Configuring Filebeat Agent on Windows

1. Download the Filebeat Windows zip file: https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-8.17.3-windows-x86_64.zip
2. Extract the contents of the zip file into C:\Program Files.
3. Rename the filebeat-8.17.3-windows-x86_64 directory to Filebeat.
4. Open a PowerShell prompt as an Administrator (right-click the PowerShell icon and select Run As Administrator).
5. From the PowerShell prompt, run the following commands to install Filebeat as a Windows service:

PS > cd 'C:\Program Files\Filebeat'

PS C:\Program Files\Filebeat> .\install-service-filebeat.ps1

Get-Service filebeat // To know the status of the service

6. Modify the filebeat.yml file under the path "C:\Program Files\Filebeat"

Note: Take a copy of the file before editing it.

7. Modify the file as shown in the screenshot and no changes are needed for remaining configuration

Note: Since this is a .yml file, proper spacing and indentation are important for correct syntax.

```
# ============================== 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: winlog

# 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.
  name: Application
  name: Security
  name: System
   #paths:
    #- /var/log/*.log
    #- c:\programdata\elasticsearch\logs\*
```

```
# ================================== Filebeat modules ==============================
  # Enable the system module for event logs
  modules:
    - module: system
      eventlog:
        enabled: true
        var.event_logs:
          - name: Application
          - name: Security
            event_id: [4624, 4625, 4776]
          - name: System
      auth:
        enabled: true

  filebeat.config.modules:
  # Glob pattern for configuration loading
  path: ${path.config}/modules.d/*.yml

  # Set to true to enable config reloading
  reload.enabled: true

  # Period on which files under path should be checked for changes
  #reload.period: 10s
```

```
# ================================== Outputs ===================================

# Configure what output to use when sending the data collected by the beat.

# ---------------------------- Elasticsearch Output ----------------------------
#output.elasticsearch:
  # Array of hosts to connect to.
#  hosts: ["localhost:9200"]

  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom".
  preset: balanced

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"

# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["65.0.96.103:5045"]

  # 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"
```

Open the port 5045 in the Security Group of Graylog Server.

8. Run the following command to test the filebeat.yml

.\filebeat.exe test config

.\filebeat.exe test output

9. Run the command

./filebeat modules enable system

10. Modify the file system.yml under the path “C:\Program Files\Filebeat\modules.d” as shown in the screenshot

```
# Module: system
# Docs: https://www.elastic.co/guide/en/beats/filebeat/8.17/filebeat-module-system.html

- module: system
  # Syslog
  syslog:
    enabled: true

    # Set custom paths for the log files. If left empty,
    # Filebeat will choose the paths depending on your OS.
    #var.paths:

    # Use journald to collect system logs
    #var.use_journald: false

  # Authorization logs
  auth:
    enabled: true

    # Set custom paths for the log files. If left empty,
    # Filebeat will choose the paths depending on your OS.
    #var.paths:

    # Use journald to collect auth logs
    #var.use_journald: false
```

11. Run the command and wait few minutes then monitor the output shown at the end

If all the configurations are correct the output will show connection is established, otherwise show exited due to some errors.

.\filebeat.exe -e

12. If connection is established the exit the command using Crl+c

13. Then start the filebeat service using the below commands

Get-Service filebeat //To know the status of the service

Start-Service filebeat //To start the serivce

==========

Note -1: Restart-Service filebeat //To Restart the service

Note-2: Stop-Service filebeat //To Stop the service

==========

Now the Agent config is completed.

To add this server to Graylog follow the steps shared earlier for collection jenkins logs

Only difference is use 5045 instead of 5044

Open Graylog Web UI and navigate to:

- System → Inputs
- Select Beats from the drop-down menu.
- Click Launch New Input and configure the following:
    - Title: eg: Windows –ADC
    - Bind address: 0.0.0.0
    - Port: 5045
    - Override Source: Windows-ADC
- Click Save & Start Input