Download filebeat in windows machine : https://www.elastic.co/downloads/past-releases/filebeat-7-17-12

(Download file beat which matches yours elk version)

Go to filebeat.yml

In filebeat inputs → type enabed ,path ,tags are configured

```
# ============================== Filebeat inputs ===============================

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

# filestream is an input for collecting log messages from files.
- type: log

  # Unique ID among all inputs, an ID is required.
  #id: my-filestream-id

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx
  tags: ["sysmon"]

    #- /var/log/*.log
    #- c:\programdata\elasticsearch\logs\*
```

In logstash output ip and port of .conf file con.d folder of logstash

```
# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.195.148:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"
```

Navigate to filbeat path :

```
PS C:\WINDOWS\system32> cd "C:\Program Files\Filebeat"
```

Apply changes

Check configuration of filebeat

.\filebeat.exe -e test config

```
PS C:\Program Files\Filebeat> .\filebeat.exe -e test config
2023-09-23T02:54:14.678+0530    INFO    instance/beat.go:698    Home path: [C:\Program Files\Filebeat] Config path: [C:\Program Files\Filebeat] Data path: [C:\Program Files\Filebeat\data] Logs path: [C:\Program Files\Filebeat\logs] Hostfs Path: [/]
2023-09-23T02:54:14.678+0530    INFO    instance/beat.go:706    Beat ID: 38f326b3-3fa1-4a17-96c2-5032a3c22cfc
2023-09-23T02:54:14.713+0530    WARN    [add_cloud_metadata]    add_cloud_metadata/provider_aws_ec2.go:79       read token request for getting IMDSv2 token returns empty: Put "http://169.254.169.254/latest/api/token": dial tcp 169.254.169.254:80: connectex: A socket operation was attempted to an unreachable network.. No token in the metadata request will be used.
2023-09-23T02:54:14.714+0530    INFO    [beat]  instance/beat.go:1052   Beat info       {"system_info": {"beat": {"path": {"config": "C:\\Program Files\\Filebeat", "data": "C:\\Program Files\\Filebeat\\data", "home": "C:\\Program Files\\Filebeat", "logs": "C:\\Program Files\\Filebeat\\logs"}, "type": "filebeat", "uuid": "38f326b3-3fa1-4a17-96c2-5032a3c22cfc"}}}
2023-09-23T02:54:14.714+0530    INFO    [beat]  instance/beat.go:1061   Build info      {"system_info": {"build": {"commit": "50d7b818d6765543bb4e995018c26670871a046d", "libbeat": "7.17.12", "time": "2023-07-18T20:14:21.000Z", "version": "7.17.12"}}}
2023-09-23T02:54:14.714+0530    INFO    [beat]  instance/beat.go:1064   Go runtime info {"system_info": {"go": {"os":"windows","arch":"amd64","max_procs":8,"version":"go1.19.10"}}}
2023-09-23T02:54:14.714+0530    INFO    [add_cloud_metadata]    add_cloud_metadata/add_cloud_metadata.go:101    add_cloud_metadata: hosting provider type not detected.
2023-09-23T02:54:14.732+0530    INFO    [beat]  instance/beat.go:1070   Host info       {"system_info": {"host": {"architecture":"x86_64","boot_time":"2023-09-22T10:00:17+05:30","name":"Loke4884","ip":["fe80::be19:c43d:2d81:95df","169.254.209.109","fe80::7ae9:409e:f3f0:f72","169.254.90.202","fe80::5faa:b6f5:c121:572e","169.254.117.95","fe80::6b58:2447:7252:c7b5","192.168.128.1","fe80::deb1:2274:25ee:91f8","192.168.195.1","2409:4070:4495:d1b9:861a:da7:bd77:1b96","2409:4070:4495:d1b9:9d81:94b1:eedf:771","fe80::e7d2:74:9200:1bf3","192.168.231.18","fe80::6801:f9ed:5c39:ee0f","169.254.126.9","::1","127.0.0.1"],"kernel_version":"10.0.22621.2283 (WinBuild.160101.0800)","mac":["00:ff:8f:b9:ed:f8","92:e8:68:1e:9c:23","92:e8:68:1e:9c:33","00:50:56:c0:00:01","00:50:56:c0:00:08","dc:30:70:68:1e:10","90:e8:68:1e:9c:22"],"os":{"type":"windows","family":"windows","platform":"windows","name":"Windows 11 Home Single Language","version":"10.0","major":10,"minor":0,"patch":0,"build":"22621.2283"},"timezone":"IST","timezone_offset_sec":19800,"id":"7d1a2ece-0d45-4127-a72f-648770a85b8b"}}}
2023-09-23T02:54:14.733+0530    INFO    [beat]  instance/beat.go:1099   Process info    {"system_info": {"process": {"cwd": "C:\\Program Files\\Filebeat", "exe": "C:\\Program Files\\Filebeat\\filebeat.exe", "name": "filebeat.exe", "pid": 10864, "ppid": 7232, "start_time": "2023-09-23T02:54:13.932+0530"}}}
2023-09-23T02:54:14.734+0530    INFO    instance/beat.go:292    Setup Beat: filebeat; Version: 7.17.12
2023-09-23T02:54:14.734+0530    INFO    [publisher]     pipeline/module.go:113  Beat name: Loke4884
2023-09-23T02:54:14.736+0530    WARN    beater/filebeat.go:202  Filebeat is unable to load the ingest pipelines for the configured modules because the Elasticsearch output is not configured/enabled. If you have already loaded the ingest pipelines or are using Logstash pipelines, you can ignore this warning.
Config OK
```

Install filebeat

PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-filebeat.ps1

```
PS C:\Program Files\Filebeat> PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-filebeat.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Program Files\Filebeat\install-service-filebeat.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R

Status   Name               DisplayName
------   ----               -----------
Stopped  filebeat           filebeat
```

Start the service of filebeat

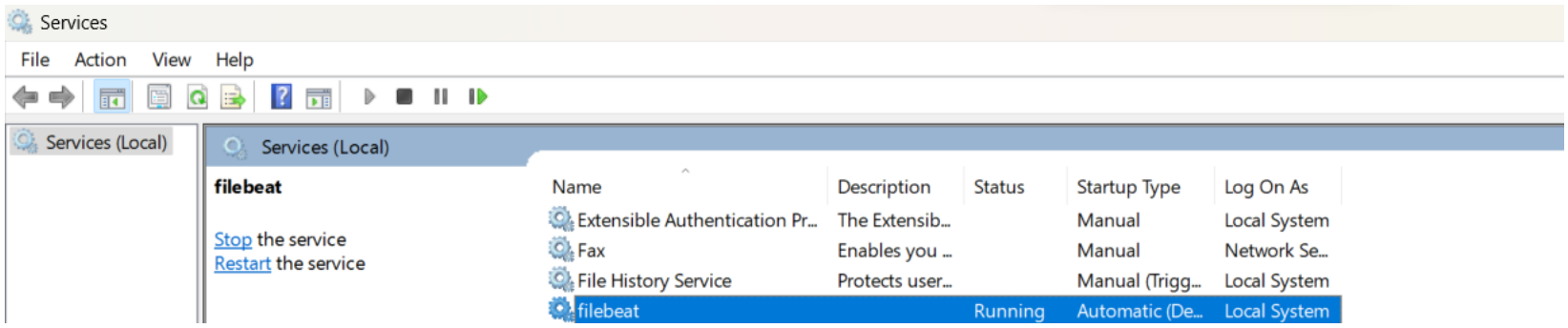
```
PS C:\Program Files\Filebeat> Start-Service filebeat
```

To check configuration of filebeat

```
PS C:\Program Files\Filebeat> .\filebeat.exe test config
Config OK
```

Search services in windows

There you can see status of filebeat



Get-Process -Name "filebeat"

```
PS C:\Program Files\Filebeat> Get-Process -Name "filebeat"

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    213      17    40360      48244       0.80  22700   0 filebeat
```

To check Filebeat logs

.\filebeat.exe -e

```
PS C:\Program Files\Filebeat> .\filebeat.exe -e
2023-09-23T08:31:43.678+0530    INFO    instance/beat.go:698    Home path: [C:\Program Files\Filebeat] Config path: [C:\Program Files\Filebeat] Data path: [C:\Program Files\Filebeat\data] Logs path: [C:\Program Files\Filebeat\logs] Hostfs Path: [/]
2023-09-23T08:31:43.680+0530    INFO    instance/beat.go:706    Beat ID: 38f326b3-3fa1-4a17-96c2-5032a3c22cfc
2023-09-23T08:31:43.755+0530    WARN    [add_cloud_metadata]    add_cloud_metadata/provider_aws_ec2.go:79       read token request for getting IMDSv2 token returns empty: Put "http://169.254.169.254/latest/api/token": dial tcp 169.254.169.254:80: connectex: A socket operation was attempted to an unreachable network.. No token in the metadata request will be used.
2023-09-23T08:31:43.756+0530    INFO    [beat]  instance/beat.go:1052   Beat info       {"system_info": {"beat": {"path": {"config": "C:\\Program Files\\Filebeat", "data": "C:\\Program Files\\Filebeat\\data", "home": "C:\\Program Files\\Filebeat", "logs": "C:\\Program Files\\Filebeat\\logs"}, "type": "filebeat", "uuid": "38f326b3-3fa1-4a17-96c2-5032a3c22cfc"}}}
2023-09-23T08:31:43.757+0530    INFO    [beat]  instance/beat.go:1061   Build info      {"system_info": {"build": {"commit": "50d7b818d6765543bb4e995018c26670871a046d", "libbeat": "7.17.12", "time": "2023-07-18T20:14:21.000Z", "version": "7.17.12"}}}
2023-09-23T08:31:43.757+0530    INFO    [add_cloud_metadata]    add_cloud_metadata/add_cloud_metadata.go:101    add_cloud_metadata: hosting provider type not detected.
2023-09-23T08:31:43.757+0530    INFO    [beat]  instance/beat.go:1064   Go runtime info {"system_info": {"go": {"os":"windows","arch":"amd64","max_procs":8,"version":"go1.19.10"}}}
2023-09-23T08:31:43.792+0530    INFO    [beat]  instance/beat.go:1070   Host info       {"system_info": {"host": {"architecture":"x86_64","boot_time":"2023-09-22T10:00:17+05:30","name":"Loke4884","ip":["fe80::be19:c43d:2d81:95df","169.254.209.109","fe80::7ae9:409e:f3f0:f72","169.254.90.202","fe80::5faa:b6f5:c121:572e","169.254.117.95","fe80::6b58:2447:7252:c7b5","192.168.128.1","fe80::deb1:2274:25ee:91f8","192.168.195.1","2409:4070:4495:d1b9:861a:da7:bd77:1b96","2409:4070:4495:d1b9:9d81:94b1:eedf:771","fe80::e7d2:74:9200:1bf3","192.168.231.18","fe80::6801:f9ed:5c39:ee0f","169.254.126.9","::1","127.0.0.1"],"kernel_version":"10.0.22621.2283 (WinBuild.160101.0800)","mac":["00:ff:8f:b9:ed:f8","92:e8:68:1e:9c:23","92:e8:68:1e:9c:33","00:50:56:c0:00:01","00:50:56:c0:00:08","dc:30:70:68:1e:10","90:e8:68:1e:9c:22"],"os":{"type":"windows","family":"windows","platform":"windows","name":"Windows 11 Home Single Language","version":"10.0","major":10,"minor":0,"patch":0,"build":"22621.2283"},"timezone":"IST","timezone_offset_sec":19800,"id":"7d1a2ece-0d45-4127-a72f-648770a85b8b"}}}
2023-09-23T08:31:43.792+0530    INFO    [beat]  instance/beat.go:1099   Process info    {"system_info": {"process": {"cwd": "C:\\Program Files\\Filebeat", "exe": "C:\\Program Files\\Filebeat\\filebeat.exe", "name": "filebeat.exe", "pid": 1852, "ppid": 16844, "start_time": "2023-09-23T08:31:42.633+0530"}}}
2023-09-23T08:31:43.793+0530    INFO    instance/beat.go:292    Setup Beat: filebeat; Version: 7.17.12
2023-09-23T08:31:43.794+0530    INFO    [publisher]     pipeline/module.go:113  Beat name: Loke4884
2023-09-23T08:31:43.795+0530    WARN    beater/filebeat.go:202  Filebeat is unable to load the ingest pipelines for the configured modules because the Elasticsearch output is not configured/enabled. If you have already loaded the ingest pipelines or are using Logstash pipelines, you can ignore this warning.
2023-09-23T08:31:43.795+0530    INFO    instance/beat.go:457    filebeat start running.
2023-09-23T08:31:43.795+0530    INFO    [monitoring]    log/log.go:142  Starting metrics logging every 30s
2023-09-23T08:31:43.797+0530    INFO    memlog/store.go:119     Loading data file of 'C:\Program Files\Filebeat\data\registry\filebeat' succeeded. Active transaction id=0
2023-09-23T08:31:43.800+0530    INFO    memlog/store.go:124     Finished loading transaction log file for 'C:\Program Files\Filebeat\data\registry\filebeat'. Active transaction id=99
2023-09-23T08:31:43.801+0530    WARN    beater/filebeat.go:411  Filebeat is unable to load the ingest pipelines for the configured modules because the Elasticsearch output is not configured/enabled. If you have already loaded the ingest pipelines or are using Logstash pipelines, you can ignore this warning.
2023-09-23T08:31:43.801+0530    INFO    [registrar]     registrar/registrar.go:109      States Loaded from registrar: 1
2023-09-23T08:31:43.801+0530    INFO    [crawler]       beater/crawler.go:71    Loading Inputs: 1
2023-09-23T08:31:43.801+0530    INFO    [crawler]       beater/crawler.go:117   starting input, keys present on the config: [filebeat.inputs.0.enabled filebeat.inputs.0.paths.0 filebeat.inputs.0.tags.0 filebeat.inputs.0.type]
2023-09-23T08:31:43.802+0530    WARN    [cfgwarn]       log/input.go:89 DEPRECATED: Log input. Use Filestream input instead.
2023-09-23T08:31:43.803+0530    INFO    [input] log/input.go:171        Configured paths: [C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx]  {"input_id": "b8908837-ce11-452e-b9b1-16ecaebe7d94"}
2023-09-23T08:31:43.807+0530    INFO    [crawler]       beater/crawler.go:148   Starting input (ID: 9677536288742867344)
2023-09-23T08:31:43.809+0530    INFO    [crawler]       beater/crawler.go:106   Loading and starting Inputs completed. Enabled inputs: 1
2023-09-23T08:31:43.809+0530    INFO    cfgfile/reload.go:164   Config reloader started
2023-09-23T08:31:43.809+0530    INFO    [input.harvester]       log/harvester.go:310    Harvester started for paths: [C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx]       {"input_id": "b8908837-ce11-452e-b9b1-16ecaebe7d94", "source": "C:\\Windows\\System32\\winevt\\Logs\\Microsoft-Windows-Sysmon%4Operational.evtx", "state_id": "native::4128768-156123-471411235", "finished": false, "os_id": "4128768-156123-471411235", "old_source": "C:\\Windows\\System32\\winevt\\Logs\\Microsoft-Windows-Sysmon%4Operational.evtx", "old_finished": true, "old_os_id": "4128768-156123-471411235", "harvester_id": "62acc4e2-3c60-472f-b8db-9e550e703193"}
2023-09-23T08:31:43.810+0530    INFO    cfgfile/reload.go:224   Loading of config files completed.
2023-09-23T08:32:13.863+0530    INFO    [monitoring]    log/log.go:184  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":31,"time":{"ms":31}},"total":{"ticks":77,"time":{"ms":77},"value":0},"user":{"ticks":46,"time":{"ms":46}}},"handles":{"open":213},"info":{"ephemeral_id":"9b44ccdc-0da7-41a3-82a3-6d43cb614083","uptime":{"ms":30235},"version":"7.17.12"},"memstats":{"gc_next":19379568,"memory_alloc":10520008,"memory_sys":45952888,"memory_total":56121168,"rss":53264384},"runtime":{"goroutines":43}},"filebeat":{"events":{"added":2,"done":2},"harvester":{"open_files":1,"running"
```

Go to conf.d folder

In this folder you write configuration code for logstash to port to elk

```
root@lokesh-manikanta:/# cd /etc/logstash/conf.d/
```

Create a file with extention .conf

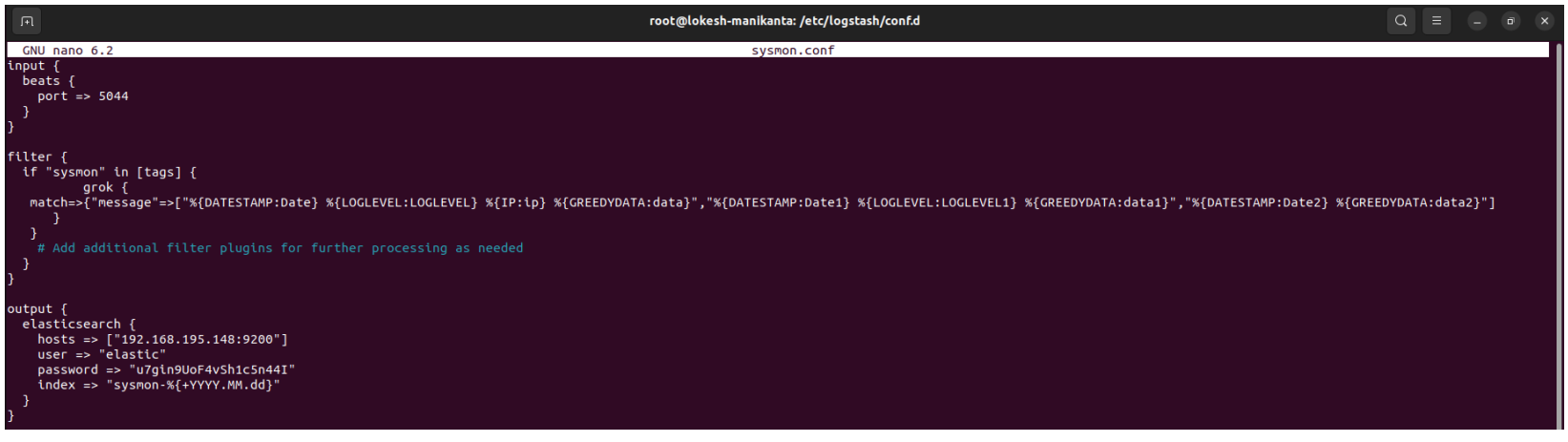
```
root@lokesh-manikanta:/etc/logstash/conf.d# touch sysmon.conf
```

To known any other conf file

```
root@lokesh-manikanta:/etc/logstash/conf.d# ls
sysmon.conf
```

Write a code inside sysmon.conf

```
root@lokesh-manikanta:/etc/logstash/conf.d# nano sysmon.conf
```



Save and close Sysmon.conf

Sysmon.conf code :

```
input {
  beats {
    port => 5044
  }
}

filter {
  if "sysmon" in [tags] {
        grok {
   match=>{"message"=>["%{DATESTAMP:Date} %{LOGLEVEL:LOGLEVEL} %{IP:ip} %{GREEDYDATA:data}","%{DATESTAMP:Date1} %{LOGLEVEL:LOGLEVEL1} %{GREEDYDATA:data1}","%{DATESTAMP:Date2} %{GREEDYDATA:data2}"]
      }
   }
    # Add additional filter plugins for further processing as needed
  }
}

output {
  elasticsearch {
    hosts => ["192.168.195.148:9200"]
    user => "elastic"
    password => "u7gin9UoF4vSh1c5n44I"
    index => "sysmon-%{+YYYY.MM.dd}"
  }
}
```

Restart logstash

```
root@lokesh-manikanta:/etc/logstash/conf.d# systemctl restart logstash
```

Start the services of the logstash

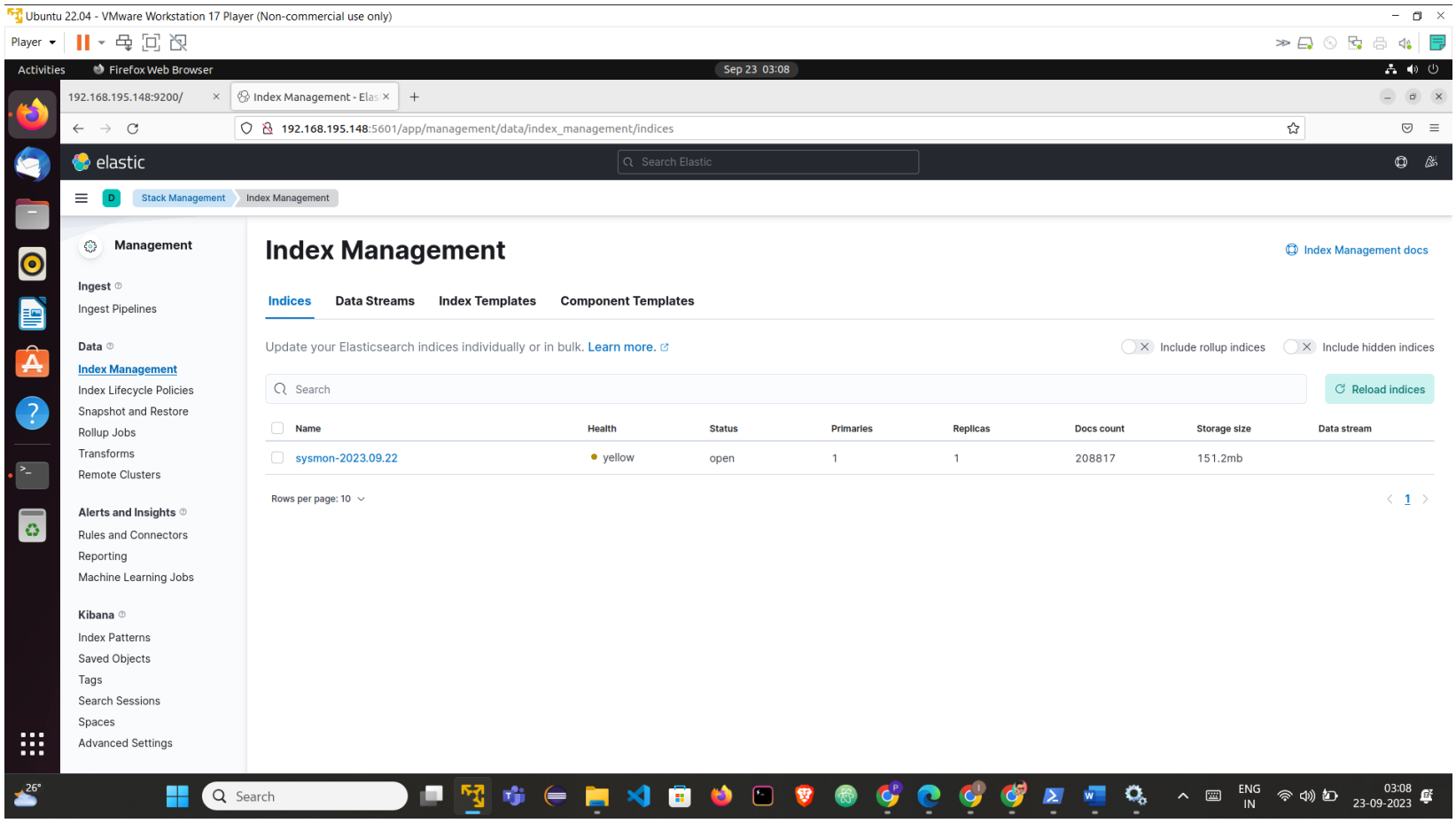
```
root@lokesh-manikanta:/etc/logstash/conf.d# sudo service logstash start
```

To see logs of logstash (logs will be stored in logstash-plain.log)

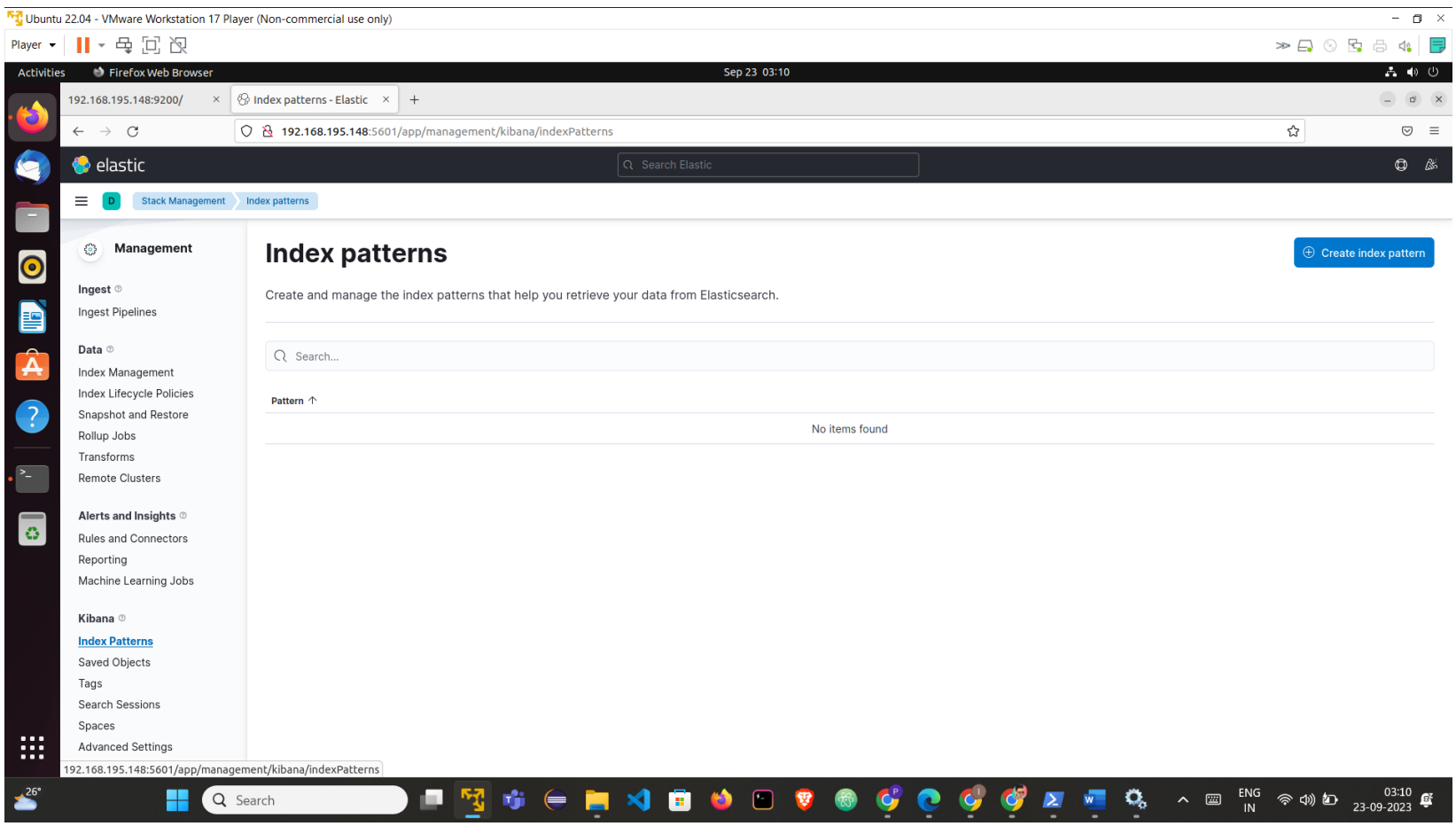
```
root@lokesh-manikanta:/etc/logstash/conf.d# tail -f /var/log/logstash/logstash-plain.log
[2023-09-23T02:46:37,850][INFO ][logstash.outputs.elasticsearch][main] Elasticsearch version determined (7.17.13) {:es_version=>7}
[2023-09-23T02:46:37,853][WARN ][logstash.outputs.elasticsearch][main] Detected a 6.x and above cluster: the `type` event field won't be used to determine the document _type {:es_version=>7}
[2023-09-23T02:46:37,993][INFO ][logstash.outputs.elasticsearch][main] Config is not compliant with data streams. `data_stream => auto` resolved to `false`
[2023-09-23T02:46:38,279][INFO ][logstash.outputs.elasticsearch][main] Using a default mapping template {:es_version=>7, :ecs_compatibility=>:disabled}
[2023-09-23T02:46:38,491][INFO ][logstash.javapipeline    ][main] Starting pipeline {:pipeline_id=>"main", "pipeline.workers"=>2, "pipeline.batch.size"=>125, "pipeline.batch.delay"=>50, "pipeline.max_inf
light"=>250, "pipeline.sources"=>["/etc/logstash/conf.d/sysmon.conf"], :thread=>"#<Thread:0x5c8da86f run>"}
[2023-09-23T02:46:39,520][INFO ][logstash.javapipeline    ][main] Pipeline Java execution initialization time {"seconds"=>1.02}
[2023-09-23T02:46:39,552][INFO ][logstash.inputs.beats    ][main] Starting input listener {:address=>"0.0.0.0:5044"}
[2023-09-23T02:46:39,587][INFO ][logstash.javapipeline    ][main] Pipeline started {"pipeline.id"=>"main"}
[2023-09-23T02:46:39,777][INFO ][org.logstash.beats.Server][main][e643d8525bbc191cf19b57eb2d17ade11541d6dc09da72a79ef066a6d0ad620f] Starting server on port: 5044
[2023-09-23T02:46:39,846][INFO ][logstash.agent           ] Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[]}
```

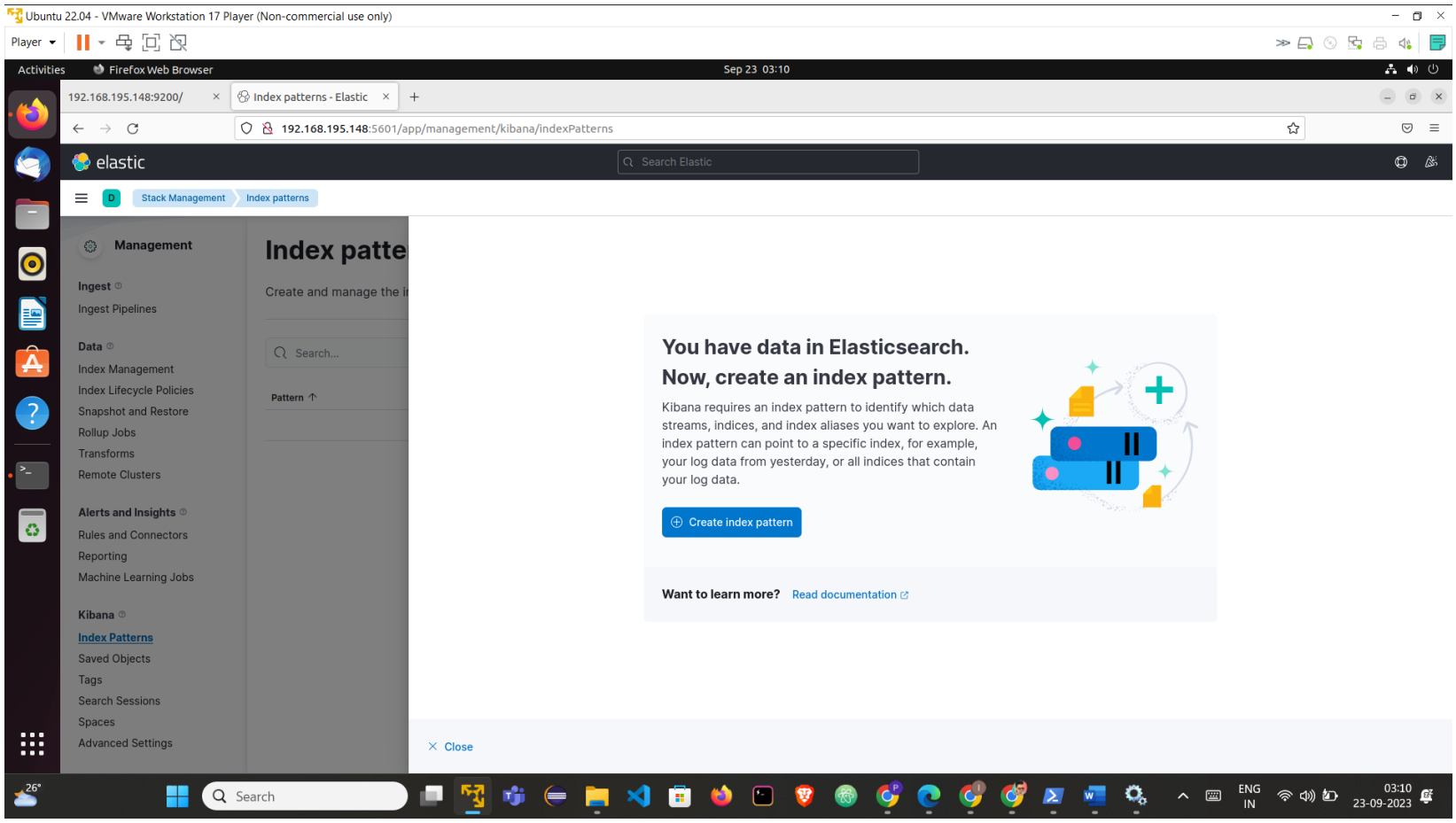
Go to Date → Index Mangement

You will get index you created in logstash configuration file(ex : sysmon.conf)

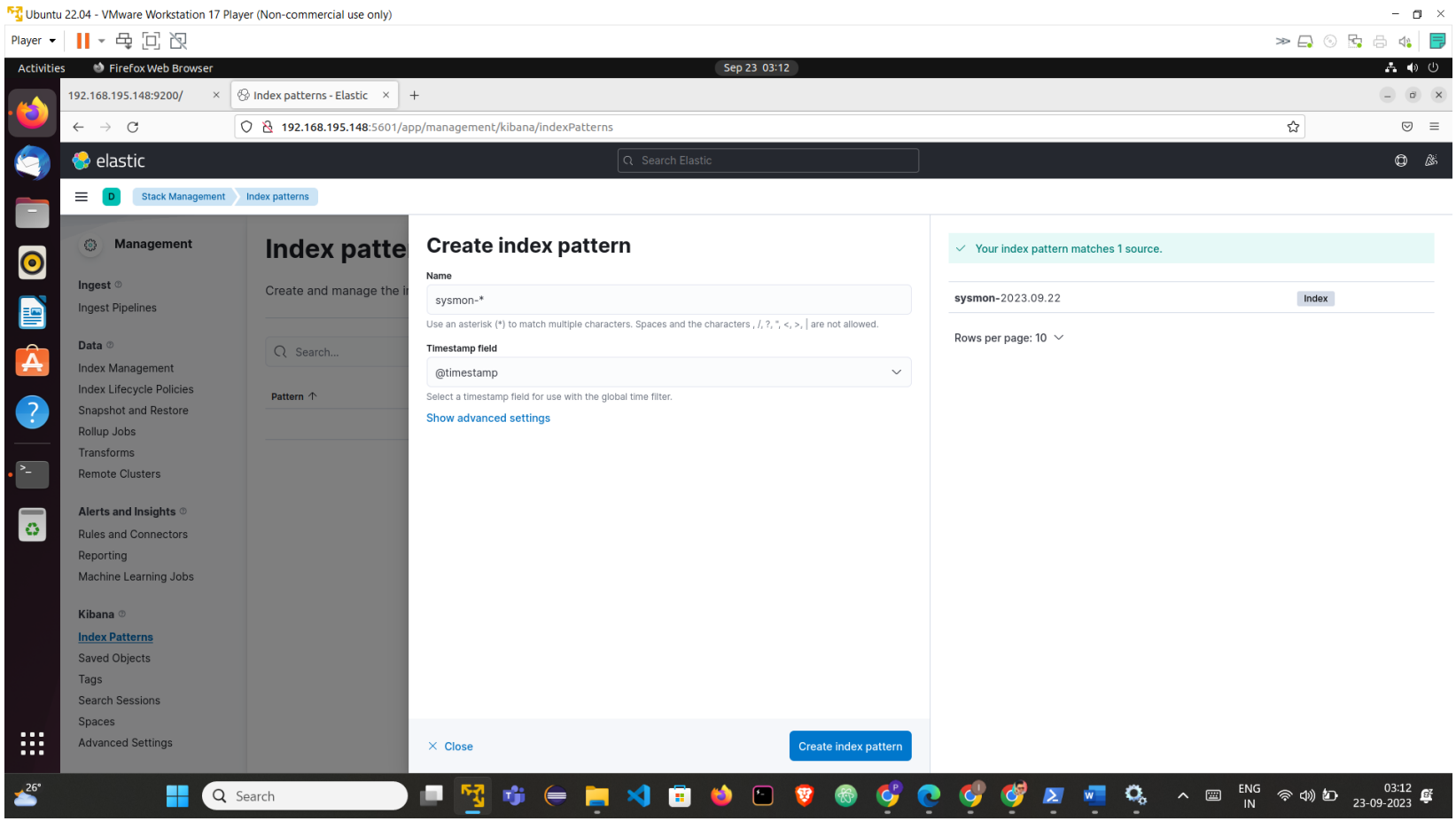


Go to kibana → Index Pattern → Create Index Pattern





Give name and time stamp and click on create index pattern



Go to discover choose what Index you created