

# Training – Day #7

15 June 2023 05:04

## #HEC (Http Event Collector)

**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](#).

Type	Inputs	Actions
Files & Directories Index a local file or monitor an entire directory.	15	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new

Showing 1-10 of 16 modular inputs

< Prev 1 2 Next >

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

**Edit Global Settings**

All Tokens	<input checked="" type="checkbox"/> Enabled	Disabled
Default Source Type	Select Source Type ▾	
Default Index	Default ▾	
Use Deployment Server	<input type="checkbox"/>	
Enable SSL	<input checked="" type="checkbox"/>	
HTTP Port Number ?	8088	

Cancel Save

Global Settings

**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.

Configure a new token for receiving data over HTTP. [Learn More](#)

Name	my_hec_tok
Source name override ?	optional
Description ?	optional

Enable indexer  acknowledgement

Add Data            < 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.

**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 >**      Selected item(s) 

Select Allowed Indexes	Available item(s)	Selected item(s)
<input type="checkbox"/> history	<input checked="" type="checkbox"/> main	
<input type="checkbox"/> main		
<input type="checkbox"/> summary		

Select indexes that clients will be able to select from.

**Default Index:**  main  Create a new index

Add Data            < 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            < Back      **Next >**

 **Token has been created successfully.**

Configure your inputs by going to [Settings > Data Inputs](#)

Token Value

**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

Edit Token: my\_hec\_tok

Description: optional

Source: optional

Set Source Type: Entered sourcetype ▾

Source Type: Select Source Type ▾

Select Allowed Indexes (optional): Available indexes add all ▾ Selected indexes remove all

- history
- main
- summary

Select indexes that clients will be able to select from.

Default Index: main ▾

Enable indexer acknowledgement

Cancel Save

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-bfe8-0a8b98204afb" -d "{\"sourcetype\" : \"trail\", \"event\":\"hello world\"}" {"text": "Success", "code": 0}
C:\Users\Ankit>
```

index="main" source="http:my\_hec\_tok"

New Search

index="main" source="http:my\_hec\_tok"

✓ 1 event (6/12/23 5:00:00.000 AM to 6/13/23 5:42:43.000 AM) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

List ▾ Format 20 Per Page ▾

Time	Event
6/13/23 5:41:44.000 AM	host = 44.202.91.207:8088   source = http:my_hec_tok   sourcetype = trail

< Hide Fields : All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

### #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 ee8e6fbcb422-4bb6-bfe8-0a8b98204afb" -d "{\"sourcetype\" : \"trail\", \"event\":\"hello world\"}{\"sourcetype\" : \"trail\", \"event\":\"hello multi-verse\"}"
```

The screenshot shows the Splunk 'New Search' interface. In the search bar, the query is `index="main" source="http:my_hec_tok"`. The results section shows **2 events** from 6/13/23 5:56:35.000 AM to 6/13/23 6:11:35.000 AM. The results table lists two events:

	i	Time	Event
>	6/13/23 6:11:20.000 AM	hello multi-verse	host = 44.202.91.207:8088   source = http:my_hec_tok   sourcetype = trail
>	6/13/23 6:11:20.000 AM	hello world	host = 44.202.91.207:8088   source = http:my_hec_tok   sourcetype = trail

On the right side, there is a terminal window showing the command used to push the data:

```
C:\Windows\system32\cmd.exe
C:\Users\Ankit>curl -k https://44.202.91.207:8088/services/collector -H "Authorization:Splunk ee8e6fbcb422-4bb6-bfe8-0a8b98204afb" -d "{\"sourcetype\" : \"trail\", \"event\":\"hello world\"}{\"sourcetype\" : \"trail\", \"event\":\"hello multi-verse\"}"
{"text": "Success", "code": 0}
C:\Users\Ankit>
```

## **#How to Push raw text**

ee8e6fbcb422-4bb

## **#Indexer Acknowledgement**

The screenshot shows the 'Add Data' configuration page for an indexer acknowledgement token. The steps are: Select Source, Input Settings, Review, Done. The 'Input Settings' step is active.

**HTTP Event Collector** (selected): 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.

**Configure a new token for receiving data over HTTP**:

- Name: `my_ack_tk`
- Source name override?: optional
- Description?: optional
- Enable indexer acknowledgement** (checkbox checked)

```
curl -k https://44.202.91.207:8088/services/collector -H "Authorization:Splunk 26ccd1d7-382f-4fc7-a64e-f97da739b53" -d "{\"sourcetype\" : \"trail\", \"event\":\"hello world\"}{\"sourcetype\" : \"trail\", \"event\":\"hello multi-verse\"}"
```

```
C:\Users\Ankit>curl -k https://44.202.91.207:8088/services/collector -H "Authorization:Splunk 26ccd1d7-382f-4fc7-a64e-f97da739b53" -d "{\"sourcetype\" : \"trail\", \"event\":\"hello world\"}{\"sourcetype\" : \"trail\", \"event\":\"hello multi-verse\"}"
{"text":"Data channel is missing", "code":10}
C:\Users\Ankit>
```

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

Go to website "[Free Online GUID Generator](https://guidgenerator.com/online-guid-generator.aspx)" => 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-f97da739b53" -d "{\"sourcetype\" : \"trail\", \"event\":\"my ack 1\"}"
```

**source="http:my\_ack Tok" (index="main")**

New Search

source="http:my\_ack Tok" (index="main")

2 events (before 6/13/23 6:26:48.000 AM) No Event Sampling

Events (2) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection × Deselect

List Format 20 Per Page

Time Event

	i	Time	Event
< Hide Fields	≡ All Fields	> 6/13/23 6:26:43.000 AM	my_ack_2 host = 44.202.91.207:8088
SELECTED FIELDS		> 6/13/23 6:26:36.000 AM	my_ack host = 44.202.91.207:8088
a host 1			
a source 1			
a sourcetype 1			
INTERESTING FIELDS			

```
C:\Windows\system32\cmd.exe
C:\Users\Ankit>curl -k https://44.202.91.207:8088/services/collector -H "Authorization:Splunk 26cccd1d7-f97da739b53" -d "{\"sourcetype\" : \"trail\", \"event\":\"hello world\"}{\"sourcetype\" : \"trail\", \"event\":\"multi-verse\"}"
{"text":"Data channel is missing","code":10}
C:\Users\Ankit>curl -k https://44.202.91.207:8088/services/collector?channel=68c44634-9167-49e2-8db5-8d6f9c44634-9167-49e2-8db5-8d6f97da739b53 -H "Authorization:Splunk 26cccd1d7-382f-4fc7-a64e-ff97da739b53" -d "{\"sourcetype\" : \"trail\", \"event\":\"multi-verse\"}"
{"text":"Success","code":0,"ackId":0}
C:\Users\Ankit>curl -k https://44.202.91.207:8088/services/collector?channel=68c44634-9167-49e2-8db5-8d6f9c44634-9167-49e2-8db5-8d6f97da739b53 -d "{\"sourcetype\" : \"trail\", \"event\":\"multi-verse\"}"
{"text":"Success","code":0,"ackId":1}
C:\Users\Ankit>
```

**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 26cccd1d7-382f-4fc7-a64e-ff97da739b53" -d "{\"acks\" :[0]}"
```

```
C:\Users\Ankit>curl -k https://44.202.91.207:8088/services/collector/ack?channel=68c44634-9167-49e2-8db5-8d6782f904dd -H "Authorization:Splunk 26cccd1d7-382f-4fc7-a64e-ff97da739b53" -d "{\"acks\" :[0]}"
{"acks":{"0":true}}
C:\Users\Ankit>curl -k https://44.202.91.207:8088/services/collector/ack?channel=68c44634-9167-49e2-8db5-8d6782f904dd -H "Authorization:Splunk 26cccd1d7-382f-4fc7-a64e-ff97da739b53" -d "{\"acks\" :[12]}"
{"acks":{"12":false}}
C:\Users\Ankit>
```

#### #JSON Extraction

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

```
curl -k https://44.202.91.207:8088/services/collector -H "Authorization:Splunk ee8e6fb-b422-4bb6-bfe8-0a8b98204afb" -d "{\"sourcetype\" : \"_json\", \"event\":{\"a\":\"value1\",\"b\":[\"value_1\", \"value_2\"]}}"
```

```
C:\Users\Ankit>curl -k https://44.202.91.207:8088/services/collector -H "Authorization:Splunk ee8e6fb-b422-4bb6-bfe8-0a8b98204afb" -d "{\"sourcetype\" : \"_json\", \"event\":{\"a\":\"value1\",\"b\":[\"value_1\", \"value_2\"]}}"
{"text":"Success", "code":0}
C:\Users\Ankit>
```

source="http:my\_hec Tok" (index="main")

source="http://my\_hec Tok" | index="main"

4 events (before 6/13/23 6:44:47.000 AM) No Event Sampling

Events (4) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection X Deselect

List Format 20 Per Page

SELECTED FIELDS  
a host 1  
a source 1  
a sourcetype 2

INTERESTING FIELDS  
a a 1  
a b[] 2  
a index 1

i Time Event

> 6/13/23 6:44:43.000 AM { [-]  
  a: value1  
  b: [ [ ]  
    value\_1  
    value\_2  
  ]  
}  
Show as raw text  
host = 44.202.91.207:8088 | source = http://my\_hec Tok | sourcetype = \_json

## #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

splunk>enterprise Apps ▾

Browse More Apps

Servicenow

Best Match Newest Popular

14 Apps

Splunk Add-on for ServiceNow

The Splunk Add-on for ServiceNow allows a Splunk software administrator to collect data from ServiceNow and create incidents and events in ServiceNow.

The add-on collects incident, event, change, user, user group, location, and CMDB CI information from ServiceNow via ServiceNow REST APIs. The add-on also provides workflow actions that allow users ... [More](#)

Category: IT Operations, Business Analytics | Author: Splunk Inc. | Downloads: 42511 | Released: 2 months ago | Last Updated: 2 months ago | View on Splunkbase

CATEGORY  
IT Operations  
Security, Fraud & Compliance  
Business Analytics  
Utilities  
IoT & Industrial Data  
DevOps  
Directory Service  
Email  
Endpoint  
Firewall  
General

## Add ServiceNow Account

Account Name  Enter a unique name for this account.

URL  Enter the URL, for example, https://myaccount.servicenow.com.

Auth Type

Username  Enter the username for this account.

Password  Enter the password for this account.

Record Count  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.

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	<input type="text"/>			
Account Name <input type="text" value="my_snow"/>	Authentication Type <input type="button" value="Basic Authentication"/>		<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Archive"/>	Actions <input type="button" value="More"/>	
vk_snow	Basic Authentication		<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Archive"/>		

splunk>enterprise Apps ▾ user11 Messages Settings Activity Help Find

Inputs Configuration Search

## Inputs

Enable ServiceNow database table inputs

23 Inputs		10 Per Page ▾	filter	Time field of the table	Date started from	Status	Actions
>	Input name <input type="text" value="change_request"/>	Account <input type="button" value="?"/>	Collection interval <input type="text" value="60"/>	Table to collect data from <input type="text" value="change_request"/>	Time field of the table <input type="text" value="sys_updated_on"/>	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Archive"/>
>	change_task	<input type="button" value="?"/>	60	change_task	sys_updated_on	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Archive"/>
>	cmdb	<input type="button" value="?"/>	60	cmdb	sys_updated_on	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Archive"/>
>	cmdb_ci	<input type="button" value="?"/>	60	cmdb_ci	sys_updated_on	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Archive"/>
>	cmdb_ci_app_server	<input type="button" value="?"/>	60	cmdb_ci_app_server	sys_updated_on	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Archive"/>
>	cmdb_ci_db_instance	<input type="button" value="?"/>	60	cmdb_ci_db_instance	sys_updated_on	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Archive"/>
>	cmdb_ci_infra_service	<input type="button" value="?"/>	60	cmdb_ci_infra_service	sys_updated_on	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Archive"/>
>	cmdb_ci_server	<input type="button" value="?"/>	60	cmdb_ci_server	sys_updated_on	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Archive"/>
>	cmdb_ci_service	<input type="button" value="?"/>	60	cmdb_ci_service	sys_updated_on	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Archive"/>
>	cmdb_ci_vm	<input type="button" value="?"/>	60	cmdb_ci_vm	sys_updated_on	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Archive"/>

## Update Inputs

X

Input name  Enter a unique name for the input.

Account  Changing this account may cause data gaps or duplication. To avoid, create a new input.

Collection interval  Collection interval for this input (in seconds).

Table to collect data from  Select a ServiceNow table from the list or enter a new custom table in the search box.

Use existing data input?  Yes  No A Checkpoint for this input already exists. Selecting 'No' will reset the data collection.

Time field of the table  Time field of the database table. Default is 'sys\_updated\_on'

## Update Inputs

X

Date started from  Start date should be in 'YYYY-MM-DD hh:mm:ss'(UTC) format. (Default is one week ago.).

Included properties  Enter comma-separated properties of the database table to include. 'Time field of the table' and 'ID Field' will be included by default.

Excluded properties  Enter comma-separated properties of the database table to exclude.

ID field  Field which uniquely identifies each row in this table (Default is 'sys\_id').

Filter parameters  Provide filters as per ServiceNow syntax. For example: key1!=value1^key2STARTSWITHvalue2^ORkey3==value3. For more details refer to TA docs.

Index

## Inputs

Create New Input

Enable ServiceNow database table inputs

1 Input		10 Per Page ▾		Incident		X	
i	Input name	Account	Collection interval	Table to collect data from	Time field of the table	Date started from	Status
>	incident	my_snow	60	incident	sys_updated_on	2023-06-06 07:17:16	<input checked="" type="checkbox"/> Enabled

**index="main" host="\$decideOnStartup"**

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

New Search

index="main" host="\$decideOnStartup"

67 events (before 6/13/23 7:18:24.000 AM) No Event Sampling

Events (67) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 month per column

List ▾ Format 20 Per Page ▾

Time	Event
6/4/23 2:15:43.000 PM	endpoint="https://dev70394.service-now.com/",parent="",dv_parent="",made_sla="true",dv_made_sla="true",caused_by="",dv_caused_by="",watch_list="",dv_watch_list="",upon_reject="cancel",dv_upon_reject="Cancel all future Tasks",sys_updated_on="2023-06-04 14:15:43",dv_sys_updated_on="2023-06-04 07:15:43",dv_child_incidents="0",dv_child_incidents="0",hold_reason="",dv_hold_reason="",origin_table="",dv_origin_table="",task_effective_number="INC0000601",dv_task_effective_number="INC0000601",approval_history="",dv_approval_history="",number="INC0000601",dv_number="INC0000601",resolved_by="62d7867c0a8010e0b03d84178ad913",dv_resolved_by="Roe Kettering",sys_updated_by="system",dv_sys_updated_by="system",opened_by="6816f79cc0a8016401c5a33be94e441",dv_opened_by="System Administrator",user_input="",dv_user_input="",sys_created_on="2023-01-27 09:43:10",dv_sys_created_on="2023-01-27 01:43:10",sys_domain="global",dv_sys_domain="global",state="7",dv_state="Closed",route_reason="",dv_route_reason="",sys_created_by="admin",dv_sys_created_by="admin",knowledge=false,dv_knowledge=false,order="",dv_order="",calendar_stc="264417",dv_calendar_stc="264,417",closed_at="2023-06-04 14:15:43",dv_closed_at="2023-06-04 07:15:43",cmdb_ci="affdc8437201000deabfc8bcbe5dc3",dv_cmdb_ci="BETH-IBM",delivery_plan="",dv_delivery_plan="",contract="",dv_contract="",impact="3",dv_impact="3 - Low",active=false,dv_active=false,work_notes_list="",dv_work_notes_list="",business_service="",dv_business_s

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

index="main" host="\$decideOnStartup" | table dv\_number, sys\_created\_on, short\_description, dv\_assignment\_group, dv\_state, dv\_closed\_at

67 events (before 6/13/23 7:23:03.000 AM) No Event Sampling

Events Patterns Statistics (67) Visualization

20 Per Page ▾ Format Preview ▾

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.



