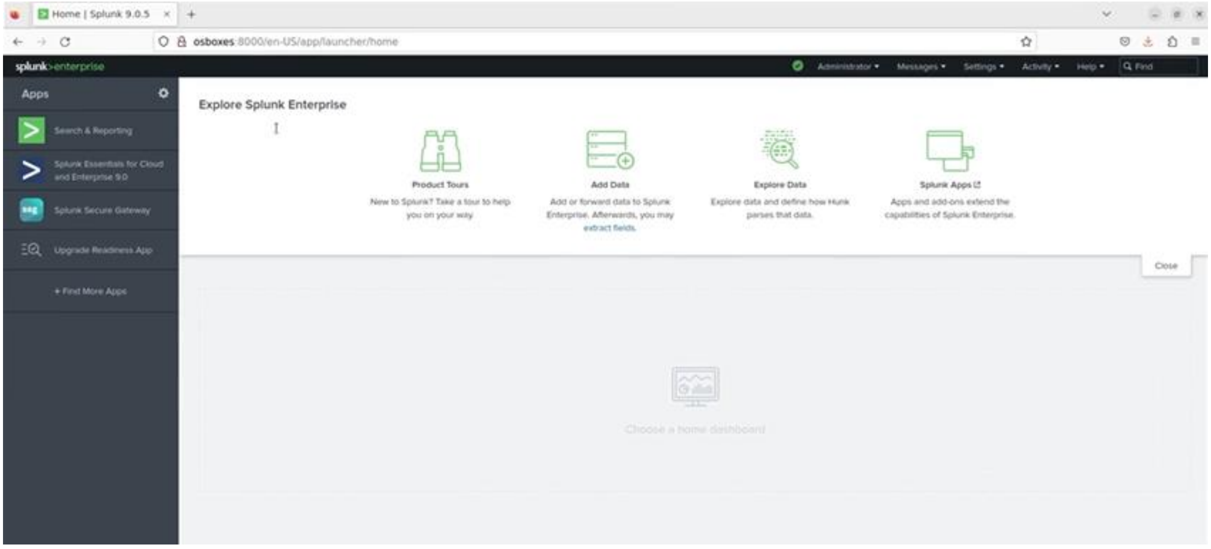
Setup Receiving Index on Splunk Server:

Now we setup the receiving index on splunk.
The reason is that after this setup we can get the logs of network.
We set port and index for this purpose.
Lets go

- ❖ Open the splunk



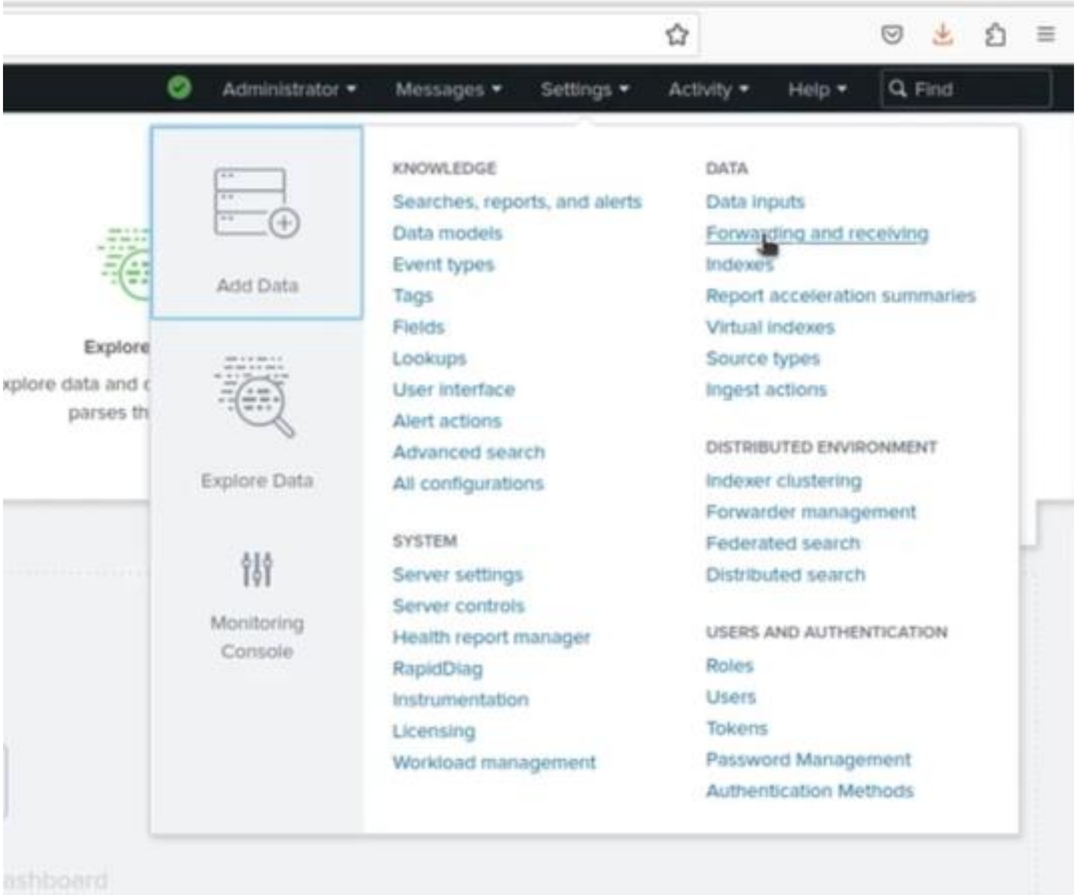
New to Splunk? Take a tour to help you on your way.

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

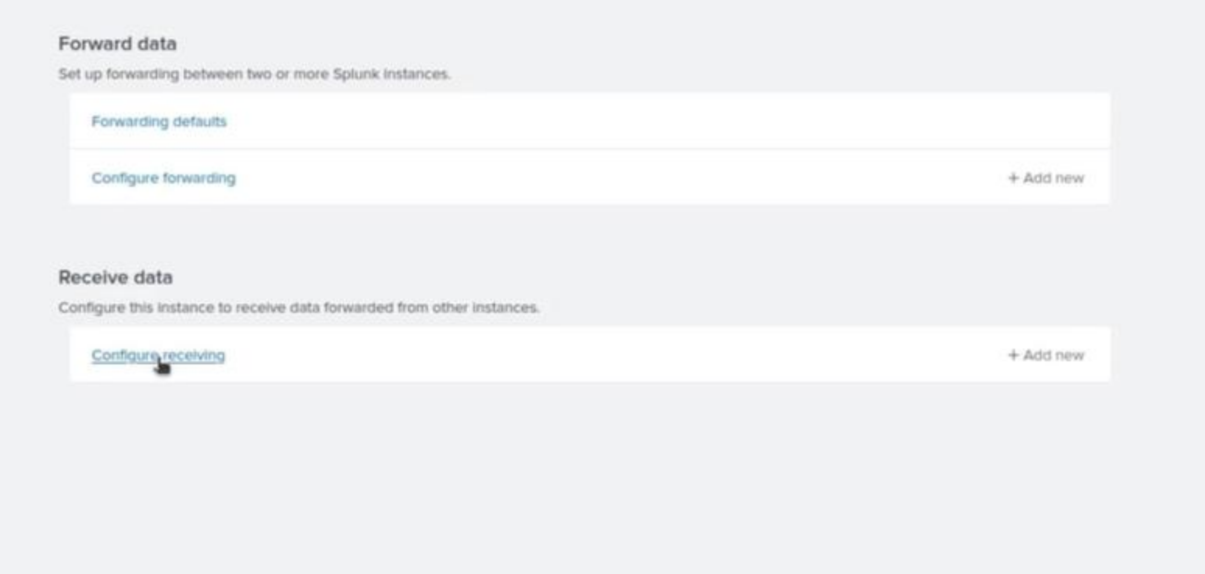
Explore data and define how Hunk parses that data.

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

- ❖ Go to settings
- ❖ Select forwarding and receiving



- ❖ In next open window select the configure receiving.



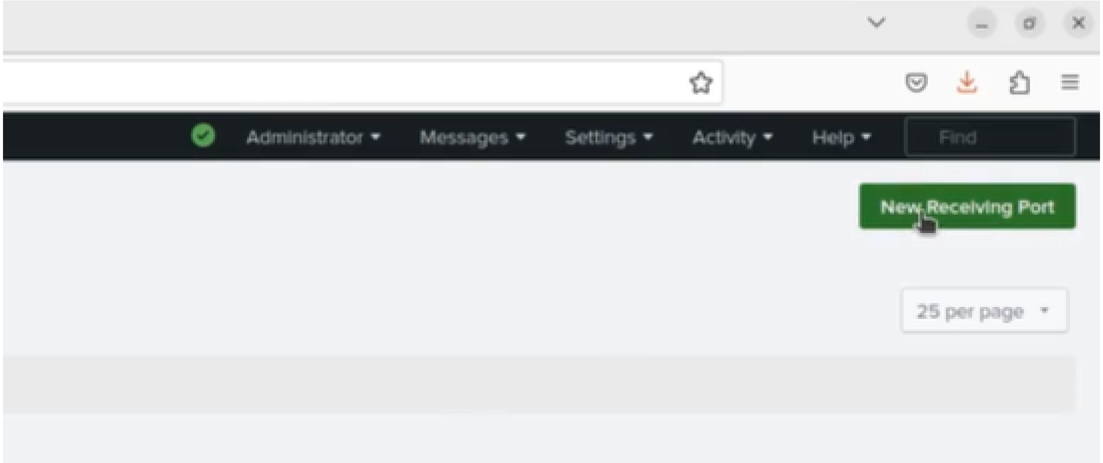
Forward data

Set up forwarding between two or more Splunk instances.

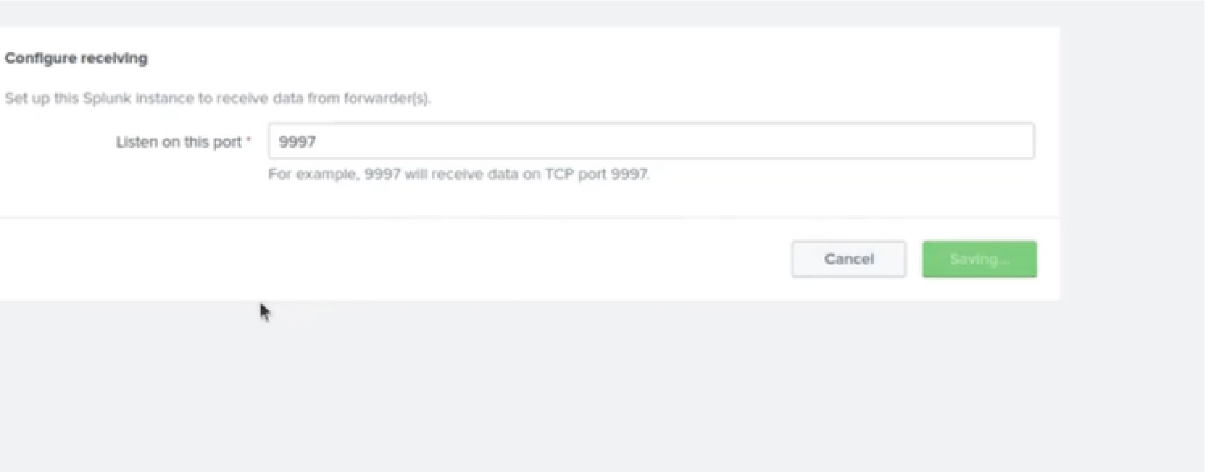
Receive data

Configure this instance to receive data forwarded from other instances.

- ❖ Then select new receiving port



- Select the port from which you get data, I use default.

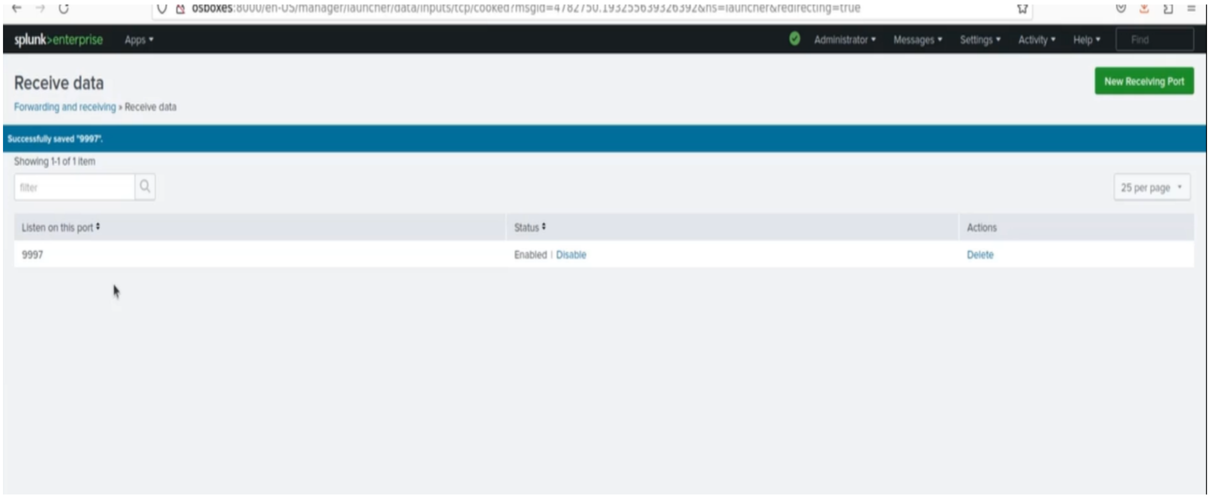


Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port * 9997

For example, 9997 will receive data on TCP port 9997.


osboxes:8000/en-US/manager/launcher/data/inputs/tcp/cooked?msgid=4782750.19325563932639 2&ns=launcher&redirecting=true
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
New Receiving Port
filter
25 per page

Receive data

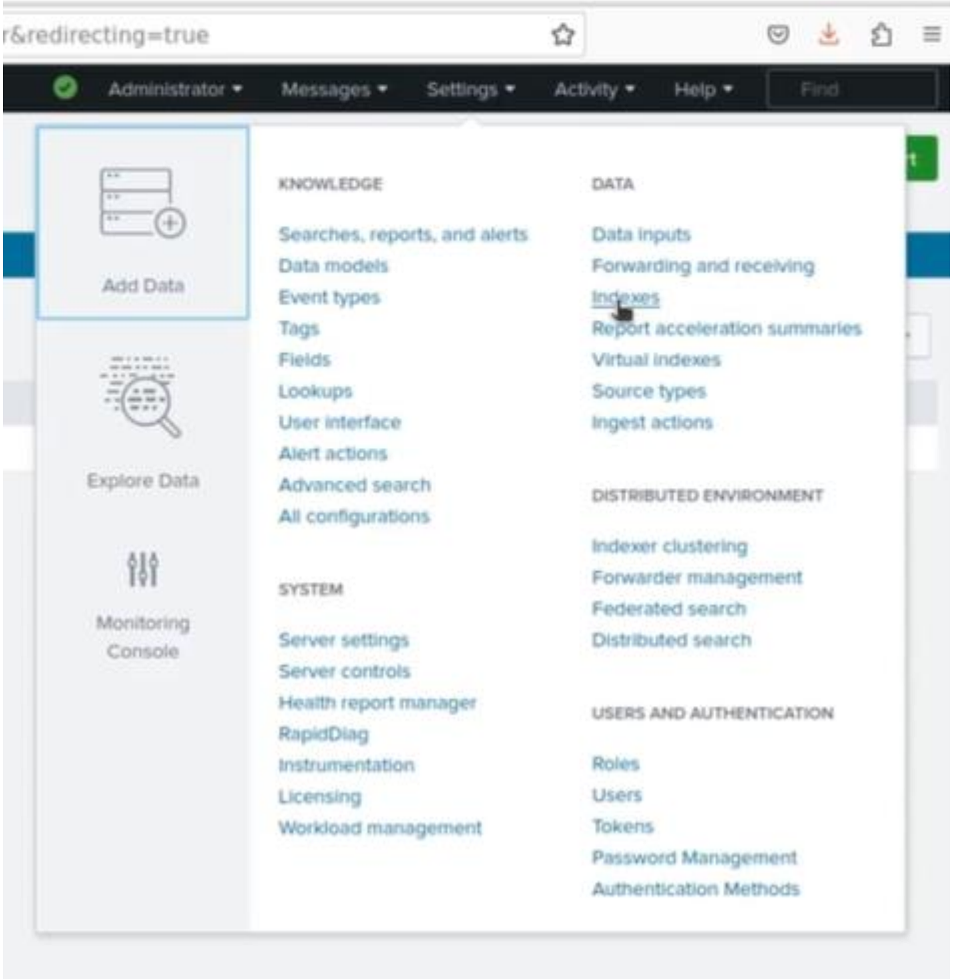
Forwarding and receiving » Receive data

Successfully saved "9997".

Showing 1-1 of 1 item

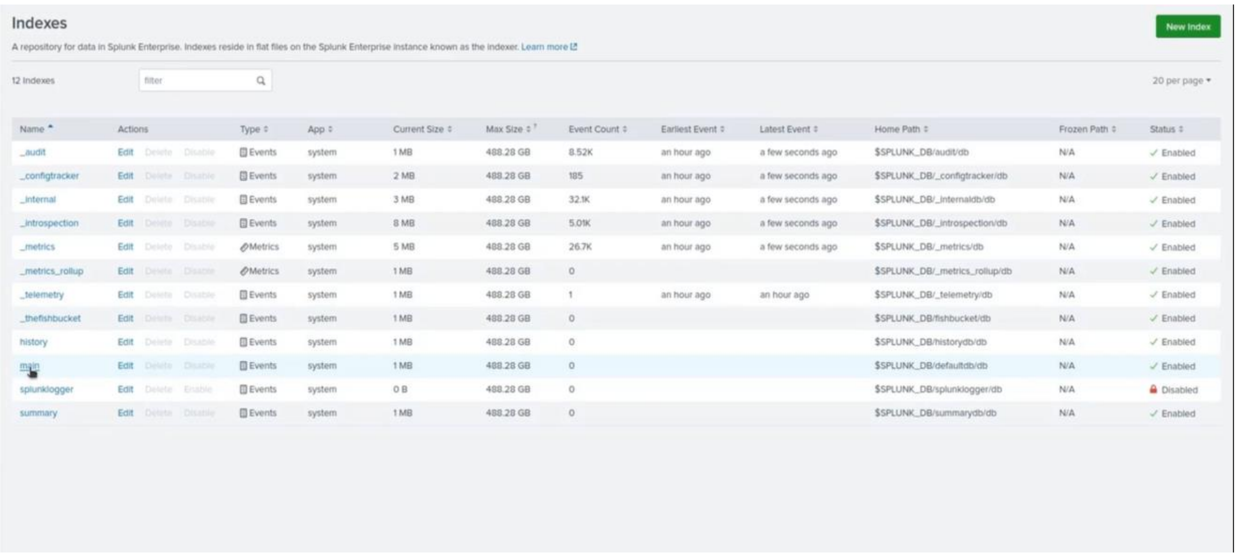
Listen on this port	Status	Actions
9997	Enabled | Disable	Delete

Now go to index



Index I add, so we can manage the collected logs easily.

- Index with underscore are of system thay cannot deleted
- The index with name main can get the all logs of network
- But in management it will create problem
- So we add new index their with name winsrvlogs

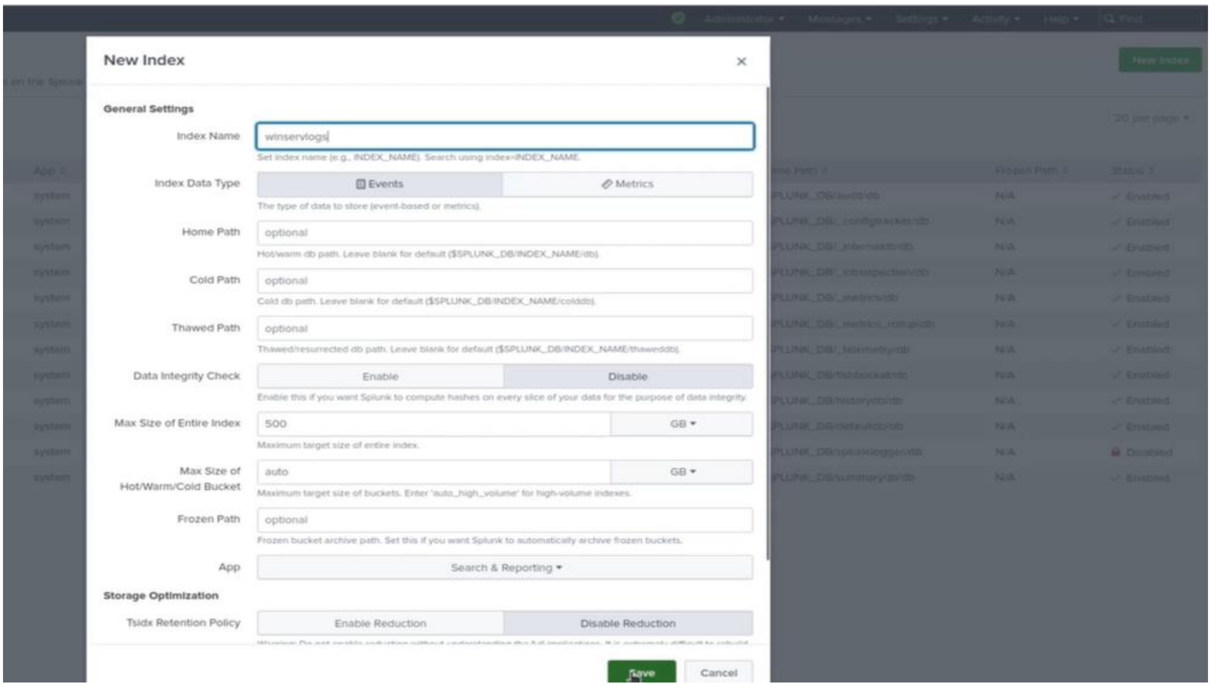


Indexes

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status
_audit	Edit Delete Disable	Events	system	1 MB	488.28 GB	8.52K	an hour ago	a few seconds ago	$SPLUNK_DB/audit/db	N/A	✓ Enabled
_configtracker	Edit Delete Disable	Events	system	2 MB	488.28 GB	185	an hour ago	a few seconds ago	$SPLUNK_DB/_configtracker/db	N/A	✓ Enabled
_internal	Edit Delete Disable	Events	system	3 MB	488.28 GB	32.1K	an hour ago	a few seconds ago	$SPLUNK_DB/_internaldb/db	N/A	✓ Enabled
_introspection	Edit Delete Disable	Events	system	8 MB	488.28 GB	5.01K	an hour ago	a few seconds ago	$SPLUNK_DB/_introspection/db	N/A	✓ Enabled
_metrics	Edit Delete Disable	Metrics	system	5 MB	488.28 GB	26.7K	an hour ago	a few seconds ago	$SPLUNK_DB/_metrics/db	N/A	✓ Enabled
_metrics_rollup	Edit Delete Disable	Metrics	system	1 MB	488.28 GB	0			$SPLUNK_DB/_metrics_rollup/db	N/A	✓ Enabled
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	1	an hour ago	an hour ago	$SPLUNK_DB/_telemetry/db	N/A	✓ Enabled
_thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/fishbucket/db	N/A	✓ Enabled
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/historydb/db	N/A	✓ Enabled
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/defaultdb/db	N/A	✓ Enabled
splunklogger	Edit Delete Enable	Events	system	0 B	488.28 GB	0			$SPLUNK_DB/splunklogger/db	N/A	🔒 Disabled
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/summarydb/db	N/A	✓ Enabled

- ❖ go to new index.
- ❖ Add the index give its name.
- ❖ Add more setting like space.
- ❖ Save it



New Index

General Settings

Index Name: winservlogs
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events | Metrics
The type of data to store (event-based or metrics).

Home Path: optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable | Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: 500 GB
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto GB
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

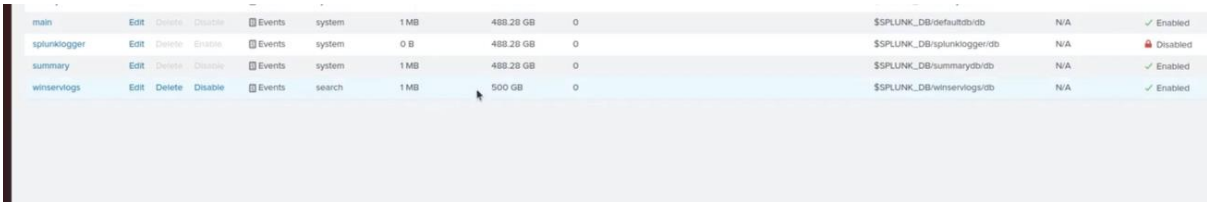
Frozen Path: optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App: Search & Reporting

Storage Optimization

Tsidx Retention Policy: Enable Reduction | Disable Reduction

- ❖ New index is added



main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/defaultdb/db	N/A	✓ Enabled
splunklogger	Edit Delete Enable	Events	system	0 B	488.28 GB	0			$SPLUNK_DB/splunklogger/db	N/A	🔒 Disabled
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/summarydb/db	N/A	✓ Enabled
winservlogs	Edit Delete Disable	Events	search	1 MB	500 GB	0			$SPLUNK_DB/winservlogs/db	N/A	✓ Enabled

Now system is ready to collect logs.