# Centralized Log Dashboard for Linux and Windows Environments

## High-Level Overview

A centralized logging solution has been implemented to collect and analyze logs from both Linux and Windows servers using the ELK (Elasticsearch, Logstash, and Kibana) stack. This solution ensures efficient log management, real-time monitoring, and structured data presentation in Kibana dashboards.

## High-Level Design (HLD) Diagram

A High-Level Design (HLD) diagram has been created and is available for reference.

## Implemented and Tested Components

1. Filebeat Installation on Linux Servers  
 - Filebeat is installed on Linux servers to collect system logs and application logs.  
  
2. WinlogBeat Installation on Windows Servers  
 - WinlogBeat is installed on Windows servers to capture Windows event logs.  
  
3. Log Forwarding to Logstash  
 - Filebeat and WinlogBeat are configured to send logs to the Logstash server on TCP port 5044.  
  
4. Logstash Configuration for Data Processing  
 - Logstash is set up to parse and structure the incoming logs before forwarding them to Elasticsearch.  
 - Separate indices are created for Linux and Windows logs in Kibana.  
  
5. Centralized Log Dashboard in Kibana  
 - The logs from both Linux and Windows environments are visualized in a unified Kibana dashboard.  
 - The structured logs allow for advanced analytics and troubleshooting.

## Logstash Configuration

input {  
 beats {  
 port => 5044  
 }  
}  
  
filter {  
 if [agent][type] == "filebeat" {  
 grok {  
 match => { "message" => "%{TIMESTAMP\_ISO8601:timestamp} %{LOGLEVEL:loglevel} %{GREEDYDATA:message}" }  
 }  
 }  
   
 if [agent][type] == "winlogbeat" {  
 mutate {  
 add\_field => { "event\_source" => "%{[winlog][channel]}" }  
 }  
 }  
}  
  
output {  
 elasticsearch {  
 hosts => ["http://elasticsearch:9200"]  
 index => "%{[agent][type]}-logs-%{+YYYY.MM.dd}"  
 }  
 stdout { codec => rubydebug }  
}

## Filebeat Configuration (Linux Servers)

filebeat.inputs:  
- type: log  
 enabled: true  
 paths:  
 - /var/log/\*.log  
  
output.logstash:  
 hosts: ["logstash:5044"]

## WinlogBeat Configuration (Windows Servers)

winlogbeat.event\_logs:  
 - name: Application  
 - name: System  
 - name: Security  
  
output.logstash:  
 hosts: ["logstash:5044"]

## Why Logstash is Used?

Initially, logs were sent directly from Filebeat and WinlogBeat to Elasticsearch, but we encountered issues where the log data was ingested as unstructured text. This caused difficulties in creating dashboards in Kibana, as log fields were not properly indexed.  
  
By introducing Logstash:  
- Logs are parsed and structured before reaching Elasticsearch.  
- Key fields are extracted to ensure compatibility with Kibana visualizations.  
- Data is properly indexed, allowing effective filtering and querying in dashboards.

## Conclusion

The centralized log dashboard provides a unified view of logs from Linux and Windows servers, allowing better monitoring and analysis. With Logstash processing logs efficiently, Kibana dashboards can now visualize data in a structured format, improving operational insights and troubleshooting efficiency.