# Training – Day #10

15 June 2023 09:15

## #Forwarder Management

**Deployment Server** = Forwarder's Management Instance

We do not touch components directly, we touch via Management Instances.

Splunk Enterprise is needed for Deployment Server. We have to enable it to act as Deployment Server.

Installed UF at 2 Server :

| | |
|---|---|
| 44.195.46.78 | 3.228.11.92 |

*wget -O splunkforwarder-9.0.5-e9494146ae5c-Linux-x86_64.tgz "https://download.splunk.com/products/universalforwarder/releases/9.0.5/linux/splunkforwarder-9.0.5-e9494146ae5c-Linux-x86_64.tgz"*

*tar -xvf splunkforwarder-9.0.5-e9494146ae5c-Linux-x86_64.tgz*

*cd splunkforwarder/bin/*

*/splunk start*

*./splunk status*

admin => admin@123

Installed Splunk Eneterprise at 1 Server => http://ip-172-31-8-243.ec2.internal:8000

| |
|---|
| 3.219.56.68 |

admin => admin@123

*wget -O splunk-9.0.5-e9494146ae5c-Linux-x86_64.tgz "https://download.splunk.com/products/splunk/releases/9.0.5/linux/splunk-9.0.5-e9494146ae5c-Linux-x86_64.tgz"*

*tar -xvzf splunk-9.0.5-e9494146ae5c-Linux-x86_64.tgz*

*cd splunk/bin/*

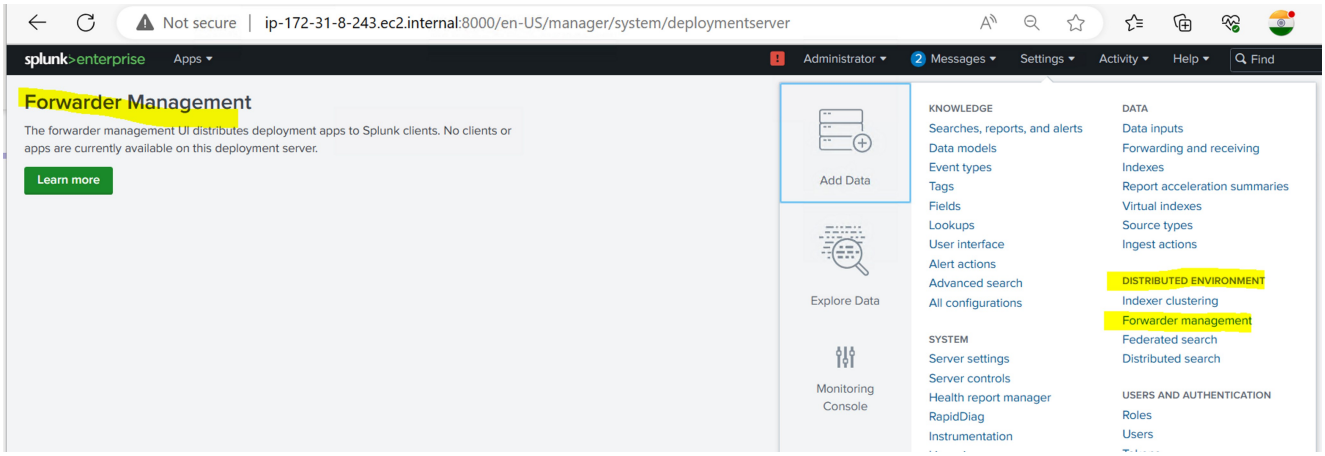
*./splunk start*

*./splunk status*

**#Enable Enterprise to add as Deployment Server :**

Note : We have to deploy one application it will automatically converted to an Deployment Server.

**Before** :



**After** creating dummy app on enterprise folder at location ***"/home/ec2-user/splunk/etc/deployment-apps"***

```
[ec2-user@ip-172-31-8-243 deployment-apps]$ pwd
/home/ec2-user/splunk/etc/deployment-apps
[ec2-user@ip-172-31-8-243 deployment-apps]$
[ec2-user@ip-172-31-8-243 deployment-apps]$ ls
README
[ec2-user@ip-172-31-8-243 deployment-apps]$
```

**Steps to create dummy app :**

***cd /home/ec2-user/splunk/etc/deployment-apps***

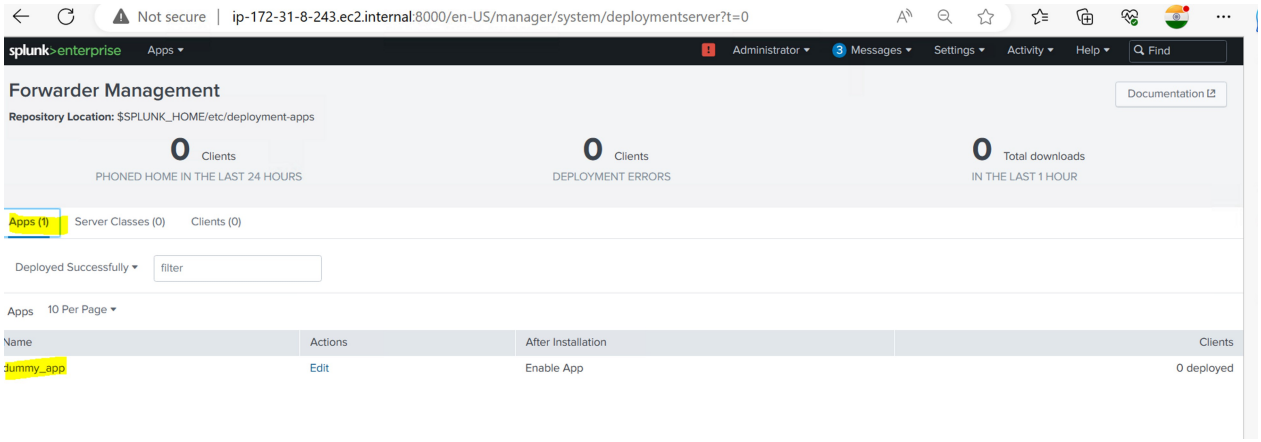
*mkdir dummy_app*

*cd dummy_app/*

*mkdir local*

*cd local/*

*vi test.txt*




**#How to Connect DS with UFs ?**

Run below command on UF, it will create **deploymentclient.conf** under "/etc/system/local/" folder :

[ec2-user@ip-172-31-1-24 bin]$ **./splunk set deploy-poll https://3.219.56.68:8089**

Warning: Attempting to revert the SPLUNK_HOME ownership

Warning: Executing "chown -R ec2-user /home/ec2-user/splunkforwarder"

WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

Splunk username: **admin**

Password:

Configuration updated.

[ec2-user@ip-172-31-1-24 bin]$

[ec2-user@ip-172-31-1-24 bin]$

[ec2-user@ip-172-31-1-24 bin]$ cd ../etc/system/local/

[ec2-user@ip-172-31-1-24 local]$ pwd

**/home/ec2-user/splunkforwarder/etc/system/local**

[ec2-user@ip-172-31-1-24 local]$ ls

README deploymentclient.conf server.conf

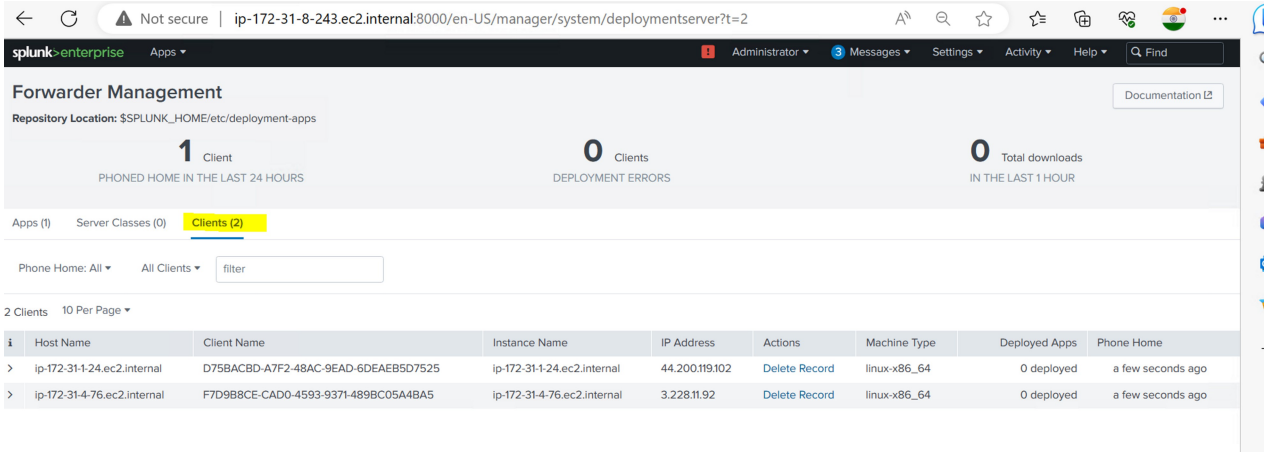
[ec2-user@ip-172-31-1-24 local]$ **more deploymentclient.conf**

**[target-broker:deploymentServer]**

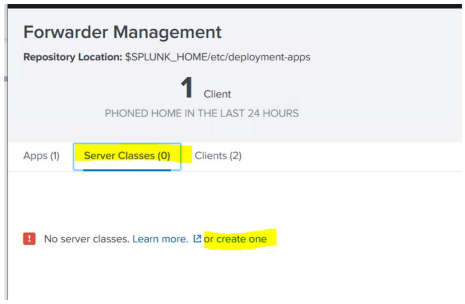
**targetUri = https://3.219.56.68:8089**

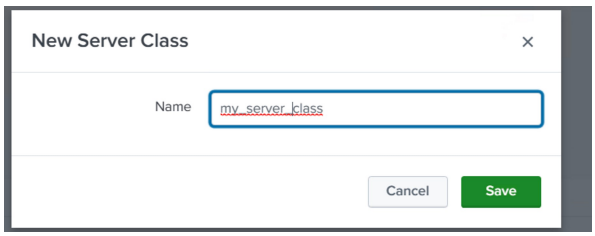
[ec2-user@ip-172-31-1-24 local]$

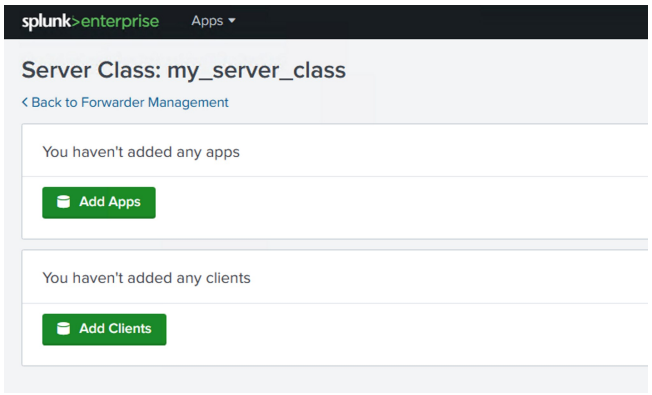
**Note** : If it is taking more time then restart the UFs.




**#How create a ServerClass to deploy delivery app on Forwarders**



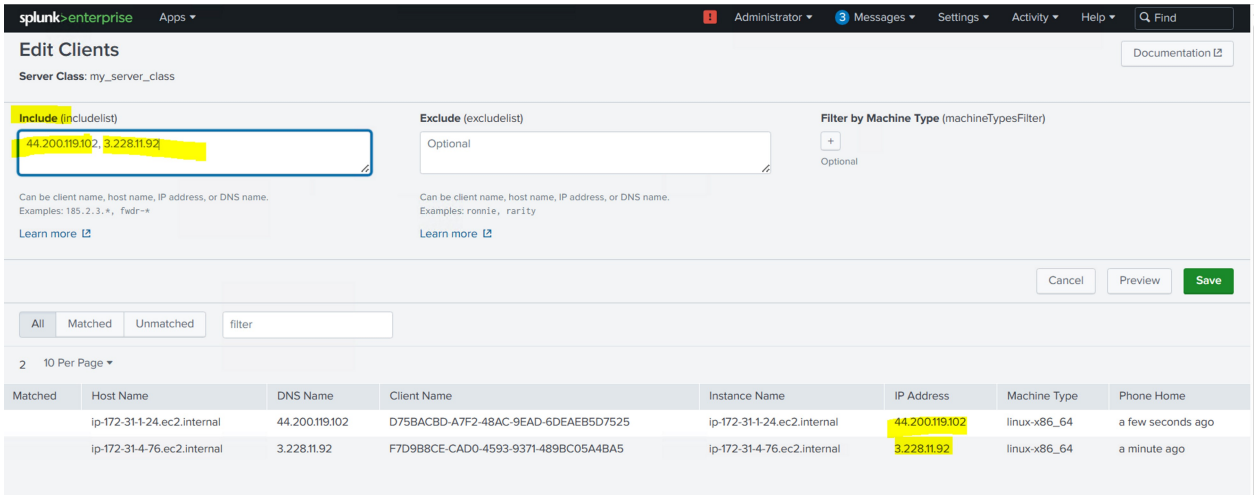



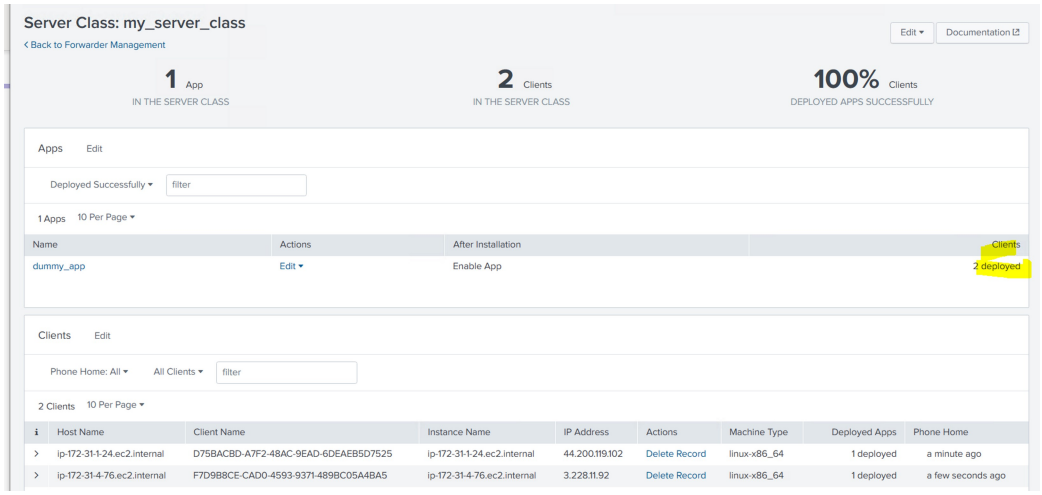



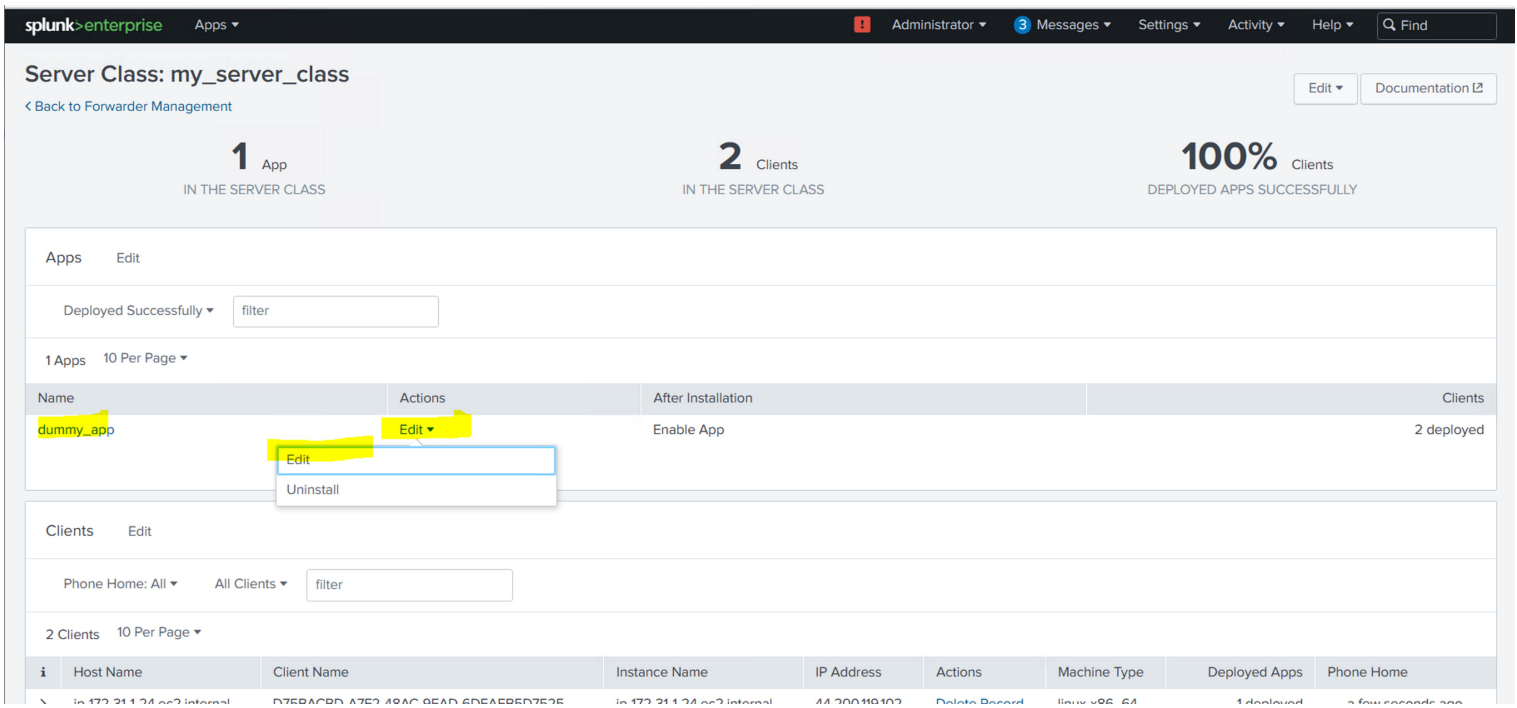

Note : If we have 10.0.0.1…10.0.0.100 and we do not want to push on 10.0.0.5 then we will add :

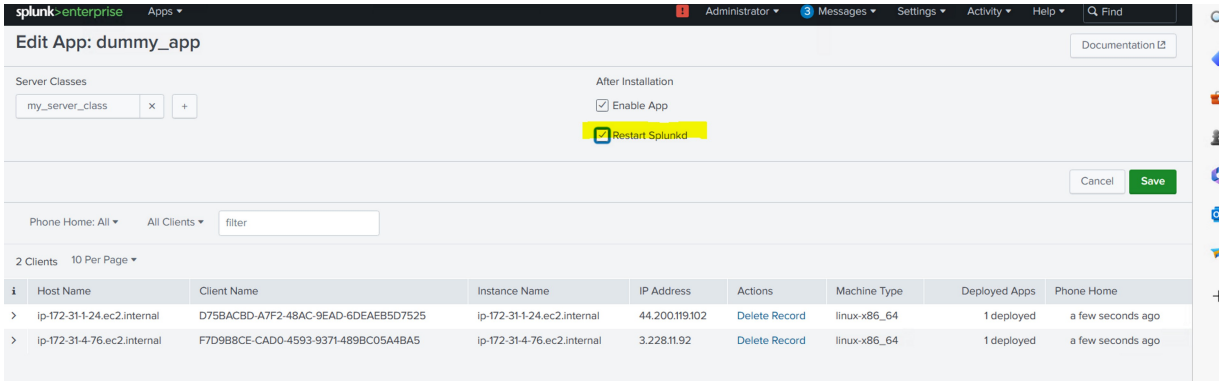
Under Include => 10.0.0.1…10.0.0.100

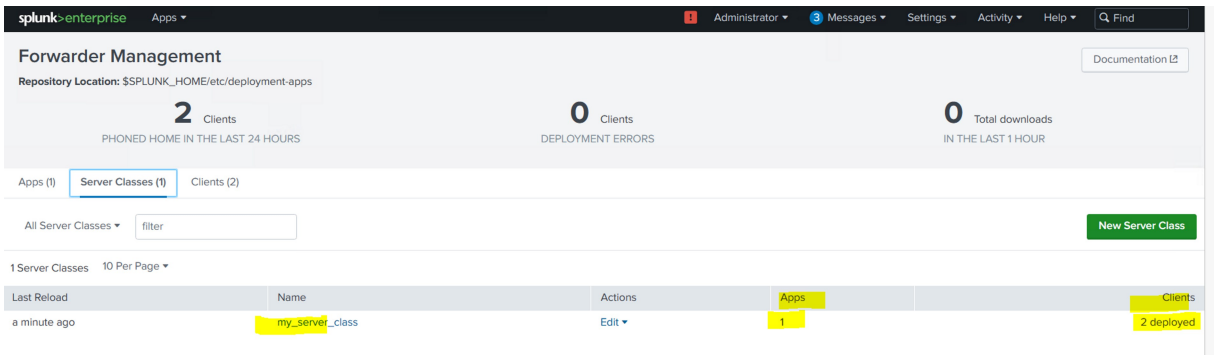
Under Exclude => 10.0.0.5


splunk>enterprise
Apps
Administrator
3 Messages
Settings
Activity
Help
Find
Edit Clients
Server Class: my_server_class
Documentation
Include (includelist)
44.200.119.102, 3.228.11.92
Can be client name, host name, IP address, or DNS name.
Examples: 185.2.3.*, fwdr-*
Learn more
Exclude (excludelist)
Optional
Can be client name, host name, IP address, or DNS name.
Examples: ronnie, rarity
Learn more
Filter by Machine Type (machineTypesFilter)
Optional
Cancel
Preview
Save
All
Matched
Unmatched
filter
2
10 Per Page
Matched
Host Name
DNS Name
Client Name
Instance Name
IP Address
Machine Type
Phone Home
ip-172-31-1-24.ec2.internal
44.200.119.102
D75BACBD-A7F2-48AC-9EAD-6DEAEB5D7525
ip-172-31-1-24.ec2.internal
44.200.119.102
linux-x86_64
a few seconds ago
ip-172-31-4-76.ec2.internal
3.228.11.92
F7D9B8CE-CAD0-4593-9371-489BC05A4BA5
ip-172-31-4-76.ec2.internal
3.228.11.92
linux-x86_64
a minute ago


Server Class: my_server_class
Back to Forwarder Management
Edit
Documentation
1 App
IN THE SERVER CLASS
2 Clients
IN THE SERVER CLASS
100% Clients
DEPLOYED APPS SUCCESSFULLY
Apps
Edit
Deployed Successfully
filter
1 Apps
10 Per Page
Name
Actions
After Installation
Clients
dummy_app
Edit
Enable App
2 deployed
Clients
Edit
Phone Home: All
All Clients
filter
2 Clients
10 Per Page
Host Name
Client Name
Instance Name
IP Address
Actions
Machine Type
Deployed Apps
Phone Home
ip-172-31-1-24.ec2.internal
D75BACBD-A7F2-48AC-9EAD-6DEAEB5D7525
ip-172-31-1-24.ec2.internal
44.200.119.102
Delete Record
linux-x86_64
1 deployed
a minute ago
ip-172-31-4-76.ec2.internal
F7D9B8CE-CAD0-4593-9371-489BC05A4BA5
ip-172-31-4-76.ec2.internal
3.228.11.92
Delete Record
linux-x86_64
1 deployed
a few seconds ago


splunk>enterprise
Apps
Administrator
3 Messages
Settings
Activity
Help
Find
Server Class: my_server_class
Back to Forwarder Management
Edit
Documentation
1 App
IN THE SERVER CLASS
2 Clients
IN THE SERVER CLASS
100% Clients
DEPLOYED APPS SUCCESSFULLY
Apps
Edit
Deployed Successfully
filter
1 Apps
10 Per Page
Name
Actions
After Installation
Clients
dummy_app
Edit
Enable App
2 deployed
Edit
Uninstall
Clients
Edit
Phone Home: All
All Clients
filter
2 Clients
10 Per Page
Host Name
Client Name
Instance Name
IP Address
Actions
Machine Type
Deployed Apps
Phone Home




Now Login to any UF :

*[ec2-user@ip-172-31-1-24 splunkforwarder]$ cd etc/apps/*

*[ec2-user@ip-172-31-1-24 apps]$ ls*

*SplunkUniversalForwarder dummy_app introspection_generator_addon journald_input learned search splunk_httpinput splunk_internal_metrics*

*[ec2-user@ip-172-31-1-24 apps]$ ls -l*

*total 0*

*drwxr-xr-x. 4 ec2-user ec2-user 37 May 26 23:29 SplunkUniversalForwarder*

*drwx------. 4 ec2-user ec2-user 35 Jun 16 05:14 dummy_app*

*drwxr-xr-x. 4 ec2-user ec2-user 32 May 26 23:29 introspection_generator_addon*

*drwxr-xr-x. 5 ec2-user ec2-user 46 May 26 23:29 journald_input*

*drwxr-xr-x. 5 ec2-user ec2-user 50 Jun 16 04:01 learned*

*drwxr-xr-x. 4 ec2-user ec2-user 37 May 26 23:29 search*

*drwxr-xr-x. 3 ec2-user ec2-user 21 May 26 23:29 splunk_httpinput*

*drwxr-xr-x. 3 ec2-user ec2-user 21 May 26 23:29 splunk_internal_metrics*

*[ec2-user@ip-172-31-1-24 apps]$ cd dummy_app/*

*[ec2-user@ip-172-31-1-24 dummy_app]$ ls*

*local metadata*

*[ec2-user@ip-172-31-1-24 dummy_app]$ cd local/*

*[ec2-user@ip-172-31-1-24 local]$ ls*

*app.conf test.txt*

*[ec2-user@ip-172-31-1-24 local]$ more test.txt*

*My first Dummy app.*

*[ec2-user@ip-172-31-1-24 local]$*

```
[ec2-user@ip-172-31-1-24 splunkforwarder]$ cd etc/apps/
[ec2-user@ip-172-31-1-24 apps]$ ls
SplunkUniversalForwarder  dummy_app  introspection_generator_addon  journald_input  learned  search  splunk_httpinput  splunk_internal_metrics
[ec2-user@ip-172-31-1-24 apps]$ ls -l
total 0
drwxr-xr-x. 4 ec2-user ec2-user 37 May 26 23:29 SplunkUniversalForwarder
drwx------. 4 ec2-user ec2-user 35 Jun 16 05:14 dummy_app
drwxr-xr-x. 4 ec2-user ec2-user 32 May 26 23:29 introspection_generator_addon
drwxr-xr-x. 5 ec2-user ec2-user 46 May 26 23:29 journald_input
drwxr-xr-x. 5 ec2-user ec2-user 50 Jun 16 04:01 learned
drwxr-xr-x. 4 ec2-user ec2-user 37 May 26 23:29 search
drwxr-xr-x. 3 ec2-user ec2-user 21 May 26 23:29 splunk_httpinput
drwxr-xr-x. 3 ec2-user ec2-user 21 May 26 23:29 splunk_internal_metrics
[ec2-user@ip-172-31-1-24 apps]$ cd dummy_app/
[ec2-user@ip-172-31-1-24 dummy_app]$ ls
local  metadata
[ec2-user@ip-172-31-1-24 dummy_app]$ cd local/
[ec2-user@ip-172-31-1-24 local]$ ls
app.conf  test.txt
[ec2-user@ip-172-31-1-24 local]$ more test.txt
My first Dummy app.
```

ServerClass has pushed the App on UF.

Now if some changes will be made on App, then automatically it will not be pushed on UFs.

To get override changes of UF, we have to reload the ServerClass.

**Step #1: Modifing the App on Enterprise Server**

[ec2-user@ip-172-31-8-243 local]$ vi test.txt

[ec2-user@ip-172-31-8-243 local]$ pwd

/home/ec2-user/splunk/etc/deployment-apps/dummy_app/local

[ec2-user@ip-172-31-8-243 local]$ more test.txt

My first Dummy app.

This is new Change.

[ec2-user@ip-172-31-8-243 local]$

**Step #2 : Reload App by command**

**To Load all server class => *./splunk reload deploy-server***

***To load specific serverclass => /splunk reload deploy-server -class my_server_class***

Best Practice to reload your own serverclass only

[ec2-user@ip-172-31-8-243 local]$ pwd

/home/ec2-user/splunk/etc/deployment-apps/dummy_app/local

[ec2-user@ip-172-31-8-243 local]$ cd /home/ec2-user/splunk/bin/

[ec2-user@ip-172-31-8-243 bin]$ ./splunk reload deploy-server -class my_server_class

WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

Splunk username: admin

Password:

Reloading serverclass(es).

[ec2-user@ip-172-31-8-243 bin]$

```
[ec2-user@ip-172-31-8-243 local]$ pwd
/home/ec2-user/splunk/etc/deployment-apps/dummy_app/local
[ec2-user@ip-172-31-8-243 local]$ cd /home/ec2-user/splunk/bin/
[ec2-user@ip-172-31-8-243 bin]$ ./splunk reload deploy-server -class my_server_class
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Splunk username: admin
Password:
Reloading serverclass(es).
[ec2-user@ip-172-31-8-243 bin]$
```

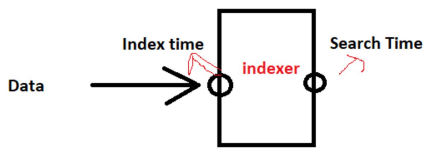
**Step #3 : check the changes on UF:**

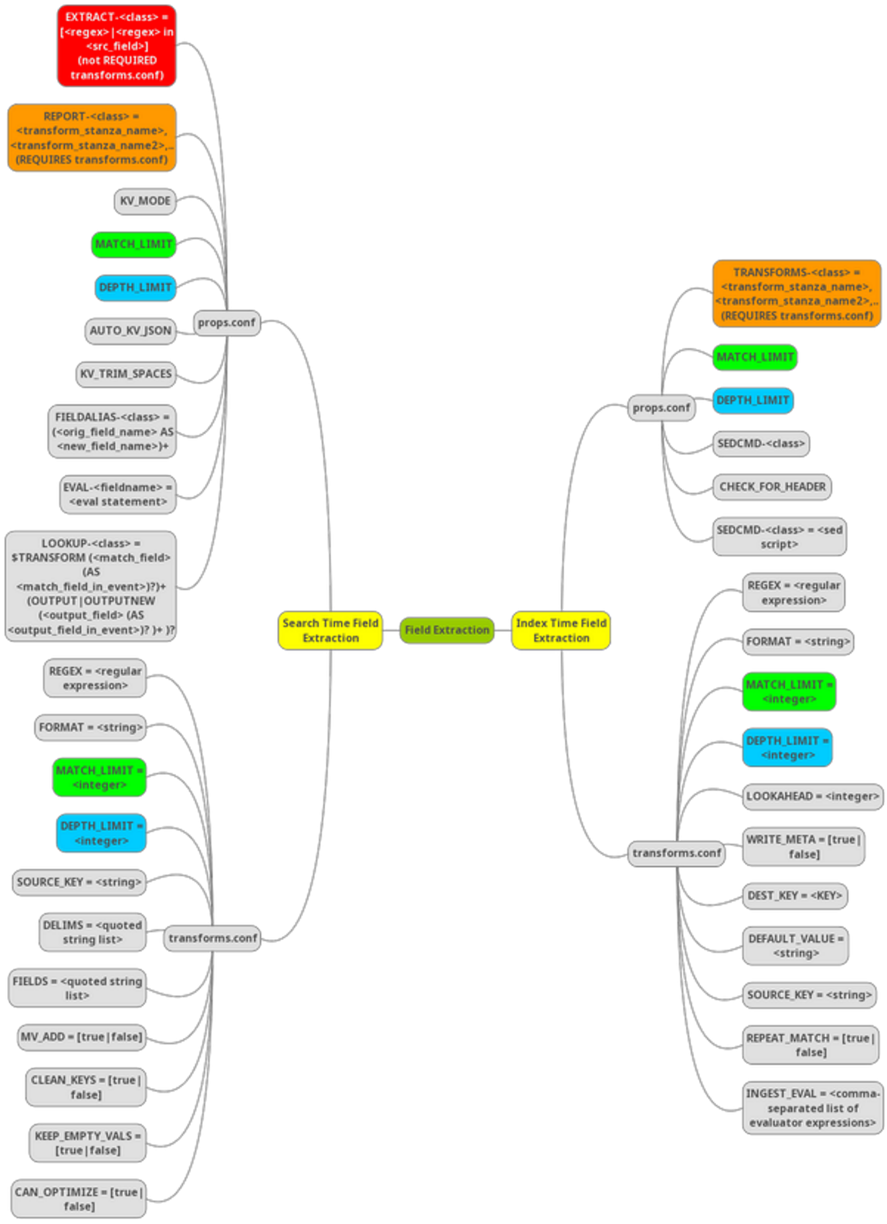
cd /home/ec2-user/splunkforwarder/etc/apps/dummy_app/local

```
[ec2-user@ip-172-31-1-24 local]$ cat test.txt
My first Dummy app.
This is new Change.
[ec2-user@ip-172-31-1-24 local]$
```

## #Index Time Field Extraction

Pull the event **at the time of ingestion** into index. Note : data yet to be indexed.



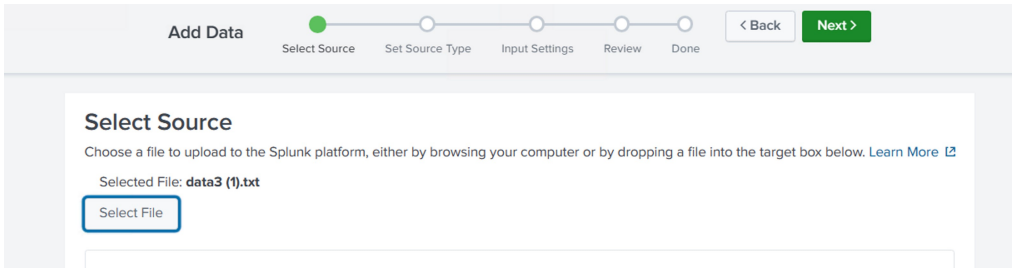



**Step #1 : Import Data**

data3 (1) - Notepad

File Edit Format View Help

<messages><timestamp>2013-04-22T11:55:13.766-07:00</timestamp><level>PROGRESS</level><thread>backup4
ee5fa1cb0c31a3e56f4fed2c99ff7745</thread><location>com.netapp.common.flow.tasks.Log</location><msgKeyClass>com.neta
pp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>PROGRESS_TASK_BACKUP_STARTING</msgKeyValue><parameters
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:nil="true"/><message>Starting backup request for card
1234-5678-9101-1213</message></messages><messages><timestamp>2013-04-22T11:55:14.156-
07:00</timestamp><level>INFO</level><thread>backup4
aaaaaaaaaajksbcjkbud7yh8y83eh38</thread><location>com.netapp.smvi.task.validation.BackupValidation</location><msgKe
yClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>BACKUP_VALIDATION_INTERNAL_BACKUP_NAME_FOR_SCHEDULE_JOB</
msgKeyValue><parameters><parameter>66fc1387-594c-48cb-b35d-94ca319a4a3c</parameter><parameter>backup_PM cDOT
Datastore_20130422115514</parameter></parameters><message>Generating backupName for the scheduleJob 66fc1387-594c-
48cb-b35d-94ca319a4a3c is backup_PM cDOT Datastore_20130422115514 card 1234-5678-9101-
1213</message></messages><messages><timestamp>2013-04-22T11:55:18.400-
07:00</timestamp><level>PROGRESS</level><thread>backup4
aaaaaaaaaajksbcjkbud7yh8y83eh38</thread><location>com.netapp.smvi.task.vmware.VmGetVirtualMachinesToBackup</locatio
n><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>BACKUP_DATASTORE</msgKeyValue><parameters><parame
ter>[NetApp_cDOT_DS1 (netfs://172.17.47.235///NetApp_cDOT_DS1)]</parameter></parameters><message>Backing up
datastore(s) ([NetApp_cDOT_DS1 (netfs://172.17.47.235///NetApp_cDOT_DS1)]) card 1234-5678-9101-
1213</message></messages><messages><timestamp>2013-04-22T11:55:18.509-
07:00</timestamp><level>PROGRESS</level><thread>backup4
aaaaaaaaaajksbcjkbud7yh8y83eh38</thread><location>com.netapp.smvi.task.vmware.VmGetVirtualMachinesToBackup</locatio
n><msgKeyClass>com.netapp.smvi.SMMsgKey</msgKeyClass><msgKeyValue>BACKUP_VIRTUAL_ENTITIES</msgKeyValue><parameters>
<parameter>[VMware vCenter Server Appliance, SN_RC1_Node1, ZM-VSA, UB_server, win08, esxi_1, SN_RC1_Node2



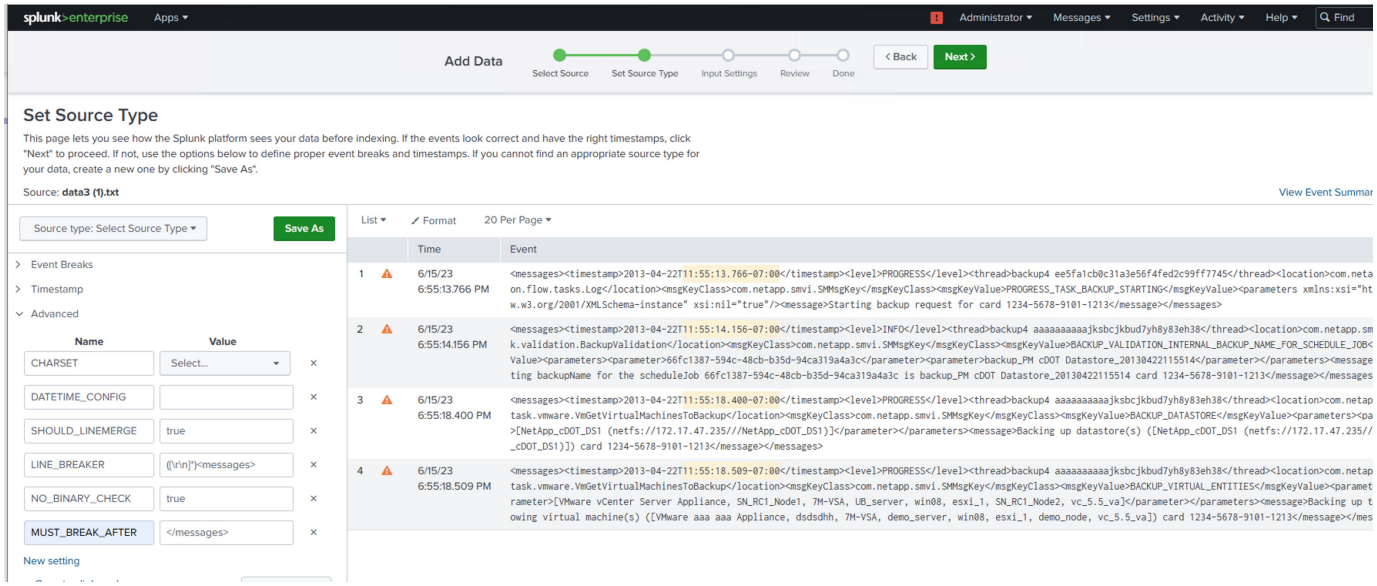

[ __auto__learned__ ]

SHOULD_LINEMERGE=true

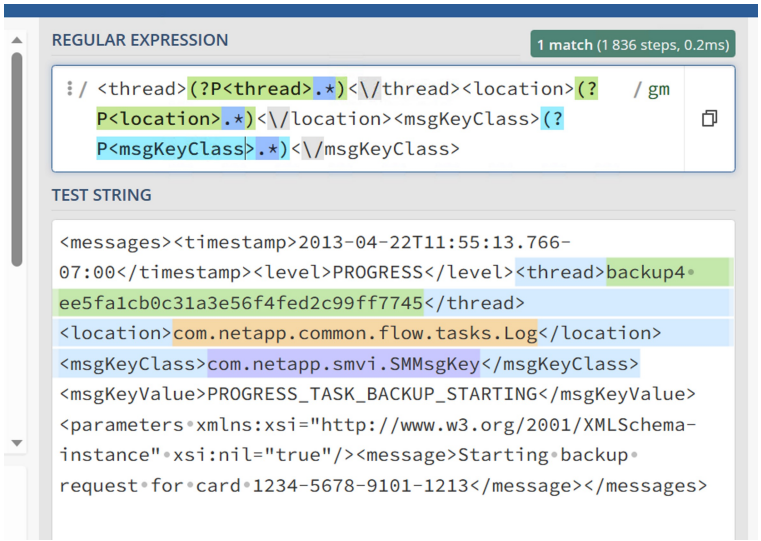
**LINE_BREAKER=([\r\n]*)<messages>**

NO_BINARY_CHECK=true

**MUST_BREAK_AFTER=</messages>**




Prepare regex to fetch thread,location,msgKeyClass




**<thread>(?P<thread>.*)<\/thread><location>(?P<location>.*)<\/location><msgKeyClass>(?P<msgKeyClass>.*)<\/msgKeyClass>**

Copy below settings and **create a props.conf under "splunk/etc/system/local"** and -

(i) edit source name

(ii) add "**TRANSFORMS-demoExtraction = XMLExtraction**"

[ my ]

SHOULD_LINEMERGE = true

**LINE_BREAKER = ([\r\n]*)<messages>**

**BREAK_ONLY_BEFORE = ([\r\n]*)<messages>**

NO_BINARY_CHECK = true

**MUST_BREAK_AFTER = </messages>**

**TRANSFORMS-demoExtraction = xmlExtraction**

**Create a transforms.conf as**

[**xmlExtraction**]

REGEX = <thread>(?P<thread>.*)<\/thread><location>(?P<location>.*)<\/location><msgKeyClass>(?P<msgKeyClass>.*)<\/msgKeyClass>

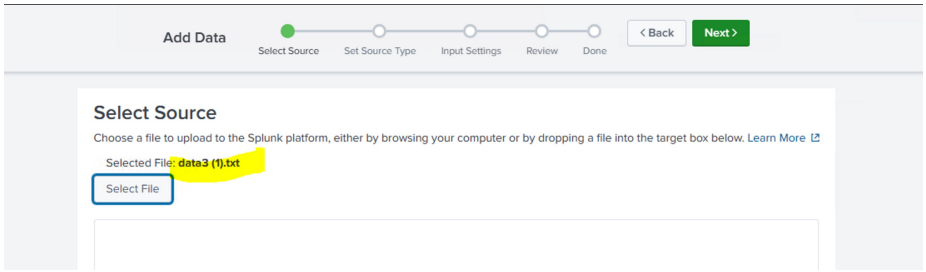
FORMAT = thread::$1 location::$2 myKeyClass::$3

WRITE_META = true

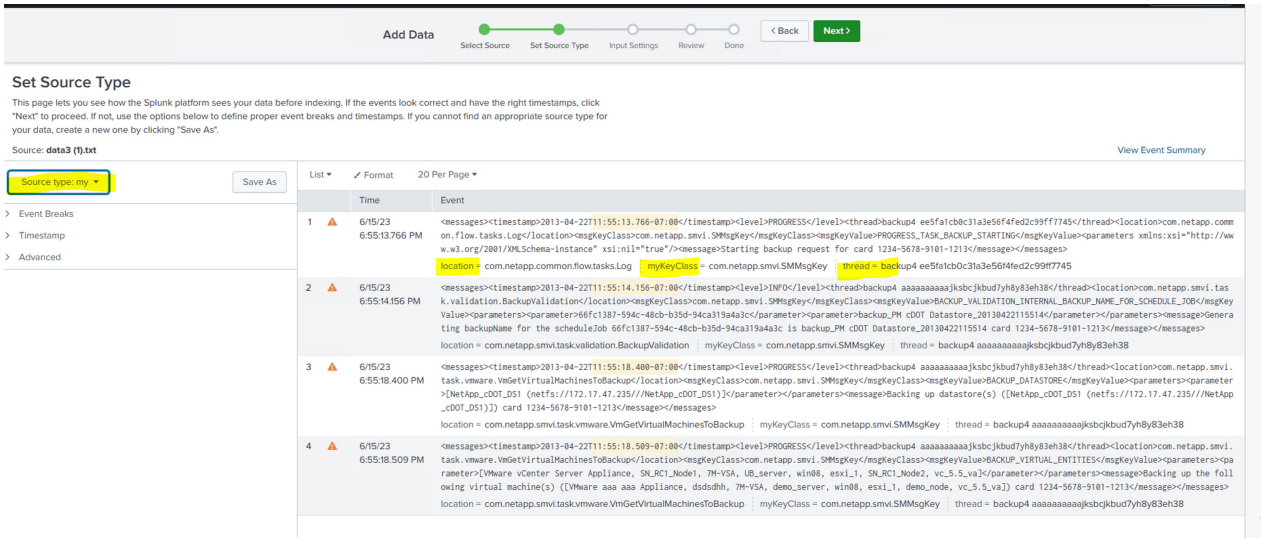
```
[ec2-user@ip-172-31-8-243 local]$ more props.conf
[ my ]
SHOULD_LINEMERGE = true
LINE_BREAKER = ([\r\n]*)<messages>
BREAK_ONLY_BEFORE = ([\r\n]*)<messages>
NO_BINARY_CHECK = true
MUST_BREAK_AFTER = </messages>
TRANSFORMS-demoExtraction = xmlExtraction
[ec2-user@ip-172-31-8-243 local]$ more transforms.conf
[xmlExtraction]
REGEX = <thread>(?P<thread>.*)<\/thread><location>(?P<location>.*)<\/location><msgKeyClass>(?P<msgKeyClass>.*)<\/msgKeyClass>
FORMAT = thread::$1 location::$2 myKeyClass::$3
WRITE_META = true
[ec2-user@ip-172-31-8-243 local]$
[ec2-user@ip-172-31-8-243 local]$
[ec2-user@ip-172-31-8-243 local]$ pwd
/home/ec2-user/splunk/etc/system/local
[ec2-user@ip-172-31-8-243 local]$
```

Restart Splunk.

Import Data again and Search "Event Break as your props.conf name :

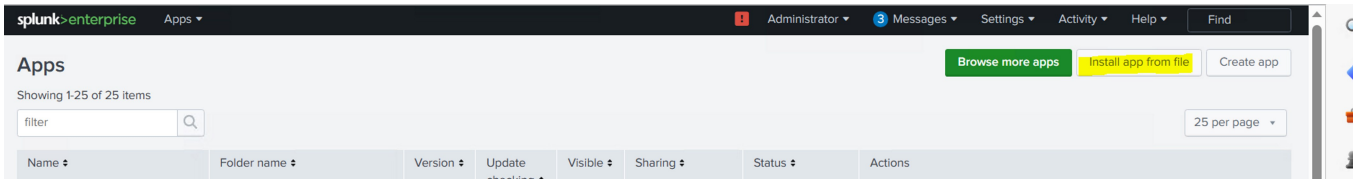


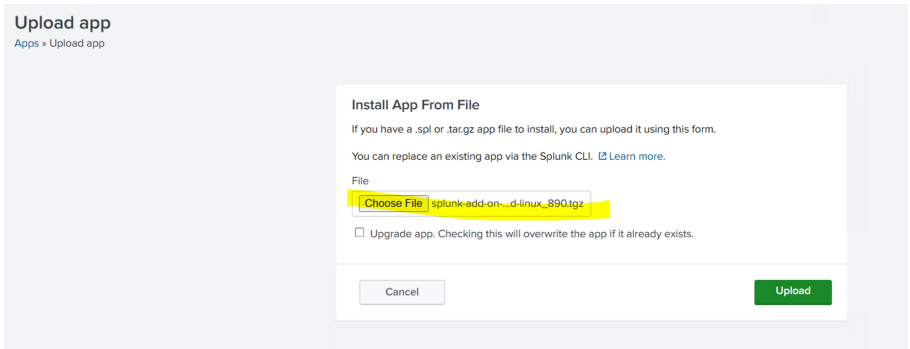

Now search the source under sourcetype, it will break the event as per regex:

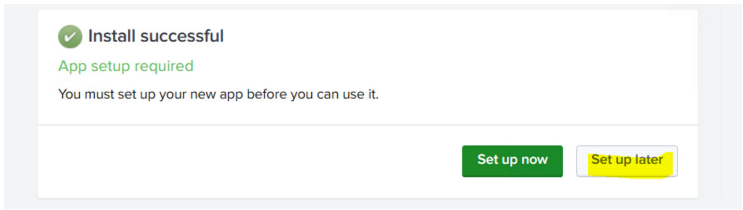


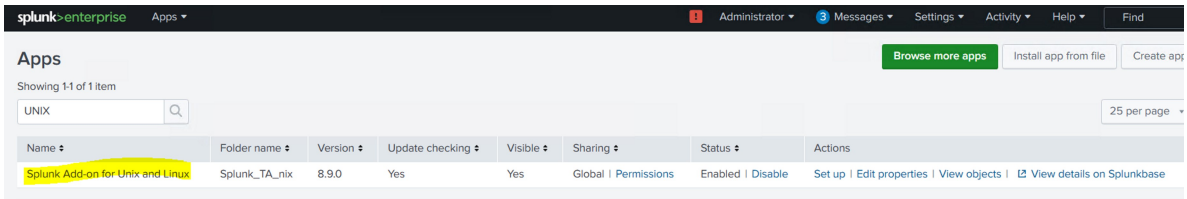

## #UNIX-Intergartion

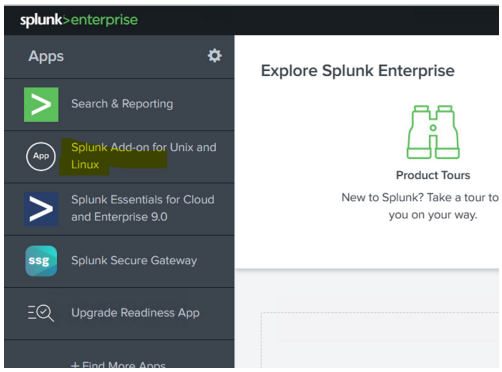
Download "Splunk Add-on for UNIX and Linux" Add-on on Splunk-Enterprise



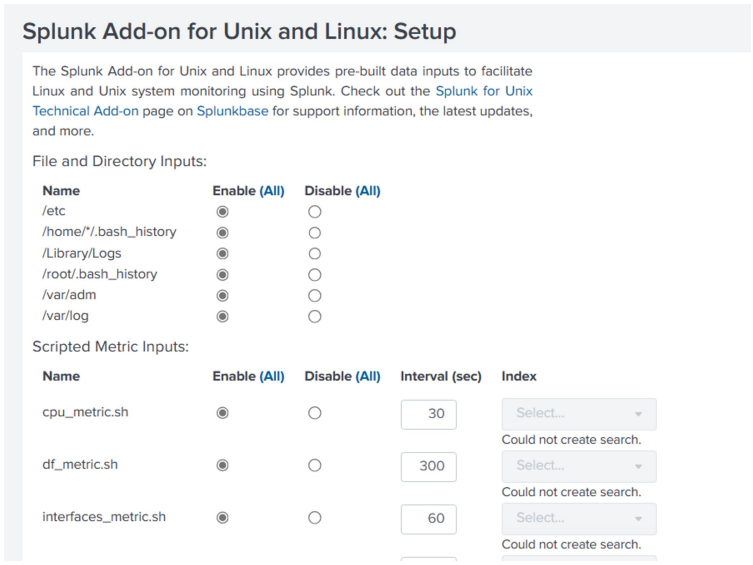



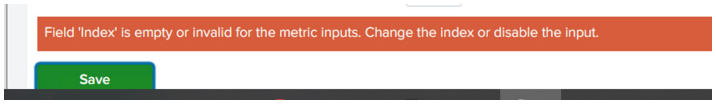






Enable and Save :




Then check the inputs.conf and manually add index and restart splunk

[ec2-user@ip-172-31-8-243 local]$ pwd

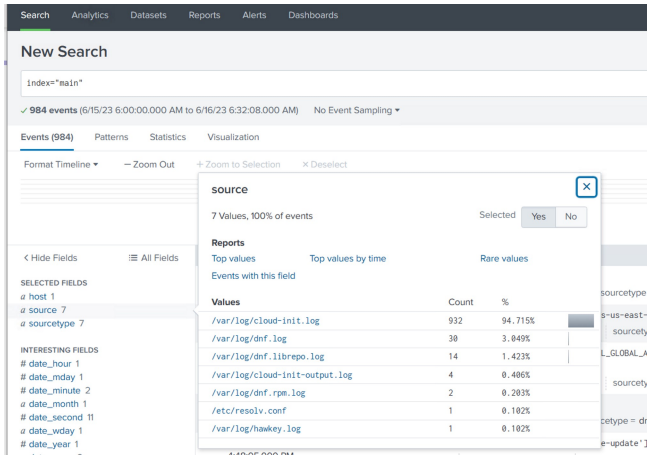
/home/ec2-user/splunk/etc/apps/Splunk_TA_nix/local

[ec2-user@ip-172-31-8-243 local]$

[ec2-user@ip-172-31-8-243 local]$

[ec2-user@ip-172-31-8-243 local]$ more inputs.conf

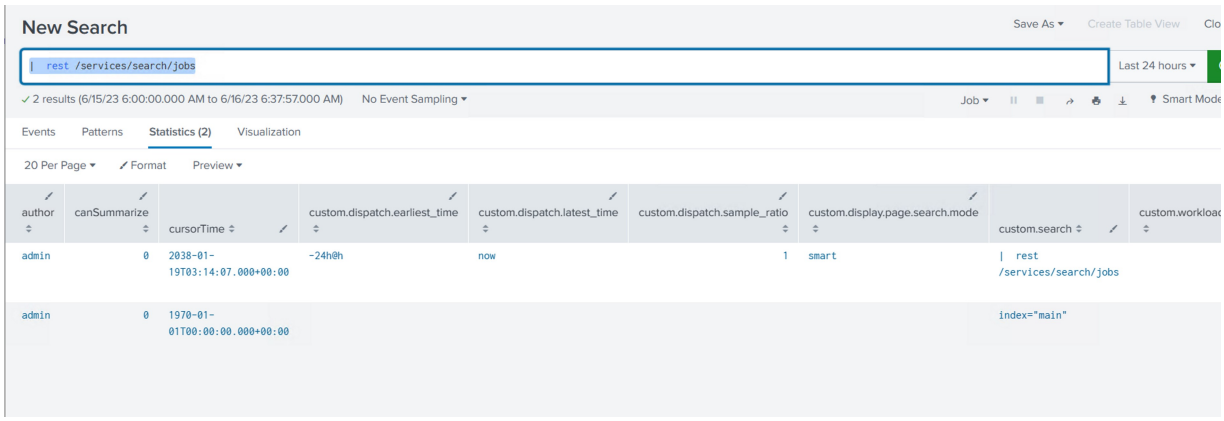
```
[script://./bin/cpu.sh]
disabled = 0
index = main
```



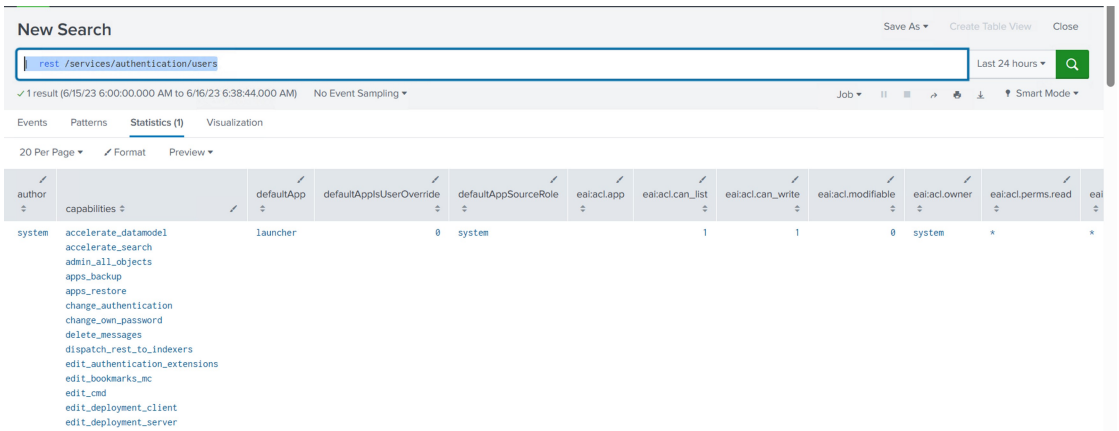

## #Rest command/call

Rest => hit the config file but searching load will be high.

***| rest /services/search/jobs***




***| rest /services/authentication/users***




Use-cases could be :

(1) current active users

(2) list of dashboards/KBs

(3) If any data(source)/index/ is getting used in any Dashboard/Alert/Report

(4) User not logged in last 2 months.

## #Syslog

Write inputs.conf as below to ingest data as syslog. No need to write [monitor] -

***[udp]***

***connection_host=ip***

For windows long

***[winevent]***

## #Folder Structure

**/home/ec2-user/splunk/etc/apps/search**

[ec2-user@ip-172-31-8-243 search]$ ll

total 16

drwxr-xr-x. 3 ec2-user ec2-user 20 May 26 23:29 **appserver** => HTML, CSS, JS, images

drwxr-xr-x. 2 ec2-user ec2-user 16384 May 26 23:29 **bin => executable files along with custom scripts**

drwxr-xr-x. 3 ec2-user ec2-user 180 May 26 23:29 **default => configs**

drwxr-xr-x. 2 ec2-user ec2-user 130 May 26 23:29 **lookups**

drwxr-xr-x. 2 ec2-user ec2-user 26 May 26 23:29 **metadata => having details about KB and their access details**

drwxr-xr-x. 2 ec2-user ec2-user 28 May 26 23:29 **scripts**

drwxr-xr-x. 2 ec2-user ec2-user 94 May 26 23:29 **static => having logos**

[ec2-user@ip-172-31-8-243 search]$

```
[ec2-user@ip-172-31-8-243 search]$ cd metadata/
[ec2-user@ip-172-31-8-243 metadata]$ ls
default.meta
[ec2-user@ip-172-31-8-243 metadata]$ more default.meta

# Application-level permissions

[]
access = read : [ * ], write : [ admin, power ]

### MANAGER

[manager]
access = read : [ * ], write : [ admin ]
export = system



### VIEWS

[views/search_status]
access = read : [ admin ], write : [ admin ]

[views/search_detail_activity]
access = read : [ admin ], write : [ admin ]

[views/search_activity_by_user]
access = read : [ admin ], write : [ admin ]

[views/scheduler_status]
access = read : [ admin ], write : [ admin ]

[views/scheduler_status_errors]
access = read : [ admin ], write : [ admin ]

[views/scheduler_savedsearch]
access = read : [ admin ], write : [ admin ]

[views/scheduler_user_app]
access = read : [ admin ], write : [ admin ]
```

```
[ec2-user@ip-172-31-8-243 static]$ pwd
/home/ec2-user/splunk/etc/apps/search/static
[ec2-user@ip-172-31-8-243 static]$ ll
total 16
-r--r--r--. 1 ec2-user ec2-user 3167 May 26 23:01 appIcon.png
-r--r--r--. 1 ec2-user ec2-user 1981 May 26 23:01 appIconAlt.png
-r--r--r--. 1 ec2-user ec2-user 2547 May 26 23:01 appIconAlt_2x.png
-r--r--r--. 1 ec2-user ec2-user 3556 May 26 23:01 appIcon_2x.png
[ec2-user@ip-172-31-8-243 static]$
[ec2-user@ip-172-31-8-243 static]$
```