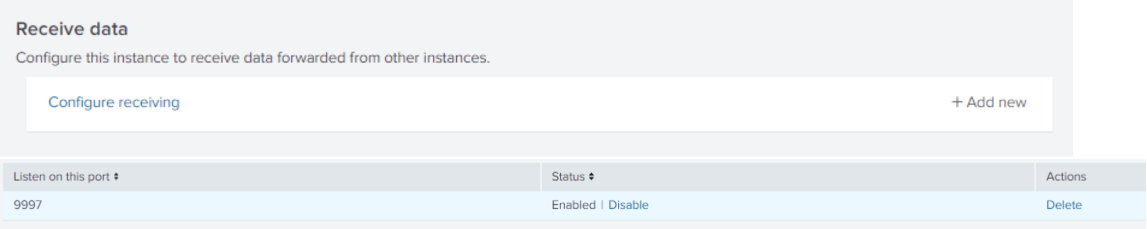


Successfully saved "Localhost:8000" in launcher.

Showing 1-1 of 1 item

Host ⇕	Automatic Load Balancing ⇕	Status ⇕	Actions
Localhost:8000	Enabled	Enabled | Disable	Clone | Delete

iv) Similarly, **configure receiving data** for a **different** machine **-> Save**

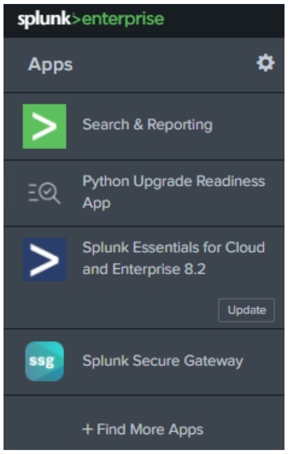


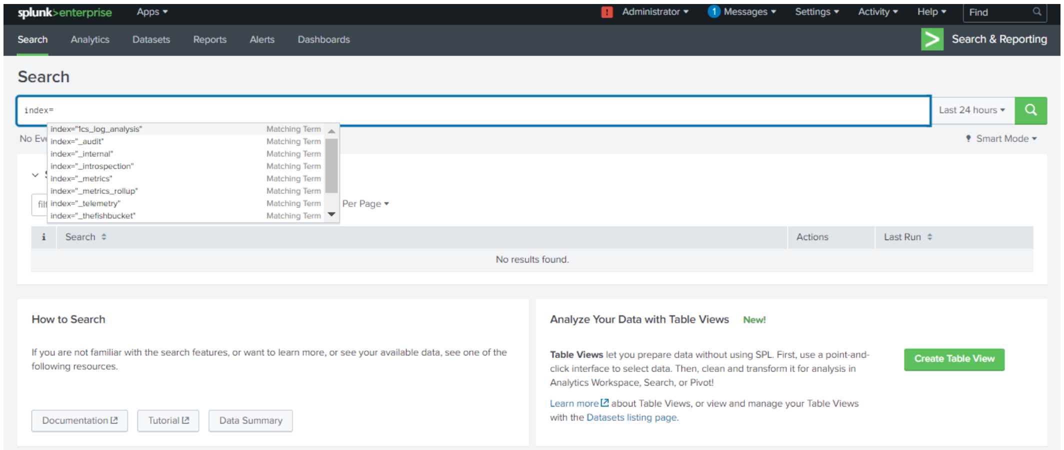
Receive data

Configure this instance to receive data forwarded from other instances.

Listen on this port ⇕	Status ⇕	Actions
9997	Enabled | Disable	Delete

C) Click **on Search & Reporting** in the homepage **-> Search History**





Search

```
index=
```

index="1cs_log_analysis"	Matching Term
index="_audit"	Matching Term
index="_internal"	Matching Term
index="_introspection"	Matching Term
index="_metrics"	Matching Term
index="_metrics_rollup"	Matching Term
index="_telemetry"	Matching Term
index="_thefishbucket"	Matching Term

i	Search	Actions	Last Run
	No results found.		

How to Search

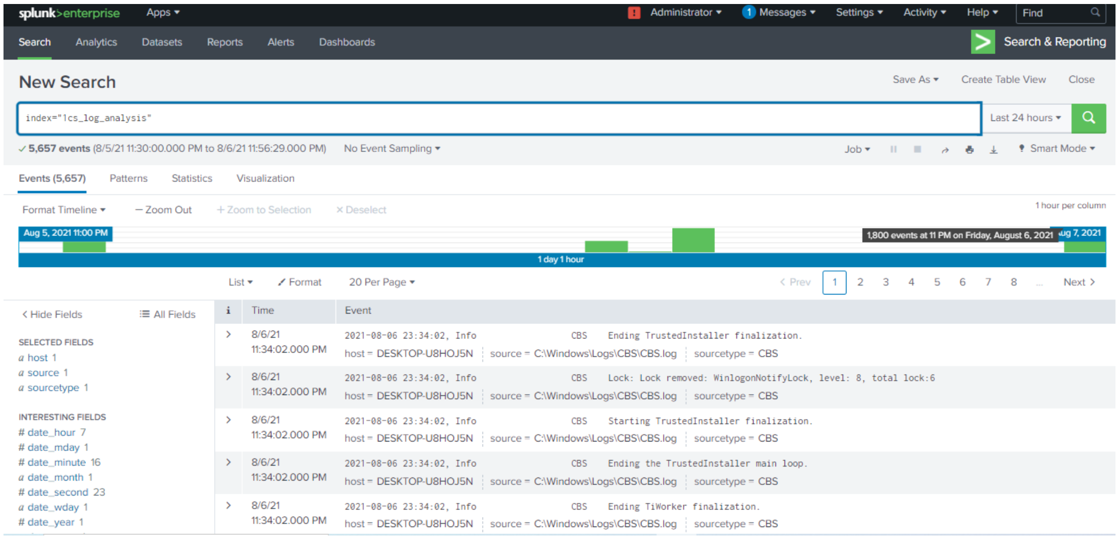
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Analyze Your Data with Table Views New!

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

i) Here we might find the index we made for log analysis **[index="1cs_log_analysis"]**



New Search

```
index="1cs_log_analysis"
```

✓ **5,657 events** (8/5/21 11:30:00.000 PM to 8/6/21 11:56:29.000 PM)

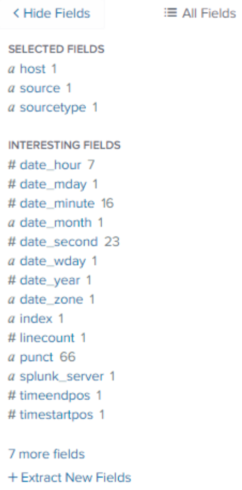
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 7
# date_mday 1
# date_minute 16
a date_month 1
# date_second 23
a date_wday 1
# date_year 1

i	Time	Event
>	8/6/21 11:34:02.000 PM	2021-08-06 23:34:02, Info CBS Ending TrustedInstaller finalization. host = DESKTOP-U8HOJ5N source = C:\Windows\Logs\CBS\CBS.log sourcetype = CBS
>	8/6/21 11:34:02.000 PM	2021-08-06 23:34:02, Info CBS Lock: Lock removed: WinlogonNotifyLock, level: 8, total lock:6 host = DESKTOP-U8HOJ5N source = C:\Windows\Logs\CBS\CBS.log sourcetype = CBS
>	8/6/21 11:34:02.000 PM	2021-08-06 23:34:02, Info CBS Starting TrustedInstaller finalization. host = DESKTOP-U8HOJ5N source = C:\Windows\Logs\CBS\CBS.log sourcetype = CBS
>	8/6/21 11:34:02.000 PM	2021-08-06 23:34:02, Info CBS Ending the TrustedInstaller main loop. host = DESKTOP-U8HOJ5N source = C:\Windows\Logs\CBS\CBS.log sourcetype = CBS
>	8/6/21 11:34:02.000 PM	2021-08-06 23:34:02, Info CBS Ending TiWorker finalization. host = DESKTOP-U8HOJ5N source = C:\Windows\Logs\CBS\CBS.log sourcetype = CBS

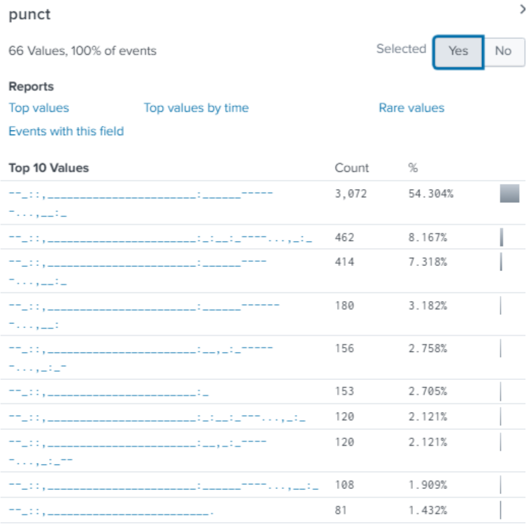
ii) We can find the **events occurred** by altering timeline e.g., last 24 hours etc.

iii) We can add **interesting field** for analysis



SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 7
# date_mday 1
# date_minute 16
a date_month 1
# date_second 23
a date_wday 1
# date_year 1
a date_zone 1
a index 1
# linecount 1
a punct 66
a splunk_server 1
# timeendpos 1
# timestartpos 1



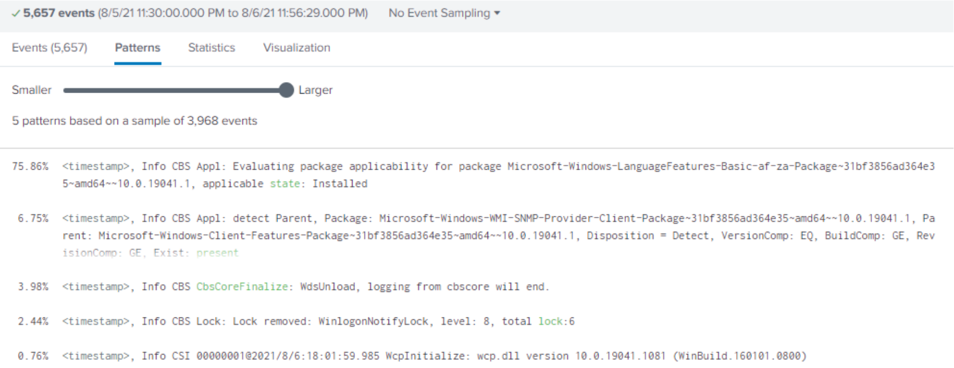
punct

66 Values, 100% of events

Reports

Top 10 Values	Count	%
--_::,_______________________:______----- -...,__:_	3,072	54.304%
--_::,_______________________:_:__:_----...,_:_	462	8.167%
--_::,_______________________:______---- -...,__:_	414	7.318%
--_::,_______________________:______------ -...,__:	180	3.182%
--_::,_______________________:__,_:_----- -...,_:_-	156	2.758%
--_::,_______________________:_	153	2.705%
--_::,_______________________:_:__:_---...,_:_	120	2.121%
--_::,_______________________:__,_:_---- -...,_:_--	120	2.121%
--_::,_______________________:______----...,__:_	108	1.909%
--_::,_________________________.	81	1.432%

iv) In pattern field we can identify the patterns related to the logs



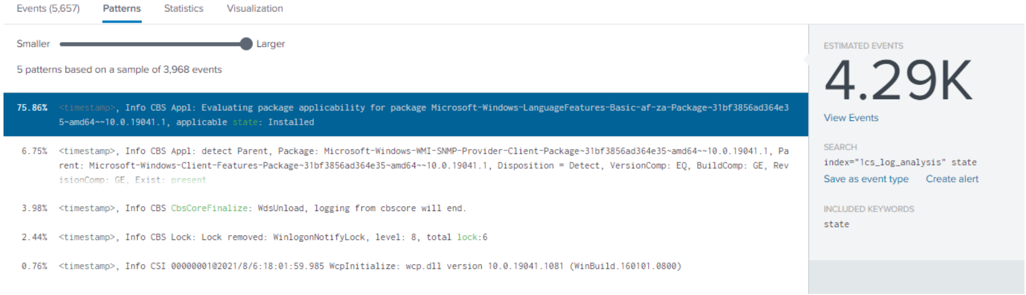
✓ 5,657 events (8/5/21 11:30:00.000 PM to 8/6/21 11:56:29.000 PM)   No Event Sampling ▾

5 patterns based on a sample of 3,968 events

```
75.86%  <timestamp>, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-LanguageFeatures-Basic-af-za-Package~31bf3856ad364e3
        5~amd64~~10.0.19041.1, applicable state: Installed

 6.75%  <timestamp>, Info CBS Appl: detect Parent, Package: Microsoft-Windows-WMI-SNMP-Provider-Client-Package~31bf3856ad364e35~amd64~~10.0.19041.1, Pa
        rent: Microsoft-Windows-Client-Features-Package~31bf3856ad364e35~amd64~~10.0.19041.1, Disposition = Detect, VersionComp: EQ, BuildComp: GE, Rev
        isionComp: GE, Exist: present

 3.98%  <timestamp>, Info CBS CbsCoreFinalize: WdsUnload, logging from cbscore will end.

 2.44%  <timestamp>, Info CBS Lock: Lock removed: WinlogonNotifyLock, level: 8, total lock:6

 0.76%  <timestamp>, Info CSI 00000001@2021/8/6:18:01:59.985 WcpInitialize: wcp.dll version 10.0.19041.1081 (WinBuild.160101.0800)
```

```
75.86%
timestamp, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-LanguageFeatures-Basic-af-za-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
6.75%
timestamp, Info CBS Appl: detect Parent, Package: Microsoft-Windows-WMI-SNMP-Provider-Client-Package~31bf3856ad364e35~amd64~~10.0.19041.1, Parent: Microsoft-Windows-Client-Features-Package~31bf3856ad364e35~amd64~~10.0.19041.1, Disposition = Detect, VersionComp: EQ, BuildComp: GE, RevisionComp: GE, Exist: present
3.98%
timestamp, Info CBS CbsCoreFinalize: WdsUnload, logging from cbscore will end.
2.44%
timestamp, Info CBS Lock: Lock removed: WinlogonNotifyLock, level: 8, total lock:6
0.76%
timestamp, Info CSI 00000001@2021/8/6:18:01:59.985 WcpInitialize: wcp.dll version 10.0.19041.1081 (WinBuild.160101.0800)
```

v) We can count the total events happened for a pattern



5 patterns based on a sample of 3,968 events

```
75.86%  <timestamp>, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-LanguageFeatures-Basic-af-za-Package~31bf3856ad364e3
        5~amd64~~10.0.19041.1, applicable state: Installed

 6.75%  <timestamp>, Info CBS Appl: detect Parent, Package: Microsoft-Windows-WMI-SNMP-Provider-Client-Package~31bf3856ad364e35~amd64~~10.0.19041.1, Pa
        rent: Microsoft-Windows-Client-Features-Package~31bf3856ad364e35~amd64~~10.0.19041.1, Disposition = Detect, VersionComp: EQ, BuildComp: GE, Rev
        isionComp: GE, Exist: present

 3.98%  <timestamp>, Info CBS CbsCoreFinalize: WdsUnload, logging from cbscore will end.

 2.44%  <timestamp>, Info CBS Lock: Lock removed: WinlogonNotifyLock, level: 8, total lock:6

 0.76%  <timestamp>, Info CSI 00000001@2021/8/6:18:01:59.985 WcpInitialize: wcp.dll version 10.0.19041.1081 (WinBuild.160101.0800)
```

ESTIMATED EVENTS

4.29K

SEARCH

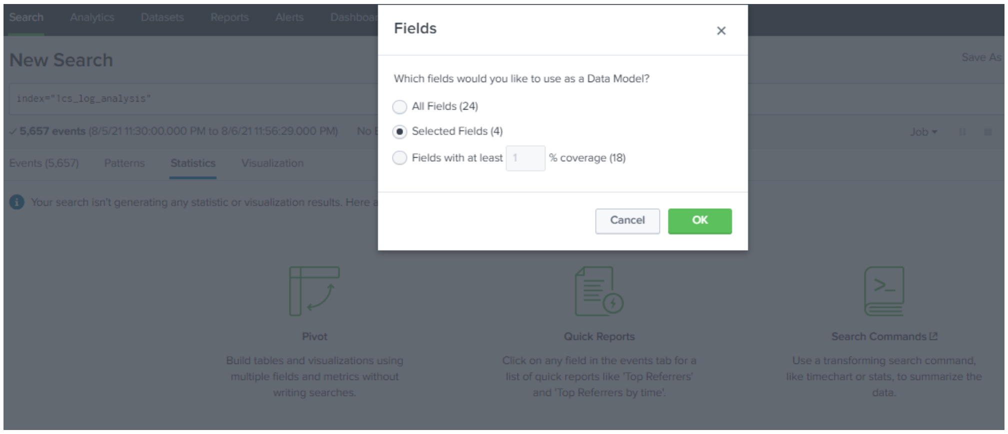
`index="1cs_log_analysis" state`

INCLUDED KEYWORDS

state

vi) We can find **the statistical analysis** of the logs

```
Queries Example: index= “main” Type= information | stats count by date_hour
(index=* OR index=_*) (index="1cs_log_analysis")  | rename punct AS RootObject.punct  |  fields  "_time"  "host"  "source"  "sourcetype" "RootObject.punct"
```



`index="1cs_log_analysis"`

✓ 5,657 events (8/5/21 11:30:00.000 PM to 8/6/21 11:56:29.000 PM) No E

Your search isn't generating any statistic or visualization results. Here a

Fields

Which fields would you like to use as a Data Model?

○ All Fields (24)

● Selected Fields (4)

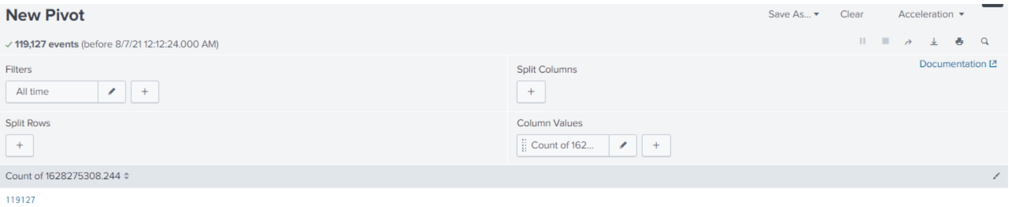
○ Fields with at least 1 % coverage (18)

Build tables and visualizations using multiple fields and metrics without writing searches.

Click on any field in the events tab for a list of quick reports like 'Top Referrers' and 'Top Referrers by time'.

Use a transforming search command, like timechart or stats, to summarize the data.

v) We can make a pivot chart based on the fields we want which can be selected here in this dialog box.



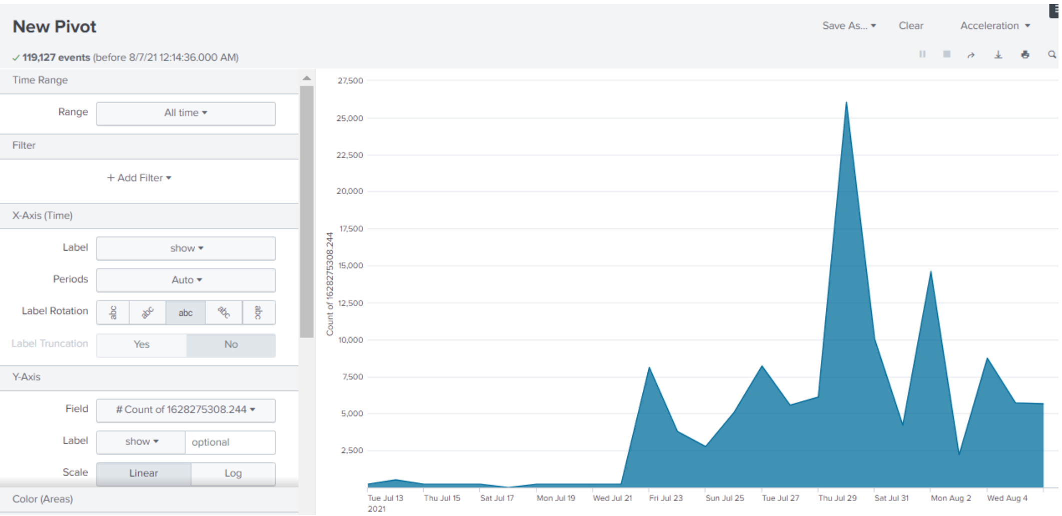
✓ 119,127 events (before 8/7/21 12:12:24.000 AM)

Filters: All time

Column Values: Count of 162...

Count of 1628275308.244
119127

vi) We can visualize the information using graphs like **line chart, pie chart, area chart, meter gauge , temperature gauge , bubble chart etc.**



New Pivot

✓ 119,127 events (before 8/7/21 12:14:36.000 AM)

Time Range

Range: All time

Filter

+ Add Filter

X-Axis (Time)

Label: show

Periods: Auto

Label Rotation: abc

Label Truncation: Yes | No

Y-Axis

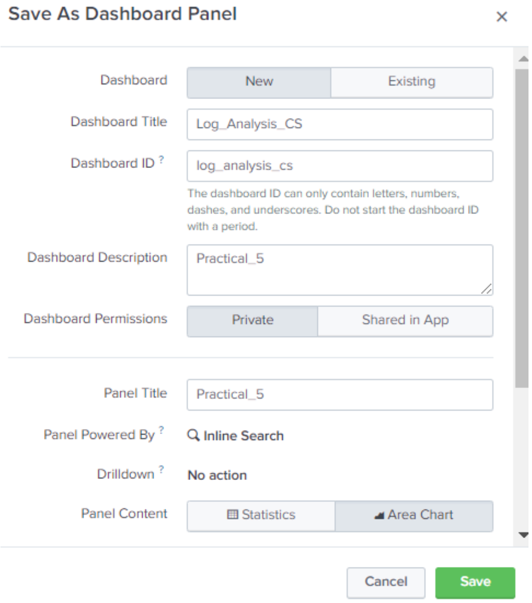
Field: # Count of 1628275308.244

Label: show | optional

Scale: Linear | Log

Color (Areas)

vii) We can **export, share and print** the graph result from top right corner or **save it in the dashboard.**



Save As Dashboard Panel

Dashboard: New | Existing

Dashboard Title: Log_Analysis_CS

Dashboard ID: log_analysis_cs

The dashboard ID can only contain letters, numbers, dashes, and underscores. Do not start the dashboard ID with a period.

Dashboard Description: Practical_5

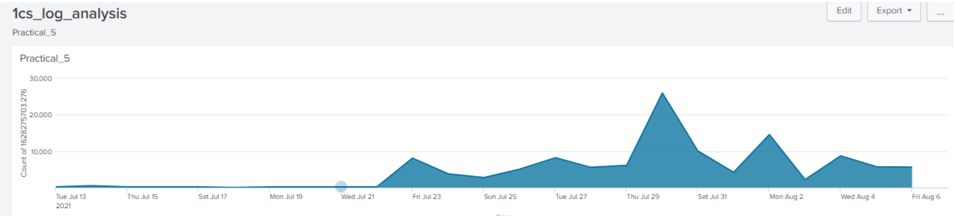
Dashboard Permissions: Private | Shared in App

Panel Title: Practical_5

Panel Powered By: Inline Search

Drilldown: No action

Panel Content: Statistics | Area Chart

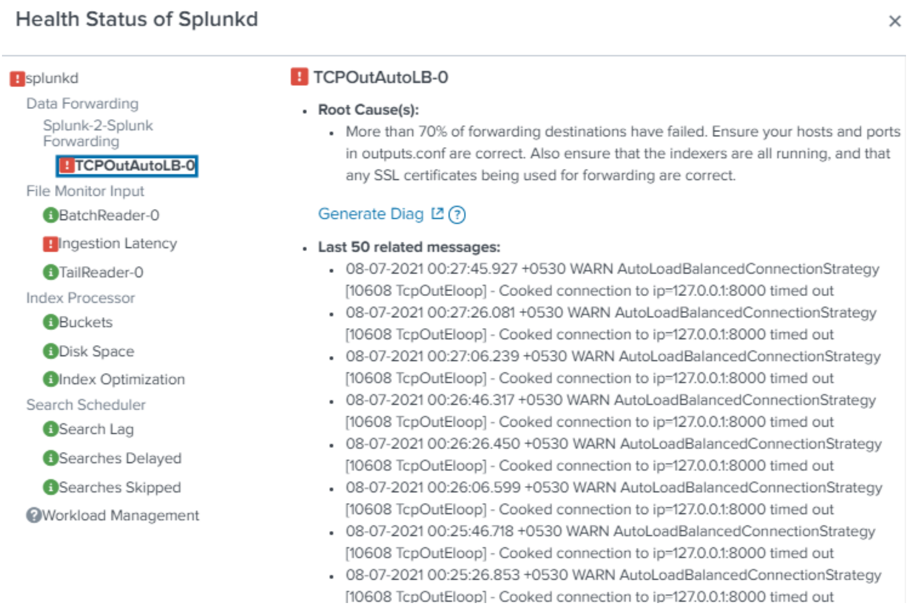


1cs_log_analysis

Practical_5

Practical_5

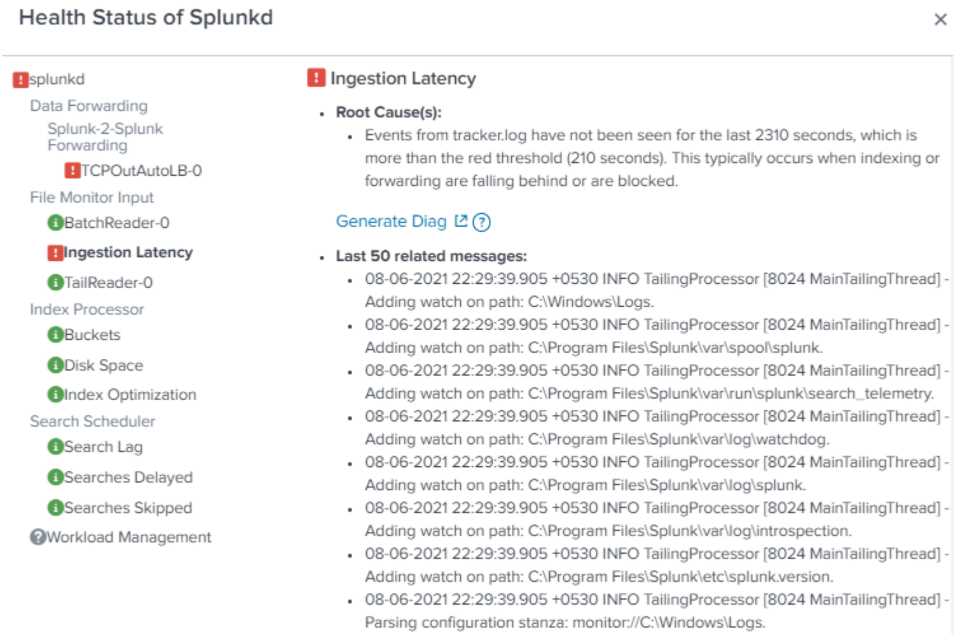
viii) We can understand the health of the system using splunk administrator



TCPOutAutoLB-0

- **Root Cause(s):**
  - More than 70% of forwarding destinations have failed. Ensure your hosts and ports in outputs.conf are correct. Also ensure that the indexers are all running, and that any SSL certificates being used for forwarding are correct.
- **Last 50 related messages:**

```
• 08-07-2021 00:27:45.927 +0530 WARN AutoLoadBalancedConnectionStrategy
  [10608 TcpOutEloop] - Cooked connection to ip=127.0.0.1:8000 timed out
• 08-07-2021 00:27:26.081 +0530 WARN AutoLoadBalancedConnectionStrategy
  [10608 TcpOutEloop] - Cooked connection to ip=127.0.0.1:8000 timed out
• 08-07-2021 00:27:06.239 +0530 WARN AutoLoadBalancedConnectionStrategy
  [10608 TcpOutEloop] - Cooked connection to ip=127.0.0.1:8000 timed out
• 08-07-2021 00:26:46.317 +0530 WARN AutoLoadBalancedConnectionStrategy
  [10608 TcpOutEloop] - Cooked connection to ip=127.0.0.1:8000 timed out
• 08-07-2021 00:26:26.450 +0530 WARN AutoLoadBalancedConnectionStrategy
  [10608 TcpOutEloop] - Cooked connection to ip=127.0.0.1:8000 timed out
• 08-07-2021 00:26:06.599 +0530 WARN AutoLoadBalancedConnectionStrategy
  [10608 TcpOutEloop] - Cooked connection to ip=127.0.0.1:8000 timed out
• 08-07-2021 00:25:46.718 +0530 WARN AutoLoadBalancedConnectionStrategy
  [10608 TcpOutEloop] - Cooked connection to ip=127.0.0.1:8000 timed out
• 08-07-2021 00:25:26.853 +0530 WARN AutoLoadBalancedConnectionStrategy
  [10608 TcpOutEloop] - Cooked connection to ip=127.0.0.1:8000 timed out
```

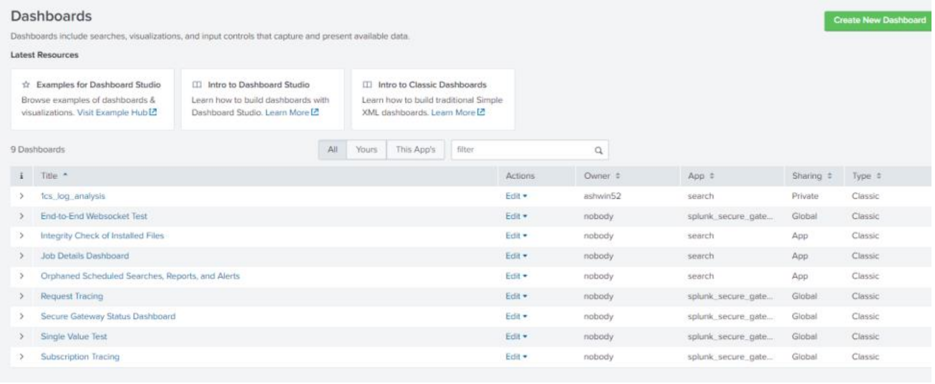


Ingestion Latency

- **Root Cause(s):**
  - Events from tracker.log have not been seen for the last 2310 seconds, which is more than the red threshold (210 seconds). This typically occurs when indexing or forwarding are falling behind or are blocked.
- **Last 50 related messages:**

```
• 08-06-2021 22:29:39.905 +0530 INFO TailingProcessor [8024 MainTailingThread] -
  Adding watch on path: C:\Windows\Logs.
• 08-06-2021 22:29:39.905 +0530 INFO TailingProcessor [8024 MainTailingThread] -
  Adding watch on path: C:\Program Files\Splunk\var\spool\splunk.
• 08-06-2021 22:29:39.905 +0530 INFO TailingProcessor [8024 MainTailingThread] -
  Adding watch on path: C:\Program Files\Splunk\var\run\splunk\search_telemetry.
• 08-06-2021 22:29:39.905 +0530 INFO TailingProcessor [8024 MainTailingThread] -
  Adding watch on path: C:\Program Files\Splunk\var\log\watchdog.
• 08-06-2021 22:29:39.905 +0530 INFO TailingProcessor [8024 MainTailingThread] -
  Adding watch on path: C:\Program Files\Splunk\var\log\splunk.
• 08-06-2021 22:29:39.905 +0530 INFO TailingProcessor [8024 MainTailingThread] -
  Adding watch on path: C:\Program Files\Splunk\var\log\introspection.
• 08-06-2021 22:29:39.905 +0530 INFO TailingProcessor [8024 MainTailingThread] -
  Adding watch on path: C:\Program Files\Splunk\etc\splunk.version.
• 08-06-2021 22:29:39.905 +0530 INFO TailingProcessor [8024 MainTailingThread] -
  Parsing configuration stanza: monitor://C:\Windows\Logs.
```

5. Playing with the **Dashboards** like we can have the detailed analysis of dashboard contents



Dashboards

Dashboards include searches, visualizations, and input controls that capture and present available data.

Latest Resources

☆ **Examples for Dashboard Studio**
Browse examples of dashboards & visualizations. Visit Example Hub

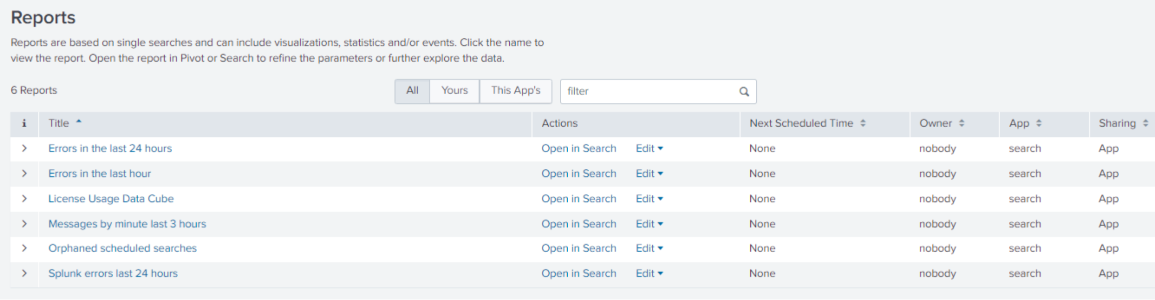
Intro to Dashboard Studio
Learn how to build dashboards with Dashboard Studio. Learn More

Intro to Classic Dashboards
Learn how to build traditional Simple XML dashboards. Learn More

9 Dashboards

i	Title	Actions	Owner	App	Sharing	Type
>	1cs_log_analysis	Edit ▾	ashwin52	search	Private	Classic
>	End-to-End Websocket Test	Edit ▾	nobody	splunk_secure_gate...	Global	Classic
>	Integrity Check of Installed Files	Edit ▾	nobody	search	App	Classic
>	Job Details Dashboard	Edit ▾	nobody	search	App	Classic
>	Orphaned Scheduled Searches, Reports, and Alerts	Edit ▾	nobody	search	App	Classic
>	Request Tracing	Edit ▾	nobody	splunk_secure_gate...	Global	Classic
>	Secure Gateway Status Dashboard	Edit ▾	nobody	splunk_secure_gate...	Global	Classic
>	Single Value Test	Edit ▾	nobody	splunk_secure_gate...	Global	Classic
>	Subscription Tracing	Edit ▾	nobody	splunk_secure_gate...	Global	Classic

6. In the **Reports** tab, we can identify the log report based for a specific timeline



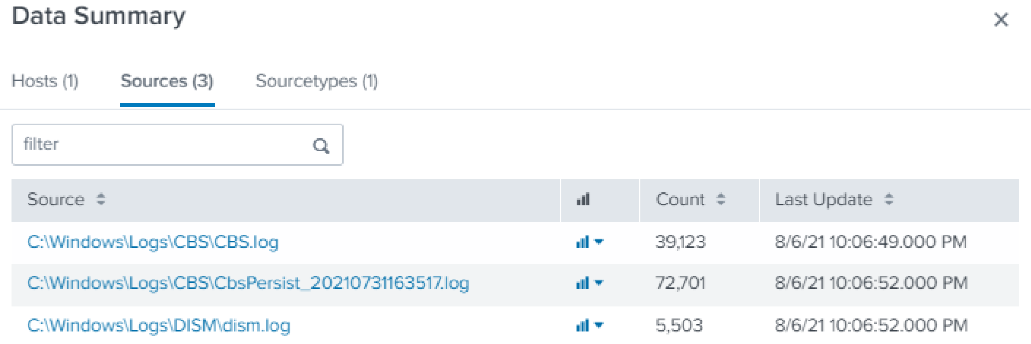
Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

6 Reports

i	Title ▴	Actions		Next Scheduled Time ⇕	Owner ⇕	App ⇕	Sharing ⇕
›	Errors in the last 24 hours	Open in Search	Edit ▾	None	nobody	search	App
›	Errors in the last hour	Open in Search	Edit ▾	None	nobody	search	App
›	License Usage Data Cube	Open in Search	Edit ▾	None	nobody	search	App
›	Messages by minute last 3 hours	Open in Search	Edit ▾	None	nobody	search	App
›	Orphaned scheduled searches	Open in Search	Edit ▾	None	nobody	search	App
›	Splunk errors last 24 hours	Open in Search	Edit ▾	None	nobody	search	App

7. Scrutinizing the **data summary**



Data Summary

Source ⇕		Count ⇕	Last Update ⇕
C:\Windows\Logs\CBS\CBS.log	▾	39,123	8/6/21 10:06:49.000 PM
C:\Windows\Logs\CBS\CbsPersist_20210731163517.log	▾	72,701	8/6/21 10:06:52.000 PM
C:\Windows\Logs\DISM\dism.log	▾	5,503	8/6/21 10:06:52.000 PM