Technical Pre-Screen

Scenario

You are a consultant for Fred's Helpers Ltd. that specializes in implementing AWS CloudWatch MetricFilter and Alerts. Your job is to review a series of suspect log lines which have been generated by a new application. The DevOps team have deployed a new service which is sending its logs to CloudWatch. You have very little insight into the business function of the software and the only information you have is the log lines. The log lines appear to be a mix of performance and error heuristics.

The dev team lead has asked that the CloudWatch MetricFilter and Alert configuration be automated so they can be implemented in test, staging, and production environments. The team has asked for CloudFormation Stack .yaml file to be created. The following log lines have occurred over the last three working days and you have been told that CloudWatch is expected to filter and alert based on the following lines.

Requirements

PLEASE NOTE ALL ASSUMTIONS AND THOUGHTS – WE WOULD LIKE TO UNDERSTAND WHY YOU ARE TAKING YOUR DECISIONS. WHY HAVE YOU TAKEN THIS APPROACH AND ANY ANALYSIS YOU WOULD DO TO COME TO THIS.

1. Please provide a CloudFormation Stack file in. yaml format that will create a number of MetricFilter and Alerts.
2. Make reasonable assumptions as to the meaning of the log lines.
3. Provide a complete description as to what the Metric is retrieving and what conditions the alarm is triggered. Please detail your assumptions.
4. Please define one Metric that utilizes a MetricValue found by parsing from the MetricFilter.

Log lines

1.

2018-01-20 03:19:48,469 ERROR [org.tomcat.as.controller.management-operation] (ServerService Thread Pool -- 56) WFLYCTL0013: Operation ("add") failed - address: ([("subsystem" => "webservices")]): java.lang.RuntimeException: java.net.UnknownHostException: ip-10-189-5-169: ip-10-189-5-169: Name or service not known

2.

172.19.1.156 - C87637 [24/Jan/2018:11:45:14 -0500] "POST /sharedpages/partymanager/partysearch/partysearchpage.jsp?plist=p2945&vsid=9498 HTTP/1.1" 302 - "https://widget-prd.foo.redprairie.com/sharedpages/partymanager/partysearch/partysearchpage.jsp?plist=p3905&vsid
=2498" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36" "JSESSIONID=-KzEy2kdxhbyNlGNQxkR60hGnm7x1BO_zh2-TjE2.ip-10-189-6-47; AWSALB=lxBOed3xqTDTYsXh64ruX6cFQLZZf0Vf4voCx2rT3JK9wwNfnG1xVESWtt9rJEsdBNFt37CoFqX4Mxeq7UvzaLqhVhfz3xQqBfxQW4f6AJGhpwkprFnSWZo/QGUc" "-" -KzEy2kd1hbyNlGNQxkR60hGnm7x1BO_zh2-TjE2 "default task-3" 0.015

3.

[2018-01-19 09:18:40,104] INFO monitor.com.redprairie.ta.persistence.resources.PersistenceImpl Unknown macro: {default task-24 ip-10-189-5-64, 10.189.5.64, "FrontOffice Web", PE} - ,Active Performance Sql Alert, FrontOffice, read(Oid= PE:11528:0000001216 relName=employeeOccupations faultRel=true), ms = 3801 size = 6126 sizeStatements = 1

4.

[2018-01-23 11:57:04,750] ERROR com.redprairie.ta.persistence.resources.ContainerConnectionSupplierImpl {TASystemThread } - Exception thrown when getting database connection FrontOffice. Number of retries left 0