Download and install Filebeat from https://www.elastic.co/downloads/beats/filebeat

Edit the filebeat.yml file:

1. Under **filebeat.prospectors** make the path the path to the directory containing the NPS log files (e.g *C:\Windows\System32\LogFiles**)
2. If there is a line **enabled: false** then change it to **true**.
3. Make sure that the **output.elasticsearch** output is commented out
4. Under **output.logstash** the key line is **hosts:[“elk.govroam.uk:5044”]** which is where the logs will be sent.
5. Everything else in that section should be commented out.
6. Start/Restart the filebeat service.

This is the bare minimum for taking the logs from NPS and sending them to the Govroam log server. Get this working first before trying the encryption.

JISC will need to know the hostname/IP address of the system sending the logs (or the public IP from which the logs originate) so that the firewall can be updated.

Adding encryption is pretty straightforward.

1. Under **output.logstash** add the line **ssl.enabled: true**
2. Change the port from **5044** to **5055**.

If you're using the hostname **elk.govroam.uk** and have a set of Root CAs installed (normally the default for the OS) then filebeat should just be able to enable encryption. Run it in command line mode to see any errors. See the official filebeat SSL guide for details.

Experimental

Suggested here: https://discuss.elastic.co/t/logstash-xml-parse-with-meta-data/103687/6 for dealing with errors in logstash.

```
filebeat.prospectors:
- type: log
  paths:
    - /path/to/log
  encoding: 'windows-1252'
  multiline.pattern: '^\<\?'
  multiline.negate: true
#  multiline.match: after
  fields_under_root: true
```

From:
https://wiki.govroam.uk/dokuwiki/ - **Govroam**

Permanent link:
https://wiki.govroam.uk/dokuwiki/doku.php?id=siteadmin:filebeat_for_windows_configuration&rev=1571406803

Last update: **2019/10/18 13:53**