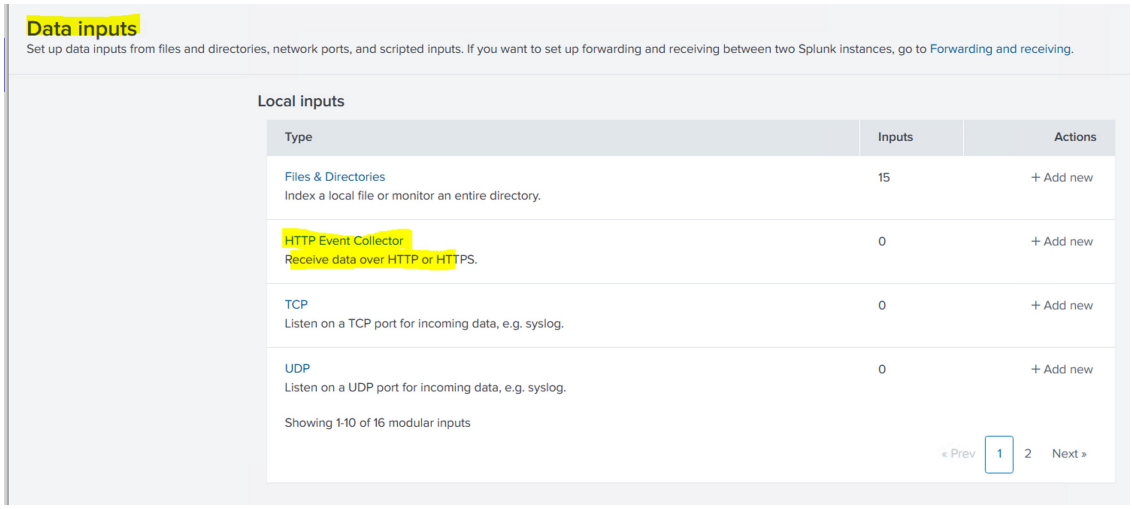
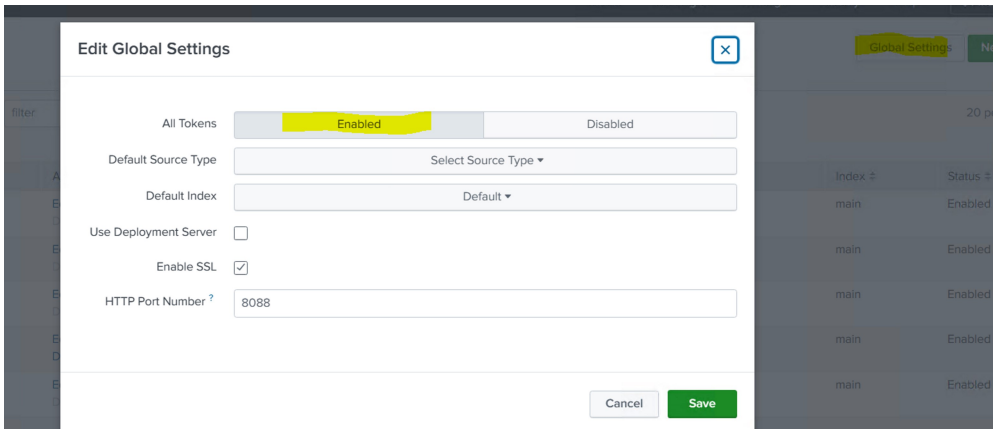
Training – Day #7

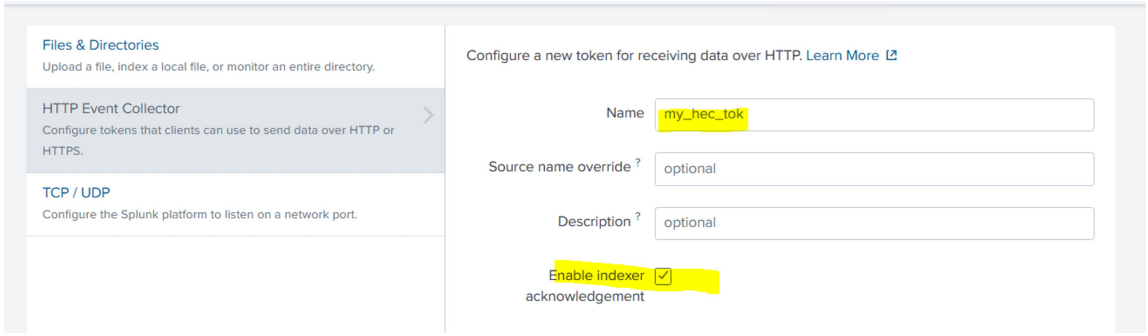
15 June 2023 05:04

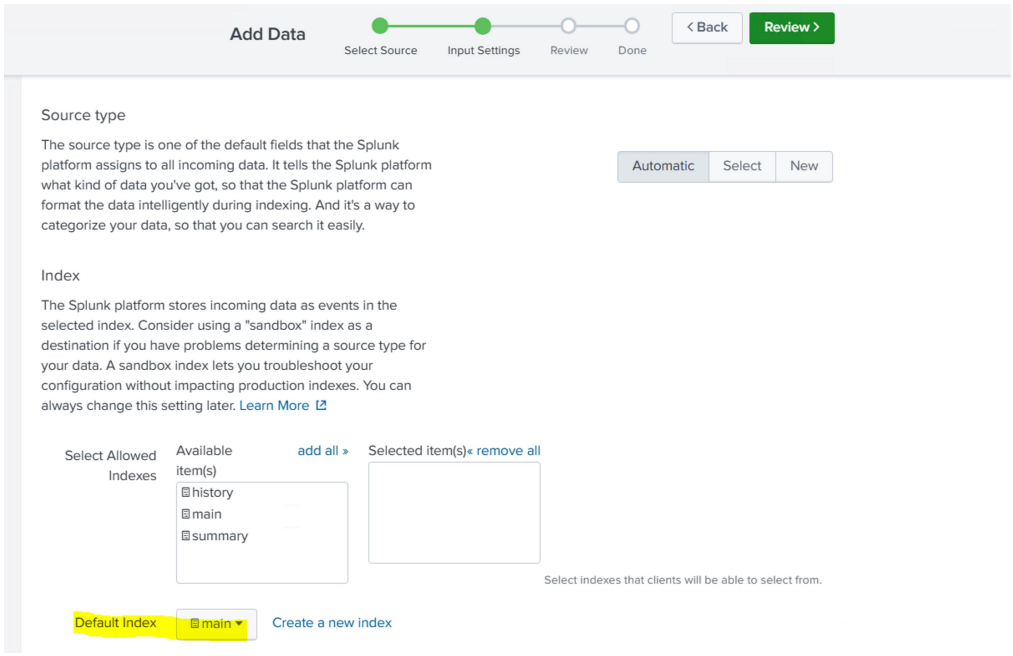
#HEC (Http Event Collector)

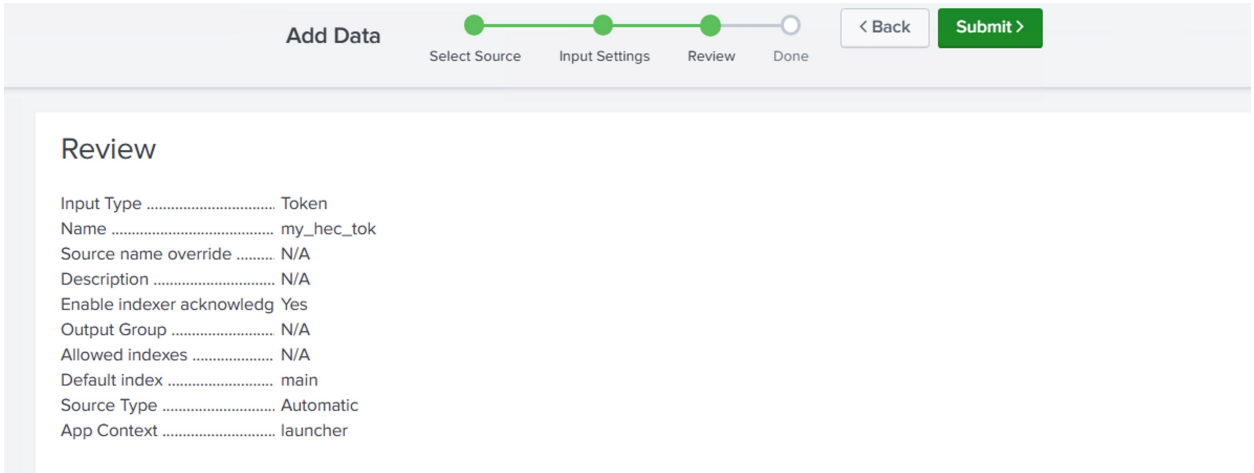


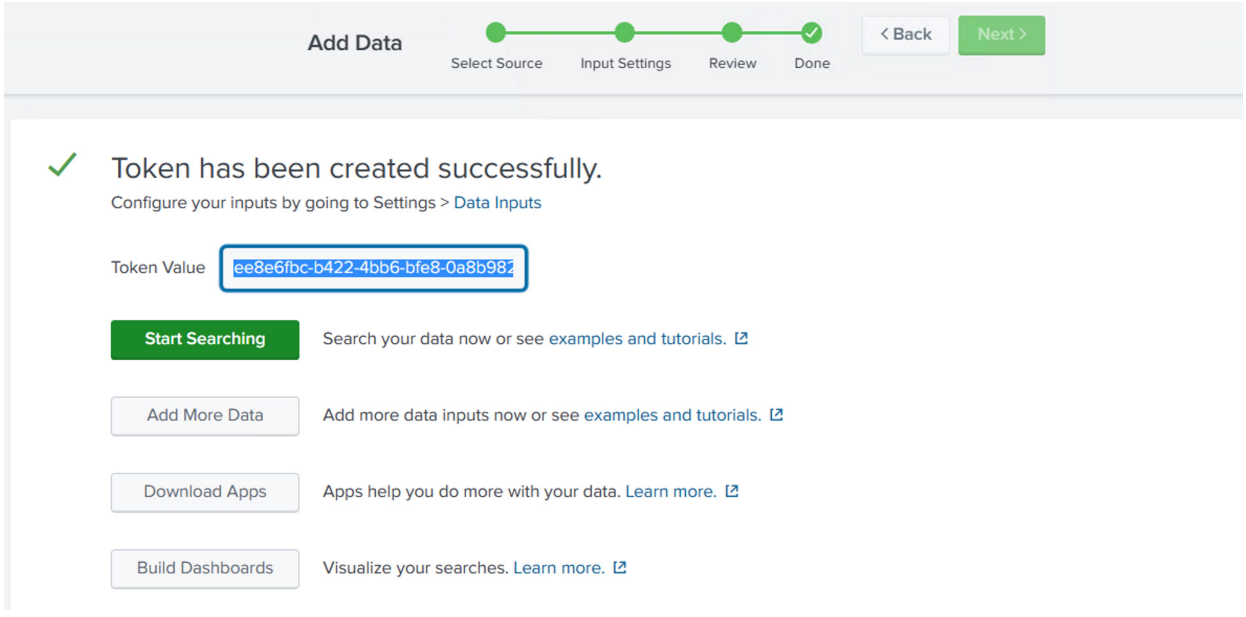
By default all tokens are disable state in "Global Settings"



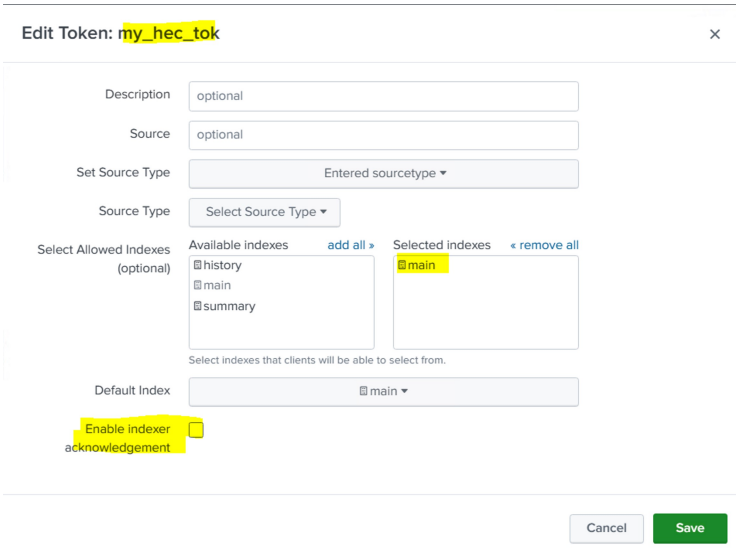



Add Data
Select Source
Input Settings
Review
Done
< Back
Review >
Source type
The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.
Automatic
Select
New
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
Select Allowed Indexes
Available item(s)
add all »
history
main
summary
Selected item(s)
« remove all
Select indexes that clients will be able to select from.
Default Index
main
Create a new index


Add Data
Select Source
Input Settings
Review
Done
< Back
Submit >
Review
Input Type ..... Token
Name ..... my_hec_tok
Source name override ..... N/A
Description ..... N/A
Enable indexer acknowledg Yes
Output Group ..... N/A
Allowed indexes ..... N/A
Default index ..... main
Source Type ..... Automatic
App Context ..... launcher


Add Data
Select Source
Input Settings
Review
Done
< Back
Next >
Token has been created successfully.
Configure your inputs by going to Settings > Data Inputs
Token Value
ee8e6fbc-b422-4bb6-bfe8-0a8b982
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.

ee8e6fbc-b422-4bb6-bfe8-0a8b98204afb

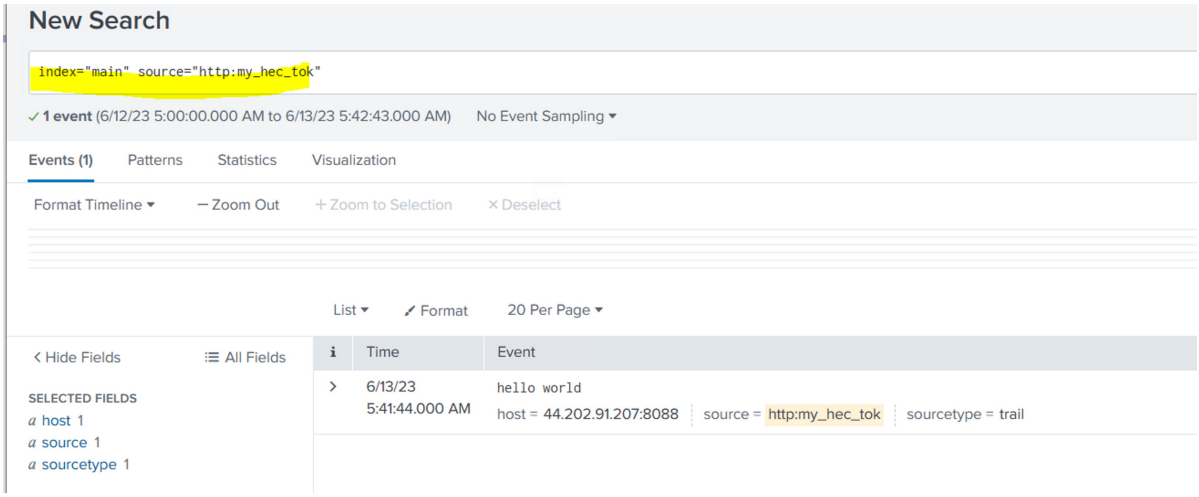


Push data through CURL command prompt using HEC token :

curl -k https://44.202.91.207:8088/services/collector -H "Authorization:Splunk ee8e6fbc-b422-4bb6-bfe8-0a8b98204afb" -d "{\"sourcetype\" : \"trail\", \"event\":\"hello world\"}"

```
C:\Users\Ankit>curl -k https://44.202.91.207:8088/services/collector -H  "Authorization:Splunk ee8e6fbc-b422-4bb6-bfe8-0
a8b98204afb" -d "{\"sourcetype\" : \"trail\", \"event\":\"hello world\"}"
{"text":"Success","code":0}
C:\Users\Ankit>_
```

index="main" source="http:my_hec_tok"



#How to Push Multiple Events

8088 => Splunk service Port

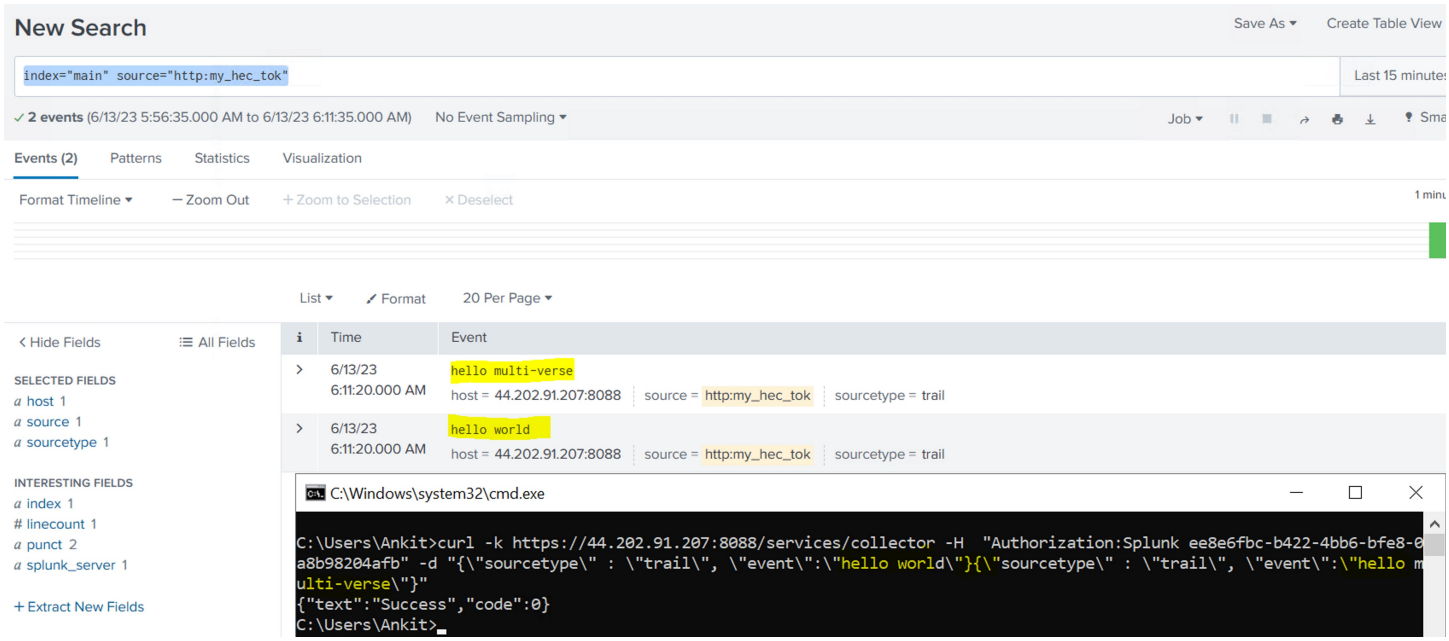
8000 => splunk web

8089 => splunkd

8091 => KV store

Payload to push multiple events :

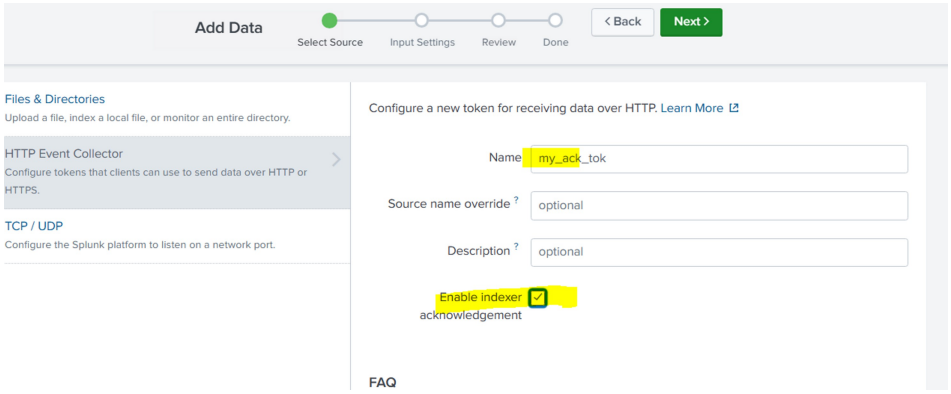
curl -k https://44.202.91.207:8088/services/collector -H "Authorization:Splunk ee8e6fbc-b422-4bb6-bfe8-0a8b98204afb" -d "{\"sourcetype\" : \"trail\", \"event\":\"hello world\"}{\"sourcetype\" : \"trail\", \"event\":\"hello multi-verse\"}"

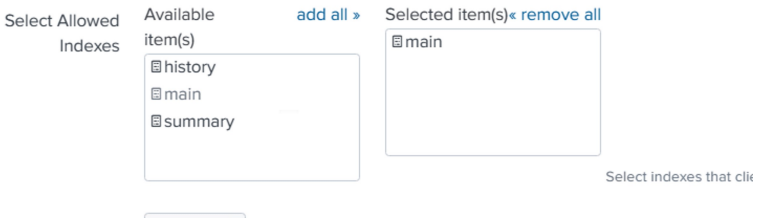


#How to Push raw text

ee8e6fbc-b422-4bb

#Indexer Acknowledgement

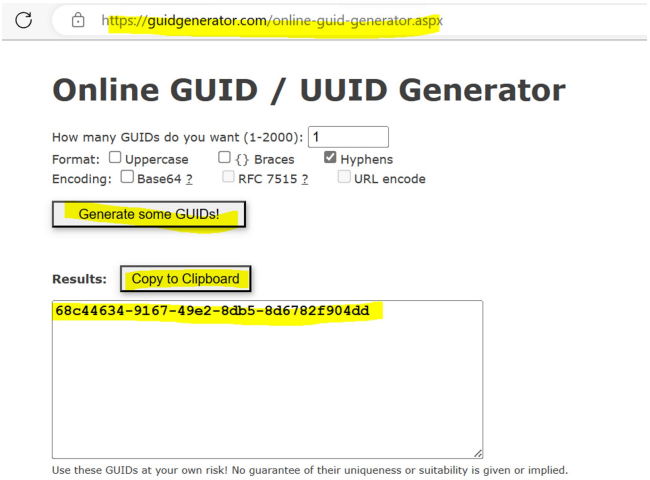




curl -k https://44.202.91.207:8088/services/collector -H "Authorization:Splunk 26ccd1d7-382f-4fc7-a64e-ff97da739b53" -d "{\"sourcetype\" : \"trail\", \"event\":\"hello world\"}{\"sourcetype\" : \"trail\", \"event\":\"hello multi-verse\"}"

It will through error "Data channel is missing" so we have to generate channel.

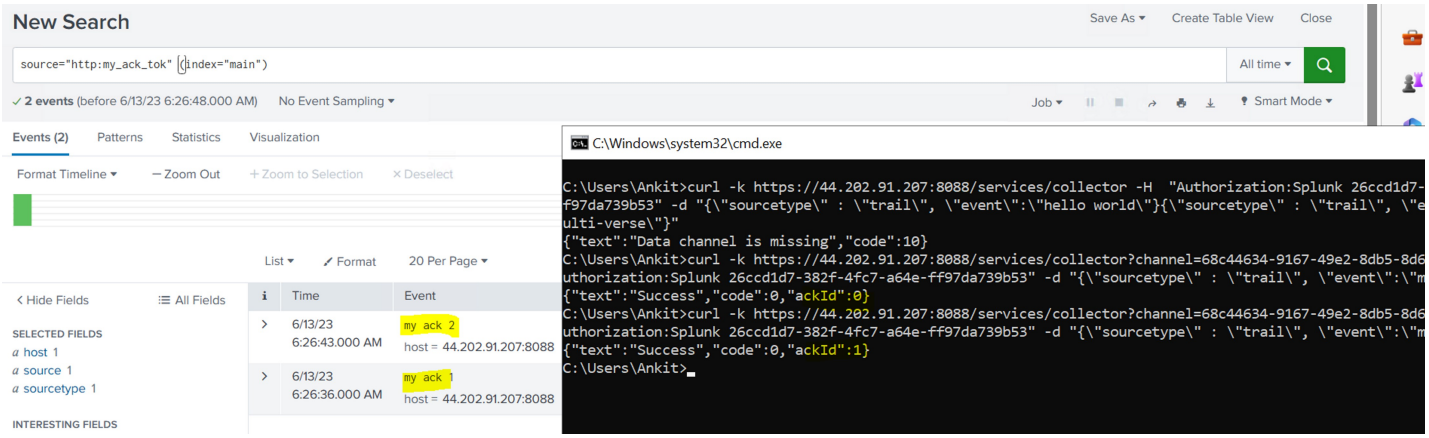
Go to website "Free Online GUID Generator" => copy unique id



Modify curl command with channel =>

curl -k https://44.202.91.207:8088/services/collector**?channel=68c44634-9167-49e2-8db5-8d6782f904dd** -H "Authorization:Splunk 26ccd1d7-382f-4fc7-a64e-ff97da739b53" -d "{\"sourcetype\" : \"trail\", \"event\":\"my ack 1\"}"

source="http:my_ack_tok" (index="main")



Note : ackId may not be in serial order.

#To check if an ackId is already pushed :

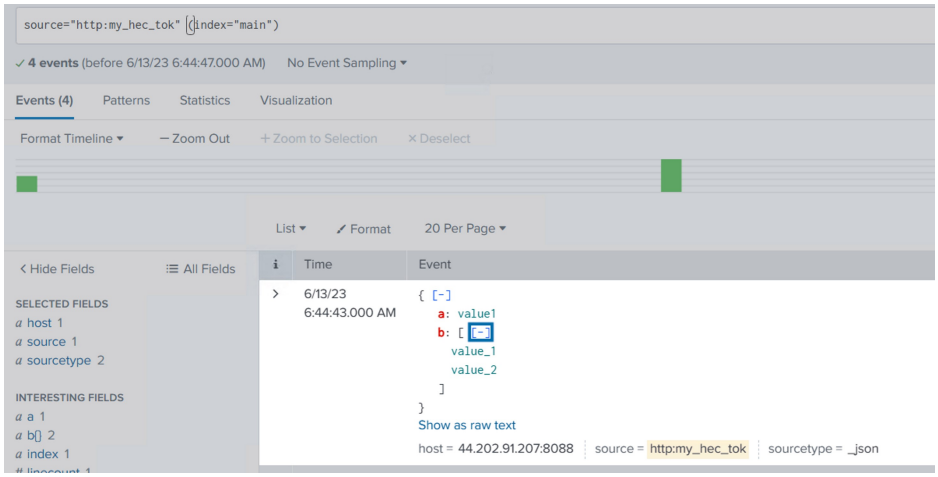
curl -k https://44.202.91.207:8088/services/collector/**ack?**channel=68c44634-9167-49e2-8db5-8d6782f904dd -H "Authorization:Splunk 26ccd1d7-382f-4fc7-a64e-ff97da739b53" -d "{\"**acks**\" :**[0]**}"

#JSON Extraction

To Push a JSON data, define sourcetype as "_json"

curl -k https://44.202.91.207:8088/services/collector -H "Authorization:Splunk ee8e6fbc-b422-4bb6-bfe8-0a8b98204afb" -d "{\"sourcetype\" : \"_json\", \"event\":{\"a\":\"value1\",\"b\":[\"value_1\", \"value_2\"]}}"

source="http:my_hec_tok" (index="main")



#Explicit JSON Extraction

#Apps/Add-on

Application => ***inputs.conf + props.conf + Transform.conf*** => create App and deploy through Deployment server.

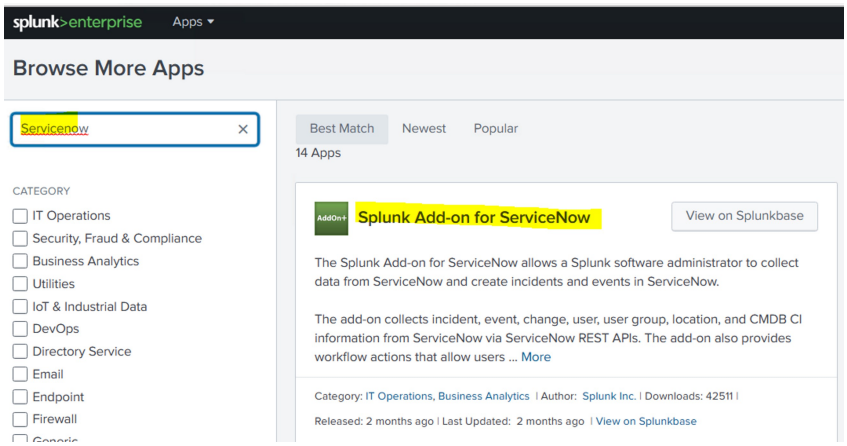
#Install ServiceNow Add-on and Integrate with Splunk

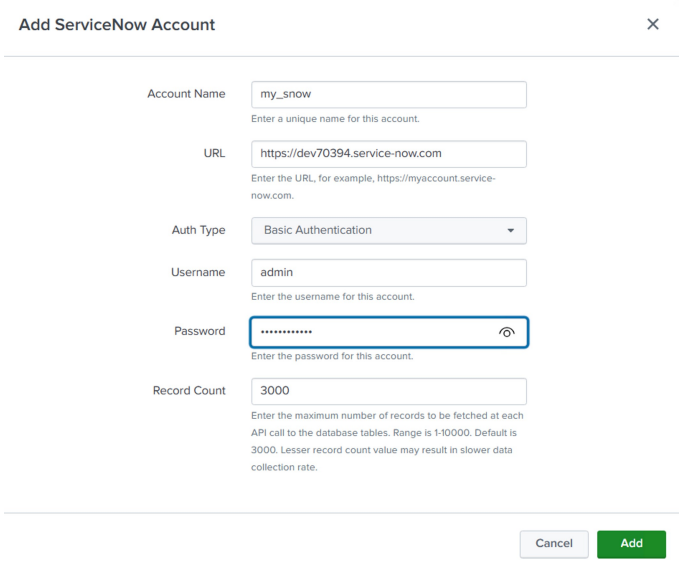
Apps => Manage App => Browse More Apps => Install "**Splunk Add-on for ServiceNow**" => Once Installed , Add "ServiceNow Account" => enter "Account Name", "URL", Username, Password, Auth Type as "Basic Authentication"

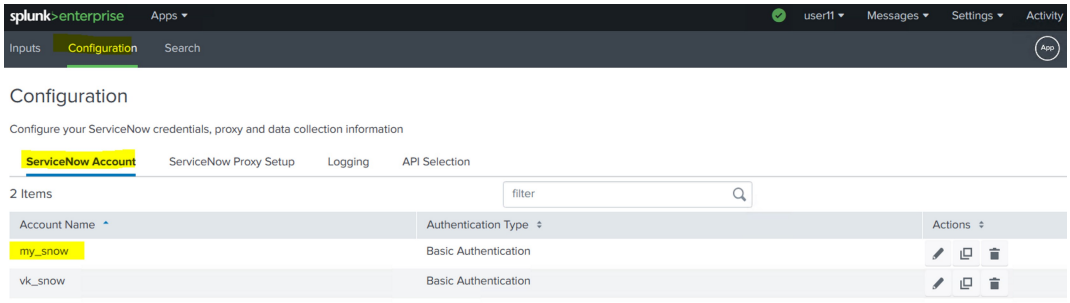
Your instance URL: https://dev70394.service-now.com

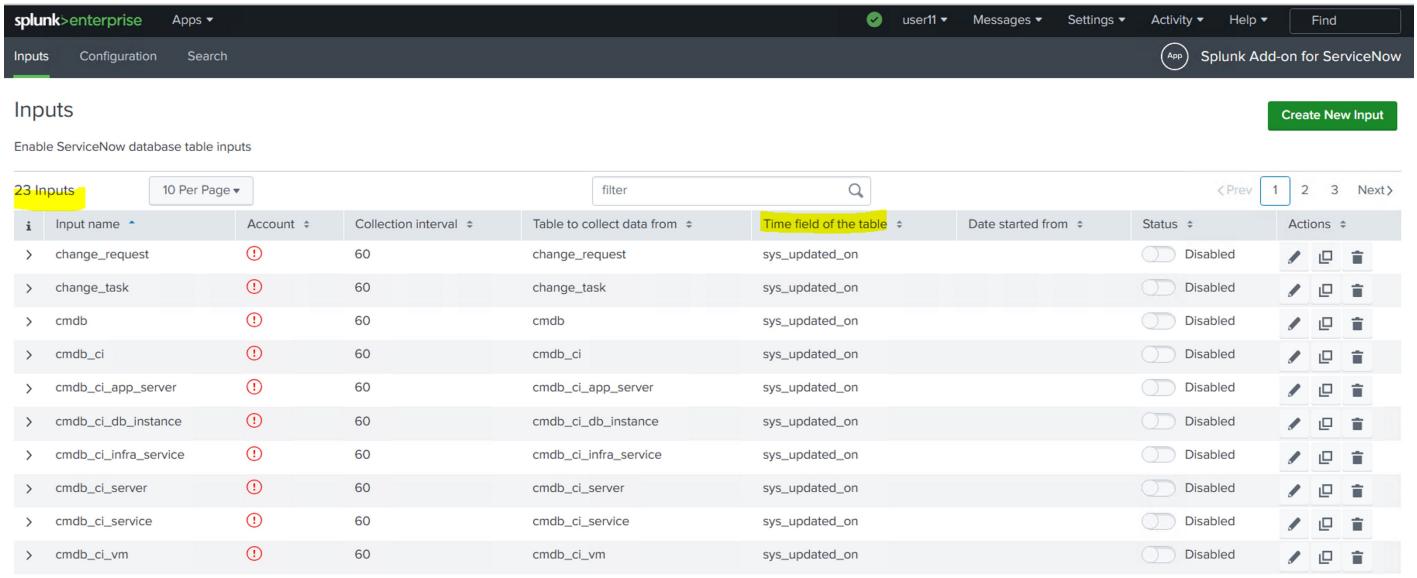
Username: **admin**

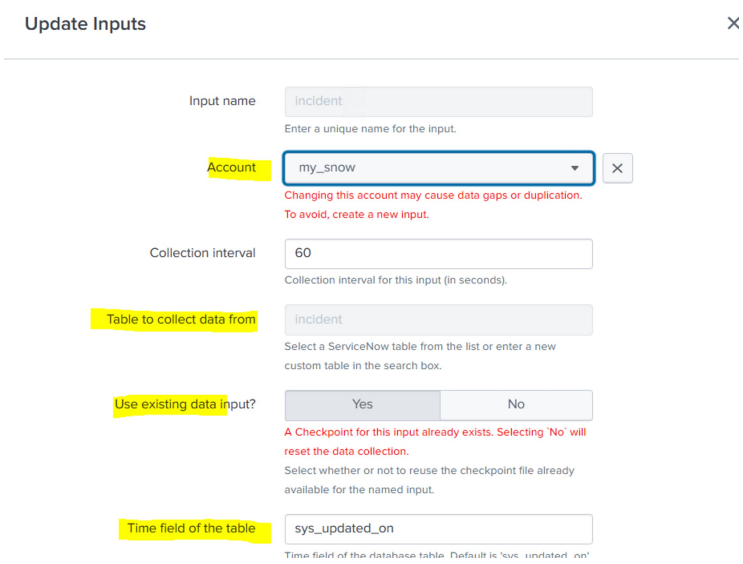
Current password: **km$PU55@oDUc**

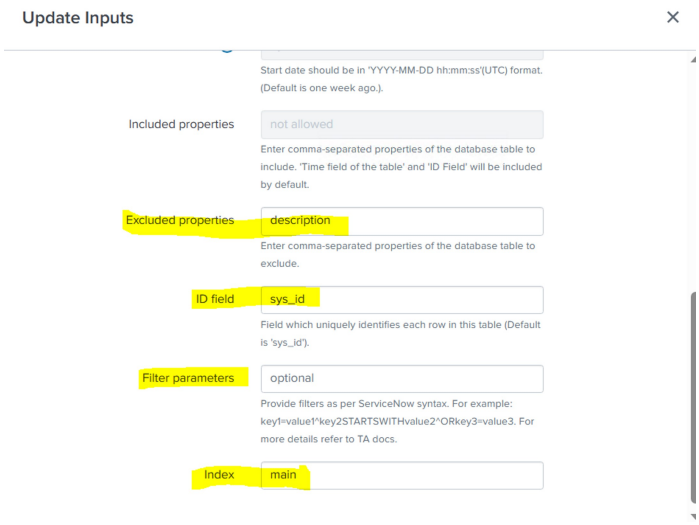


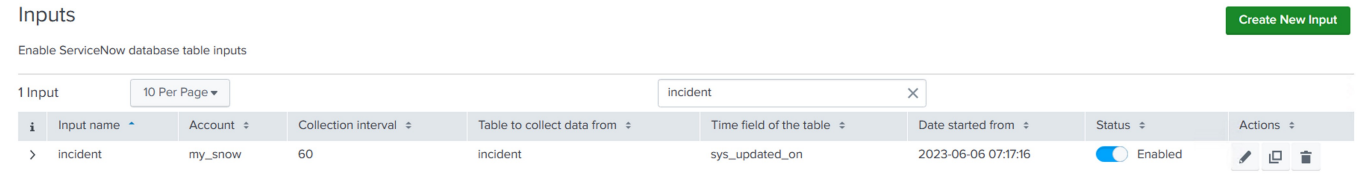

Add ServiceNow Account
Account Name
my_snow
Enter a unique name for this account.
URL
https://dev70394.service-now.com
Enter the URL, for example, https://myaccount.service-now.com.
Auth Type
Basic Authentication
Username
admin
Enter the username for this account.
Password
Enter the password for this account.
Record Count
3000
Enter the maximum number of records to be fetched at each API call to the database tables. Range is 1-10000. Default is 3000. Lesser record count value may result in slower data collection rate.
Cancel
Add


splunk>enterprise
Apps
user11
Messages
Settings
Activity
Inputs
Configuration
Search
Configuration
Configure your ServiceNow credentials, proxy and data collection information
ServiceNow Account
ServiceNow Proxy Setup
Logging
API Selection
2 Items
filter
Account Name
Authentication Type
Actions
my_snow
Basic Authentication
vk_snow
Basic Authentication


splunk>enterprise
Apps
user11
Messages
Settings
Activity
Help
Find
Inputs
Configuration
Search
Splunk Add-on for ServiceNow
Inputs
Create New Input
Enable ServiceNow database table inputs
23 Inputs
10 Per Page
filter
Prev
1
2
3
Next
Input name
Account
Collection interval
Table to collect data from
Time field of the table
Date started from
Status
Actions
change_request 60 change_request sys_updated_on Disabled
change_task 60 change_task sys_updated_on Disabled
cmdb 60 cmdb sys_updated_on Disabled
cmdb_ci 60 cmdb_ci sys_updated_on Disabled
cmdb_ci_app_server 60 cmdb_ci_app_server sys_updated_on Disabled
cmdb_ci_db_instance 60 cmdb_ci_db_instance sys_updated_on Disabled
cmdb_ci_infra_service 60 cmdb_ci_infra_service sys_updated_on Disabled
cmdb_ci_server 60 cmdb_ci_server sys_updated_on Disabled
cmdb_ci_service 60 cmdb_ci_service sys_updated_on Disabled
cmdb_ci_vm 60 cmdb_ci_vm sys_updated_on Disabled

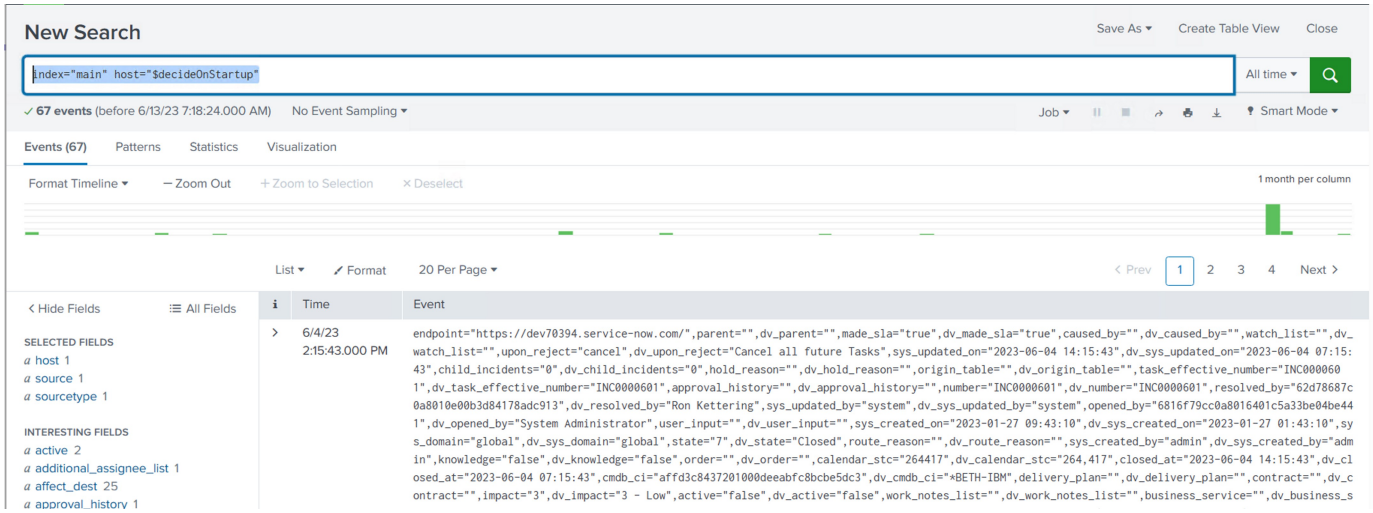




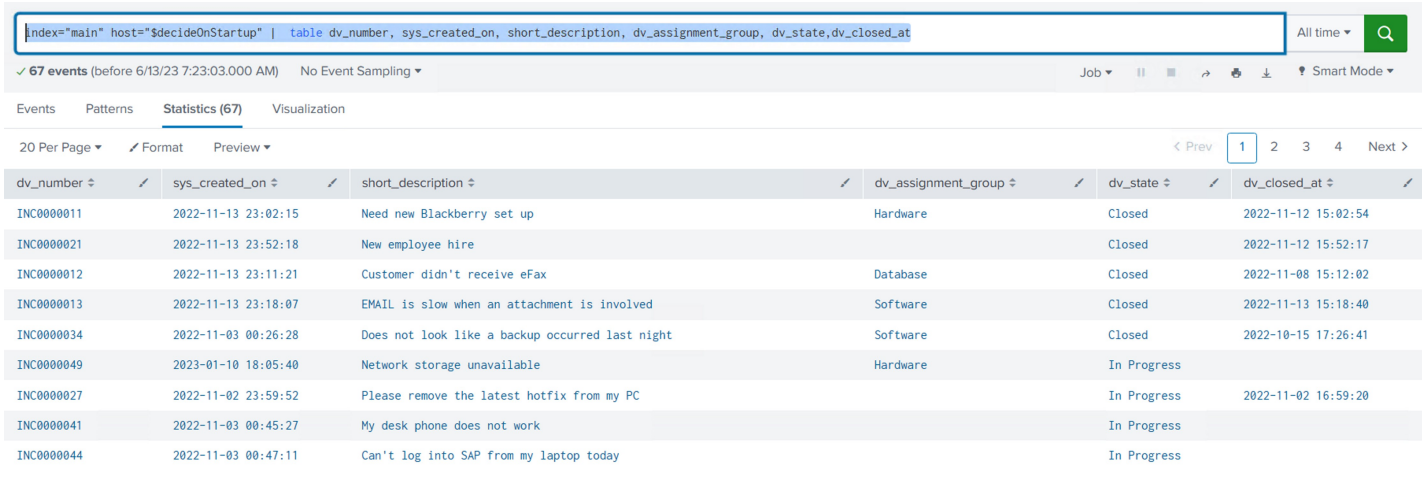


index="main" host="$decideOnStartup"

NOTE : ***$decideOnStartup*** will be shared by Service-now.



index="main" host="$decideOnStartup" | table dv_number, sys_created_on, short_description, dv_assignment_group, dv_state,dv_closed_at



dv_number	sys_created_on	short_description	dv_assignment_group	dv_state	dv_closed_at
INC0000011	2022-11-13 23:02:15	Need new Blackberry set up	Hardware	Closed	2022-11-12 15:02:54
INC0000021	2022-11-13 23:52:18	New employee hire		Closed	2022-11-12 15:52:17
INC0000012	2022-11-13 23:11:21	Customer didn't receive eFax	Database	Closed	2022-11-08 15:12:02
INC0000013	2022-11-13 23:18:07	EMAIL is slow when an attachment is involved	Software	Closed	2022-11-13 15:18:40
INC0000034	2022-11-03 00:26:28	Does not look like a backup occurred last night	Software	Closed	2022-10-15 17:26:41
INC0000049	2023-01-10 18:05:40	Network storage unavailable	Hardware	In Progress	
INC0000027	2022-11-02 23:59:52	Please remove the latest hotfix from my PC		In Progress	2022-11-02 16:59:20
INC0000041	2022-11-03 00:45:27	My desk phone does not work		In Progress	
INC0000044	2022-11-03 00:47:11	Can't log into SAP from my laptop today		In Progress	

#Forwarder Management

For **UF** => **Deployment Server** is management instance.

For **Indexer** => **Cluster Master** is management instance.

For **Search-Head** => **Deployer** is management instance.

So Once cluster environment is set up, then we do not touch each component directly but through management instance.

Note :

(1) Cluster-Master and Deployment Server should not run on same server.

(2) Job of Search-Head (captain) to create replica of KBs

(3) Since data is not getting sync among Search-Heads, hence a "**Deployer**" is needed to sync

(4) There is no need of multiple Deployment Server, but there is a max limit of UF which one DS can

handle. We can create **"ServerClass"** to manage multiple UF from one DS.