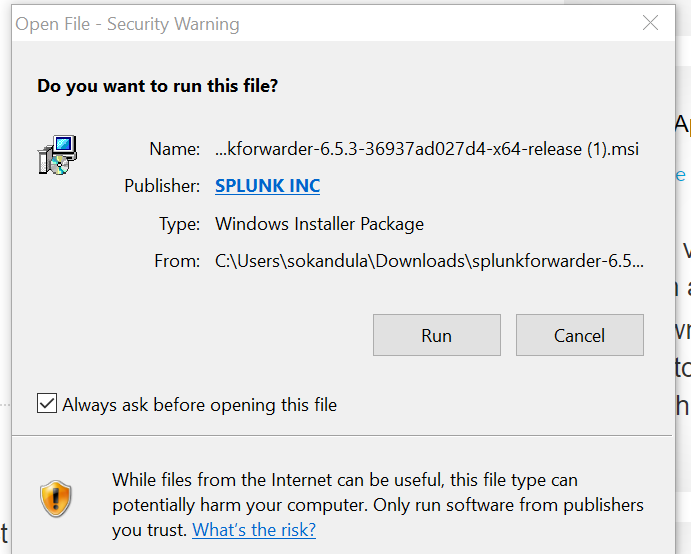
**Splunk Forwarder Installation Documentation:**

Step1 : Create account for splunk , if already exists please proceed to step 2

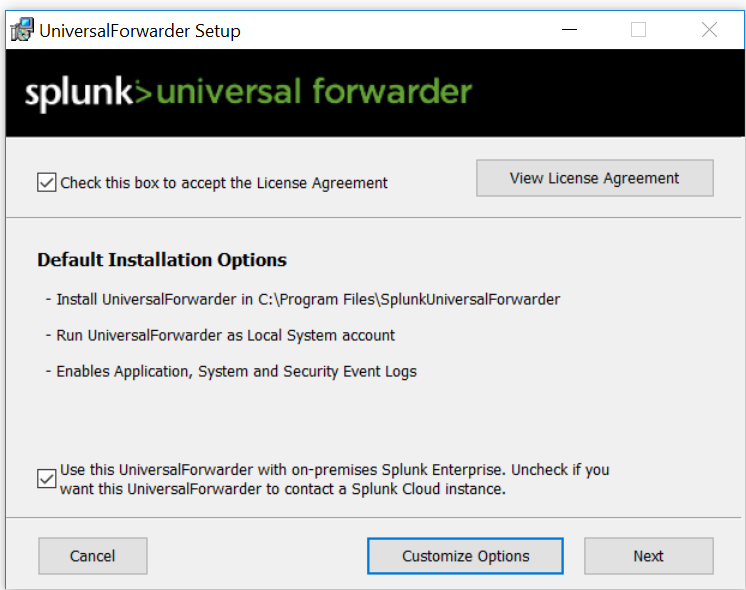
Step 2 : Download Splunk universal forwarder for windows from :

https://www.splunk.com/page/previous\_releases/universalforwarder#x86\_64windows

Step 3: Open msi file and run

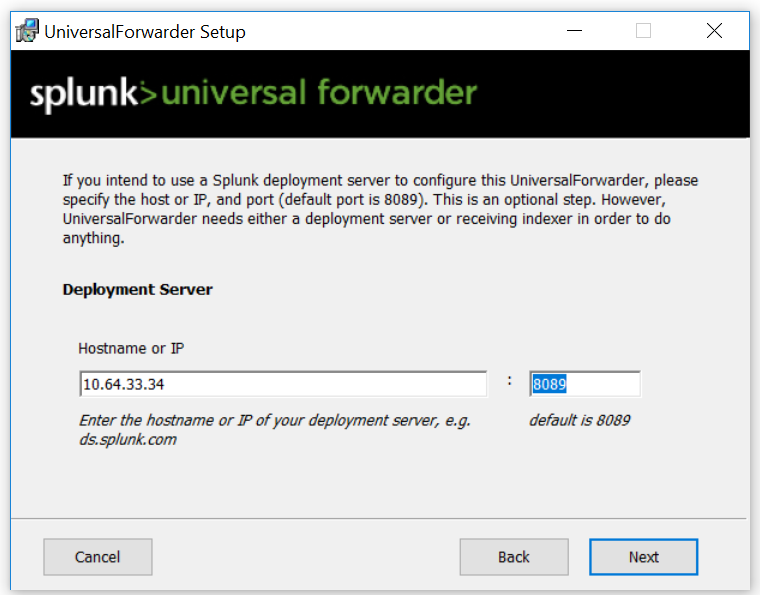


Check license box :

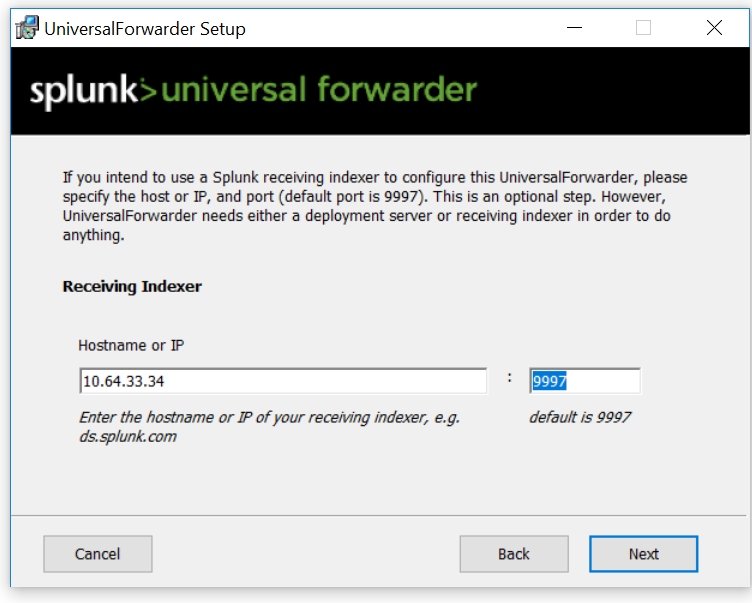


Click next

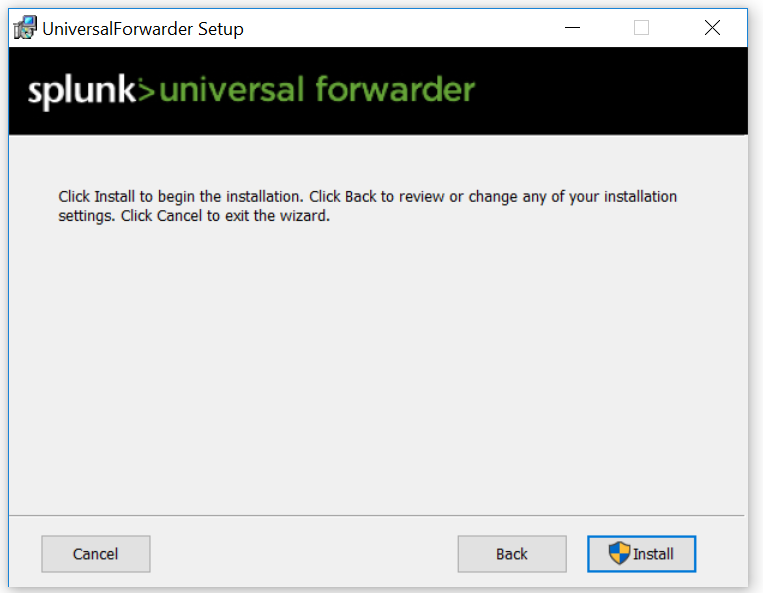
Provide prod deployment server ip and port and click next



Provide prod indexer ip and port and click next



Install the splunk forwarder



**Monitoring logs on client / end machine :**

Edit : C:\Program Files\SplunkUniversalForwarder\etc\system\local\inputs.conf file

[default]

host = hostname

[monitor://logs\_location]

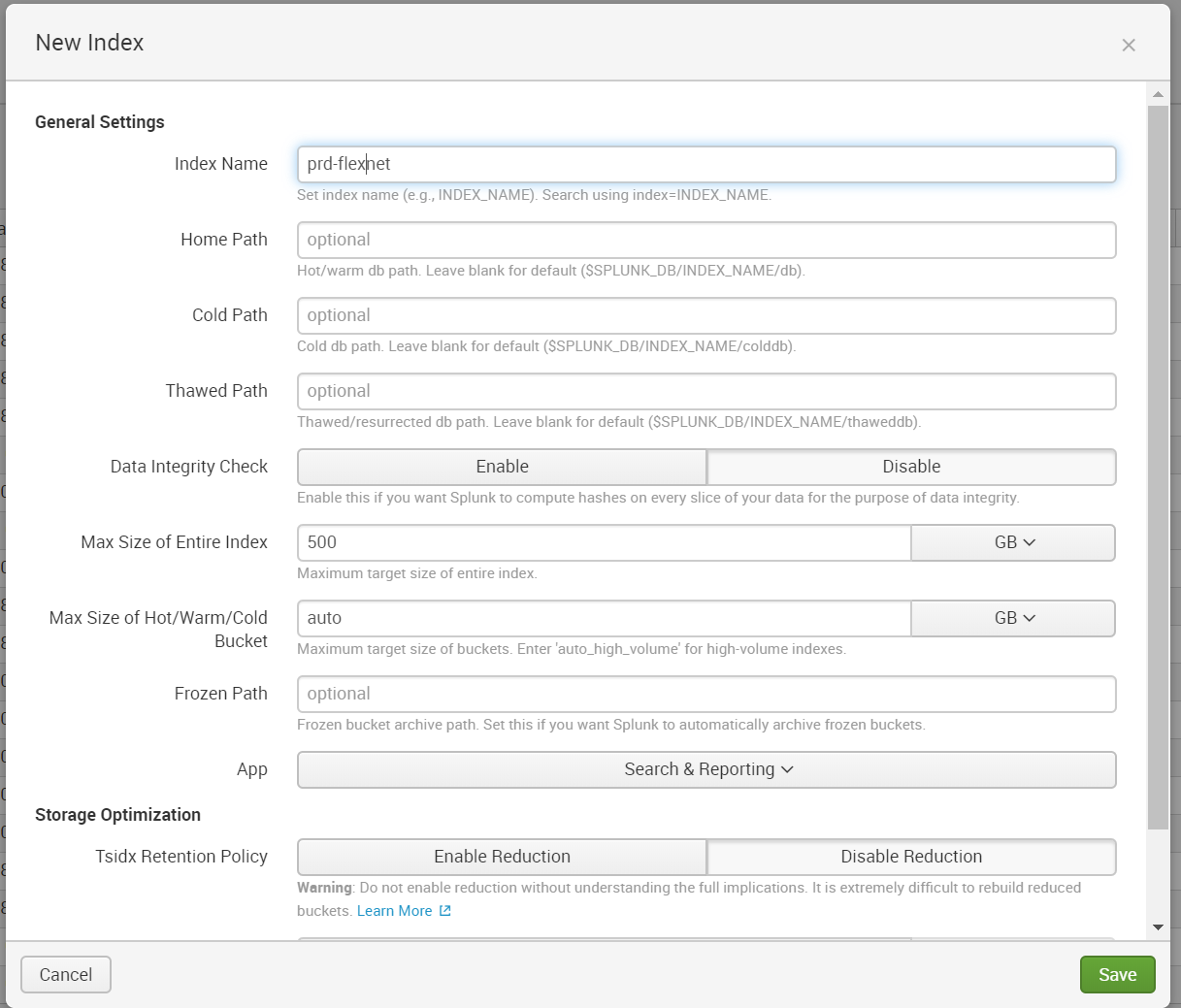
index = index\_name

After editing inputs file , restart splunk agent :

Run 🡪 services.msc 🡪 splunkforwarder 🡪 restart

**Create index on splunk indexer if not represent :**

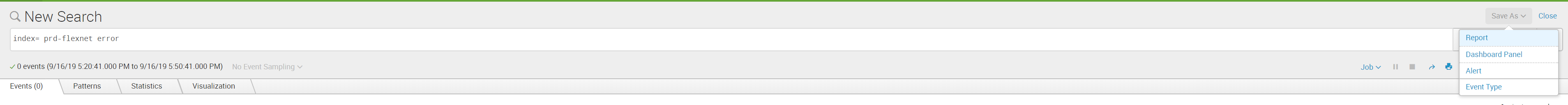
Goto settings 🡪 indexes 🡪 create new index

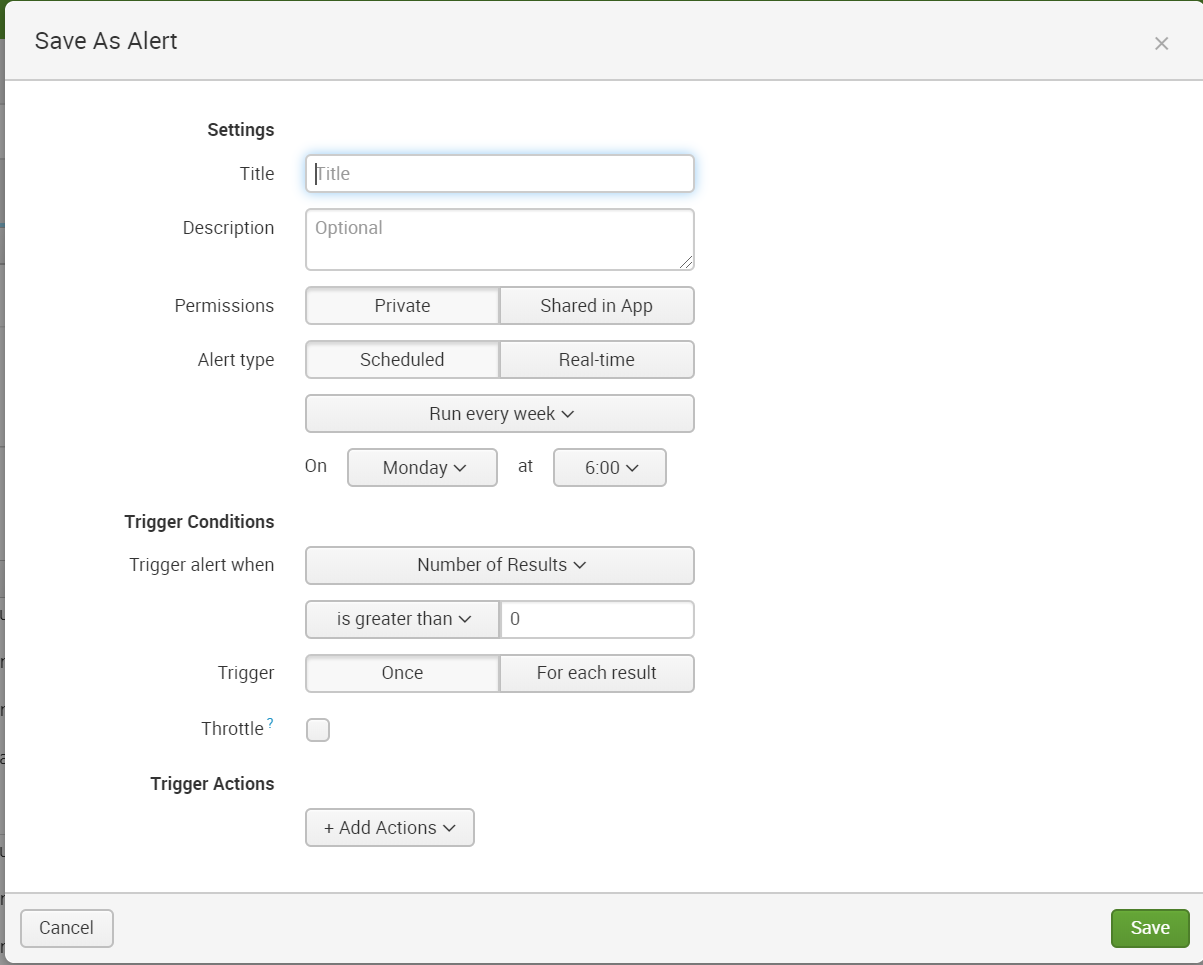


**Create Alert :**

1. Get the alert strings from concerned team
2. Search strings including index name and click on save as alert as shown below :

index= prd-flexnet error





Check already configured alerts for reference