**Setting up and using Kapaciton**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Download and install Kapacitor for ubuntu by running the following commands in terminal.

wget <https://dl.influxdata.com/kapacitor/releases/kapacitor_1.5.2_amd64.deb>

sudo dpkg -i kapacitor\_1.5.2\_amd64.deb

1. To start kapacitor, enter the following command in the terminal

sudo service kapacitor start

1. Create a new tick script.

gedit cpu\_alert.tick

1. In the new tick script specify the database name and the retension policy of the database for which the alert has to be generated.
2. Specify the measurement and all the essential requirements in the following manner:

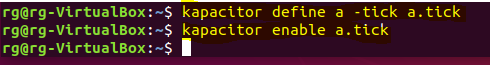
|  |
| --- |
| dbrp "xD"."autogen"  stream  |from()  .measurement('win\_cpu')  .groupBy(\*)  |stateDuration(lambda: "Percent\_Interrupt\_Time" >= 0.25)  .unit(1s)  |alert()  .id('Kapacitor alerts')  .message('Duration: {{.Duration}}')  .warn(lambda: "Percent\_Interrupt\_Time" > 0.25)  .crit(lambda: "Percent\_Interrupt\_Time" > 0.3)  .post('http://146.122.193.185:8080/x/abc.html')  topic('cpux')  .log('/etc/kapacitor/alert\_log.txt')  .idField('id')  .levelTag('level')  |where(lambda: "id" != '')  |influxDBOut().create()  .database('kapacitor\_alertss')  .retentionPolicy('autogen')  .measurement('win\_cpu')  .tag('kapacitor', 'true')  .tag('version', '0.2') |

* In the 1st line of the above script we have specified the database name (xD) and the retention policy (autogen).
* Then we have specified the data which we need (\* From win\_cpu).
* Stateduration gives us the duration of the event specified by “Lambda”, in this case it is the same as the alert parameters
* Then we define the alert, specifying an alert\_id and message in which the Stateduration is displayed. Then warning parameter and a critical warning parameter is defined.
* Then specify a post address if you want to send the alert to some other location via the post method .
* Also define the alert topic in order to check the alerts on terminal locally or remotely.
* In order to store only the alert logs in a new database in influxDb i have generated a condition which selects all the entries with an id.
* Then i have created a new database in InfluxDb using influxDBOut().create(). Specify the database details.

* Now go to terminal and “*define*” and “*enable*” the TICK Script.

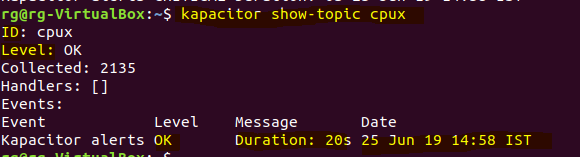
kapacitor define <file\_name> -tick <file\_name>.tick

kapacitor enable <file\_name>.tick



* We can view the real time alerts and their status and message via the topic defined in the TICK script.

kapacitor show-topic <topic\_name>



* Now you can define more alerts as per your requirement for different databases and different measurements.
* In order to view to alerts in a topic from another system on the same network, use the following commands in the terminal of the new system:

kapacitor -url http://<ip\_adr\_of\_host>:9092 show-topic <topic\_name>