

# Training – Day #8

15 June 2023 06:14

## #Event Breaking

Define at what point the one event can break into multiple.

Source type = type of data

If some events patterns are not clear and if we want to split the event from a particular position, then we use "Event-Line Breaking"

Use "**"BREAK\_ONLY\_BEFORE"**" while setting sourcetype.

Props.conf

## #Event splitting on JSON File:

Settings => Add Data => Upload =>

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: data\_json.txt

Source type: Select Source Type ▾ Save As

List Format 20 Per Page ▾

	Time	Event
1	6/14/23 4:47:36.000 AM	{ "id": "0001", "type": "donut", "name": "Cake", "ppu": 0.55, "batters": [ { "id": "1001", "type": "Regular" }, { "id": "1003", "type": "Blueberry" }, { "id": "1004", "type": "Devil's Food" } ], "topping": [ { "e": "None" }, { "id": "5002", "type": "Glazed" }, { "id": "5005", "type": "Sugar" }, { "id": "5007", "type": "Powdered" }, { "id": "5006", "type": "Chocolate with Sprinkles" }, { "id": "5003", "type": "Chocolate" }, { "id": "5004", "type": "Maple" } ], "id": "0002", "type": "donut", "name": "Raised", "ppu": 0.55, "batters": [ { "id": "1001", "type": "Regular" }, { "id": "5001", "type": "None" }, { "id": "5002", "type": "Glazed" }, { "id": "5005", "type": "Sugar" }, { "id": "5003", "type": "Maple" } ] } timestamp = none

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: data\_json.txt

Source type: Select Source Type ▾ Save As

List Format 20 Per Page ▾

> Event Breaks

> Timestamp

< Advanced

Name	Value
CHARSET	Select...
DATETIME_CONFIG	
SHOULD_LINEMERGE	true
LINE_BREAKER	(\r\n ^\n)
NO_BINARY_CHECK	true
BREAK_ONLY_BEFORE	1

New setting [Copy to clipboard](#)

1 6/14/23  
4:47:36.000 AM { [-]  
batters: { [+]  
}  
id: 0001  
name: Cake  
ppu: 0.55  
topping: [ [+]  
]  
type: donut  
}  
Show as raw text  
timestamp = none

2 6/14/23  
4:47:36.000 AM { [-]  
batters: { [+]  
}  
id: 0002  
name: Raised  
ppu: 0.55

Copy these line and paste in **props.conf**

Source: data\_json.txt

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Event Breaks

Timestamp

Advanced

Name Value

- CHARSET Select...
- DATETIME\_CONFIG
- SHOULD\_LINEMERGE true
- LINE\_BREAKER `(\r\n)*`
- NO\_BINARY\_CHECK true
- BREAK\_ONLY\_BEFORE `]]`

New setting

[Copy to clipboard](#)

Cancel

props.conf text:

```
[__auto_learned__]
SHOULD_LINEMERGE=true
LINE_BREAKER=(\r\n)*
NO_BINARY_CHECK=true
BREAK_ONLY_BEFORE=]]]
```

```
[__auto_learned__]
SHOULD_LINEMERGE=true
LINE_BREAKER=(\r\n)*
NO_BINARY_CHECK=true
BREAK_ONLY_BEFORE=]]]
```

#### #Event splitting on XML File

Before :

##### Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: data3.txt

Source type: Select Source Type ▾ Save As

Event Breaks

Timestamp

Advanced

Name Value

- CHARSET Select...
- DATETIME\_CONFIG
- SHOULD\_LINEMERGE true
- LINE\_BREAKER `(\r\n)*`
- NO\_BINARY\_CHECK true

View Event Summary

Time Event

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:13.766-07:00</time><@version>1</@version><@level>INFO</@level><@thread>backup4</@thread><@location>com.netapp.common.flow.tasks.Log</location><msgKeyClass>com.netapp.smvi.SMsgKey</msgKeyClass><msgKeyValue>PROGRESS_TASK_BACKUP_STARTING</msgKeyValue><parameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="true"><message><@timestamp>2013-04-22T11:55:14.156-07:00</time><@level>INFO</level><@thread>backup4</thread><@location>com.netapp.smvi.task.validation.BackupValidation</location><msgKeyClass>SMsgKey</msgKeyClass><msgKeyValue>BACKUP_VALIDATION_INTERNAL_BACKUP_NAME_FOR_SCHEDULE_JOB</msgKeyValue><parameters><parameter>66fc1387-594c-48cb-b15d-94ca319a43c</parameter><parameter>b35d-94ca319a43c</parameter><parameter>PM</parameter><parameter>cDOT_Datastore_20130422115514</parameter><parameters><message>Generating backupName for the scheduleJob</message><parameter>66fc1387-594c-48cb-b35d-94ca319a43c</parameter><parameter>is backup</parameter><parameters><message><@timestamp>2013-04-22T11:55:18.400-07:00</time><@version>1</@version><@level>INFO</@level><@thread>backup4</@thread><@location>com.netapp.smvi.task.vmware.VmGetVirtua...</location><msgKeyClass>com.netapp.smvi.SMsgKey</msgKeyClass><msgKeyValue>BACKUP_DATASTORE</msgKeyValue><parameters><parameter>Netapp_cDOT_DSI</parameter><parameter>Netapp_cDOT_DSI</parameter><parameters><message>Backing up datastore(s) ([Netapp_cDOT_DSI (netfs:/i172.17.47.235//Netapp_cDOT_DSI)])</message><messages><@timestamp>2013-04-22T11:55:18.509-07:00</time><@level>INFO</level><@thread>backup4</thread><@location>com.netapp.smvi.task.vmware.VmGetVirtualMachinesToBackup</location><msgKeyClass>com.netapp.smvi.SMsgKey</msgKeyClass><msgKeyValue>BACKUP_VIRTUAL_ENTITIES</msgKeyValue><parameters><parameter>[VMware vCenter Server Appliance, SN_RCI_Node1, iH-VSA, U8_server, win08, esxi_1, SN_RCI_Node2, vc_5.5_v1]</parameters>
```

After setting "MUST\_BREAK\_AFTER" and "LINE\_BREAKING"

```
LINE_BREAKER=(\r\n)*<messages>
MUST_BREAK_AFTER=\r\n<messages>
```

**Note :** here in LINE\_BREAKER, it is \* sign instead of +.

## Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: `data3.txt`

[View Event Summary](#)

Source type: Select Source Type [Save As](#)

List ▾ Format 20 Per Page ▾

Name	Value
CHARSET	Select...
DATETIME_CONFIG	
SHOULD_LINEMERGE	true
LINE_BREAKER	(\r\n)*<messages>
NO_BINARY_CHECK	true
MUST_BREAK_AFTER	\vmessages

New setting [Copy to clipboard](#) [Apply settings](#)

Time Event

1 6/12/23 <?xml version="1.0" encoding="UTF-8"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:13.766-07:00</@timestamp><@level>INFO</@level><@thread>backup4 ee5fa1cb0c31a3e56f4fed2c99ff7745</@thread><@location>com.netapp.common.flow.tasks.Log</@location><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>PROGRESS\_TASK\_BACKUP\_STARTING</msgKeyValue><parameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:nil="true"></parameters><message>Starting backup request</message></message>

2 6/12/23 <?xml version="1.0" encoding="UTF-8"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:14.156-07:00</@timestamp><@level>INFO</@level><@thread>backup4 aaaaaaaaaajksbcjkbud7yh83eh38</@thread><@location>com.netapp.common.flow.tasks.Log</@location><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>BACKUP\_VALIDATION\_INTERNAL\_BACKUP\_NAME\_FOR\_SCHEDULE\_JOB</msgKeyValue><parameters><parameter>6fcf1387-594c-48cb-b35d-94ca19a43c</parameter><parameter>backup\_PM cDOT\_Datstore\_20130422115514</parameter><parameters><message>Generating backupName for the scheduleJob 6fcf1387-594c-48cb-b35d-94ca319a43c is backup\_PM cDOT\_atastore\_20130422115514</message></messages>

3 6/12/23 <?xml version="1.0" encoding="UTF-8"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:18.400-07:00</@timestamp><@level>INFO</@level><@thread>backup4 aaaaaaaaaajksbcjkbud7yh83eh38</@thread><@location>com.netapp.smvi.task.validation.BackupValidation</@location><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>BACKUP\_VALIDATION\_INTERNAL\_BACKUP\_NAME\_FOR\_SCHEDULE\_JOB</msgKeyValue><parameters><parameter>6fcf1387-594c-48cb-b35d-94ca319a43c</parameter><parameters><message>BackupName for the scheduleJob 6fcf1387-594c-48cb-b35d-94ca319a43c is backup\_PM cDOT\_Datstore\_20130422115514</message></parameters><message>Backing up data store(s) (NetApp\_cDOT\_Datstore\_20130422115514)</message></messages>

4 6/12/23 <?xml version="1.0" encoding="UTF-8"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:18.509-07:00</@timestamp><@level>INFO</@level><@thread>backup4 aaaaaaaaaajksbcjkbud7yh83eh38</@thread><@location>com.netapp.smvi.task.validation.BackupValidation</@location><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>BACKUP\_VIRTUAL\_ENTITIES</msgKeyValue><parameters><parameter>VMware vCenter Server Appliance, SN\_RCI\_Node1, 7M-VSA, UB\_server, win08, esxi\_1, SN\_RCI\_Node2, vc\_5\_va</parameter><parameters><message>Backing up the following virtual machine(s) ([VMware vCenter Server Appliance, SN\_RCI\_Node1, 7M-VSA, UB\_server, win08, esxi\_1, SN\_RCI\_Node2, vc\_5\_va])</message></messages>

To remove <?xml version> as separate line, user setting "BREAK\_ONLY\_BEFORE"

## Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: `data3.txt`

[View Event Summary](#)

Source type: Select Source Type [Save As](#)

List ▾ Format 20 Per Page ▾

Name	Value
CHARSET	Select...
DATETIME_CONFIG	
SHOULD_LINEMERGE	true
LINE_BREAKER	(\r\n)*<messages>
NO_BINARY_CHECK	true
MUST_BREAK_AFTER	\vmessages
BREAK_ONLY_BEFORE	<messages>

New setting [Copy to clipboard](#) [Apply settings](#)

Time Event

1 6/12/23 <?xml version="1.0" encoding="UTF-8"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:13.766-07:00</@timestamp><@level>INFO</@level><@thread>backup4 ee5fa1cb0c31a3e56f4fed2c99ff7745</@thread><@location>com.netapp.common.flow.tasks.Log</@location><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>PROGRESS\_TASK\_BACKUP\_STARTING</msgKeyValue><parameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:nil="true"></parameters><message>Starting backup request</message></message>

2 6/12/23 <?xml version="1.0" encoding="UTF-8"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:14.156-07:00</@timestamp><@level>INFO</@level><@thread>backup4 aaaaaaaaaajksbcjkbud7yh83eh38</@thread><@location>com.netapp.smvi.task.validation.BackupValidation</@location><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>BACKUP\_VALIDATION\_INTERNAL\_BACKUP\_NAME\_FOR\_SCHEDULE\_JOB</msgKeyValue><parameters><parameter>6fcf1387-594c-48cb-b35d-94ca319a43c</parameter><parameters><message>Generating backupName for the scheduleJob 6fcf1387-594c-48cb-b35d-94ca319a43c is backup\_PM cDOT\_Datstore\_20130422115514</message></parameters><message>Backing up data store(s) (NetApp\_cDOT\_Datstore\_20130422115514)</message></messages>

3 6/12/23 <?xml version="1.0" encoding="UTF-8"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:18.400-07:00</@timestamp><@level>INFO</@level><@thread>backup4 aaaaaaaaaajksbcjkbud7yh83eh38</@thread><@location>com.netapp.smvi.task.validation.BackupValidation</@location><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>BACKUP\_VALIDATION\_INTERNAL\_BACKUP\_NAME\_FOR\_SCHEDULE\_JOB</msgKeyValue><parameters><parameter>6fcf1387-594c-48cb-b35d-94ca319a43c</parameter><parameters><message>BackupName for the scheduleJob 6fcf1387-594c-48cb-b35d-94ca319a43c is backup\_PM cDOT\_Datstore\_20130422115514</message></parameters><message>Backing up data store(s) (NetApp\_cDOT\_Datstore\_20130422115514)</message></messages>

4 6/12/23 <?xml version="1.0" encoding="UTF-8"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:18.509-07:00</@timestamp><@level>INFO</@level><@thread>backup4 aaaaaaaaaajksbcjkbud7yh83eh38</@thread><@location>com.netapp.smvi.task.validation.BackupValidation</@location><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>BACKUP\_VIRTUAL\_ENTITIES</msgKeyValue><parameters><parameter>VMware vCenter Server Appliance, SN\_RCI\_Node1, 7M-VSA, UB\_server, win08, esxi\_1, SN\_RCI\_Node2, vc\_5\_va</parameter><parameters><message>Backing up the following virtual machine(s) ([VMware vCenter Server Appliance, SN\_RCI\_Node1, 7M-VSA, UB\_server, win08, esxi\_1, SN\_RCI\_Node2, vc\_5\_va])</message></messages>

5 6/12/23 <?xml version="1.0" encoding="UTF-8"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:18.509-07:00</@timestamp><@level>INFO</@level><@thread>backup4 aaaaaaaaaajksbcjkbud7yh83eh38</@thread><@location>com.netapp.smvi.task.validation.BackupValidation</@location><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>BACKUP\_VIRTUAL\_ENTITIES</msgKeyValue><parameters><parameter>VMware vCenter Server Appliance, SN\_RCI\_Node1, 7M-VSA, UB\_server, win08, esxi\_1, SN\_RCI\_Node2, vc\_5\_va</parameter><parameters><message>Backing up the following virtual machine(s) ([VMware vCenter Server Appliance, SN\_RCI\_Node1, 7M-VSA, UB\_server, win08, esxi\_1, SN\_RCI\_Node2, vc\_5\_va])</message></messages>

[\_\_auto\_learned\_\_]

**SHOULD\_LINEMERGE=true**

**LINE\_BREAKER=(\r\n)\*<messages>**

**NO\_BINARY\_CHECK=true**

**MUST\_BREAK\_AFTER=\vmessages**

**BREAK\_ONLY\_BEFORE=<messages>**

## Difference between LINE\_BREAKER and MUST\_BREAK\_AFTER ?

**LINE\_BREAKER => will break the event's line in multiple lines but in same the event, It will not create new event.**

**MUST\_BREAK\_AFTER => will convert each break into new events.**

## Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: `data3.txt`

[View Event Summary](#)

Source type: Select Source Type [Save As](#)

List ▾ Format 20 Per Page ▾

Name	Value
CHARSET	Select...
DATETIME_CONFIG	
SHOULD_LINEMERGE	true
LINE_BREAKER	(\r\n)*<messages>
NO_BINARY_CHECK	true

New setting [Copy to clipboard](#) [Apply settings](#)

Time Event

1 6/12/23 <?xml version="1.0" encoding="UTF-8"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:13.766-07:00</@timestamp><@level>INFO</@level><@thread>backup4 ee5fa1cb0c31a3e56f4fed2c99ff7745</@thread><@location>com.netapp.common.flow.tasks.Log</@location><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>PROGRESS\_TASK\_BACKUP\_STARTING</msgKeyValue><parameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:nil="true"></parameters><message>Starting backup request</message></message>

<?xml version="1.0" encoding="UTF-8"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:14.156-07:00</@timestamp><@level>INFO</@level><@thread>backup4 aaaaaaaaaajksbcjkbud7yh83eh38</@thread><@location>com.netapp.smvi.task.validation.BackupValidation</@location><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>BACKUP\_VALIDATION\_INTERNAL\_BACKUP\_NAME\_FOR\_SCHEDULE\_JOB</msgKeyValue><parameters><parameter>6fcf1387-594c-48cb-b35d-94ca319a43c</parameter><parameters><message>Generating backupName for the scheduleJob 6fcf1387-594c-48cb-b35d-94ca319a43c is backup\_PM cDOT\_Datstore\_20130422115514</message></parameters><message>Backing up data store(s) (NetApp\_cDOT\_Datstore\_20130422115514)</message></messages>

<?xml version="1.0" encoding="UTF-8"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:18.400-07:00</@timestamp><@level>INFO</@level><@thread>backup4 aaaaaaaaaajksbcjkbud7yh83eh38</@thread><@location>com.netapp.smvi.task.validation.BackupValidation</@location><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>BACKUP\_VALIDATION\_INTERNAL\_BACKUP\_NAME\_FOR\_SCHEDULE\_JOB</msgKeyValue><parameters><parameter>6fcf1387-594c-48cb-b35d-94ca319a43c</parameter><parameters><message>BackupName for the scheduleJob 6fcf1387-594c-48cb-b35d-94ca319a43c is backup\_PM cDOT\_Datstore\_20130422115514</message></parameters><message>Backing up data store(s) (NetApp\_cDOT\_Datstore\_20130422115514)</message></messages>

<?xml version="1.0" encoding="UTF-8"?><logs schemaVersion="0"><message><@timestamp>2013-04-22T11:55:18.509-07:00</@timestamp><@level>INFO</@level><@thread>backup4 aaaaaaaaaajksbcjkbud7yh83eh38</@thread><@location>com.netapp.smvi.task.validation.BackupValidation</@location><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>BACKUP\_VIRTUAL\_ENTITIES</msgKeyValue><parameters><parameter>6fcf1387-594c-48cb-b35d-94ca319a43c</parameter><parameters><message>VMware vCenter Server Appliance, SN\_RCI\_Node1, 7M-VSA, UB\_server, win08, esxi\_1, SN\_RCI\_Node2, vc\_5\_va</parameter><parameters><message>Backing up the following virtual machine(s) ([VMware vCenter Server Appliance, SN\_RCI\_Node1, 7M-VSA, UB\_server, win08, esxi\_1, SN\_RCI\_Node2, vc\_5\_va])</message></messages>

## #Event splitting on Random File

Before:

### Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **data4.txt**

Source type: Select Source Type		Save As				
List <input checked="" type="checkbox"/> Format <input type="checkbox"/> 20 Per Page <input type="checkbox"/>						
<table border="1"> <thead> <tr> <th>Time</th> <th>Event</th> </tr> </thead> <tbody> <tr> <td>1 6/14/23 5:12:01:000 AM</td> <td> Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3119_20160826_T014444.xml.ent succeeded  Finished building request for JOB.....  Batch tasks have been completed.  To finish press any key.  Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3120_20160826_T014555.xml.ent succeeded  Finished building request for JOB.....  Finished putting files.....  Batch tasks have been completed.  To finish press any key.  Collapse  timestamp = none </td> </tr> </tbody> </table>			Time	Event	1 6/14/23 5:12:01:000 AM	Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3119_20160826_T014444.xml.ent succeeded Finished building request for JOB..... Batch tasks have been completed. To finish press any key. Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3120_20160826_T014555.xml.ent succeeded Finished building request for JOB..... Finished putting files..... Batch tasks have been completed. To finish press any key. Collapse timestamp = none
Time	Event					
1 6/14/23 5:12:01:000 AM	Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3119_20160826_T014444.xml.ent succeeded Finished building request for JOB..... Batch tasks have been completed. To finish press any key. Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3120_20160826_T014555.xml.ent succeeded Finished building request for JOB..... Finished putting files..... Batch tasks have been completed. To finish press any key. Collapse timestamp = none					
New setting <input type="button" value="Copy to clipboard"/> <input type="button" value="Apply settings"/>						

After using "MUST\_BREAK\_AFTER"

### Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **data4.txt**

Source type: Select Source Type		Save As						
List <input checked="" type="checkbox"/> Format <input type="checkbox"/> 20 Per Page <input type="checkbox"/>								
<table border="1"> <thead> <tr> <th>Time</th> <th>Event</th> </tr> </thead> <tbody> <tr> <td>1 6/14/23 5:12:01:000 AM</td> <td> Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3119_20160826_T014444.xml.ent succeeded  Finished building request for JOB.....  Batch tasks have been completed.  To finish press any key.  timestamp = none </td> </tr> <tr> <td>2 6/14/23 5:12:01:000 AM</td> <td> Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3120_20160826_T014555.xml.ent succeeded  Finished building request for JOB.....  Finished putting files.....  Batch tasks have been completed.  To finish press any key.  timestamp = none </td> </tr> </tbody> </table>			Time	Event	1 6/14/23 5:12:01:000 AM	Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3119_20160826_T014444.xml.ent succeeded Finished building request for JOB..... Batch tasks have been completed. To finish press any key. timestamp = none	2 6/14/23 5:12:01:000 AM	Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3120_20160826_T014555.xml.ent succeeded Finished building request for JOB..... Finished putting files..... Batch tasks have been completed. To finish press any key. timestamp = none
Time	Event							
1 6/14/23 5:12:01:000 AM	Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3119_20160826_T014444.xml.ent succeeded Finished building request for JOB..... Batch tasks have been completed. To finish press any key. timestamp = none							
2 6/14/23 5:12:01:000 AM	Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3120_20160826_T014555.xml.ent succeeded Finished building request for JOB..... Finished putting files..... Batch tasks have been completed. To finish press any key. timestamp = none							
New setting <input type="button" value="Copy to clipboard"/> <input type="button" value="Apply settings"/>								

Property "MUST\_NOT\_BREAK\_BEFORE"

### Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **data4.txt**

Source type: Select Source Type		Save As						
List <input checked="" type="checkbox"/> Format <input type="checkbox"/> 20 Per Page <input type="checkbox"/>								
<table border="1"> <thead> <tr> <th>Time</th> <th>Event</th> </tr> </thead> <tbody> <tr> <td>1 6/14/23 5:12:01:000 AM</td> <td> Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3119_20160826_T014444.xml.ent succeeded  Finished building request for JOB.....  Batch tasks have been completed.  To finish press any key.  timestamp = none </td> </tr> <tr> <td>2 6/14/23 5:12:01:000 AM</td> <td> Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3120_20160826_T014555.xml.ent succeeded  Finished building request for JOB.....  Finished putting files.....  Batch tasks have been completed.  To finish press any key.  timestamp = none </td> </tr> </tbody> </table>			Time	Event	1 6/14/23 5:12:01:000 AM	Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3119_20160826_T014444.xml.ent succeeded Finished building request for JOB..... Batch tasks have been completed. To finish press any key. timestamp = none	2 6/14/23 5:12:01:000 AM	Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3120_20160826_T014555.xml.ent succeeded Finished building request for JOB..... Finished putting files..... Batch tasks have been completed. To finish press any key. timestamp = none
Time	Event							
1 6/14/23 5:12:01:000 AM	Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3119_20160826_T014444.xml.ent succeeded Finished building request for JOB..... Batch tasks have been completed. To finish press any key. timestamp = none							
2 6/14/23 5:12:01:000 AM	Upload of C:\SAMPLE_DATA\Feeds\daily\JOB\request\aaaaaaaaa_P_3120_20160826_T014555.xml.ent succeeded Finished building request for JOB..... Finished putting files..... Batch tasks have been completed. To finish press any key. timestamp = none							
<input type="button" value="Kill session"/>								

[\_\_auto\_learned\_\_]

**SHOULD\_LINEMERGE=true**

**LINE\_BREAKER=[\r\n]+**

**NO\_BINARY\_CHECK=true**

**MUST\_BREAK\_AFTER=To finish press any key.**

**MUST\_NOT\_BREAK\_BEFORE=Batch tasks have been completed**

## #Timestamp Customization

Before :

### Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: data2 (1).txt

[View Event Summary](#)

Source type:	Select Source Type	Save As
List ▾ <input checked="" type="checkbox"/> Format 20 Per Page ▾		
Time	Event	
1 6/13/23, 10:31:07.330 PM	41785:11 INFO [machine] 150 GMT2020-12-08T22:31:07.330Z (18 ms) [uuid] 13683279 [firm] 9001 [sn] 866562 onRequestExpired: request id: 6353697407667535883 41785:11 INFO [machine] 150 GMT2021-12-07T22:31:07.330Z (18 ms) [uuid] 13683279 [firm] 9001 [sn] 866562 postApplicationDataEvent roomId BCAST-fs:582CDE21190C0000 data: {"retractEvent": {"retractType": "BY_TIMER"}} 41785:11 INFO [machine] 150 GMT2012-12-10T22:31:07.689Z (59 ms) [uuid] 13683279 [firm] 9001 [sn] 866562 BCAST-fs:582CDE21190C0000 processRetractEvent	

After using "BREAK\_ONLY\_BEFORE\_DATE" and "TIME\_PREFIX" and "TIME\_FORMAT" settings

### NOTE :

(1)There is certain limit that Splunk can handle older data. We can change this by using property "MAX\_DAYS\_AGO"

(2) 2016 = %Y

16 = %Y

### Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: data2 (1).txt

[View Event Summary](#)

Source type:	Select Source Type	Save As
List ▾ <input checked="" type="checkbox"/> Format 20 Per Page ▾		
Time	Event	
1 12/9/20, 10:31:07.330 PM	41785:11 INFO [machine] 150 GMT2020-12-08T22:31:07.330Z (18 ms) [uuid] 13683279 [firm] 9001 [sn] 866562 onRequestExpired: request id: 6353697407667535883	
2 12/7/21, 10:31:07.330 PM	41785:11 INFO [machine] 150 GMT2021-12-07T22:31:07.330Z (18 ms) [uuid] 13683279 [firm] 9001 [sn] 866562 postApplicationDataEvent roomId BCAST-fs:582CDE21190C0000 data: {"retractEvent": {"retractType": "BY_TIMER"}} 41785:11 INFO [machine] 150 GMT2012-12-10T22:31:07.689Z (59 ms) [uuid] 13683279 [firm] 9001 [sn] 866562 BCAST-fs:582CDE21190C0000 processRetractEvent	
3 12/10/21, 10:31:07.589 PM	41785:11 INFO [machine] 150 GMT2012-12-10T22:31:07.689Z (59 ms) [uuid] 13683279 [firm] 9001 [sn] 866562 BCAST-fs:582CDE21190C0000 processRetractEvent	

For 2102 event => warning will be "Accepted time is suspiciously far away from previous event time  
but still accepted as it is extracted by same pattern"

```
[__auto_learned__]
SHOULD_LINEMERGE=true
LINE_BREAKER=([\\r\\n]+)
NO_BINARY_CHECK=true
TIME_PREFIX=GMT
TIME_FORMAT=%Y-%m-%dT%H:%M:%S.%N%
MAX_DAYS_AGO=10000
MAX_TIMESTAMP_LOOKAHEAD=24
BREAK_ONLY_BEFORE_DATE=true
```

### NOTE :

(1) If setting "ADD\_EXTRA\_TIME\_FIELDS" is set to false -> then it will not add any extra timestamp field after processing.

## Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: data2 (1).txt

Event Breaks

Timestamp

Advanced

Name	Value
CHARSET	Select...
DATETIME_CONFIG	
SHOULD_LINEMERGE	true
LINE_BREAKER	(\r\n +)
NO_BINARY_CHECK	true
TIME_PREFIX	GMT
TIME_FORMAT	%Y-%m-%dT%H:%M:%S.%3N
ADD_EXTRA_TIME_FIELDS	false
MAX_DAYS_HENCE	15
MAX_TIMESTAMP_LOOKAHEAD	24

New setting

View Event Summary

List Format 20 Per Page

Time	Event
12/8/20 10:31:07:000 PM	41785:11 INFO [machine] 150 GHT2020-12-08T22:31:07.330Z (18 ms) [uuid] 13683279 [firm] 9001 [sn] 866562 onRequestExpired: request id: 6353697407667535883
12/7/21 10:31:07:000 PM	41785:11 INFO [machine] 150 GHT2021-12-07T22:31:07.330Z (18 ms) [uuid] 13683279 [firm] 9001 [sn] 866562 postApplicationDataEvent roomid BCAST-fs:582CDE21190C0000 data: {"retract":true,"retractType":"BY_TIMER"} 41785:11 INFO [machine] 150 GHT2021-12-07T22:31:07.689Z (59 ms) [uuid] 13683279 [firm] 9001 [sn] 866562 BCAST-fs:582CDE21190C0000 processRetractEvent
12/7/21 10:31:07:000 PM	41785:11 INFO [machine] 150 GHT2021-12-07T22:31:07.689Z (59 ms) [uuid] 13683279 [firm] 9001 [sn] 866562 BCAST-fs:582CDE21190C0000 processRetractEvent

```
[__auto_learned__]
SHOULD_LINEMERGE=true
LINE_BREAKER=(\r\n|+)
NO_BINARY_CHECK=true
TIME_PREFIX=GMT
TIME_FORMAT=%Y-%m-%dT%H:%M:%S.%3N%
ADD_EXTRA_TIME_FIELDS=false
MAX_DAYS_HENCE=15
MAX_TIMESTAMP_LOOKAHEAD=24
```

## #User and Roles

**(1) Capabilities =>** Features like :

- (i) feature to add data
- (ii) feature to create Alert/Report/Dashboard
- (iii) Create/Modify/Customize Index
- (iv) Resource consumption user-wise
- (v) to remove real-time search
- (vi) Access to License

**NOTE :**Users' activities get saved on disk. We can customize the max space used by an user.

**(2) Role =>** Combination of features/Access

(1) **4 default** roles => admin, can\_delete, power, user

Roles		
Name	Actions	Native capabilities
admin	Edit ▾	105
can_delete	Edit ▾	6
power	Edit ▾	10
splunk-system-role	Edit ▾	0
user	Edit ▾	29
vitrис_role2	Edit ▾	0

**(2) admin don't have "can\_delete" role by default.**



Question : How to delete data ?

Answer : Search the data and then "**I delete**"

**(3) Native Capabilities** => capabilities which we **add manually** to that particular role only

**Inherited Capabilities** => capabilities which we **get automatically by assigning an existing Role**.

**Capabilities => C1, C2,C3.....C10**

**Roles => R1, R2, R3**

**R1 = C1 + C2 + C3**

**R2 = R1 + C4 + C5**

= inherited capabilities will be C1,C2,C3 + Native Capabilities will be C4,C5

**R3 = R2 + C9 + C10**

= inherited capabilities will be C1,C2,C3,C4,C5 + Native Capabilities will be C9,C10

New Role

Name \*

1. Inheritance    2. Capabilities    3. Indexes    4. Restrictions    5. Resources 

Specify roles from which this role inherits capabilities and indexes. Inherited capabilities and indexes cannot be disabled. If multiple roles are specified, this role inherits capabilities and indexes from all selected roles.

Role name  Showing all ▾

admin  
 can\_delete  
 power  
 splunk-system-role  
 user  
 viatris\_role2

1. Inheritance    2. Capabilities    3. Indexes    4. Restrictions    5. Resources

Specify roles from which this role inherits capabilities and indexes. Inherited capabilities and indexes cannot be disabled. If multiple roles are specified, this role inherits capabilities and indexes from all selected roles.

1. Inheritance    2. Capabilities    3. Indexes    4. Restrictions    5. Resources

Select specific capabilities for this role.

Capability Name   
 accelerate\_datamodel

1. Inheritance    2. Capabilities    3. Indexes    4. Restrictions    5. Resources

**Wildcards**  
Instead of selecting individual indexes, you can create a Wildcard index to dynamically capture all indexes that match the Wildcard. After you add a Wildcard index, it appears in the Indexes table. Wildcard indexes are limited to this role.

Enter a value that contains \*\*\*

**Indexes**  
Enable both the "Included" and "Default" checkboxes for an index to make that index searchable by default for this role. You must save this role before you can see its inherited wildcards.

1. Inheritance    2. Capabilities    3. Indexes    4. Restrictions    5. Resources

**Restrict searches**  
Create a search filter to set search restrictions for this role. You can enter a valid search filter or use the search filter generator to add queries.

**⚠ Select at least one index in the Indexes tab to enable the search filter generator.**

**1 Search filter generator**  
Indexed field and values time range  
60 seconds  
Increasing the time range beyond the default of 60 seconds can increase the time it takes to populate the "Indexed Fields" and "Values" text boxes.

**Indexed fields**  
Select or type an indexed field...

**Values**  
Select one or more values  
You can type in custom values that do not appear in the list, including wildcards. Example: "syslog\_\*\*"

**Concatenation option**

**2 Search filter**  
Enter a valid search filter here, or use the search filter generator on the left to generate a search filter

## New Role

1. Inheritance    2. Capabilities    3. Indexes    4. Restrictions    5. Resources

### This role

Default app

Select...

#### 1 Role search job limit

Set a limit for how many search jobs that all users with this role can run at the same time. [?](#)

Standard search limit

0

Real-time search limit

0

#### 2 User search job limit

Set a limit for how many search jobs that a single user with this role can run at the same time. [?](#)

Standard search limit

3

Real-time search limit

6

#### 3 Role search time window limit

Select a maximum time window for searches for this role. Inherited roles can override this setting.

Unset

Select the earliest searchable event time for this role. Inherited roles can override this setting.

Unset

#### 4 Disk space limit

Set the maximum amount of disk space, in megabytes, that search jobs for a specific user with this role can use.

Standard search limit

100

MB

### (3) User => End User

Create User

Name	<input type="text"/>
Full name	<input type="text"/> optional
Email address	<input type="text"/> optional
Set password	<input type="password"/> New password
Confirm password	<input type="password"/> Confirm new password
Password must contain at least 8 characters	
Time zone	<input type="button" value="– Default System Timezone –"/>
Default app	<input type="button" value="launcher (Home)"/>
Assign roles	<input type="button" value="Available item(s)"/> add all <input type="button" value="Selected item(s)"/> remove all
<input type="checkbox"/> Create a role for this user	
<input checked="" type="checkbox"/> Require password change on first login	
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

If giving "admin" role, it will ask to acknowledge a message "**I acknowledge that users assigned to roles with the `fsb_manage` capability can send search results data outside the compliant environment.**"

Available item(s): admin, can\_delete, power, splunk-system-role, tact\_role

Selected item(s): admin, user

Note: Acknowledge that users assigned to roles with the full\_manage capability can send search results outside the environment.

**Note:**

- (1) Once LDAP is set we **cannot use** local account.
- (2) Roles mapping of Splunk with LDAP (using *authorization.conf*)

## #License Management

Settings => Licensing

Trial license group: Trial license group

This server is configured to use licenses from the Trial license group.

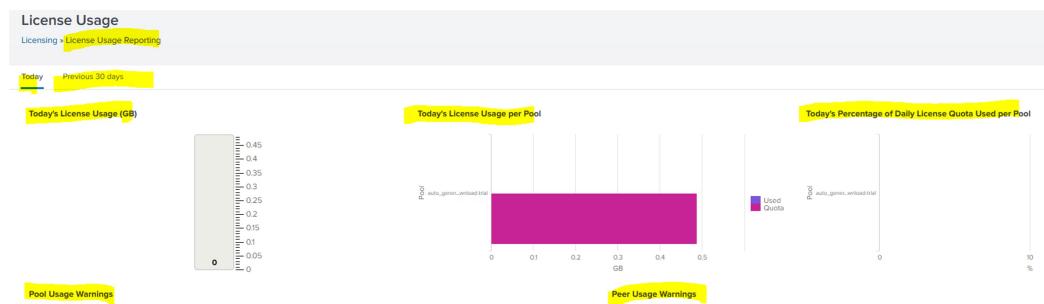
Add license Usage report

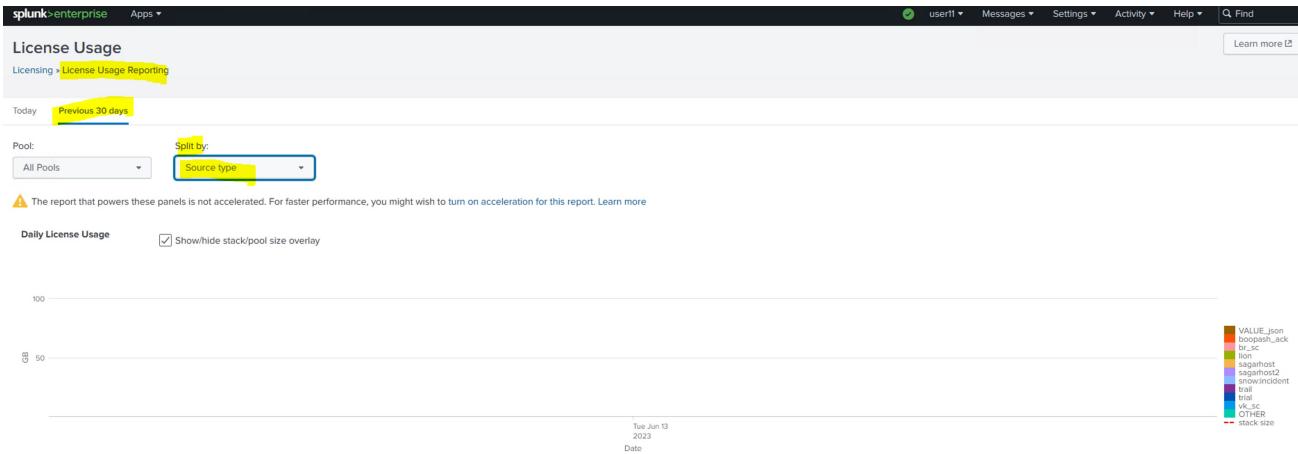
Alerts: No licensing alerts, No licensing violations

Local server information:

- Indexer name: ip-172-31-87-147.ec2.internal
- License expiration: Aug 11, 2023, 6:22:40 PM
- Licensed daily volume: 500 MB
- Volume used today: 0 MB (0% of quota)
- Warning count: 0
- Debug information: All license details, All indexer details

License file of splunk looks like an XML file.





### Change license group

Licensing > Change license group

**Change license group**

The type of license group determines what sorts of licenses can be used in the pools on this license server. [Learn more](#)

- 1  **Enterprise license**  
This license adds support for multi-user and distributed deployments, alerting, role-based security, single sign-on, scheduled PDF delivery, and unlimited data volumes.  
There are no valid Splunk Enterprise licenses installed. You will be prompted to install a license if you choose this option.
- 2  **Forwarder license**  
Use this group when configuring Splunk as a forwarder. [Learn more](#)
- 3  **Free license**  
Use this group when you are running Splunk Free. This license has no authentication or user and role management, and has a 500MB/day daily indexing volume. [Learn more](#)
- 4  **Enterprise Trial license**  
This is your included download trial. IMPORTANT: If you switch to another license, you cannot return to the Trial. You must install an Enterprise license or switch to Splunk Free.

[Cancel](#) [Save](#)

