Client Computer (A Computer which we have to monitor in Our Network) Configuration.

We have to install Any Shipper-Service for sending logs to Server Computer We Install Winlogbeat.

Step-1: Download the Winlogbeat zip file from the
https://www.elastic.co/downloads/beats/winlogbeat

Step-2: Extract the contents into C:\Program Files.

Step-3: Rename the winlogbeat- <version> directory to Winlogbeat.

Step-4: Open a PowerShell prompt as an Administrator (Right-click on the PowerShell Icon and Select Run as Administrator).

Step-5: From the PowerShell prompt, run the following commands to install the service.

```
PS C:\Users\Administrator> cd 'C:\Program Files\Winlogbeat'
PS C:\Program Files\Winlogbeat>.\install-service-winlogbeat.ps1
```

Note: If Script execution is disable on your System, you need to set the execution policy for the current session to allow the script to run.

```
For Example: PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-winlogbeat.ps1
```

Step-6: Replace winlogbeat.yml file by Given File.

We Disable ElasticSearch Output and Kibana Output by Putting # in front of line. and Enable Logstash Output for Example:

```
output.logstash:
hosts: ["192.168.137.1:5044"]
```

Note: Here hosts is Server Ip Address and Port is Number Where logstash service is Running.

Step-7: Start Service from Entering In PowerShell

```
PS C:\Program Files\Winlogbeat> Start-Service winlogbeat
```

Or Either Manually from Service.msc

Server Computer (A Computer Where We collect Network Logs) Configuration.

Step-1: Download and Install the Elasticsearch, Logstash, Kibana from the

https://www.elastic.co/products/

Step-2:

-Open elasticsearch-<version>/config/elasticsearch.yml File.

network.host: 192.168.137.1
http.port: 9200

Note: Here network.host is Server Ip Address and Port is Number Where we want to run elasticsearch service by default is 9200.

-Run The elasticsearch from bin folder

Step-3:

-Open kibana-<version>-*/config/kibana.yml File.

server.port: 5601
server.host: "192.168.137.1"
elasticsearch.hosts: ["http://192.168.137.1:9200"]

Note: Here server.host Address is Server Ip Address and Port is Number Where we want to run kibana service by default is 5601. And elasticsearch.hosts is where elasticsearch service is running.

-Run the kibana from bin folder

Step-4:

-Open logstash-<version>-*/config/

-Replace pipelines.yml file from Given pipelines.yml file

-Add the logstash_monitor.conf file in bin folder.

Step-5:

-Open the cmd in Administration mode

-Set Path of logstash\bin folder

-Enter `logstash -f logstash_monitor.conf`

Kibana Data Visualization and dashboard Settings

-Enter URL 192.168.137.1:5601 to Open Kibana .

-Create Index Pattern which is in logstash_monitor.conf file

-Click on Discover tab to see logs from Machine which are config. In Network

-We Can Create New Visualization and Search on demand. And Create Dashboard.

-Created Dashboard also we can place in web application as real time performance by option share.

-Copy iframe of dashboard by clicking in share option->Saved Object

-Place in web page where we have to see.

For Example:

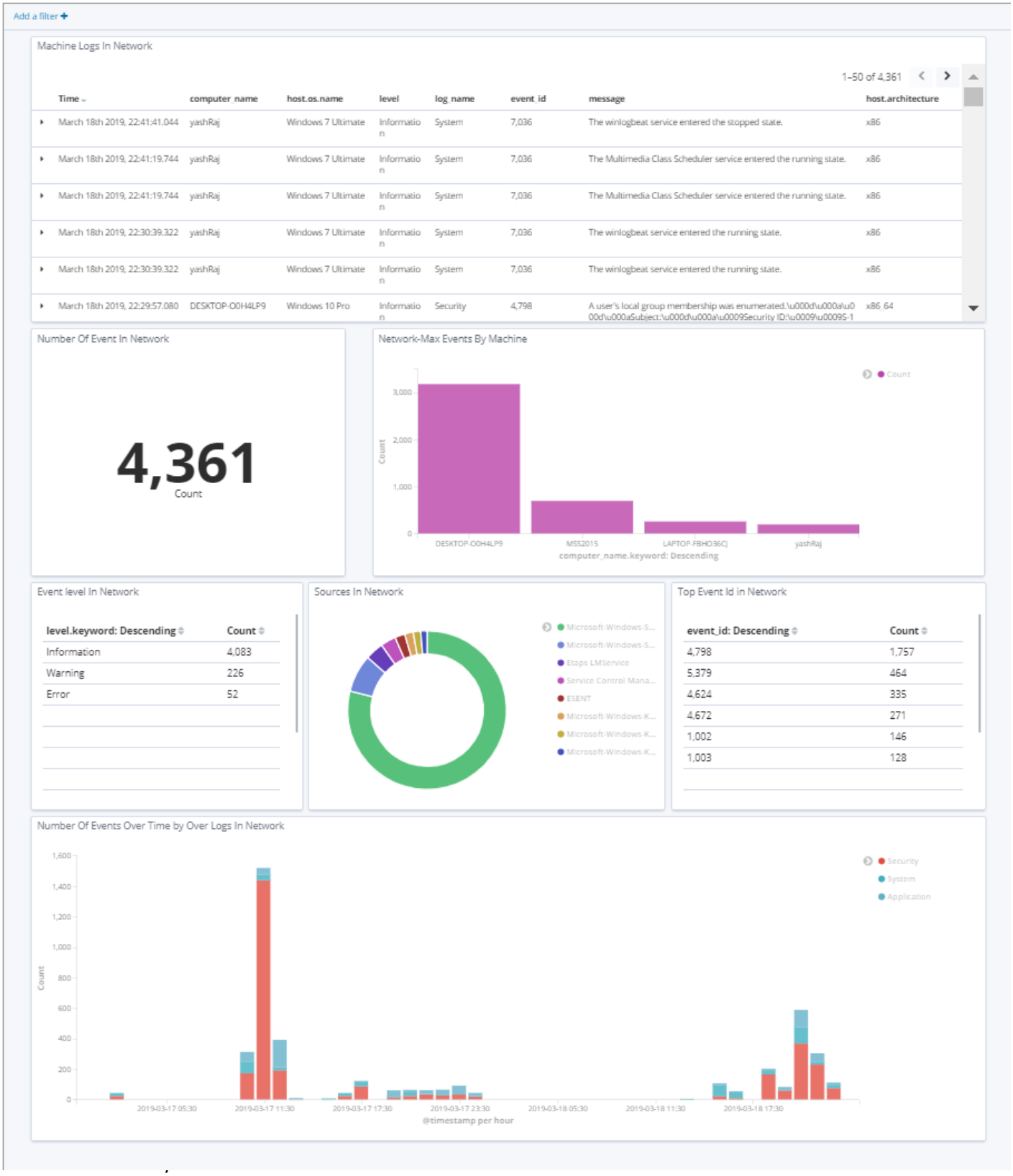
<html>

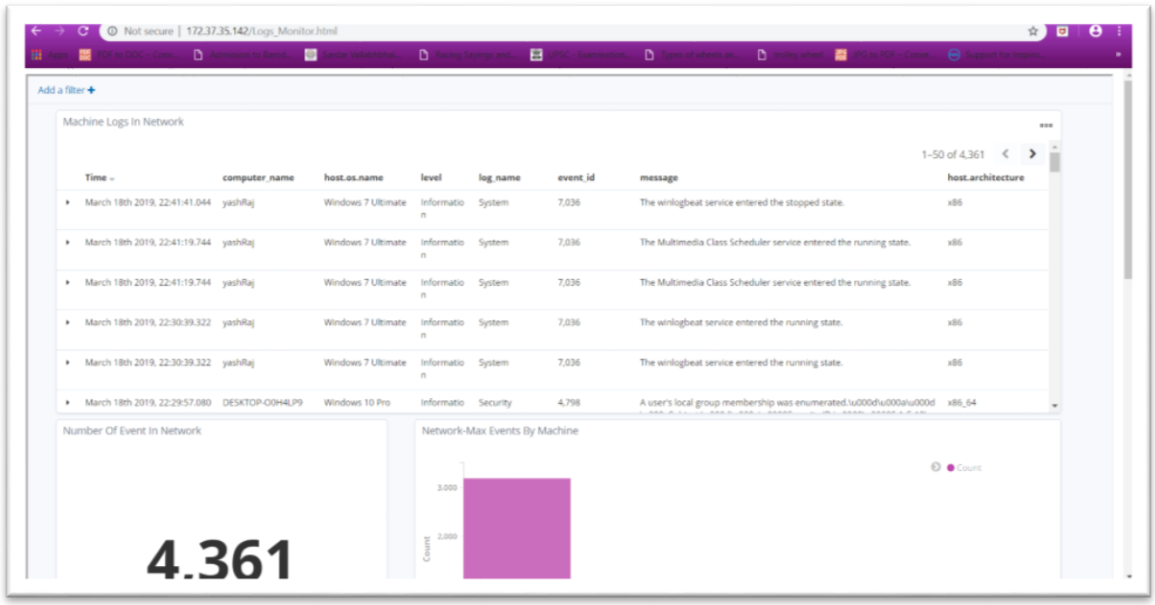
<iframe src="http://192.168.137.1:5601/app/kibana#/dashboard/8e4584b0-4a3a-11e9-aa6c-ad4620f73848?embed=true&_g=(refreshInterval%3A(pause%3A!t%2Cvalue%3A5000)%2Ctime%3A(from%3A'2019-03-16T18%3A30%3A00.000Z'%2Cmode%3Aabsolute%2Cto%3A'2019-03-18T18%3A29%3A59.999Z'))" height="1720" width="1480"></iframe>

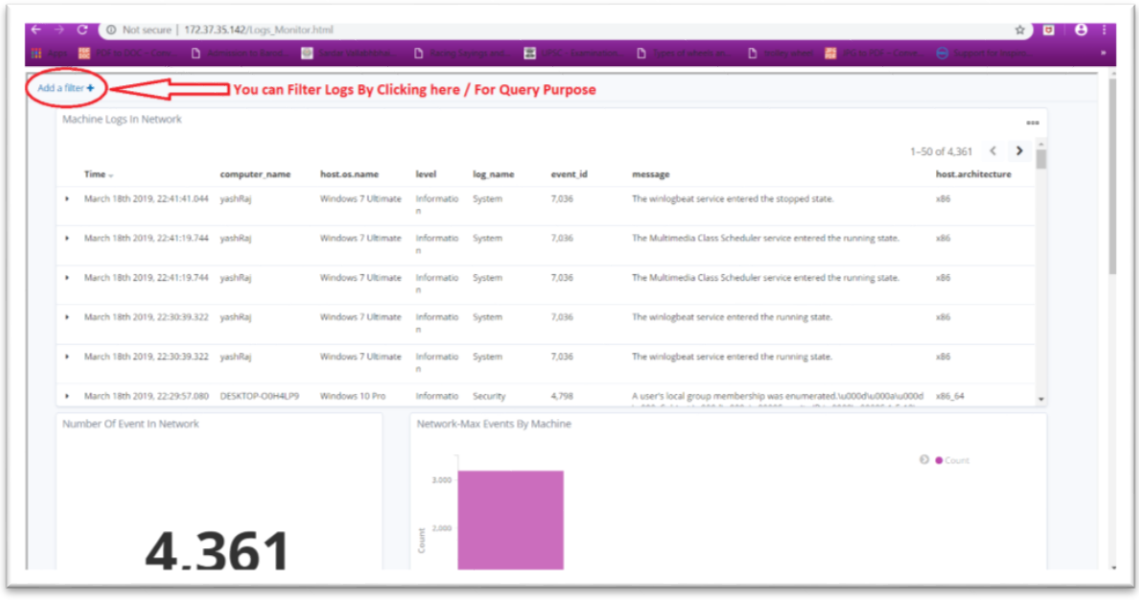
</html>

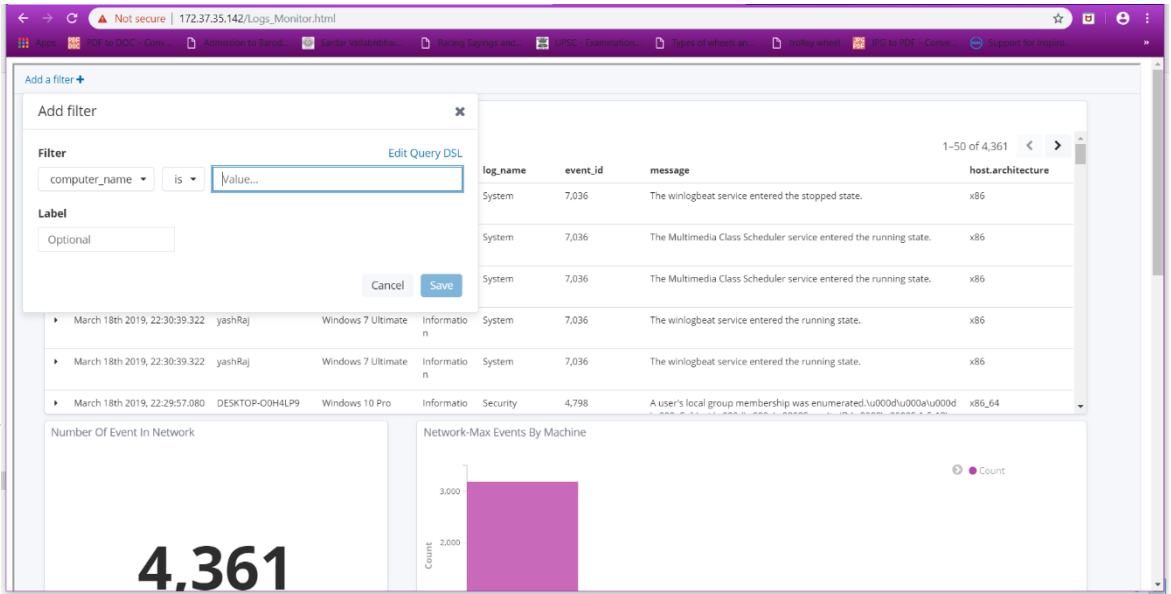
Note: Here iframe code is depend on Server Computer. I am showing My webpage just for Demonstrate purpose.

Here is Sample Dashboard of my iframe for given Problem Statement.




Not secure | 172.37.35.142/Logs_Monitor.html
Add a filter +
Machine Logs In Network
1–50 of 4,361
Time
computer_name
host.os.name
level
log_name
event_id
message
host.architecture
March 18th 2019, 22:41:41.044 yashRaj Windows 7 Ultimate Information System 7,036 The winlogbeat service entered the stopped state. x86
March 18th 2019, 22:41:19.744 yashRaj Windows 7 Ultimate Information System 7,036 The Multimedia Class Scheduler service entered the running state. x86
March 18th 2019, 22:41:19.744 yashRaj Windows 7 Ultimate Information System 7,036 The Multimedia Class Scheduler service entered the running state. x86
March 18th 2019, 22:30:39.322 yashRaj Windows 7 Ultimate Information System 7,036 The winlogbeat service entered the running state. x86
March 18th 2019, 22:30:39.322 yashRaj Windows 7 Ultimate Information System 7,036 The winlogbeat service entered the running state. x86
March 18th 2019, 22:29:57.080 DESKTOP-O0H4LP9 Windows 10 Pro Information Security 4,798 A user's local group membership was enumerated.\u000d\u000a\u000d x86_64
Number Of Event In Network
4.361
Network-Max Events By Machine
Count
3,000
2,000


Not secure | 172.37.35.142/Logs_Monitor.html
Add a filter +
You can Filter Logs By Clicking here / For Query Purpose
Machine Logs In Network
1–50 of 4,361
Time
computer_name
host.os.name
level
log_name
event_id
message
host.architecture
March 18th 2019, 22:41:41.044 yashRaj Windows 7 Ultimate Information System 7,036 The winlogbeat service entered the stopped state. x86
March 18th 2019, 22:41:19.744 yashRaj Windows 7 Ultimate Information System 7,036 The Multimedia Class Scheduler service entered the running state. x86
March 18th 2019, 22:41:19.744 yashRaj Windows 7 Ultimate Information System 7,036 The Multimedia Class Scheduler service entered the running state. x86
March 18th 2019, 22:30:39.322 yashRaj Windows 7 Ultimate Information System 7,036 The winlogbeat service entered the running state. x86
March 18th 2019, 22:30:39.322 yashRaj Windows 7 Ultimate Information System 7,036 The winlogbeat service entered the running state. x86
March 18th 2019, 22:29:57.080 DESKTOP-O0H4LP9 Windows 10 Pro Information Security 4,798 A user's local group membership was enumerated.\u000d\u000a\u000d x86_64
Number Of Event In Network
4.361
Network-Max Events By Machine
Count
3,000
2,000


Not secure | 172.37.35.142/Logs_Monitor.html
Add a filter +
Add filter
Filter
Edit Query DSL
computer_name
is
Value...
Label
Optional
Cancel
Save
1–50 of 4,361
log_name
event_id
message
host.architecture
System 7,036 The winlogbeat service entered the stopped state. x86
System 7,036 The Multimedia Class Scheduler service entered the running state. x86
System 7,036 The Multimedia Class Scheduler service entered the running state. x86
March 18th 2019, 22:30:39.322 yashRaj Windows 7 Ultimate Information System 7,036 The winlogbeat service entered the running state. x86
March 18th 2019, 22:30:39.322 yashRaj Windows 7 Ultimate Information System 7,036 The winlogbeat service entered the running state. x86
March 18th 2019, 22:29:57.080 DESKTOP-O0H4LP9 Windows 10 Pro Information Security 4,798 A user's local group membership was enumerated.\u000d\u000a\u000d x86_64
Number Of Event In Network
4.361
Network-Max Events By Machine
Count
3,000
2,000

Output Of Given Filter/Query Also we visualize in Webpage.

Computer_name as yashRaj