# Rotating Logfile

Requires: log4bash (Included)

<http://code.google.com/p/log4bash/>

Create directory /opt/check\_apache

Copy log4bash.conf and log4bash.core to /opt/check\_apache

Copy check\_apache.sh to /opt/check\_apache

Logfiles will be created under /opt/check\_apache/logs by default, this is configurable in log4bash.conf

# Logstash Configuration

Download and extract <https://download.elasticsearch.org/logstash/logstash/logstash-1.4.2.tar.gz> to /opt/logstash

Create file /opt/logstash/conf/logstash\_agent.conf

input {

file {

path => ["/opt/check\_apache/logs/\*"]

}

}

output {

syslog {

appname => "check\_apache"

facility => "log alert"

host => "Logstash-server"

port => 1514

protocol => "udp"

severity => "alert"

sourcehost => WebServer

}

}

Execute logstash agent, output directive will require updating dependent on individual logstash implementations.

/opt/logstash/bin/logstash agent -f /opt/logstash/conf/logstash\_agent.conf



# Push logfile into Zabbix

Under Configuration Hosts select the host you would like to monitor the logfile on

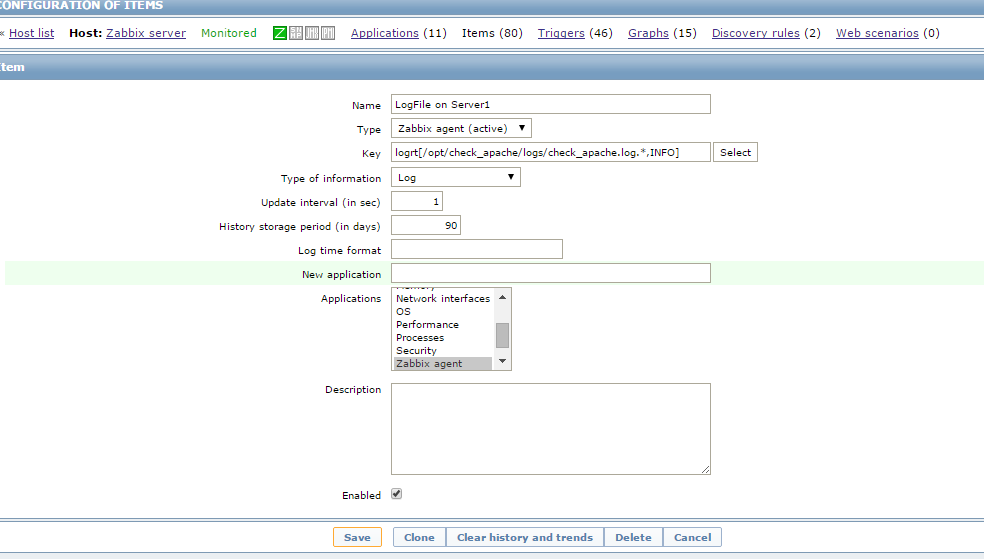
Under the host screen Click on items

In the top corner click “Create Item”

Give the item descriptive name

Choose Zabbix agent (active) from the Type drop down menu

Provide the path to the logfile and the regex pattern to match (INFO, WARN, CRITICAL) under the key field. Eg. logrt[/opt/check\_apache/logs/check\_apache.log.\*,INFO]



The zabbix agent runs under the zabbix user. This user will require permissions on the logfiles that are being pulled. This can be done by either updating zabbix\_agent.conf to enable AllowRoot=1, this will allow the zabbix\_agent to run under the root account, an alternative is to grant the zabbix account permissions on the logfile either directly or via group membership

