# ELK Stack Logging Base Package

## ELK (Elasticsearch Logstash Kibana)

This package is a set flat rate which includes up to 10 nodes for the HA ELK Stack, many different templates and dashboards included for Windows, IIS, Apache, Nginx, EXIM4, Postfix, VMware ESX(i), VMware vCenter or standard rsyslog from Linux distros and much more to come. If this base package is not right for you then we can scale it larger for you.

The price of the base package includes initial consultation and sizing, implementation, templates, dashboards and up to 10 hours of post implementation training and handover of support. if additional templates or nodes are required beyond what is offered in the base package there will be additional fees associated as such. These additional costs will be outlined below. The cost of this package is all inclusive based on the fact that these are mainly open-source solutions which means that you are paying for services provided. The option of obtaining official Elasticsearch support for the ELK core components based on your SLA requirements. They provide 3 different levels of production support as well as development support.

This solution is meant to be an on premise deployment therefore you will be responsible for providing the hardware resources required for setting up this environment. These resources preferably will be virtual as this allows the most flexibility in deployments and scale. The amount of disk space required will be determined based on your retention requirements and the number of devices being logged. A sample will need to be captured in order to get a sense of the amount of data being collected per day. There is not a limit on the amount of data that can be retained but good data retention policies will ensure a much better user experience. To help ensure your data retention policies, there will be daily cron jobs that run and will be adjusted to fit your needs so that user intervention is not required.

## Package Cost and contents - $11,500 (All inclusive)

10-nodes (2-HAProxy Clustered Load Balancers, 2-ELK-Broker Nodes, 2-ELK-Pre-Processor Nodes, 2-ELK-Processor Nodes and 2-ELK-ES data Nodes). Additional nodes may be required based on your specific environment and will be an additional charge. You may choose the sizing of these 10-nodes based on your specific hardware availability and requirements. Typical sizing for each node type is below.

- HAProxy Load Balancer Nodes – 1vCPU, 1GB Memory, 36GB Disk
- ELK-Broker Nodes – 1vCPU, 4GB Memory, 72GB Disk
- ELK-Pre-Processor Nodes - 2vCPU, 4GB Memory, 72GB Disk
- ELK-Processor Nodes – 4vCPU, 4GB Memory, 72GB Disk
- ELK-ES Nodes – 4vCPU, 8GB Memory, Disk space is based on the amount of data collected and retention policy

Logstash parsing templates which include Microsoft Windows EventLog, Microsoft IIS, Apache, Cisco ASA, VMware NSX, Nginx, EXIM4, Postfix, VMware ESX(i), VMware vCenter (Appliance or Windows based) and general generic syslog types (rsyslog, network gear syslog, etc.) Any customized or additional templates required will be an additional charge.

Kibana dashboards to get you started which include Microsoft Windows EventLog, Microsoft IIS, Apache, Cisco ASA, VMware NSX, Nginx, EXIM4, Postfix, VMware ESX(i), VMware vCenter, SSH logins (rsyslog based), IPTables Firewall (rsyslog based) and general Syslog.

## Additional Costs (Only if requested)

The following costs are only assessed if your needs determine them. These are not mandatory charges but are represented below only for your viewing.

- Additional nodes of any type in the stack - $625/node
- Customized templates beyond what is provided in the base package - $500/template
- Customized Kibana dashboards beyond what is provided in the base package - $500/dashboard

## Elasticsearch Support

If you would like to obtain Elasticsearch support for your solution; a sales engineer from Elasticsearch can be available during the initial consultation of requested service. As stated above all solutions will be fully supported by Elasticsearch if a support agreement is purchased.